AN OUNCE OF PREVENTION

STAYING SAFE IN TODAY'S DIGITAL WORLD

BROUGHT TO YOU BY YOUR CREDIT UNION

TABLE OF CONTENTS

KEEPING YOUR GUARD UP AGAINST THE NEWEST SCAMS

It seems like there's a new data leak or identity theft trick to be worried about every week. If you're not informed, you risk becoming a victim. Sitting back and waiting for news about scams to come to you may not be enough. In an ever-changing security climate, you need to stay on top of new threats to your personal information security.

WHY THE LANDSCAPE CHANGES SO FAST

The bad news is that humans have become the weak link in the information chain. Breaking modern encryption algorithms takes high-powered supercomputers months to accomplish, if not years. The chance that information you send online or over the phone will be hijacked is slim. The biggest danger is sending information to people you don't intend to be the recipients.

That's why scams crop up so quickly. Humans can be tricked in any number of ways. Scammers can play on fear, greed or sentimentality in different forms to con information out of you. They also rely on our natural humanistic inattention to detail or carelessness. This is because humans have a number of built-in vulnerabilities.

Unlike a computer, you can't just download the latest anti-virus software to your brain. You can, however, do the next best thing: Stay current on evolving cyber-crime situations.

WEBSITES TO VISIT REGULARLY

The FTC regularly updates its website with phone, email and web-based scams. Its website, consumer.ftc.gov/scam-alerts, features several articles each week. As one of the strongest consumer watchdog agencies, it investigates illegal or fraudulent business communications with zeal. It then publishes the results of these investigations in the hope that fewer people will become victims.

You can also pitch in and be a good cyber citizen by reporting scams you see to the FTC. Report them online using the FTC's form at ftccomplaintassistant.gov or call their toll-free number at 1-877-FTC-HELP. It's one way you can make sure scammers are stopped before they really get started.

The Better Business Bureau (BBB) also maintains a list of scams from criminals posing as businesses here: bbb.org/council/news-events/lists/bbb-scam-alerts This is a helpful place to look if you've received an offer that seems too good to be true. For identity theft-specific scams, the Identity Theft Resource Center maintains a list of schemes to steal personal information. Their website is located at idtheftcenter.org/ID-Theft-Blog/Scams-Alerts

GAMES TO PLAY

Keeping up with the latest threats isn't all work. There are also fun and interactive games you can play! The FTC's weight loss challenge game tests your knowledge of common weight loss scams. It can be a fun way to start talking with kids about the dangers of online ads. You'll find it at consumer.ftc.gov/media/game-0026-weight-loss-challenge

If you're feeling advanced, check out Admongo at admongo.gov This creative, sci-fi-themed platform introduces the hidden dangers of advertisements. It can also make a great stepping stone into a conversation with kids about caution around advertisements.

NEWS TO FOLLOW

You're not alone in the effort to protect yourself against fraud. The National Consumer League is a not-for-profit organization with over 100 years of history helping to protect consumers from scammers. It maintains a list of current scams and monitors old ones. It also interacts with law enforcement where possible to bring scamming groups down.

One of the services the National Consumer League provides is an email list. It sends

out alerts whenever a new threat to consumer well-being emerges. In addition to covering scams, it monitors product recalls, food safety conditions and truth in advertising concerns. It's a great resource in helping you make smart consumer choices in a market that's crowded with information. To join the mailing list, visit their website: nclnet.org

Remember, the computer age brought us wonderful improvements in our quality of life. We can seek entertainment, educate ourselves and stay in touch with friends and family using devices that fit in our hands. With that greater connectivity, though, comes the need for constant and careful scrutiny of the information coming across our screens. In this struggle, too, knowing is half the battle.

AN OUNCE OF PREVENTION

INTERNET HYGIENE – THE BEST COMPUTER TIME INVESTMENT YOU CAN MAKE

Wash your hands after using the bathroom. Cover your mouth when you sneeze. Brush your teeth daily. These are all basic elements of personal hygiene. We practice them, in part, to minimize the amount of gross stuff that our bodies do, but we also practice them to help protect us from disease.

You might think "internet hygiene" means wiping down keyboards after you use them and not spilling things on your computer. While these are good habits, there's another range of behaviors that security experts call "internet hygiene," and it can be the difference between a safe and effective internet and a world of hackers, bots and identity thieves.

For most people, the beginning and end of cyber-security is anti-virus software. Assuming that there is nothing on their computer worth stealing, most users don't take their online security seriously. Increasingly, that's the attitude hackers are counting on.

One common cyber attack, a malicious worm called Game Over Zeus, infected around 10,000 computers. The worm allowed hackers to remotely control infected computers, using them to launch attacks on major websites. In addition, users frequently found their personal files encrypted. A window created by the worm would inform them that, unless they paid a ransom that sometimes was as much as a few thousand dollars, they would lose access to the contents of their hard drive forever.

How did such a vicious worm spread so quickly? For starters, hackers have become better about choosing their targets. It's easy to find out-of-date software and exploit known structural weaknesses to gain control of a computer. From there, it's a trivial task to create emails that look like they come from the owner of that computer, which makes it easier to infect the computers of that person's family members and friends.

Security expert Tom Kellerman compares the state of a compromised computer to a neighbor who always leaves the front door to an apartment complex unlocked. Not only can thieves break into the neighbor's apartment, but they can use their expanded building access to more easily break into other units. If you aren't maintaining the security protocols on your computer and being vigilant about the links you click, you aren't just putting your own security at risk. You're creating a more dangerous internet for your friends, coworkers and family, too.

The lesson of Game Over Zeus is pretty simple: Computer viruses spread a lot like human viruses. They infect people who don't practice good hygiene, then spread to their friends and family. If you wouldn't sneeze on your hand before pushing buttons on an elevator, don't practice unsafe internet behaviors.

How can you practice good internet hygiene? You don't need to be a tech guru to keep your PC safe. Security experts consistently recommend you take at least these five steps.

1. **Download antivirus software, like AVG or McAfee, and keep it updated.**
   Schedule updates for it to run when your computer is on, and don't interrupt the process. Do the same thing with an anti-malware program, like MalwareBytes. Tens of thousands of new malicious programs are created every day. If you're not regularly updating your security software, you might as well not have it.

2. **Run scans of both anti-virus and anti-malware software on a weekly basis.**
   Just as people having strong immune systems can get sick, even if you have a Mac computer, you can still be infected with malicious programs. If you're on the internet, you're at risk.

3. **Do it right away.**
   If your computer gives you a message that it needs to download or install critical updates, do it the first time you see the alert. It's annoying to stop what you're doing and restart your computer, but it's better than having your computer compromised. When IT professionals call something a "critical update," it usually means it fixes a known software exploit. Make sure the message that pops up is from a trusted source, however. There are malware programs around that use

fake “critical update” pop-ups to infiltrate your computer.

4. **Don’t click links taking you to sites you don’t recognize.**
   This is true even if they’re emailed to you by a friend or family member. These emails are frequently generated by bots to keep malicious software spreading. Clicking that link might make you yet another disease vector.

5. **Don’t download, install or run any software you don’t recognize.**
   For these bots to keep spreading, human beings have to authorize them at some point. If you’re installing software you think might be dangerous, you’re putting your computer and the computers of everyone you know in jeopardy.

This might seem like a lot of work, but it’s the price of doing business and living in a digital age. With the convenience of a world of information at your fingertips comes the responsibility to maintain the health of that system. Do your part – install and update security software, and constantly be on guard for threats!

WHAT IS THE CLOUD AND IS IT SAFE?

WHY DO WE USE THE CLOUD?

There was a time we used to buy furniture to hold our media. CD racks, DVD racks, photo albums and filing cabinets filled our living rooms, guest room closets and wherever else we could pile them. Even in our cars, we would install massive CD changers to keep our music flowing or carry enormous books of CDs so we could have our tunes while on the open road.

If you try to explain this to today’s young people, they’ll look at you like you just described preparing your covered wagon rather than a mid-2000s Honda Civic. If you try to explain audio cassettes, they might just suspect you have a loose screw or two.

Today’s media and data is so small, it might as well not even exist. Using the Apple Music and Spotify libraries as a guideline, every song that’s ever been recorded and released would fit into flash storage drives the size of a 12-ounce can of Crystal Pepsi. Even as our data gets smaller, we make so much more of it that it can get out of hand. That’s because, much like processor speed, the amount of information the world produces doubles every two years. Some of that information is pictures of kittens and makeup tutorials, but we also produce a lot of data that isn’t nearly that important.

In such a data-driven world, we are trusting more of our lives to the cloud, and it often seems like blind faith. After all, what is the cloud? How much do you know about it? Are there laws governing the way people use it? Most importantly, have you taken enough steps to protect yourself when all of your information exists on what is, if we're really honest about it, not much more than a metaphor for the shared hallucination that is modern life?

WHY SHOULD I START TO CARE NOW?

The cloud has maneuvered itself into a variety of news stories over the last few years, from the theft of intimate photos belonging to Hollywood stars like Jennifer Lawrence to the operation for ending corruption in FIFA. Cloud storage is behind the surge in Amazon's stock valuation, because it is the largest provider of cloud storage to businesses, including Netflix, the largest private user of bandwidth on the planet.

The cloud is the basis for Google's push into the laptop business via Chromebooks, and by extension, the efforts of a variety of organizations to get low-cost laptops into the hands of less-privileged kids. It's even changed Microsoft Office, probably the most ubiquitous piece of software in the world, by forcing Microsoft to create free versions of its Office suite and charge for excess storage of the files you create.

In other words, your investments, your data and the future of law enforcement may be intimately tied to cloud-based computing, and something as simple as a server-side bug can have an enormous ripple effect for millions of users.

The issue won't be going away any time soon. As more people use the web more often on mobile devices, it will eclipse 50% of personal internet usage in the next few years. These devices rely on storage in the cloud to compensate for smaller on-device storage capabilities and a lack of long-term storage peripherals.

SO, WHAT IS THE CLOUD?

The cloud is a series of servers storing data that can be accessed by users whenever it's needed. This frees up hard drive space while protecting us from data loss due to hardware failure, including a stolen laptop or dropping your phone into the pasta you're boiling on the stove. It's not magical, and your information doesn't live on the internet in any particularly novel way. Instead of a home video being stored on your local storage, it is stored on someone else's storage, far away. These server farms are enormous undertakings, and if you're into mechanical processes and design, they're also beautiful and fascinating. For example, check out the pictures

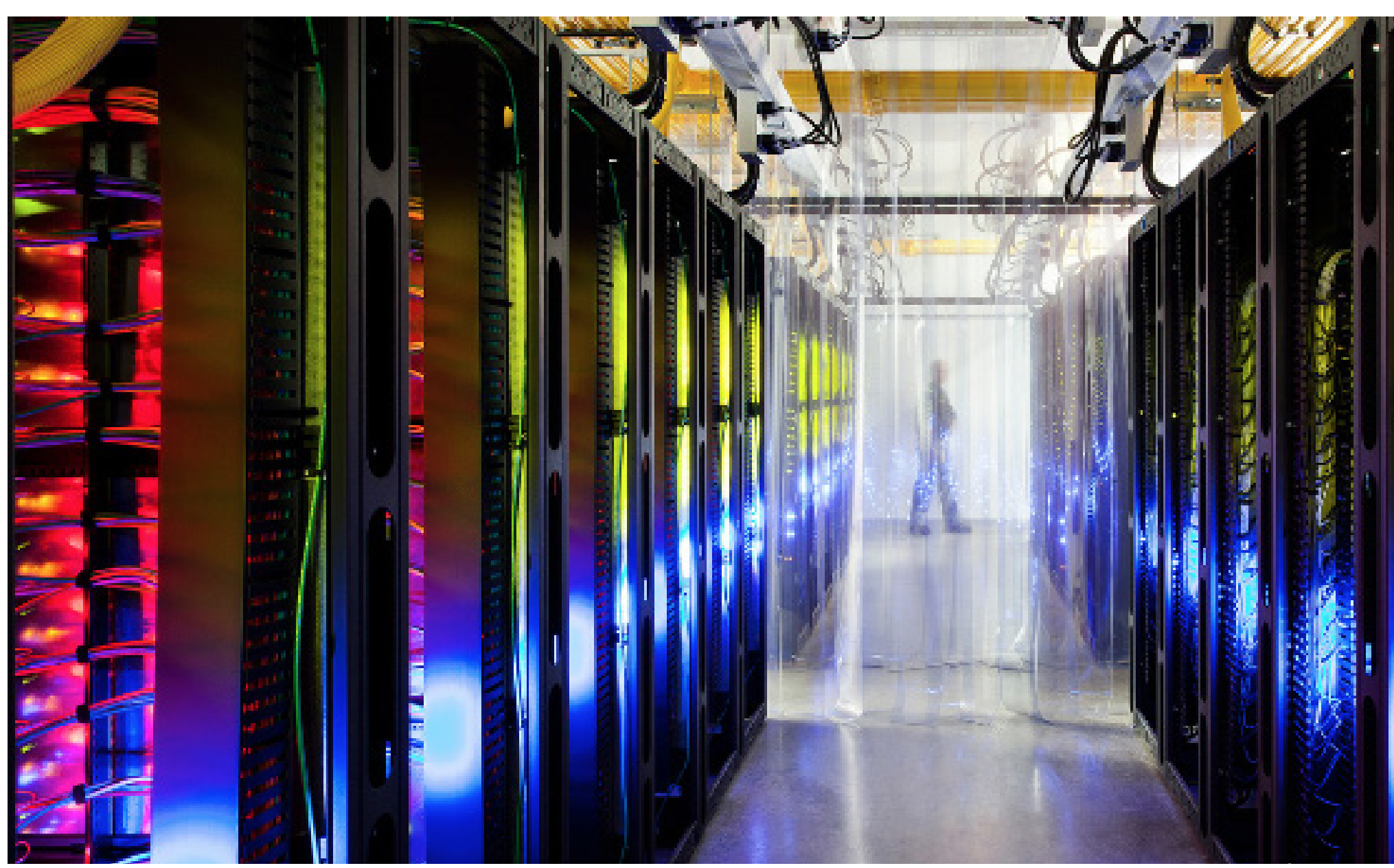
of Google's data centers at google.com/about/datacenters.

HOW MUCH OF MY DATA IS STORED ON THE CLOUD?

The amount of information stored on the cloud varies from person to person, but if you're reading this on a device that plugs into a wall at any point, you've got at least some data on the cloud. If you own an iPhone, your device backs up your photos, videos and music to the cloud, in addition to storing periodic backups of your phone. If you have a web-based email address, like one from Gmail, Yahoo or AOL, your emails are backed up there as well. Depending upon the apps you use, your health details, dating history or even your exact current location could be on the cloud as well, possibly being shared with third parties.

WAIT--WHO CAN SEE WHAT?

For the time being, the government can probably see more of your data than you realize. Exact details are fuzzy, and you can make your own moral judgments on homeland security, domestic spying and Edward Snowden. However, if you think the government doesn't want access, keep in mind that Apple is currently fighting both California and the United States federal government to keep a form of encryption on your data that it can't break.



Apple no longer wants to surrender data to the government, so it has blinded itself from seeing large swaths of your data. The government is less than happy about this, because that data might point to potential threats to homeland security. Again, this book isn't trying to make a moral or political claim. The point is that the government is a third party which wants the ability to look at your data, which represents another point of vulnerability to a malicious attack.

Outside the government, a lot of the companies that maintain those expensive server farms pay for all of that technology by sharing some or all of your personal information with private businesses. You should already know that, of course. If a web service is free to you, then the company providing it makes its money some other way. If they're charging you, they still might make money by selling your data.

You'll never know, because you (probably) accepted the terms without reading them. Don't feel bad, though; we all do that. The iTunes end user license agreement (EULA) is over 20,000 words long, about four times as long as the Constitution of the United States. There are, however, some helpful resources. For a shortened and simplified version of various EULAs, try tosdr.org, which is a donations-based organization that explains what you're agreeing to and offers an add-on for your browser so it's only a click away.

IS MY DATA SAFER WHEN IT'S IN MY CONTROL?

That question is up for debate, but the answer is usually no. In most instances, end users are the most vulnerable point of attack for cyber scammers. However, when you have control of your data, you can work to make it safer. When you don't, you're trusting someone else with it.

To put it another way, Apple Pay, Samsung Pay and other tokenized payment plans are the safest way to make a purchase because they require your thumbprint, protect your data with single-use encryption that's worthless to a third party, and don't store your info in the cloud. Doing your best to emulate those services is a good idea.

SO, WHAT DO I DO TO PROTECT MYSELF FROM THE CLOUD?

The easiest solution for protecting your data in the cloud is to spend some time and some money. Find a single site to store your files, whether it's with Google, Microsoft, Apple or Dropbox. Read each of their EULAs and decide for yourself. Then, pay them to get as much storage as you need, rather than spreading your files among various services in order to stay under the amount for free storage.

Next, make a list of which sites and services have what information of yours. Determine your level of comfort. Delete what you can live without and move the rest to a place where you feel safe. Clear out your email inbox whenever you can. Don't archive private data, like medical records or financial statements, with your email provider.

Instead, save them locally on storage you have at home or work, which you can disconnect from the internet. A 2-terabyte solid state removable storage drive is less than $100 and offers great protection. As an added measure, back up your drive in a second location once a month, in case something happens to your house.

Finally, as you move forward, try to think critically about what you're telling people. If someone can make money off your information, they'll find a way to do so. The only way to protect your information and that of your family is by being vigilant.

HOW 10 SECONDS OF DILIGENCE CAN KEEP YOU SAFE FROM FRAUD

We're all bombarded with information. Nowhere is this truer than in our mailboxes, both real and virtual. After all, everyone who wants to get in touch with us has a phone number, social media accounts and a million other low-cost ways to get in touch. In fact, it can seem like the only people who send USPS mail are the folks who want to sell us something.

If you treat your mail like most people, you skim through it on your way from the mailbox to the door, stuff it in a mail sorter and promise to deal with it later. Your inbox gets treated the same way. If it's something from someone you know, you read it, chuckle and respond. If not, it's probably safe to ignore.

This is the kind of behavior that identity thieves are counting on. Petr Murmylyuk, a Russian immigrant living in New York, was convicted in 2014 of breaking into a number of online brokerage accounts, like Scottrade, E*Trade Financial, Fidelity and Charles Schwab, among others. His purpose was to initiate trades that moved the price of assets in a complicated combination of identity theft and security manipulation. He cost his victims more than a million dollars in losses, and he will likely only have to pay about $500,000 in restitution. He didn't get away with his fraud, but his victims still lost a lot of money.

Imagine this happened to you. You keep your retirement fund in an online brokerage account. You regularly deposit a few hundred dollars a month and you don't want to withdraw the money any time soon. So you just log in every so often to make sure your auto payments are being made and to check the balance. One day, you check

the balance and discover tens of thousands of dollars are just gone.

If you're counting on your brokerage to reimburse you, you might be waiting a while. Scottrade, for example, "does not cover situations in which... you failed to take reasonable precautions to protect your privacy." Fidelity, too, specifies the need to ensure that transactions were not made by someone you "allowed" to access your account. Other online brokerage firms have similar policies to protect their own interests over yours.

What can you do to stop it? You may already know how to maintain security on your online accounts. Choose strong, complex passwords. Don't access sensitive websites from public computers. Don't click links in emails that look suspicious. This is all the same financial personal hygiene you probably already practice.

However, when it comes to online financial accounts, like brokerages and draft accounts, there's an extra step to take. Read your statements carefully.

Here's why and how the process works:

- **Pick a day each month.** Making it the same time each month will help you remember as well as help you establish a reliable control. You don't need much time, just 20 or 30 minutes. Take care of it while you're drinking your coffee in the morning.
- **Go through monthly statements and confirmations for all your accounts.** Make sure you or your spouse recognize every transaction that's been made. Keep an eye out for the following types of transactions:
    - Transactions originating in foreign countries or other distant places. Identity thieves will often try to throw you off the trail and avoid prosecution by committing their crimes in distant places.
    - Small transactions. It's tempting to write off a dollar here or there, but thieves are frequently counting on that tolerance. They'll use a small transaction to test a stolen credit card or breached account. If they get away with that, they'll try bigger amounts.
- **Ask for a login history if you suspect something is wrong with your security.** This is a document a company can provide listing the dates, times and locations of every access that's been made to your account. This will help you see if someone else has gained access. Obviously, if that's the case, you'll want to change your passwords and let your financial institutions know immediately.
- **If you notice anything else that's amiss, call the financial institution**

immediately. The longer you wait, the more likely it is they'll conclude it was something you authorized. Even if it's off business hours, call immediately and leave a message. Starting the process as soon as possible creates a trail that will be useful in the event of a dispute about responsibility.

YOUR GREATEST STRENGTH MIGHT BE YOUR GREATEST WEAKNESS

We've all had that moment when we were shopping on eBay at 3 a.m. and spotted the deal of the century – an Omega Speedmaster Moonwatch for just $100? That's the watch that's been on the moon! Then we realize the price is too good to be true when we see our newest find will ship from the other side of the planet and the listing features blurred photos obscuring key details.

Maybe that Moonwatch spelled Saturday with a "B," because some scams are really easy to spot. We've all seen a scam like this, and after catching ourselves, we've all asked ourselves the same question: Who falls for this garbage?

From behind a computer screen, spotting a scam is as easy as a stroll in the park on a beautiful Saturday afternoon. What investigators have realized, though, is that it gets much tougher when fraud happens in person. In person, all of those skills we've developed online go away and we become easy marks.

THE IRL PROBLEM

It's easy to act differently online. No one knows us there, so we can make up the life we want to live or act without repercussions. Otherwise calm, respectable people can become maniacs online if certain topics come up – from vaccinations to the recent play of the local professional quarterback. For others, the digital world is a place of exploration and indulgence in hobbies that are unavailable offline, as players of World of Warcraft or the thousands of people who left reviews on Food.com's recipe for ice cubes can attest.

However we change ourselves while behind the computer, it's easy to see that we think of ourselves and others differently while online. Offline, you wouldn't constantly harass your friends about a game to crush candy, would you?

The same is true when it comes to scams. When we sympathize with people, we lose the critical distance we need to spot scammers. If we can connect with a person, we are far more likely to fall for a scam, and talking to them away from the computer increases that personal connection.

Think about it this way: The FTC says the most common forms of scams all involve human interaction, not computers.

The most common form of online identity theft isn't breaking into your credit union – we're really good at security – it's phishing, where scammers convince victims to willingly give up their credit card information.

The most common phone scam is the grandparent scam, in which the bad guys use our natural concern for our family to get money out of us. The most common scam ever might be the basis for the modern home improvement scam: using a hard-luck story or the victim's greed to convince them to pay up front, and then never actually doing the work.

HOW TO AVOID IN-PERSON SCAMS

Be wary of surprises and secrets. Two things that should tip you off right away are really big surprises and really private secrets. If you won money in a contest you don't remember entering, you probably didn't enter it. If you're getting a big payday, but you can't tell anyone about it, you're probably not getting a big payday.

In reality, if a company runs a contest, it wants to get publicity. If you've got contest winnings coming, that company probably made you put down your email address and a bunch of other info. It took time for the company to get all of your data. You'd remember speaking or interacting with that company. Even in old TV shows, they understood that surprises and secrets were a bad sign – if a 1960s sitcom hero inherits a mansion from an uncle he's never met, you better believe it's haunted.

Take your time. If someone needs you to act quickly, that's often a clear sign of a scam, particularly if the sudden rush is coupled with a surprise, as described above. Scammers understand the power of groupthink – what psychologists call that likelihood of humans to make worse decisions in groups than by themselves – largely stems from an impending time deadline. By denying you time to catch your breath, scammers are trying to rush you into a bad decision and keep you from getting advice from someone with distance and perspective.

Try to be a robot. NPR's "Planet Money" podcast aired an episode covering the danger of our humanity very well. In it, a banker named Toby convinced dozens of people to help him perpetrate a large-scale fraud simply by telling them his hard-luck story. He claims that not one of them turned him down. The case made in the episode is that, for each person who heard the story, the ethical decision to commit a fraud and the rational decision to trust a scammer was completely overwhelmed by their sense of sympathy and injustice.

Don't let that be you.

Hopefully, you're not going to have to deal with in-person scammers very often. If you do, contact the FTC at ftccomplaintassistant.gov and the FBI at ic3.gov.

USING PRECAUTION WHEN ONLINE

Though the Internet offers a wealth of information and convenience, the mostly unregulated and anonymous framework is an identity thief's dream. Here are just a few tips for staying safe online.

- **Know how your information with be used.** If your personal information — your name, email or home address, phone number, account numbers or Social Security number is requested, find out how it's going to be used and how it will be protected. Check for indicators that the site is secure, such as a lock icon on the browser's status bar or a website URL beginning with "https" because the "s" stands for secure. Teach your children not to give out their last name, home address or phone number on the internet.
- **Read the security policies** of any company you interact with to ensure they are not using deceptive practices and that they are providing a secure environment.
- **Don't respond to any email urgently asking you to update or validate your account information.** Often, such emails will direct you to a website that looks like the real one, but is really a fake. Don't click on the link. Instead, contact the company you are dealing with directly. Legitimate companies will not ask you for sensitive information via email.
- **Protect your passwords, and be original in the passwords you use.** They should not all be identical, and they should not be similar to your user name.
- **Install and use anti-virus software and firewall protection.**
- **Use parental controls on your computer.** Remember, parental controls are a supplement but not a substitute for parental supervision.

PROTECTING YOUR CREDIT

CONSIDER A SECURITY FREEZE TO PROTECT YOUR IDENTITY

Is there any downside to building and maintaining a high credit score?

Yes. It makes you more vulnerable to fraud and identity theft.

After carefully budgeting and paying your bills on time for many years, it can be frustrating to learn that scammers and thieves are out there searching specifically for you. They want what you have. They want to steal your good credit for their own purchases, or to sell it to other scammers and thieves.

Honest people often have a hard time understanding how scammers and thieves think and behave in our digital world. And it's easy to imagine the crooks are people living far away in foreign countries.

Having a home security system and anti-theft locks on your vehicles may be a common matter for you, but it's possible you haven't thought about protecting your identity as securely as your other possessions.

Even though protection from vandalism and theft is usually covered by homeowners insurance, most of us want to deter vandals and thieves from even trying to damage or steal our possessions. We don't want to experience violation or loss in any way. And yet, our personal identity and good credit may be very vulnerable.

WHAT DOES IDENTITY THEFT LOOK LIKE?

Unfortunately, most people aren't aware of their right to control who is able to access their credit report. But all three major credit reporting agencies, Equifax, Experian and TransUnion, offer you the option to restrict access to your credit report. They also make it possible for you to decide when and with whom your credit report may be shared. It's called a security freeze or a credit freeze, and it's important to understand how that works.

Here's a real-life example of a credit union member in Texas who didn't know he had the right to restrict access to his credit report. Without his knowledge, an identity thief - who was also a resident of Texas - was able to establish a new cellphone service and qualify for the purchase of a new vehicle using this man's high credit score profile. The cellphone service was already established when the thief shopped for a vehicle online. But that was the beginning of the end of the crime spree.

Three different auto dealerships called the credit union member to verify he was, in fact, going to take possession of the car he'd arranged to buy online. They had found his legitimate phone number on his credit report. You can imagine this consumer's surprise each time he got a call. Every dealership alerted the local police, who contacted the credit union member directly for more information.

Turns out, the identity thief was using the cellphone that was obtained in the stolen name, and also presenting a new, temporary Texas driver's license, which were also in the stolen name. Both were obtained prior to the thief's attempts to purchase a car.

The member was advised to call all three credit reporting agencies and put a freeze on his credit report. The identity thief still had his Social Security Number, address and credit card numbers, but could no longer use them. The fraudulent cellphone account was closed, at no cost to the member, and the State of Texas rescinded the temporary driver's license.

Without a credit freeze in place, the member would continue to be vulnerable to fraudulent use of his identity by the Texas thief. And he would be vulnerable to other thieves who may have purchased his credit report, as well.

PROTECTING YOUR IDENTITY WITH A SECURITY FREEZE

Call the credit union to report fraudulent use of your account or credit card if it has been breached.

Call the fraud department of every credit card that is issued in your name. You don't

need to cancel the cards, just report the fraudulent use and announce your plans to set up a security freeze with the credit reporting agencies.

Call each of the three major credit reporting agencies to set up a security freeze. Each has its own process, and there may be a small fee for the service, approximately $10 per agency.

- Equifax – 1-800-349-9960
- Experian – 1-888-397-3742
- TransUnion – 1-888-909-9972

Once the freeze is in place, you will need to contact each credit reporting agency whenever you want a particular vendor to access your credit report. This is called a "temporary lift" of the credit freeze for one vendor only. The permanent credit freeze remains in place until you choose to remove it entirely. Note, though, that there may be a fee for each temporary lift. However, it's a small price to pay for peace of mind.

Making the choice to control who can access your credit report (and who cannot) gives you the most security possible, but it requires more work on your part, too. And it may involve occasional but nominal fees. The member in our story decided it was worth the time and small expense to control access to his credit report, because he never wants to go through identity theft issues again.

PAY FOR DELETE SCAMS

You may already be checking your credit report regularly and you might have developed the habit of challenging or reporting any suspicious activity. But what do you do with a stubborn charge that won't go away? You know you shouldn't have to pay it, but for whatever reason, you can't get it off your report. You call the creditors in question and they tell you they understand, it's no big deal and they'll gladly delete it from your credit report if you pay a small fraction of the charge.

What do you do in that scenario?

For a lot of people, paying a couple hundred dollars is better than the headache or the full amount of the charge. They don't have to worry about the charge, and they know that, over time, they'll more than make up that money in savings on credit card interest charges. It's all part of the cost of doing business, they think, so they cut a relatively small check.

For the rest of us, though, we don't want injustice to stand. Or maybe we can think of a better way to spend a few hundred dollars than paying a scammer. We could put

it toward retirement, our kids' college funds or buy ourselves a nice gift! The point is: Spending a few hundred dollars on a personal luxury, no matter how frivolous, is still a better idea than spending it on a scam.

Legitimate credit agencies don't engage in pay-for-delete schemes. The way it's supposed to work is that, if a debt is reported as being sent to collections, it stays on your credit report for seven years, with certain exceptions, including some medical bills. Often, big credit agencies will sell the debt to smaller ones for less than what is owed, so they can receive guaranteed income, and then the smaller agencies are looking to get some amount paid off, generally more than they paid for the debt.

Those smaller agencies are often less scrupulous, and they offer to report the whole debt as a mistake if you pay a certain amount. Sometimes, that amount is the debt in full, which nets them a tidy profit. Other times, it's a smaller amount. In theory, this could have a very positive effect on your credit.

However, there's no guarantee they'll follow through, nor is there a reason for them to put the offer in writing, because the process isn't above board. In addition, if a creditor creates a charge that shouldn't be there, they'll often ask for pay-for-delete so they can mark it as removed, making it harder to identify a fraudulent charge after the fact.

Arm yourself with knowledge. Here are three scenarios in which a charge can be removed from your credit report:

- **You never got the bill (or the bill was for an incorrect amount)** – This is pretty obvious, and you shouldn't have to pay a dime. Make sure to challenge suspicious charges. If you don't believe that you incurred a debt, let the collection agencies know. Ask to see evidence of the bill; sometimes the creditor can't produce it, and they will waive the charge. Make sure to follow up and confirm that the charge was removed.
- **The bill was for a medical debt** – As mentioned earlier, some forms of medical debt can be removed from your record. Double check this with your accountant or lawyer. Make sure you also check with your insurance company so you know thake sure they're billing correctly. Every case is different, so be detail-oriented, write down everything the provider and insurer tell you and seek help from a professional. A single medical bill can be worth 25 points on your FICO score, so it pays to follow through. Remember, a creditor is not a medical provider, so they will have much less freedom to rework old bills, which is why they may be more interested in pay-for-delete.
- **It's a small-time creditor** – This is where the line between good security and under-the-table scam starts to blur. Small-time creditors want the revenue,

and they're going to be more likely to offer shady deals in exchange for money. Make sure to get everything you can in writing, and be suspicious. If they're unscrupulous enough to try pay-for-delete, then they probably didn't do all of their due diligence to find out if you paid the bill. Ask for evidence. Make sure you really owe the money. Be persistent; this is real money that you can spend in better ways than on scams.

It's important to stay on top of your credit report, but don't let that number at the top dictate your life. Yes, you'd like it as high as possible, but that's not a reason to give money to scammers. If you do the work on your end, you can often get to the bottom of these charges, save your credit score and keep cash in your pocket.

CREDIT REPAIR SCAMS

So, you've been monitoring your credit score, and you don't like what you see. You want those numbers to improve, and you want that to happen as soon as possible.

Here's where credit repair scams come into play. Unscrupulous scammers will take note of the fact that you've been making positive changes in your credit history or that you've been researching a major loan, such as a mortgage or auto loan.

They'll contact you, and offer to make credit repair quick and easy. Unfortunately, when they're done with you, your score still be low, you'll be out lots of money and you may even be facing criminal charges.

Here are the warning signs of a credit repair scam:

1. **Up front payment -** Under the Credit Repair Organizations Act (CROA), credit repair companies are forbidden to request or receive payment until they've completed the services they've promised.
2. **Big promises -** Scammers may assure you that they can remove negative information from your credit report, even information that is accurate and current. Don't believe them; no one can do this. They might also promise to boost your score in just a few weeks. This, too, isn't true; it takes at least 30 days for changes to be evident on your credit report.
3. **Offers a "new credit identity" -** In these scams, companies promise to create a new credit identity in exchange for a fee. After you pay, the company will provide you with a nine-digit number. They may refer to this number as a CPN — a credit profile number or a credit privacy number. Alternatively, they may direct you to apply for an EIN — an Employer Identification Number. The company will then instruct you to use this form of ID to apply for credit.

It will tell you this process is legal; it's not – and you've just been scammed! These companies are selling you a stolen SSN. They walk away with your money, leaving you in hot water: You've just committed multiple federal crimes. Yes, falling for a credit identity scam could mean facing fines or prison time.

4. **Tells you to dispute accurate information on your credit report -** Disputing accurate information on your credit report is illegal.

5. **Evasiveness when questioned -** The CROA made it illegal for credit repair companies to lie about your rights and about their services. These companies must explain:

   - Your legal rights and detail the services they'll perform in a written contract
   - Your three-day right to cancel the contract without charge
   - The anticipated amount of time it will take until results are evident
   - The total cost you will need to pay for their services
   - Their guarantee

If you've hired a credit repair company that hasn't lived up to its promise, you can choose to sue the company for your losses in federal court. Together with other victims, you can also file a class action lawsuit against the company.

It's best to report the scam to your local consumer affairs office or to your state Attorney General. You can also file a complaint with the Federal Trade Commission at ftc.gov/complaint or call 1-877-FTC-HELP.

Finally, if you're in financial trouble of any kind, we can help! Stop by the credit union today to ask about our credit counseling services and assistance with budgeting.

4 STEPS FOR CHECKING YOUR CREDIT REPORT

If there were a song about keeping yourself safe from financial scams, the refrain to that song would be "Check your credit report!" But practically speaking, what does that mean? How can that one piece of advice keep you safe from so much?

Though it sounds like an advanced financial maneuver, checking your credit report is easier than balancing your checkbook. All you have to do is get it, read it, report errors and stay on it. Let's look at each step in detail:

GET YOUR CREDIT REPORT

There are three different credit reporting agencies: Equifax, TransUnion and Experian. They share data, but each makes its own report. You're entitled to one free report from each agency every year. If you know you've got a major purchase, like a car or house, coming up in the next year, you'll want to check all three bureaus before you start shopping. This way, you can catch inaccuracies before lenders see your information and score. Otherwise, it makes sense to stagger them and view one report every four months. This puts the shortest amount of time between checks.

You can get your credit report for free at annualcreditreport.com. This is the only website approved by the Federal Trade Commission (FTC) for this purpose. Take care to avoid "imposter" websites operated by scammers. They may use similar-sounding website names or common misspellings in an attempt to trick you and get your personal information.

There are other situations in which you can get a free copy of your credit report. If you are denied credit, you can request a copy of the information that was used to make that determination, provided you do so within 60 days. If you have been the victim of certain kinds of fraud, the service will also provide you with a free copy of your credit report to help you make it right. These checks will never hurt your credit score.

If you've requested your report online, it should be available immediately. You may need to answer a few questions to verify your identity. Once you answer these questions, you'll get your credit report.

GO OVER YOUR REPORT

With your credit report in hand, it's time to look it over. You'll want to look for three specific things. You want to find accounts that are open in your name and you want to see if there's any collection activity. You'll also want to take a look at the number and frequency of inquiries.

There are slight differences in the three reports, but each has a list of accounts. They may be broken down by type (mortgage, installment, revolving and other) or listed by date. You'll want to look through each one to make sure you recognize them. This can be a tricky task, as every store credit card you open and every installment loan you make is listed. If there are any accounts you don't recognize, you'll want to make a note of them and potentially contact the credit reporting agency. Look particularly for accounts going to P.O. boxes, or those listed with addresses in other states.

"Negative items" include bankruptcies, accounts in collection or accounts reporting as past due. Such activity is another good place to check for fraud. If someone else

opened an account in your name, they likely won't be paying the bills. You'll also want to look for inaccuracies that may be hurting your credit score. If there's an account listed here that was discharged in bankruptcy, for example, you'll want to make note of that, too.

The list of inquiries shows you the number of times someone has checked your credit. No one can do this without your permission, so if there are more inquiries than you remember, it could be a sign someone has stolen your identity. It might be worthwhile to put a freeze on an ability to open new accounts until you've gotten everything resolved

Report inaccuracies - Each reporting agency maintains a separate error-reporting process, so you'll have to report each error to the agency that made it. For basic errors, like address, name or personal information, the agency can make those corrections with minimal trouble. For more serious errors, you'll need to send a dispute letter.

The FTC has a template for a dispute letter available on its website. You can use that or you can draft your own. Either way, you'll need to clearly identify the accounts or items you're disputing. Where possible, use partial account numbers or other numerical information. You'll also need to explain why you consider the item an error. Attach copies, but not originals, of documents that support your claim. Examples include police reports for stolen or lost wallets, bankruptcy orders that discharged a debt or letters from a lender indicating that an account was opened fraudulently.

Send your letter via certified mail. This costs a little more than a stamp, but you'll get proof of receipt. This is important because the agency has 30 days to make a determination about your dispute. They'll send your dispute to the information provider (the company that told the agency about the account or negative item).

If the reporting agency finds your claim to be correct, you can request that it send copies of the updated report to anyone who received your credit report in the last six months, and to any employer who pulled your credit report over the last two years. They're also required to send you an updated copy with any new information in it.

Stay on it - Checking your credit report periodically is the only way to keep yourself safe from identity theft and other modern crimes.

ONLINE SAFETY

IT'S ALL FUN AND GAMES UNTIL SOMEONE LOSES A CREDIT CARD: SAFETY IN ONLINE GAMES

Before the cellphone era, gaming was a pretty secure business. You bought a disk or deck of cards and played it many times until you grew bored. On the surface, today's gaming seems like an improvement. It is incredibly convenient to have all your games on a single device in your pocket.

The downside, though, is that everything else — your phone number, your email address, even your financial information — may all be on that device, too. It's become easier for online scammers to take what they want. Be on the lookout for these three ways mobile games take your money so you can better protect yourself!

- **In-app purchases** - In-app purchases are deceptively simple. You "buy" a free game in the app store, thinking you got a bargain. You play the game for a few minutes, enjoying yourself as you take on your friends at trivia or popping bubbles. Then, you hit a snag — you've maxed out the number of games you can play in one day and you'll have to wait 24 hours to play again. You're frustrated and willing to do anything to keep playing. The game offers you a solution: pay a small fee of "just" $0.99 to continue playing — and paying.
- **Phishing scams** - This type of app requires you to set up an account with the app manufacturer's website, to ensure your game is secure. It asks for your email address, as well as a username and password. As would most consumers, you input your email info, a username and password you use for everything. Any other system you use that password for can now be compromised.

  Another version of this scam is when an email supposedly from the game company tells you to login through a link in the email to get a fabulous in-game prize. Of course, there is no prize, and the email was a tool for scammers to

collect your login information.

The best way to prevent losing your information from this approach is by doing your research. Do a quick search of the app you're considering to ensure it's a safe one.

- **"Bonus credit"** - This one begins the same way an in-app purchases scam does. You buy the app, you play it for awhile and then it says you've run out of credits. To get more credits, you have to watch an advertisement or take an IQ quiz. The advertisements are almost always legit, but the "IQ quiz" includes an agreement to pay $10 a month on a phone bill!

  This scam is especially sneaky because crooks don't need access to a credit card number or a login. All that's necessary is for one user on a family plan, even a child, to click through a service agreement without reading it carefully.

Awareness and common sense are the keys. Avoid apps that ask you for purchases to play or use. Research apps before you give them any personal information. Have fun – but stay safe!

ONLINE SCAMS

Word is out about cancer-stricken widows of Nigerian cabinet members who are looking for your help, "Beloved," to distribute their fabulous wealth to the deserving poor.

The businesses in the United Kingdom (or elsewhere) that want you to act as collection agent and want you to help them evade taxes don't quite smell right either. But you might be tempted. What could go wrong, as long as the check they send you clears before you deduct your 10% and wire the money overseas?

A lot could go wrong.

In spite of the Internet and electronic banking, money transfers between financial institutions are not, for the most part, actually completed overnight or even in three days. If you have a good relationship with your banking institution, the staff will probably let you have access to funds you deposit before the check has actually, totally and completely, cleared.

So, if you withdraw that money, and then it turns out that the check you deposited was written on an account on the other side of the world that doesn't exist, you will get stuck for the money you withdrew. And your relationship with that institution isn't quite as good as it was before.

ONLINE BANKING: IS IT SAFE?

With so much talk of identity theft today, you might be concerned about doing business with your credit union online. However, identity theft can also happen through traditional banking. For example:

- Your mail (statements, bills, etc.) can be intercepted.
- The use of an ATM can expose you to either physical theft or thefts of your information (such as your PIN).
- If you pay your bills by paper check, you expose yourself to theft of your account number, as well as your phone number, which are printed right on the check.

Online banking, on the other hand, is more secure in these ways:

- The nature of the process ensures your business is done from the security of your home or office.
- Since there is an ongoing awareness of identity theft, there has been a real focus on security.
- The computers are protected by a firewall and multiple factor authentication (MFA) of login information.
- All data transfers use SSL encryption.
- You can also maintain control over access to your computer, whether it is at your home or office.
- When you have completed a transaction, log off so that you break the connection with the host server.
- Never conduct transactions while multiple browsers are open on your computer.

Yes, you need to be careful when banking online, but in today's world, it may actually be more secure than many in-person banking activities.

A BID FOR SAFETY: KEEPING YOURSELF OUT OF EBAY SCAMS

Summer is the perfect time for clearing out the stuff cluttering your garage. And any forward-thinking entrepreneur looking to sell stuff thinks of eBay. In fact, much of your garbage can fetch a substantial sum if sold successfully on eBay. The global reach of the world's largest bidding site offers tremendous potential.

Unfortunately, the big audience and big bucks also attract lots of scammers who

abuse the site's good name and your trust. Here are three common eBay scams and how to avoid them:

- **The fake payment.** You've sold a big-ticket item and you're thrilled. But before you're paid, the buyer offers more than they agreed to if they can skip the PayPal fees and instead send a certified check. Alternatively, you get an email from what appears to be PayPal telling you that the payment — more than you agreed to — is in transit, but won't be released until you provide a shipping number. Once you ship the item, the promised check never shows or bounces, or the "in transit" money from "PayPal" never comes. You've lost your money and the item.

  The rules are simple: Never send an item until you have the cash, and never accept non-electronic payment from someone you don't know.

- **The third party payment system.** A buyer refuses to use eBay's checkout system. They insist you remove your listing, send the item to them directly and they'll pay you directly.

  After you've shipped the item and received payment, though, they'll contact you again, claiming it was broken or it wasn't as described. They'll demand a full refund or threaten to have your eBay account banned. Since agreeing to settle a transaction outside the service is a violation of eBay's terms, they've got you cornered. You refund their money or stop selling on eBay.

  If you use a site to sell, use it to finish the deal. This keeps the company involved if things go sideways and ensures you're using the site legally and following the rules.

- **It was like that when I got it!** In this transaction, when the buyer receives the item, he sends you pictures of it with serious damage. He demands a refund, stipulating that you cough it up or take it up with eBay's Buyer Protection Program, which will force you to issue a refund.

  Quite likely, the buyer is showing pictures of another, similar item. Here are two ways to prove it:

  - Insist buyers purchase shipping insurance on all expensive or fragile items, and take time-stamped pictures of the item before it's sent. You now have proof the device was working, and the buyer can take up damage claims with the shipping company.
  - Include a disclaimer in the item description about refunds; a statement like "no refunds" puts you in the clear.

Using eBay is a great way to get rid of trash and earn some cash, but it's also a great way for scammers to take advantage of your naïveté. To sell safely on eBay, simply follow the rules.

TRUST YOUR INTUITION TO SHOP ONLINE (AND OFFLINE) SAFELY

In one way, shopping online is very similar to shopping at kiosks, in shops and in malls.

Personal and financial safety is always of great importance, but it's easy to forget about safety when we're distracted or in a rush. Either way, online or offline, searching for the best item at the best price can be very distracting, and distraction can be a real problem.

Think about the actions of a pickpocket for a moment. Professional pickpockets are looking for victims who are distracted, making it much easier to lift wallets, phones, purses and bags from preoccupied shoppers. Victims in hectic airports and on busy sidewalks are often distracted by the crowd, and they might be talking or texting on their phones at the same time.

How many times have you passed through an airport and consciously thought about a pickpocket or a thief? And whenever you're making your way through a downtown crowd or attending a special event, are you thinking about your personal and financial protection?

If you're not inclined to think about your safety while in a crowd, you're probably not thinking too much about your safety online either. Sadly, unscrupulous online vendors are well aware of that fact. They may set up a website, or a Craigslist or eBay listing, based upon the fact that most shoppers are too busy and too distracted to take a moment to consider their personal shopping safety.

Trusting your intuition is a very useful safety measure... assuming you pay attention to it.

If you just don't feel right about a particular brick-and-mortar store, you probably avoid it. But do you avoid a website or auction listing just because something doesn't look or feel right about it? If so, good for you. You are ahead of many folks in this area.

Most people who have used online dating sites become well-acquainted with profiles that don't seem to make sense. It's not always easy to identify the problem, but something just seems off, so they click away and check out other profiles as they shop for a possible date. Maybe it's just a feeling, but they learn to trust it.

Online dating can teach you a lot about using your intuition when you shop online. Even if you haven't explored online dating yourself, no doubt you've heard stories about fakers and scammers who compromised the personal and financial safety of someone they met online. Sadly, it's not an uncommon experience.

That's why internet shopping safety is primarily a matter of considering the real person or company behind every website and each listing you visit. Trust your intuition to guide you. To do this, you have to set aside distractions, and you can't be in a rush.

Look for:

- **Product descriptions that are too short, clipped and inadequate.** If a normal person needs more information to make an intelligent purchase, move on to another site to make your purchase. Something may not be right.
- **Spelling and grammar errors that stick out and detract from your shopping experience.** Reputable companies hire experienced copywriters and editors to eliminate basic spelling and grammar mistakes. Scammers, many of whom are not located in the United States, skip the expense and try to do it themselves.
- **A physical address in the United States.** If you can't find a physical address at the bottom of a website, or on the About or Contact pages, there's a problem. The CAN-SPAM Act requires commercial emails to include the physical address of the sender in the email and on the website to which any commercial email is linked. But, CAN-SPAM does not require websites to list a physical address, and it does not impose a fine as it does on commercial emails without physical addresses.

  In other words, the law does not protect you by requiring a physical address on every website, but your own intuition can protect you by raising a red flag whenever you can't locate a physical address. Reputable sellers are eager to provide the information buyers need to identify and verify them. Go elsewhere to shop if you don't find a physical address you can verify online by making sure it matches the business you found on the web.
- **A secure payment portal.** Look carefully at the website address in the address bar at the top of your browser screen. It should begin with "https://" because the "s" indicates a level of security you need whenever you're going to enter credit card or other personal information.

  However, you may visit a site with an address beginning with "http://" (without an "s"), and it can also be safe because it will direct you to a secure site for credit

card or checking account information when you check out. Usually, you'll need to begin a purchase transaction before you know how a merchant is set up to collect your data. So, it's not a bad idea to select one item and simply begin the checkout process, stopping short of clicking, "confirm." That way, you'll know what to expect with your real purchase.

SAFELY SHOPPING ONLINE

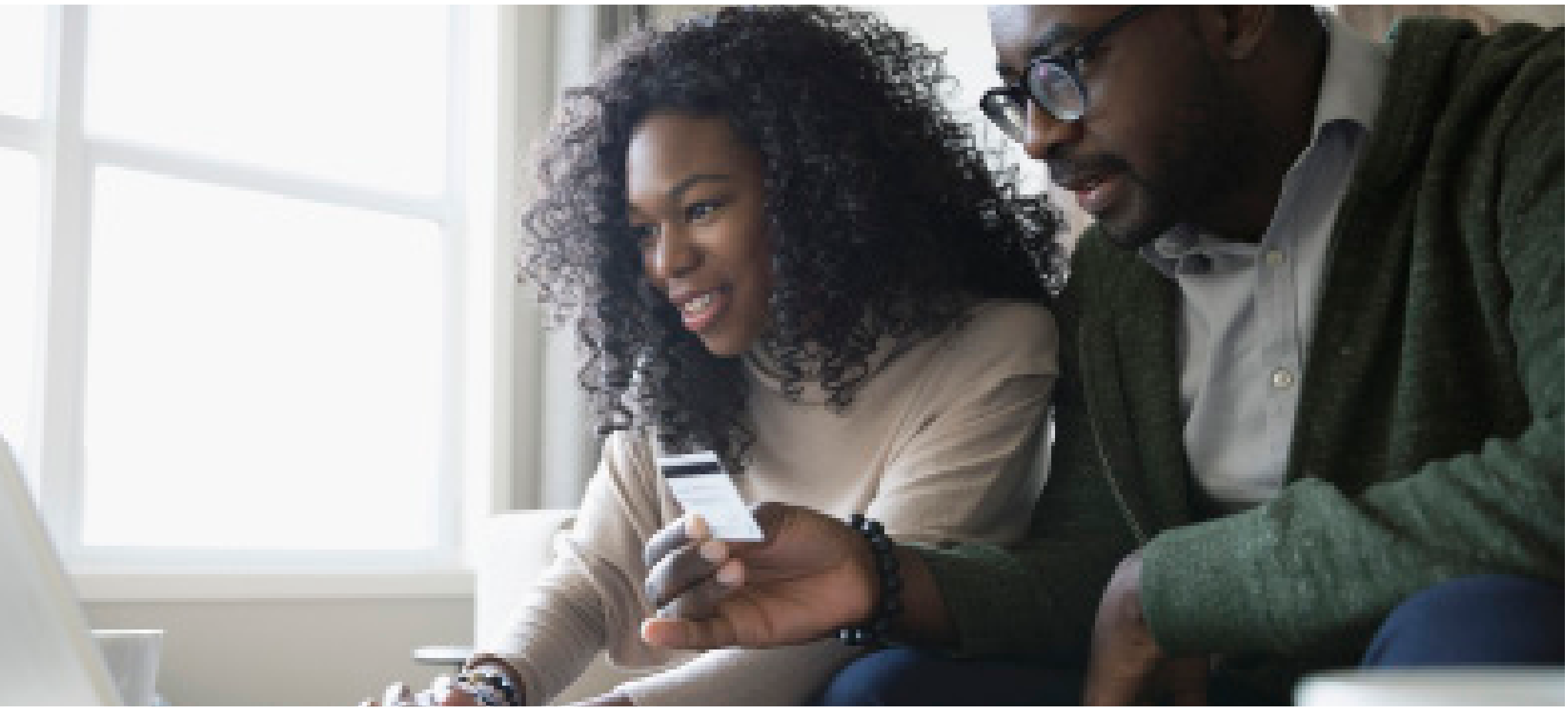
A safe and secure online shopping experience is possible by using these safety precautions.

Make sure your online shopping is completed on a website that starts with https://. Sometimes the "s", which shows the website is secure, does not appear until you are on the actual order page. You can also look for a closed padlock or an unbroken key at the bottom of the screen.

Make your online purchases with a credit card, not a debit card or a check. The credit card will protect you under the Federal Fair Credit Billing Act in case of questionable charges. A debit card does not offer the same protection. A check or debit card can also leave your account vulnerable. After making online purchases, monitor your credit card statement frequently and take care of any problems immediately.

Make sure you either know or research the company you will use for the online purchase. Also look for a physical business address and a phone number on the website. This will give you contact information in case of problems or questions.

If something just doesn't seem right, don't continue with the order.



SOCIAL MEDIA

SOCIAL MEDIA SCAMS: WHAT TO LOOK OUT FOR AND HOW TO STAY SAFE

New social media platforms seem to crop up all the time. The media moves at the speed of information, and it seems like overnight, Tinder and Snapchat went from complete unknowns to must-have apps. Each new technology offers something fun and unique to users, which is why the popularity of these apps has attracted so much attention.

Some of that attention has come from people with malicious intent. Scam artists take advantage of the newness of the medium and the lack of familiarity that people have with these apps. They've developed some cunning scams to harvest data, spread malicious software and commit identity theft.

In 2014, an Illinois man pleaded guilty to abusing social media site LinkedIn to sell more than $500 billion in fake securities. Make no mistake: Social media fraud is big business. While not all scammers set their sights that high, there's a lot of money to be had (and lost) from illegitimate social media use. Let's take a look at a few of the most common schemes.

- **The Fake App:** You get an invitation to install an app that will give you instant likes and shares on Facebook, Instagram or Twitter. The application does nothing, but buried in the user agreement is language which allows the app to broadcast messages without further permission. A scammer uses the app to make your profile broadcast links to phishing sites and other malicious webpages.
- **The Hidden Charge:** A fun personality quiz pops up in your news feed and

wants to use your cell number to text you the results. You enter your phone number, and unknowingly sign up for a $9.99 a month "service," which you won't hear about until your next cellphone bill. Removing the charges will prove difficult, and stopping them from recurring will cause hours of frustration.

- **The Emergency Request:** A friend sends you a message saying they're on vacation and they've had their wallet stolen. They need money to get back home. Being the generous person you are, you send them money by following instructions they provide. When you next speak to your friend, he or she has no idea what you're talking about. They didn't send the request – a hacker compromised their social media presence and used it to spread the scam.
- **The Age Verification:** Dating apps like Tinder have become a spawning ground for bots advertising "adult dating" services. These services will ask for your credit card number for "age verification." These sites will promise racy pictures and adult cam chats, but will hide the charges they bill to your credit card. Sites like these may also attempt to entice married people onto their platform and later attempt to blackmail them.
- **The Lottery Winner:** You may have seen stories on your social media feed about generous lottery winners who promise a share of their winnings to the first 1,000 people to share their good news. What you don't see is people donating money for "postage," or having their email addresses used to spread scams. Needless to say, the money never comes.
- **Profile Spy:** Facebook or Twitter apps promising to let you see who's been looking at your profile are another popular road for scam artists. The app will get permission, through the install process, to send messages to your friends, access your login information and post links to your profile. Any information the app provides you will be inaccurate and useless.

Identifying these schemes is half the battle. Thwarting them, then, is as easy as not doing whatever it is they want you to do. If you want to raise your social media security level, here are some steps you can take to protect your personal information.

- ***Don't install any social media application*** that can make posts to your feed, access your account information or see your friends list. That way, your name won't be the reason someone else clicks a malicious link.
- ***Don't enter your credit card information*** on any service if you don't intend to buy something. Not only will this keep you safe from scams, but it will also help cut down on impulse purchases on reputable websites.
- ***If anyone sends you a request for money through email or social media,***

get in touch with them through another means. Confirm they are in need, then send money via a service you know and trust.

- ***Change your social media passwords every six months,*** at least. Use complex passwords that don't contain information in your profile. Make sure someone can't answer your security questions with information you put out there.

Social media has made the world smaller and helped bring people closer together. It's now possible to keep up with friends who are all around the country and the world, while sharing cool experiences and stories with new, exciting individuals. At the same time, it's also exposed us to some new dangers. Keeping up with the latest scams helps make you a more responsible social media user and will make the world a little safer for all of us.

PINTEREST SCAMS: PROTECT YOURSELF

Social media is an ideal place to relax and find people who share your interests. Sites like Pinterest are great for keeping your recipes and projects organized. They're also a great way to keep up with the people in your life whom you don't see every day.

Scammers have recognized these sites as ideal places to strike. A Better Business Bureau report from 2014 reveals that scammers have found a way to use Pinterest. They sell counterfeit products, push dubious work-from-home schemes and fish for your personal information.

The scam works like this: You receive an email that a friend has shared a "pin," which is what the site calls its scrapbook items. This link looks legitimate, complete with a headline and a realistic photo.

You open the email and click the link, which directs you to a fake login site that looks like the Pinterest login page. You log in with your username and password, which are then stored in the scammer's database. They can use this information to commandeer your other social media accounts. Then, they can spread the scam to all your friends, providing the ideal environment for continued growth of the scam.

Worse yet, they can use the information you've stored on your social media profiles as part of a social engineering scheme. Efficient hackers can use the information in your profile to pretend to be you for financial transactions. Gaining control over your social media accounts is a first step toward identity theft.

It seems that the price of recreation is eternal vigilance. Even when in the parts of

the Internet that seem devoted to relaxing and unwinding, you must always be on your guard against identity theft. Here are some steps the Better Business Bureau recommends you take to avoid getting pinned in a social media scam.

- **Watch where you login** - Check the web address every time you log into social media sites. It should always be pinterest.com or twitter.com or the trusted web address of your intended social media destinations. If there's another word, or if there are a bunch of jumbled letters in there, it's a sure sign that someone is fishing for your password. Close the link immediately.
- **Practice good net hygiene** - Log out of your social media accounts when you're not using them, and don't share your password with anyone. Keep your social media accounts separate and use different passwords for each. This will prevent scammers from accessing several accounts if one of them gets hacked.
- **See something, say something** - Legitimate social media platforms hate scammers just as much as you do. They know that you'll only keep using their service if you trust it. You can use the "report this" link to let the administrators of the site know that something's amiss with the pin or page. They can investigate and close it down before it spreads further.

  If you see a friend sharing something that seems out of character or suspicious, let them know. They may have been hacked without knowing it. Be a good friend and let them know so they can take steps to protect themselves.
- **Be security-conscious** - Choose complex passwords that include numbers, letters and punctuation. Try to avoid using dictionary words. You can use names of streets, companies or celebrities to get a password that's easier to remember but harder to crack.
- **Change your password at least every six months.** If you develop two or three strong passwords, you can rotate between them to make sure no one is sneaking into your account. If you suspect your account has been compromised, change your password immediately!

With a little bit of added security, you can continue to enjoy all the benefits of social media. So go ahead and share your wedding plans, your house remodel, or your arts and crafts. Just be careful what you share from others and pay attention to what you click on in your email inbox. You never know who might be on the other side.

IDENTITY THEFT AND TECHNOLOGY – INCLUDING SOCIAL MEDIA

A study put together by The Javelin Group has some disturbing findings: The incidence of identity theft was up 13 percent in 2017, compared to the previous year. The total amount stolen was about the same, but the thieves successfully scammed more people.

Facebook, Google+ and LinkedIn users take heed: The study found that there were specific factors that put social media users at elevated risk of getting scammed:

- 68% of social media users publicly shared their birthday.
- 63% shared the name of their high school.
- 18% shared their phone number.
- 12% shared their pet's name.

All of the above information represents the kinds of things a company would use to verify your identity, according to the study's authors. In some cases, scammers have been known to bluff their way through customer service representatives to get access to other important information – and even wipe out entire accounts. When young or vulnerable people share this information, it could make them more susceptible to stalkers or sexual predators.

THE SMARTPHONE FACTOR

The study also found that smartphone users were a third more likely to be victims of identity theft than non-smartphone users. This doesn't mean, necessarily, that smartphones are to blame. But it does seem to indicate that the people who use smartphones are doing something to make them more vulnerable or attractive to scammers.

What can you do to avoid being a victim?

1. Password protect your phone.
2. Don't use credit cards for Internet transactions over public networks. Thieves have "sniffers" that can extract that data.
3. Don't store credit card numbers or bank account information on your laptop.
4. Use different passwords for mobile banking apps on your phone than you do for your phone and email.
5. Promptly report any suspicion that your sensitive personal information has

been compromised.

6. Keep documents that list Social Security numbers off your laptop, or encrypt that data if you do store it there.
7. Keep private information private. If any company uses specific information about you to verify your identity – your mother's maiden name, pet names, birthdays, etc., keep it off Facebook and any other social media site.

Tip: Is your mother on your Facebook page? Does she use her maiden name? You are vulnerable.

Pro tip: If your mother is on your Facebook page, and you share your date of birth, you are a prime candidate for ID theft.

ARE YOU INVITING THIEVES AT SOCIAL NETWORKING SITES?

Social media sites like Facebook, Twitter, Instagram and Snapchat boasts millions of active users, and continue rapid growth every year.

Although social networking sites are a convenient way to keep up with friends and family, remember that everything you post becomes open to the public. Of course, you would never post your bank information or Social Security number. But did you consider the fact that posting your pet's name, hometown, local newspaper and other "harmless" information gives anyone who wants it the answer to many typical questions that are often used to reset your banking and other sensitive passwords?

Is your home address or phone number posted? How about your birthday? With enough information, a thief can set up a personal profile and reset passwords so they can access your financial accounts, credit cards or investments.

"Most often, identity thieves need look no further than your own social network homepage to find personal information that can help them steal your identity or reset banking and other sensitive passwords," said Howard Schwartz, a spokesman for the Connecticut Better Business Bureau in Wallingford, CT.

Better safe than sorry. Take a few minutes to review your social networking profile on any site on which you participate. While you want to give friends enough information, make sure it isn't so much that people you don't know can use it against you.

MOBILE DEVICES

SMARTPHONES AND IDENTITY THEFT

The *Washington Post* ran a story about mobile phones bringing to light something most consumers don't know: When you reset your phone to wipe out your personal data, you're not really deleting anything.

Instead, you're deleting the pointers to where the data is located. Once you sell or recycle your phone, anyone who knows what they're doing can access the information you may have thought was long gone.

Although it may seem secure, you never know when your mobile phone could be lost or stolen. Carefully consider the information that is stored on your phone, and go to WirelessRecycling.com for instructions on how to delete what's there. Once on the site, click on online tools/cellphone data eraser.

STOLEN CELLPHONES

A few years back, a woman's handbag was stolen. One of the items in the handbag was her cellphone. Unfortunately, due to a common mistake, that was not all she was left without. When she finally succeeded in reaching her husband, he told her that he had answered her text message asking for the PIN to their joint checking account. It was too late to tell him that it had not been she who asked for the PIN. The thief had found "hubby" on the phone, got the PIN, and emptied the account.

This couple learned the hard way about a form of identity theft that most people are unaware of, but which is very simple to avoid. When adding contacts to your

cellphone, do not indicate their relationship to you, lest the phone fall into the wrong hands. Also, when someone requests sensitive information from you via text, take a moment to call them back and verify who you are giving this information to. As always, better safe than sorry.

SMARTPHONE THEFT: THE LATEST TREND IN CRIME

Although the national crime rate is very low historically, the Federal Communication Commission reports on a new trend in crime. One in three robberies involves the theft of a smartphone. This mirrors trends in major urban centers. In San Francisco, the SFPD reports that 50% of robberies involve a smartphone. In New York, the NYPD puts the figure as high as 75%. Stats like this firmly support the fact that smartphone robberies have become the latest epidemic in crime.

The reason for this new trend is simple. Smartphones are small and easy to conceal, are carried by about half of the population and have tremendous resale value. They're comparable in value to jewelry, but because they're so common, they're much harder to identify. The spread of online resale sites like Craigslist has made it even easier for thieves to sell stolen hardware. Demand for smartphones in the booming secondhand market makes it far harder for consumers to distinguish between legitimate resellers and criminals who are trying to move stolen property.

It's not just a domestic market, either. According to Businessweek, a new iPhone is

worth more than $1,100 in Italy and as much as $1,200 in Brazil. This international trade makes it very easy for criminal elements like drug cartels and terrorist organizations to reap tremendous profits from so-called "Apple Picking." Even a generation-old smartphone could sell for as much as $400 internationally, making it a lucrative source of funding for criminal organizations. In 2009, the Department of Justice busted a criminal ring that had engaged in the re-selling of stolen smartphones. The California group was arrested with more than $4 million worth of technology they intended to resell in Hong Kong.

While it's less common, some thieves use the access to personal data on your phone to commit identity theft. If you have your credit card number stored in the iTunes, Google Marketplace or other mobile app store, that information can be accessed by technology thieves to commit credit card fraud or other crimes. The same is true if you monitor your credit card or other financial instruments on your smartphone.

This trend doesn't just threaten your property; it may even threaten your life. Last year, Hwangbum Yang, a 26-year old Korean immigrant who was working as a cook in an upper-end Manhattan restaurant, was shot in the chest after refusing to hand over his smartphone to a man with a gun. He died on the sidewalk with the signature white earbuds of his iPhone still in his ears. Police apprehended the suspect by responding to a Craigslist ad offering to sell the phone for $400. The FCC cautions that robberies are violent crimes and many instances have been reported of robbers targeting cellphones while inflicting serious injury or even killing to acquire them.

This report is part of the impetus toward a national "kill switch" program. Several senators have proposed legislation requiring every smartphone in the US to come equipped with a remote function to wipe all data and permanently deactivate the device. The rationale here is that, if the user can destroy the functionality of the device with a phone call, the tremendous profit that's available in stolen cellphones will dry up, thus discouraging criminal behavior. Major smartphone distributors object to the program, as installation of this protocol would require new hardware for phones for the US market, therefore requiring a costly and significant change in manufacturing practices.

While the fate of the legislation is still up in the air, it represents only one of the possible solutions to the epidemic of smartphone theft. Here are a few steps you can take to protect yourself against this kind of crime:

- **Don't use the default headphones that come with the phone.** These are easily recognizable to potential thieves, which helps them quickly identify you as a target. Get a small, discrete set of earbuds instead.

- **Don't use your phone in areas where you're uncertain of your safety.** This means keeping it in your bag or pocket while you're on the bus, while walking home at night, or while walking through dangerous areas.
- **Check with your cellphone carrier about insurance for your phone.** You can often get replacement technology if your phone is stolen or destroyed. This knowledge can help keep you from losing more than your phone in a violent crime.
- **Know how to de-link your account from your phone.** Whether from a computer, phone or by stopping in to your carrier's store, you should be able to get your personal information off a device remotely. Being able to do this quickly can help minimize your losses.

As always, practice the same kind of good judgment and safe thinking. Be conscious of your surroundings and avoid situations that seem risky. Take a few sensible precautions, so you don't become a statistic.

BEWARE OF FAKE MOBILE PHONE APPS

Millions of people use their smartphones to check credit union accounts, bank accounts and other financial accounts. They are convenient, of course, and they have some terrific uses.

But be careful before you enter your credit union account password into a mobile phone app – especially if you aren't 100 percent sure of the application's source.

The reason: A growing industry of sophisticated criminals who exploit cellphone applications to capture passwords or to infect cellphones with spyware designed to route phone calls or texts to overseas premium numbers that bill cellphone carriers $1 to $15 for every transmission.

In one case, criminals lured thousands of children into downloading a fake cellphone game application of Angry Birds – a popular video game. The app was rigged to generate a $15 charge, billed to parents' cellphone bills or credit cards – every time the game was opened.

This particular scam was centered in the UK and Europe. But there have been attempts closer to home as well.

Here's how you can protect yourself:

- Don't let children use your mobile device unsupervised.
- Set up password permissions on your computer, your phone and your child's

phone to prevent them from downloading applications without your knowledge.

- Download cellphone apps only from trusted, reliable sources. For example, Apple's App Store, and the Android site make a concerted effort to screen new apps for spyware, malware and other scams. Use these established manufacturer web sites, or download apps directly from your financial institution's web page.
- Don't click on links within email messages. They frequently direct your browser to fake "spoof" websites designed to fool you into downloading apps or keying in confidential information.
- Don't give out passwords over the phone. Legitimate financial institutions will not call you and ask you to give out your password or PIN. Always call back, and get the number from a trusted source.

WHAT TO DO IF YOUR CELLPHONE IS LOST OR STOLEN

Here's a little known fact: If your cellphone is stolen, the wireless company can hold you liable for all charges made from the time it was stolen until you report the theft. One woman was reportedly charged $26,000 when her cellphone was stolen just before she left for a vacation in another country. Credit card issuers are required by law to limit the liability a consumer has for fraudulent charges, but cellphone companies are not. So you'll want to report a lost or stolen cellphone immediately. It's also a good idea to note the name of the person you spoke with, along with the time and date. Ask for confirmation in writing that your phone has been disabled. You might want to consider filing a police report, too.

However, fraudulent charges may be the last thing on your mind when your cellphone is stolen. All the information, such as phone numbers, stored in your phone is now in the potentially dangerous hands of a stranger. Contact anyone whose phone number you have stored by relationship ("Mom," "Grandpa," "Hubby") instead of their name to let them know your phone was stolen so they can be wary of calls and text messages coming through. Identity theft has been known to take place when a stolen cellphone was used to text "hubby" asking for a PIN reminder.

Better yet, don't save any names this way. Why take a chance on identity theft?

BEWARE OF TEXT-MESSAGING

Unethically creative identity thieves have a new trick up their sleeves: sending text messages to your cellphone as if they were a financial institution and asking you to

"confirm" your account number, PIN or other pieces of information.

As a member of our credit union, you should know that we will never ask for your personal information by email or text messaging. NEVER give information that is private and confidential over your cellphone's text feature, and don't call the 800 number that spam text messages ask you to call.

Here are other steps you can take to ensure that you don't become an identity thief's next victim:

- Be careful when asked for your telephone number. Giving your phone number in response to contests or online promotions can lead to unwanted calls and messages.
- Never respond to unsolicited text messages. It only lets the sender know they've reached a working number and may lead to more messages in the future.
- Consider blocking all text message services for your phone. While this may be somewhat inconvenient if you like texting your friends, it will protect you from this growing form of identity theft.
- Be cautious about the services you subscribe to.
- Be wary of urgent messages that request personal information.
- Report any messages that seem "too good to be true" or advertise illegal items to your local consumer protection agency.

Many unsolicited electronic ads and scams originate overseas, often making it extremely difficult to track the individuals who are responsible. Take initiative and protect yourself by never responding to spam text messages.

SMISHING

Installed a spam filter on your computer and feeling safe? Why not demand a similar service from your cellphone provider?

Smishing, the latest trend in identity theft, targets those who do mobile banking via text messaging. By taking advantage of the lack of spam filters on cellphones, the scammers send text messages to consumers alerting them that their "bank account is locked" and request that a given phone number be called to "provide the necessary financial information" to unlock it.

Many phone owners fall prey to this scam every day, and the scammers have increased their network to include non-mobile bankers as well, by sending messages to random phone numbers. Never respond to these types of messages no matter

how legitimate they appear. Your credit union will not use such a method to ask for personal information.

And perhaps, in response to this new crisis, we'll soon see providers offer plans to protect our cellphones!

CHARGING YOUR PHONE IN PUBLIC? WATCH THAT PORT!

Smartphones have become ubiquitous, and having a charged cellphone provides a sense of security. That's why, when the battery meter starts to dip, a cold sense of panic rises in your stomach.

Many public places have begun to adapt to this change by providing USB ports in addition to electrical outlets. That means smartphone owners can now plug directly into the wall.

Sadly, though, this public good has become a playground for thieves. Scammers have hooked tiny computers into some of those ports. When you plug in, they can then install programs on your phone which report back personally identifiable information that's used to commit identity theft. Alternately, thieves use the connection to look through your phone's contents, stealing browser history data – including passwords.

It's called "Juice Jacking," and it can take as little as three minutes to break your phone wide open.

Obviously, these scammers choose places where they can do the most damage — airports, shopping malls and other places where people linger. If you're at a place you trust, feel free to use the power. However, if you're in a public place use these tips to stay safe and avoid Juice Jackers.

1. **Carry (or borrow) a power plug** - The easiest way to thwart the scam is to only plug your phone into electrical outlets. There's no computer on the other side. Yes, it's a hassle to carry one more thing, but it's worth it to avoid compromising your personal information. Shop around to find a compact converter and keep it in your bag. If a power plug is a real hassle, only carry it when your phone is low on juice. In a pinch, you can also borrow a plug from a laptop user. While not quite universal, chargers are pretty interchangeable.
2. **Pick up a battery** - Consider carrying your power solutions with you. Advancements in battery technology have made them smaller and more efficient than ever. A battery pack the size of a pen can completely charge your

smartphone. Slightly larger packs can provide several days' worth of charge. You can also keep a battery pack in your glove compartment. That way, you get the security of knowing you've got a charge when you need one without having to lug it around.

3. **Conserve your power** - The easiest way to avoid using a public charging station is not to need one in the first place. There are several things you can do to save your phone's charge if it's running low, like changing your wallpaper to all black.

For slightly more savings, keep your apps updated. Running outdated software could be chewing up your battery life. Similarly, don't enable auto-update. This can quickly drain data while also burning through battery life. Update apps manually when you're connected to WiFi, or just disable automatic updates if your battery situation is dicey.

WATCH THAT WI-FI!

In yet another scam that capitalizes on the desperation we might feel when we're out and our mobile devices are on the blink or not connected, this one is particularly nefarious.

We've all been there. It's been a long day of shopping at the mall, or waiting in an airport, or driving across the country, and we finally get a chance to pull out our phones or laptops and look for Wi-Fi. Good news: You've found one that doesn't require a password! Free Wi-Fi saves the day. You click accept and head to your favorite place to watch videos of kittens, or whatever people normally do on the internet ... we mostly watch kittens.

There's just one problem: What if that free Wi-Fi was a trap? One of the cleverest phishing scams out there right now is built on the lure of free Wi-Fi using rogue access points, and it has enough variations to stay ahead of the security teams at Apple, Samsung, Microsoft and our own security for one simple reason: The soft spot in your security is you.

Here's how phishing on rogue access points works: The scammer will set up a wireless router offering free internet, often marked "Free Wi-Fi," "ATT Wi-Fi," or "Starbucks." Would you be suspicious of those networks? Many people just look for the strongest "free" network, while most of the rest of us look for a name we trust. How paranoid do you have to be to not connect to Starbucks Wi-Fi at the mall? Once you connect, though, they have a variety of ways to get any information they want off your phone or laptop.

Even scarier, some scammers are using programs that tell your phone that the name of the free wireless available from the scammer's router is whatever name your phone is looking for, so it can even connect automatically while in your pocket. You can get phished over your phone just by walking in the wrong area.

Once you're on their network, they have a variety of ways to steal your info, from just grabbing your session cookies to using keystroke monitors to get logins and passwords, to the traditional phishing technique of creating dummy sites that look like Facebook or major credit card websites to prompt you for your info.

Here's what you can do to stay safe:

- **Turn off your Wi-Fi unless you're at home or work.** I know, I know. The only thing worse than mobile network data speed is mobile data network pricing. Well, maybe mobile network customer service. Unfortunately, all that Wi-Fi you grab every day can be dangerous. Even if you're not running into rogue access points, you've still got to hope that the coffee shop or burger joint actually pays attention to the security of their wireless router, which few even think to do. Even those businesses that do think about security rarely spend money on it – rarely are they bringing in a professional. No, they're asking a minimum wage employee to "take care of it" because "You're young and good at computers."
- **Make sure your home and work Wi-Fi are safe.** Endpoint security, like Norton antivirus, is not as effective as it once was, simply because there are so many more points of vulnerability than there were a few years back. We'll have an extended look at securing your Wi-Fi network in a future installment, but for today, set up your password with WPA2 Enterprise encryption. If your router does not support it, it's time for a new router.
- **Rename your home network something like "This Public Wi-Fi is UNSAFE."** It might sound weird, but if a scammer tries to use software to tell your phone the name of his network is the same as your home network, your phone will tell you it's connected to "This Public Wi-Fi is UNSAFE" and you can get off of it.
- **Apps are your friend.** Most apps use HTTPs security, rather than HTTP. This can actually stop some of the tactics many scammers use. Remember, they don't want to beat the best security; they want to do as little work as possible and beat those unwary souls who rely on the worst security. A simple step up is enough to keep many scammers at bay.
- **Get an app that prevents rogue access.** Depending on your operating system (OS), you have different options, but search your app store. It's worth

the trouble and $4.99.

PHONE CLONING

Even when you think you're taking all necessary precautions to protect your mobile device and the sensitive information it contains, you might be vulnerable to identity theft just by owning a phone and using it in public – because someone might be cloning your phone without your knowledge!

Cloning a phone involves copying the identity of one phone to another.

In today's digital world, when we use them for everything from ordering an Uber to paying for purchases, mobile phones can be a major source of security breaches. And as frightening as it sounds, the only thing a hacker needs to launch a major attack is your phone number.

Hackers clone phones so they can use them, or sell them to people who use them, to make calls and access the phone's data. When a phone is cloned, the calls made by the hackers are billed to your account. But that's just the beginning.

Phones often contain enormous amounts of personal information. Once the hacker has access to the phone, they can cause devastating financial damage.

The hacker can listen to you from their own phone and watch you through your camera. They can read your messages, access your passwords and view your contacts.

Cloned phones are also convenient for criminals, particularly in drug-related crime, because they are harder to trace. If your phone is used this way, it may appear to authorities as if you are engaged in criminal activity.

There are a number of ways to clone a phone. When a cellphone is cloned, it is reprogrammed to transfer the serial settings and phone number from a legitimate phone. The easiest way to clone a phone is to use specialized software, which is readily available online.

How can you tell if your phone's been cloned?

You may not know your phone has been cloned until you notice unusual financial activity.

However, you may detect hints that the phone has been cloned, such as lots of wrong-number calls, difficulty making outgoing calls or retrieving messages and unfamiliar numbers on your phone bill.

PROTECTING YOURSELF

Here are some proactive and reactive steps you can take against phone-cloning:

- Review your phone bill for unfamiliar numbers and charges. If something looks suspicious, have your provider check for viruses that may have resulted from cloning.
- Input your phone number into a search engine to see if any links include your number.
- Use another phone to call your number to see if someone picks up.
- Contact your financial institution to verify whether anyone has tried to open credit cards or loans in your name.
- Make sure your phone is password-protected. Create different passwords and PINs for all the accounts accessible via your phone.
- If you suspect cloning, you may have to restore your phone to its factory settings.

If you determine that your phone was cloned, contact your phone provider and the FBI immediately.

IRL

SHOULDER SURFING

While you are paying for your groceries, filling out a form or using your ATM card, another person may be "shoulder surfing" to gather your personal information. Shoulder surfing happens when a person sees and quickly memorizes your personal information to use as his or her own. It can be done by looking directly over your shoulder or from a distance with binoculars or other devices.

Shoulder surfing can be prevented with some basic precautions.

- Block the view of your paperwork, your credit or debit card, or the keypad by moving your body or hand.
- Have your credit or debit card ready when you are at the register. The longer it takes to search for your wallet or right card, the longer others can see the contents and the greater risk you run of other vital pieces of information falling from your purse or wallet.
- Never carry your Social Security card.
- Respect your hunches. If something doesn't seem right or someone is standing too close, move away or pause. The most important way to prevent shoulder surfing is to be alert and aware of your surroundings at all times.

SLIDING AND PURSE SAFETY

You've heard the stories and seen the video clips of purses being stolen from vehicles while parked at gas stations. "Theft by sliding" is what it is commonly called. While you are pumping your gas, you probably don't think anything of that car that is pulling up alongside yours. After all, aren't they just going to use the pump next to

you?

You get back into your car and (sooner or later) realize your purse is gone. They weren't going to pump gas after all. Once they drove up next to your car, they quietly opened their door and then yours to "slide" into your vehicle to take your purse. It was quiet. It was fast. It happened without you even realizing it.

The "sliding" trend may be new, but purse snatching isn't. It can happen anywhere. Gas station, grocery store, church, park bench. Anywhere you sit or stand, you could be a potential target for having your purse stolen. While the makeup, notepads, pens or toys in your purse can be easily replaced, replacing your financial identity requires much more effort.

Here are some simple ways to protect your purse and your financial identity.

- At a gas station, take your purse with you to the pump. Don't leave it on the passenger seat. Don't leave it in between the two front seats. Lock your doors. Keep your windows up. Be aware of your surroundings. It is easy to get distracted by the music that's playing, kids trying to talk to you or even in watching other people.
- The same applies to your purse while you are in public settings. Don't leave it in the cart at the grocery store while you shop. Don't leave it at the restaurant table while you step away. Don't leave your purse unattended while at that concert, museum, movie or church service.
- You can also be prepared in case your purse is stolen. Don't carry irreplaceable valuables in your purse. That could include an expensive new electronic device or that family photograph (by the way, you really should make a copy of that for home). Don't carry your Social Security card with you. Make copies of the fronts and backs of any credit cards that are in your wallet. Consider cleaning out your wallet, too. Do you really need to carry every store credit card with you when you go to the grocery store?

And always remember, your life is more valuable than your purse or even your financial identity!

SKIMMING

When you are at a restaurant and paying your bill with a credit card, you may not be giving your card another thought. Unfortunately, skimming can occur any time your credit card leaves your direct possession.

Skimming happens when the person processing your payment also swipes your

card through a special tool that collects and stores credit card information. This data is later downloaded to be used by others.

Some precautions can be taken to help prevent skimming.

- If you hand your credit card to someone, keep a close eye on your card. When the card is returned, make sure it is your card and not a fake or someone else's.
- Protect your credit card number. Take your receipts with you, and later shred them. When you leave the credit card payment slip at a restaurant, make sure to cover the part with your card number, name and signature.
- Monitor your credit card bills and balances. If something isn't right, take care of it right away.
- Most importantly, make sure you are aware of your surroundings and follow any hunches you have about your credit card.

ATM FRAUD ON THE RISE: STAYING SAFE WHILE GETTING CASH

Scammers are everywhere in web-based commerce. You might think you're safe using cash, but scammers wait in one location you can't avoid: the ATM.

ATM fraud is an old concern, but technological advances mean consumers need to be even more aware. Be cautious of the following:

1. **ATMs in weird locations** - Cash is convenient. While it's tempting to use whatever ATM is handy when the need arises, that can be risky. ATMs in financial institutions are regularly monitored, maintained and covered by security cameras. In contrast, an ATM in a store corner may not get that same attention. Most of these machines are privately owned, and the operators assume little liability for their safety.

   Use ATMs in secure locations, like financial institutions. They're safer and well maintained. If you must, choose ATMs in highly visible and public areas to minimize encountering a tampered machine.

2. **Recent work** - Two modifications are common in ATM scams. The first is a duplicate keypad on top of the existing one which relays PIN information to a third party, enabling fraud at a later time. The second is a phony card reader which processes your card information and sends it elsewhere. These scams have become more common and harder to detect as 3-D printing technology has improved and become more accessible.

Several signs hint at a machine that has been tampered with. First, keypads get worn over time. If an old machine has new-looking keys, something may have been modified. Similarly, card readers develop scuffs and scratches; new-looking card readers are another red flag. Second, scammers install devices quickly, and may use quick fixes like electrical tape which leave signs of modification.

If you think an ATM has been modified, don't use it.

3. **Nearby strangers** - Some scammers use their own senses to rob you. Standing behind you, the scammer will watch you enter your PIN. If successful, the scammer will mark you for pickpocketing and then use your ATM card to empty your account.

   Other scammers use an accomplice who drops a bag behind you just after you enter your PIN and may also engage you in conversation. While you're distracted, the scammer grabs your card and replaces it with a phony, or just takes the cash you've withdrawn and runs.

   To protect yourself, cover your hand when entering your PIN, stand close to the machine and keep an eye out for anyone sitting near the machine on a laptop – they may be monitoring a camera designed to capture your PIN. Most importantly, stay focused. Watch your belongings, and ignore anyone who approaches you until you've finished your transaction.

If you think you've been victimized by ATM fraud, report it immediately. Waiting to report the scam could mean you're responsible for all the bills the criminal racks up, but if you report it within two days, your liability is capped at $50.

12 WAYS TO PRACTICE SAFE ATM TRANSACTIONS

ATM fraud is on the rise. Here are 12 ways to protect yourself and your account from theft!

1. **Look for recent device modifications** – bulky keypads, electrical tape, fresh glue, unworn plastic, etc. These can be signs of a PIN capture device being used.
2. **Check for cameras** – tiny pinholes provide clear views of the keypad and are a prime target for recording PINs. Security cameras designed for safety are obvious and usually mounted further away.
3. **Cover the PIN pad with your other hand** to keep your transaction safe from prying eyes.

4. **Look for people sitting nearby.** Take note of anyone who is using laptops, handheld computers or cellphones. If they're sitting there for more than a few minutes, they may be eavesdropping using the device.
5. **Do not share your PIN** with anyone you don't want using your card (and that should be a very small circle). If you write down your PIN, keep it in a secure location away from the card. Don't carry it in your wallet or record it in your phone!
6. **Only use ATMs in well-lit, public spaces.** Prefer those that offer drive-up service and don't have buildings or heavy foot traffic nearby.
7. **Go to the nearest bank branch or use another ATM** if you have trouble with an ATM. Do not let strangers "help" you with the transaction.
8. **Avoid ATMs in tourist hotspots** like shopping malls – these high-traffic areas make it easier for thieves to work.
9. **Monitor your checking account statement** regularly for suspicious or unknown charges.
10. **Report any unusual account activity** to your credit union right away.
11. **Remember that all terminals are vulnerable.** Even gas station consoles and other payment locations are just as vulnerable as standalone ATMs.
12. **Process your debit card transaction as a "credit" transaction**, if possible, so you will be prompted to sign for it rather than enter a PIN. This helps ensure it cannot be seen by the next person in line.

SAFE-CATIONS

STAY SAFE FROM AIRBNB SCAMS

Going on vacation should mean truly experiencing a new location. That's part of the appeal behind room-sharing sites like AirBNB, where anyone with a spare room can become a host. As a guest of a local, you'll get a real sense of a location – and you'll save money, too!

However, the system is based on trust, which means crooks will try to exploit it. The Australian Better Business Bureau reported a six-fold increase in scams related to AirBNB in 2016. The service recently expanded its offerings, allowing users to book independently-run guided tours or experiences in addition to rooms.

This expansion has been part of the drive behind the increase. Before you book at AirBNB, be aware of these scams.

1. **Fake websites** - An AirBNB host you were interested in sends you a link to several other properties they have for rent. These properties come complete with reviews, logos, a live chat service and other hallmarks of authenticity. So you think nothing of wiring a fee to reserve your room.

   But when you try confirming your reservation with AirBNB, they have no record of your transaction and don't even have the properties listed. What happened?

   A scammer capitalized on your trust by directing you to a fake booking website that's not hosted by AirBNB. These groups go to extreme lengths to create accurate reproductions of the official site.

   There are two ways to avoid this scam. First, always check the URLs of sites you visit, making sure the word AirBNB occurs right next to the ".com." This tells you it's not a phony site. Second, only pay through AirBNB's official checkout platform, which uses modern encryption technology.

2. **Phony excursions** - A new feature of AirBNB is the ability to book "experiences," or days out on the town with locals.

   This creates a new opportunity for scammers who can now offer phony tours. While the company vets the potential tours carefully, it's difficult for them to monitor a distributed network of service providers.

   Local experiences appeal to many visitors. However, proceed with caution. Always check reviews (on a legitimate AirBNB site) before paying for anything!

3. **External payment** - AirBNB charges a 3% commission on bookings done through its website. This prompts some landlords to offer a discount in exchange for direct payment through a third-party processing site. Tightfisted travelers might be tempted to save a few bucks this way.

   Resist the temptation. Payments outside the website don't have the conflict resolution procedures usually covered by AirBNB, so there's no guarantee you'll have a room at all if you use one.

   Also, no legitimate business will have you wire funds directly to their account. With services like PayPal, even small businesses can now accept credit cards. When you use a card, you can always stop a payment. After you wire money, it's gone. It's always a good idea to use only secured forms of payment.

AIN'T NOTHING LIKE THE REAL THING – TIPS TO AVOID BEING TAKEN BY RENTAL SCAMS

Renting an apartment can be scary. As you consider available options for your new home, you likely search for a clean, affordable apartment in a safe neighborhood. Those qualities are important, but mostly, you want it to be real.

Rental scams are one of the fastest-growing types of fraud nationwide. With sites like Apartments.com, apartment-searching is easier than ever. Unfortunately, that convenience has a price. Anyone can list anything "for rent" for any price. While most listings are legitimate, some are not. With a few pictures and emails, scammers can convince you they actually have a luxury apartment available.

Here are three ways to keep your money safe from rental scammers:

1. **Know what 'too good to be true' looks like** - Check rental prices of similar-sized apartments in the area. You can research the average renting price in most major cities at Rentbits.com. If your apartment is being offered for considerably cheaper than most others, it's probably a scam.

   If the landlord has a supposedly tragic reason for the low rental cost, don't be

fazed. Odds are, the story isn't true. If it is, let someone else help your poor landlord-to-be.

If the posting is written in poor English, be cautious. Legitimate companies usually use listing agents who have experience writing postings; individual lessors are rare. If you're asked to wire money – especially if you haven't seen the apartment yet – that's a scam.

"Showing fees" and "pre-screening charges" do not exist. Don't ever rent an apartment, sign a lease or pay a deposit without seeing the actual apartment.

2. **Guard your personal information** - Don't give anyone unnecessary personal information. Your email address and phone number are important for communication — your credit card number is not. You may need to leave a copy of your driver's license with a rental agent while touring an apartment, but no one else should need personal information prior to showing you a house. Anyone asking to run a credit check before showing you a property wants you as a victim, not a tenant.

   Where possible, try to work with someone local. Ask the person offering the apartment to meet you in person and show you the property so you can see it's real and not inhabited by someone who doesn't want to move.

3. **Trust ... but verify - If something seems fishy, research it.** Google the name of the person or company listing the property to verify that they're actually listing it.

   There are many forums dedicated to outing scammers. Check Reddit's personal finance section (reddit.com/r/personalfinance). If you notice something off-putting about your potential landlord, add a post and move on.

Wherever there's money changing hands, someone will take advantage. Scammers can quickly produce photographic proof that a place exists and then ask you to pay them immediately. As a renter, you're taking risks, but following these rules can keep you safe.

Now, go get your dream apartment!

VACATION RENTAL SCAM

Going on vacation? Staying at a hotel is one option, but there's another: renting a home that someone else owns either as a vacation property they sometimes rent out or as an investment that they rent as much as they can.

It may be a nice way to vacation, but recently scammers have been pretending

they own properties that they don't. People have been finding a property they like, making a large deposit, "to reserve the rental" and then learning, upon arriving at the destination, that they can't get in.

At that point, they contact the owner of the home, who hears about the rental agreement for the first time, and never received the deposit. So there you are, stuck in a place with nowhere to stay and short hundreds of dollars for your deposit.

Avoid this scam by renting only from legitimate websites that guarantee your rental. It's also a good idea to take some time to read the reviews left by other vacationers before making your reservations.

HOUSE STEALING

What if you want to sell your house and found out it wasn't yours? How about if you came home from vacation and found someone else living in your home?

House stealing happens when mortgage fraud and identity theft come together. While it is not that common, it does happen; especially with homes with high resale value, rental homes, vacation homes or vacant homes.

House stealing starts with a thief researching public records about properties and owners. The identity theft happens when the thief assumes the homeowner's identity through fake documents, IDs, and Social Security cards. The mortgage fraud happens when the thief then completes the forms and process to transfer the house's deed. Once the forms are properly filed through the county, the house has been "stolen" and now has new owners who can move into or even sell what was your home.

How, then, do you protect yourself from house stealing? Review any mailings you receive from any mortgage companies. Review the names and signatures on your home's deed in the county's deed office. Also, make sure you keep up with identity theft prevention in general by reviewing your credit report. You will want to follow up with any questionable information on the mortgage company mailings, your home's deed or your credit report. If you think you are a victim of house stealing, contact your local police and the FBI.

BOGUS HOME RENTALS

With thousands of homes empty as a result of recent foreclosures, there's a fairly new scam involving unsuspecting renters. A criminal will find a likely house and call a locksmith, saying they have locked themselves out. Once inside, he changes the locks and then puts up a "For Lease" sign in front of the house.

The house is then advertised for rent. Unsuspecting tenants view the house and are quoted a low rental price, because the owner is desperate to get rid of the house. The criminal then takes a deposit from the victim and gives him a bogus lease with a set of keys.

After that, one of two things can happen. In some cases, the scammer continues to show the house and take deposits in exchange for keys, leases and a move-in date. Alternatively, they'll allow the unsuspecting tenant to move in and pay rent to a mailbox or untraceable bank account.

The tenants either try to move into the house and find their keys do not work and the landlord cannot be found; or worse – they move in, pay rent for a few months and then get a visit from the bank, asking why they are living there.

Either way, the tenant has lost hundreds, if not thousands of dollars. When renting a house, be sure to check the landlord's phone number, physical address and credentials.

IN BUSINESS AND CAREER

BUSINESS DIRECTORY SCAM

Every business owner knows there's no such thing as bad publicity, especially

when it's free. Newspaper articles, business exchanges and other means to get more people exposed to your company's name are great, especially if your business is small. When you don't have a big advertising budget, these organizations can be a lifesaver.

Unfortunately, scammers realize that this desire for publicity is a powerful motivation. Scams targeting business owners involving fake business directories are on the rise. These schemes come in a variety of flavors.

One variant has the scammer call, fax or email asking the business to "confirm" or "verify" its contact information for a business directory. No discussion about price occurs. The scammer usually tries to target office professionals, receptionists and personal assistants who are more likely to be bullied into saying yes. In the case of a fax or email, the terms and conditions on the statement may include fine print about exorbitant listing fees. Of course, there is no directory, but that won't stop them from billing.

After the initial contact, the next step is a slew of invoices marked "urgent," for anywhere from a few hundred dollars to thousands. Many scammers are counting on a low-oversight accounts payable system, where invoices are posted and paid without much investigation. If the invoice is not paid, the scammer will escalate to collection notices and calls, and may threaten the business's credit. They may even discuss litigation.

At this point, the scammer will usually offer a "settlement" amount which seems incredibly generous. This is a powerful psychological tactic which takes advantage of the contrast effect. Paying $500 when you've previously been told you have to pay $1,000 seems much more reasonable than just being told to pay $500.

Other variants may claim to confirm Yellow Pages listings. They may also claim to represent a charity network and target small not-for-profit groups like churches or

community food banks. The process is the same in all cases.

Authorities suspect the scams originate in a small number of large call centers located outside the U.S. Recently, the FTC filed suit against a Montreal-based call center which had defrauded thousands of businesses and charities in the U.S. Despite these charges, the scam continues to grow in popularity.

If your business or charity is targeted by this scam, there are a few things you need to know. To keep your business out of trouble, make sure you do the following:

- **Protect and educate your employees** - If you have a marketing department, establish a policy that all promotion efforts go through that department. Add language to your employee handbook or other documentation specifying who is authorized to make promotional deals on behalf of your business. Make sure it's written down and that your employees know about it. This language will protect them should they be the ones to sign one of these fake agreements.

  Also, make it a point to discuss this and other scams with your employees during regular meetings. This scam preys on the unwary and relies on ignorance to make a cheap buck. Knowledge is your best defense!

- **Don't pay them a dime** - If you notice an invoice like this, you should check with the Better Business Bureau (BBB) in your area to see if complaints have been filed against the organization that issued it. If there is, you should store the invoice somewhere safe. You should never ever agree to pay it.

- **Most of these "contracts" are unenforceable.** Particularly if they use Yellow Pages branded icons and names to establish their legitimacy, they were agreements made under false pretenses. A verbal agreement, even one recorded over the phone, likely isn't binding, especially if no discussion of price occurs.

  Even if they were, the litigation to collect the debt would be hopelessly expensive. Reporting the debt to credit reporting agencies would expose the group doing the reporting to defamation liability. The bluster surrounding the collection process is just that.

- **Inspect, collect and notify** - If you haven't before, now's a good time to take a look at your accounts payable processes. Make sure tight controls exist to ensure that invoices are checked for legitimacy before being paid. Double check to make sure you're only paying for services you receive.

  If you do get fraudulent invoices, don't throw them away! File them in a safe place. You may need them to help an investigation of scammers down the line. They may also be helpful if you need to contest a report with a credit reporting agency.

You should also notify the FTC immediately. Misrepresentations like these over the phone, fax or email are a violation of FTC rules regarding advertisement. The FTC can be reached at 877-FTC-HELP or online at ftc.gov/complaint.

- **Be proactive** - The best way to stay ahead of this scam is to stay abreast of new promotional opportunities in your community. Your local chamber of commerce likely maintains a directory of local businesses and is an excellent place to start for help promoting your business. Get involved with local organizations and charities that represent the values of your business. Don't sit back and wait for those opportunities to call you up. Get out and take charge of them yourself!

JOB SEEKERS BEWARE: 'REPACKING' JOBS COULD LEAD TO JAIL TIME!

We keep hearing the economy is improving, but that news rings hollow for many Americans. Long-term unemployment is still a reality for close to two million people. They're isolated and increasingly desperate, making them a perfect target for cyber-criminals.

The Better Business Bureau has reported a creative breed of cyber-crime that turns innocent people into accessories in the distribution of stolen merchandise. The scam starts like a lot of others, with a job offer from an anonymous company. The work sounds ideal. It's work-from-home, set your own hours and work as much or as little as you like. Best of all, it's easy. You receive shipments at your house, then repack them and ship them to another address.

If you sign up, you'll receive packages containing products and instructions about shipping them to other addresses, sometimes overseas. Your employer will want you to cover shipping, but promises to reimburse you for costs on top of your salary. At the end of the month, you get a check from your employer.

The first bad news comes when you attempt to cash that paycheck and it turns out to be fake. All the work you've done, plus the shipping costs you paid out of pocket, are gone. It'd be bad enough if it ended there.

Worse yet, you might end up facing criminal charges. At the very least, you'll be an accessory to the theft of the goods you handled. If you helped to redistribute those goods, you handled stolen property. Even if you didn't know the goods were stolen, if you didn't ask questions where a reasonable person would have, you're guilty.

To make matters worse, if you shipped those items internationally, you likely had to lie on customs documents. That's a federal offense. The scammers just tricked

you into taking all of the legal risk while they keep the money.

Similar scams are common in money laundering. A scammer will contact you or leave a post on a job board asking for financial service assistance. They'll send a check and ask you to deposit it, then wire them back some of the money. You can keep a portion of it as your payment. The check was written against stolen funds and the issuing institution refuses to pay it. You're out whatever you wired the scammer and could face charges as an accessory to fraud.

These scams are an unfortunate part of the job search process. They prey on the uncertainty and desperation that characterizes long-term unemployment. The widely anonymous nature of the internet provides a perfect cover for schemers. If you want to keep yourself safe, follow these tips:

1. **Be proactive in your job search** - It's possible that your dream job may fall in your lap, though it's far more likely that you'll have to work really hard to get it. If you post your resume on a job site and walk away, it's possible that the only people who are going to contact you are scammers. If you work with a recruiter or employment agency, you'll form a contact that can help you land the job you want.

   Working with an agency will also help you weed out the scams. You'll have someone you know and trust to sort the real opportunities from the bogus ones. They'll help put your resume in places where it needs to be instead of in the wrong hands.

2. **Check the links** - Many of these scams work by "spoofing" a legitimate job posting. You'll see an email saying that X company has reviewed your resume and thinks you would be a good fit for this position. The email will contain a link to something designed to look like a legitimate job posting on a big job board like Monster or Indeed.

   Checking to see where links are really going is a hassle, but a quick mouse-over the link will show you the URL. If you don't recognize the domain (the first part after the http:// and before the .com or .org), don't click the link. Report the email as the scam attempt it is.

3. **Watch for keywords** - "Repackaging" or "reboxing" are common keywords in these scams. For money-laundering, scammers often refer to the work they are proposing as "payment processing" or "wire transfer assistance." It's worth taking a moment to think about what you'd be doing. No legitimate business would need a personal checking account to move money around. If they're a business that can pay for your services, they have a checking account. Similarly, they have an address and postal services.

If an employer is seeking your personal information before they've hired you, they're not a potential employer. They're crooks trying to steal your identity. It's as simple as that.

AVOIDING SCAMS IN THE WORKPLACE: KEEPING YOURSELF AND THE REST OF US SAFE

Pop quiz: What do the data breaches at Target, Home Depot and Sony all have in common? Give up? They were all caused by employee errors. These, along with about 500 other breaches, are confirming what many security professionals have worried about for years. In the digital age, the weakest link in our information security is us: humans.

The most common cause of data breaches around the world is employee error or negligence.

This kind of negligence can take a few forms. It can be an employee responding to a phishing email or downloading a piece of malicious software on a company computer. An employee could fail to adequately secure his login information (by, say, writing it on a sticky note and attaching it to the monitor) or could leave company technology vulnerable to theft.

As with many other complex, human-focused problems, no single solution can address this problem. There are structural and technological changes that can help mitigate the risks posed by employee error. While these changes are developed and implemented, here are three simple steps you can take to help keep your workplace safe from hacks.

Read something, say something - Everyone thinks they can detect a scam. It's a line of thinking called the general attribution error: what's true of "most people" can't possibly be true of us and the people we know. We constantly believe we're the exception rather than the rule, and our susceptibility to fraud demonstrates this well. Most people consider themselves intelligent, discerning internet consumers. Yet, a recent Google study found that 45% of users fell victim to a fake login page.

Scammers wouldn't keep using these tactics if they weren't working, and even if you are savvy enough to spot 99 phishing attempts in a row, the one you miss is all it takes for another big data breach to happen. If you work at a company with 100 people who are all as adept as you are at catching these emails, every scam attempt works on one person on average. Worse still, some hacking attempts begin by sending out emails from the first victim to people on that person's contact list. When that happens, one person falling victim to an attack can quickly increase the

credibility of subsequent attacks.

The solution to the general attribution error is the power of collective wisdom. If you receive an email that's clearly an attempt to solicit sensitive information, don't just delete it and move on. Forward it to your company's IT representative. Mention it to a colleague. Ensure that everyone knows this scam is circulating at your company.

If you do fall victim to one of these hoaxes, don't try to cover it up. You might face disciplinary action for opening malicious emails, but you will face disciplinary action if your login credentials are used to expose sensitive information!

Off the clock? Lock it up! - The VA breach, one of the biggest data leaks that hit some of the most secure data in the nation, was caused when an employee improperly took confidential information home to continue working. The information was stolen, and the integrity of the VA's servers was compromised. Taking work home with you might be a good way to get ahead, but unless your home can provide the same level of security as your office, it's just not worth it.

If you must take work outside the office, keep it in a secure place. Ideally, you should place it in a safe or locking file box. Failing that, keep it in a locking briefcase or other lockable container. If you're working with paper copies, don't forget to destroy or return them once you're done.

If you have a standing arrangement with your employer to do some work remotely, there are still a number of steps you can take to keep your work technology safe. If you work on a laptop, invest in a cable lock. This piece of hardware works like a bicycle lock. You loop it around a heavy object and fit the lock into your computer's power port. Should a dedicated thief rip the lock out of the port, the computer will be rendered inoperable, turning a catastrophe into a hardware replacement.

Also, don't connect to unsecured wireless networks. Anyone can join these and set up monitoring software on them to steal data in transit. If you work on your home Wi-Fi, set up a security protocol. Don't forget to change the default administrator password on your router. Most manufacturers have a default router password which would enable scammers to access your network.

Keep it out of the office! - Most people spend at least some part of their work day browsing the Internet. Modern technology has made work more efficient, so most people don't begrudge five minutes on Facebook here or there. The problem is that recreational browsing can expose the office to risks.

Even the tamest hobbies can have risks. Searching for "download sewing templates" could take you to websites dotted with malicious software masquerading as

innocuous archives and executables. If your interests run to games or gambling, the internet can be a very dangerous place for your work computer.

Be wary when using private USB drives at work. If you're interested in gaming, you might be tempted to load up a USB drive with a few fun titles. It's very easy to accidentally save sensitive information to that USB, which becomes a liability. USB drives are the bane of IT security people everywhere, since they're easy to lose, steal or swap.

If you have downtime at the office, stick to browsing sites you know and trust. Check your personal email, read CNN headlines or find the latest scores at ESPN. If you feel the need to explore the darker side of the internet, be sure you do so at home where you can better control the sensitive information on your computer.

A GROWING THREAT TO SMALL BUSINESSES

If you are a small business owner, ID theft is something you need to be concerned about. As a business owner, you are responsible for safeguarding personally identifiable information (PII) in your possession. This means you have a strict responsibility not to divulge your employees' or customers' identification, medical histories, coverage details, birth dates, Social Security numbers or credit card numbers.

But your potential liability isn't limited to the unauthorized release of PII you actually own: If you have an employee whose purse gets stolen in the employee lounge – and someone steals her identity and uses it, you could potentially be held liable.

Lastly, your employees could be in on the con – using their access to your employee and client records to steal credit card numbers, account numbers and the like.

So as a business owner, how can you protect yourself and your honest employees?

1. Appoint a privacy officer in your company and invest in training.
2. Develop a company privacy and data security policy, and put it in the employee handbook. Have each employee sign an acknowledgement.
3. Conduct background checks on new hires.
4. Go into all your employees' copies of Outlook and turn off Autocomplete.
5. Consolidate all sensitive information onto a single server and password protect that server.
6. Password-protect all sensitive files. These are any files that include

personally identifiable personal, medical or financial information.

7. Change all the passwords. Then give the new password only to those employees with a need to know. Better yet, make sure they all have their own passwords whenever possible. That way, the user log can be audited if there ever is a breach in security.
8. Increase your company's liability and errors and omissions insurance coverage.
9. Invest in a good shredder and ensure your employees use it. Identity thieves commonly go through trash to find sensitive information.
10. Don't tolerate employees leaving valuables unsecured.
11. Create a culture that emphasizes the value of confidentiality.
12. Implement strict controls on the use of your company's credit and debit cards, as well as business checking accounts.
13. Use E-verify to verify employees' Social Security numbers. According to the Center for Immigration Studies, 98 percent of perpetrators who steal Social Security Numbers use their own names with stolen credit card numbers. Using E-verify can help you detect this problem.
14. Change passwords and physical security passcodes anytime someone leaves your employ, for any reason.

None of these steps are a guarantee against identity theft and other data security breaches. But by creating an atmosphere of vigilance, you can substantially reduce the chances that you, your clients and your employees will become victims.

BUSINESS IDENTITY THEFT

Protecting your business from identity theft is just as important as protecting your personal identity. You can decrease the potential of having business identity theft happen to your company through some basic precautions.

- Install a security system on external doors and windows.
- Securely store company records and customers' personal information in password-protected files or locked filing cabinets.
- Shred unwanted mail and unnecessary business records.
- Do not release business or customer information over the phone until you are able to confirm the caller's identity.

- Password protect programs and databases that hold sensitive information.
- Limit the amount of sensitive information posted on your website.
- Password protect or encrypt any sensitive information you do post on your website.
- Be sensitive when asking customers for personal information. For example, don't repeat private information loudly in crowded waiting rooms.
- Make sure computer screens and customer files are not in plain view for other customers or employees to see.
- As soon as an employee no longer works for you, remove that employee's access to your company data and computer network.

LOOKING FOR A JOB? SCAMMERS MAY BE LOOKING FOR YOU

Job searching is already a frustrating process. Between the stress of unemployment and the sting of rejections, job hunting for any length of time can make you desperate. Unfortunately, that's exactly what identity thieves are counting on.

Many con artists are relying on a sophisticated new scam by trolling for job seekers on job boards like Monster or Indeed. They reach out to job seekers by pretending to represent a major company that has a supposed interest in the job seeker's credentials or experience. They claim they need a few more pieces of information to conduct a background check before hiring. They'll ask for personal information, such as a Social Security number. Then, they'll take you for everything you've got.

Or, they set up fake job postings on sites like Craigslist or LinkedIn and wait for job seekers to contact them. This practice provides them with a steady stream of desperate and vulnerable applicants. It also saves them the trouble of tracking down email addresses, and makes the contact seem more legitimate.

These schemes work, like most other identity theft scams, by preying on people's hopes. You need this job offer to be true, so you are willing to rush into the "opportunity" without waiting, thinking or researching. It only takes one slip to wipe out your savings and ruin your credit, which can also undermine your future job search efforts.

You can't give up your job search, and you wouldn't want to refuse a reasonable request from a legitimate employer. So what can you do to keep yourself safe from identity thieves when looking for work? Follow these pieces of advice, which you can remember using the acronym KISS:

- **Know the hiring process.** For most businesses, the hiring process includes job posting, interview, background check, job offer. Background checks cost money to run. No business is going to start running background checks on every potential applicant, and most will only do so as a component of a job offer. Before they've hired you, that's all they'd do with a Social Security number. Also, the company would need your signature to run a background check or fill out immigration paperwork. A legitimate business won't ask for your Social Security number out of the blue.
- **Identify the poster.** If a job offer comes from a major company, odds are good that it's not just on the job boards. It's also on their web page. Copy the text of the job description and paste it into a search engine. You should get results from several job boards as well as the company's website. You can use tools like WHO IS to determine the ad's country of origin. This can help find hidden red flags. If the posting claims to be from a company that's located in the U.S., its domain registration should reflect that. If it's a company that's been in operation for years, its website registration shouldn't be from the last few weeks or months.
- **Sanitize your online presence.** Tools like Facebook and LinkedIn can help you in the job search process, but they can also help identity thieves. Remove unnecessary personal information like your hometown or your birthday from your social media profiles. This information can help identity thieves bluff their way past human security. As an added benefit, putting your date of birth on your resume may be a turnoff for employers. Age discrimination in employment is illegal, and employers can land in hot water if they ask you any questions that hint at trying to determine your age.
- **Stay vigilant.** Look for all the typical scam warning signs: unbelievable salaries, vague descriptions, misspellings, grammar errors and unprofessional email service providers. Someone offering you a job isn't that much different from someone offering you a large sum of money. You should be skeptical of everyone you don't know who contacts you wanting personal information. Take the time to do your due diligence in every instance. Don't let the pressures of the job search crumble your common sense. If it sounds too good to be true, it probably is.

FINANCIAL INSTRUMENTS

BEWARE OF FAKE CHECKS! PROTECT YOURSELF FROM THE LATEST SCAM

Personal checks look simple and innocent. Recently, though, the Federal Trade Commission (FTC) and other agencies have warned about increases in fake check scams.

There are several variations of the scam, and they all end with you losing thousands of dollars.

The scam may be done under the pretext of a work-at-home job, an online sale or a sweepstakes that you've miraculously "won." You'll be asked to deposit a check or money order that's worth thousands of dollars more than what you're owed and then to wire the difference to your contact.

Of course, these checks are phony. Unfortunately, because they can be extremely difficult to recognize, it can take several weeks for a financial institution to identify them as fake. By that time, you may have already paid the requested amount to the scammer, and when you realize the check was fraudulent, it's too late to reclaim your money. Worse yet, you'll be responsible to pay the fee for the bounced check on top of what you lost.

Keep yourself safe by following these tips:

1. **Wait for clearance** - It's hard to tell if an online job you just took is bogus until the first paycheck clears. Wait several weeks until you see the funds from a deposited check are completely available before making any transfers using that money. Never use funds from a deposited check from an unknown source until you are absolutely certain that it has cleared.
2. **Ask questions** - If an online sale or job sounds suspicious, don't be afraid to

be curious. Ask about the overpayment and the inflated checks. When you're told a long, rambling tale about avoiding complicated tax scenarios, overseas charges and company errors, ask more questions. Demand a new check and answers. If you don't receive what you ask for, opt out.

3. **Play hard to get** - Scammers find your information by buying lists of potential victims from other scammers, randomly calling thousands of numbers and by checking your online activity to see if you're a good target.

Beat their game by keeping yourself as anonymous as possible. Add your number to the FTC's Do Not Call List at donotcall.gov. Strengthen your spam filter and ignore emails that sound too incredible to be true. Be wary of answering calls from unknown numbers – just picking up the phone makes you a credible target.

Lastly, if you or someone you know has been victimized by a fake check scam, be sure to report the scam to your local law enforcement agency and to file a complaint with the FTC. This will help law enforcement agencies track down the criminals.

Remember: The best protection against scams is to be informed and to be aware. Stay in the know, and stay safe!

BEWARE THE FAKE TAX FORM SCAM

Tax season means a paperwork blizzard. Often, someone loses a copy of an important document and needs it to be re-issued. Naturally, everyone's too busy to verify the authenticity of each request.

That's what scammers are counting on with a recent ploy targeting people who prepare tax forms. In this scheme, the scammer sends an email claiming to be a hired company or someone from the IRS requiring duplicate copies of W-2s. An overworked clerk fears noncompliance with the tax authority and sends the forms.

Those forms contain personally identifiable information, including a name, address and a Social Security number. With that information, fraudsters can open fake credit cards, apply for loans, or file a fraudulent tax return in an attempt to grab a refund check.

IF YOU'RE TARGETED

If you prepare W-2s, be on guard for these fake emails. Here's the sample text from one such message:

> "ATTN: Due to some complains (sic) we had concerning the W-2 mismatch,

> We advice (sic) you to send your 2015 filled W-2 form in (PDF) format for confirmation."

Notice the abbreviations, the typographical errors and the poor punctuation. These should tell you this isn't the professional work of the IRS.

You may also get a similar message that appears to be from your boss. Watch for the same typos and always confirm these requests in another message. Also, look out for emails from former employees. Scammers may be relying on outdated information.

If someone really needs another copy, it's safest to mail it to them. Email is never fully secure. It's also unlikely that someone would need duplicate copies of ALL W-2s. Be suspicious of any such request.

IF YOUR INFORMATION HAS BEEN COMPROMISED

If your information has been unwittingly released by your employer, don't panic. Minimize the impact of this data breach with these three steps:

- First, call one of the major credit bureaus, Experian, Equifax or TransUnion, to request a fraud alert on your account. This will force anyone who wants to issue credit in your name to verify their identity.
- Next, order a copy of your credit report to see all the accounts open in your name. If there's anything you don't recognize, immediately close the account. Also, review statements for the accounts you have. If you see any charges you don't recognize, call the issuing institution and shut the account. Alerting them about fraud as soon as possible limits your liability.
- Third, file a complaint with the Federal Trade Commission (FTC) at identitytheft.gov. This will create a fraud affidavit, a document certifying that fraud occurred. This will help when you need to file a police report.

It's worth filing your taxes early. If a thief tries to file a tax return using your information after you've already done so, the IRS will be alerted to the fraud.

CHECK FRAUD

When we think of identity theft, we are most often concerned about credit cards, debit cards and Social Security numbers. Checks, however, are also susceptible to identity theft. Different types of check fraud can happen. Someone could forge your signature or endorsement.

Someone could create an altered or counterfeit check based on one of your checks.

A few simple things can be done to help put your mind at ease related to check fraud.

1. Store any bank and check information in a secure place. This includes checks, deposit slips, canceled checks and statements.
2. Never leave bank information in your vehicle.
3. Reconcile your bank statement when you receive it and be alert for any potential fraudulent activity.
4. Unless it is needed for tax purposes, shred any canceled checks, statements, deposit slips and ATM receipts.
5. Don't list your Social Security number, driver's license, or telephone numbers on your checks.
6. Use permanent blue ink to write your checks.
7. When writing your checks, don't leave any spaces that could be changed, such as the payee or amount.
8. Whenever possible, try to use a gel pen since it is the most difficult for criminals to "bleach."

If you think check fraud has happened to you, notify the credit union as quickly as possible.

SECRET SHOPPERS AND COUNTERFEIT CHECKS SCAM

"You are hired as a paid 'Mystery Shopper.' Here is your check based on the survey you entered online for us where you indicate your interest in becoming a Mystery Shopper," says the letter you just opened.

You look at the check. Sure enough. Your credit union's logo, name and address appear on it. It has to be real. After all, mystery shoppers and secret shoppers exist. Unfortunately, so do counterfeit checks and scams.

How can you tell this is a scam? First, and most obviously, a legitimate secret shopper program won't send you a check before you complete your assignment. Additionally, secret shopping is not a high-paying profession. Most of the time, it exists as a part-time opportunity, so be aware of any large amounts in such checks. And finally, did you really fill out an online survey? Even if you did. It doesn't mean the company is legitimate.

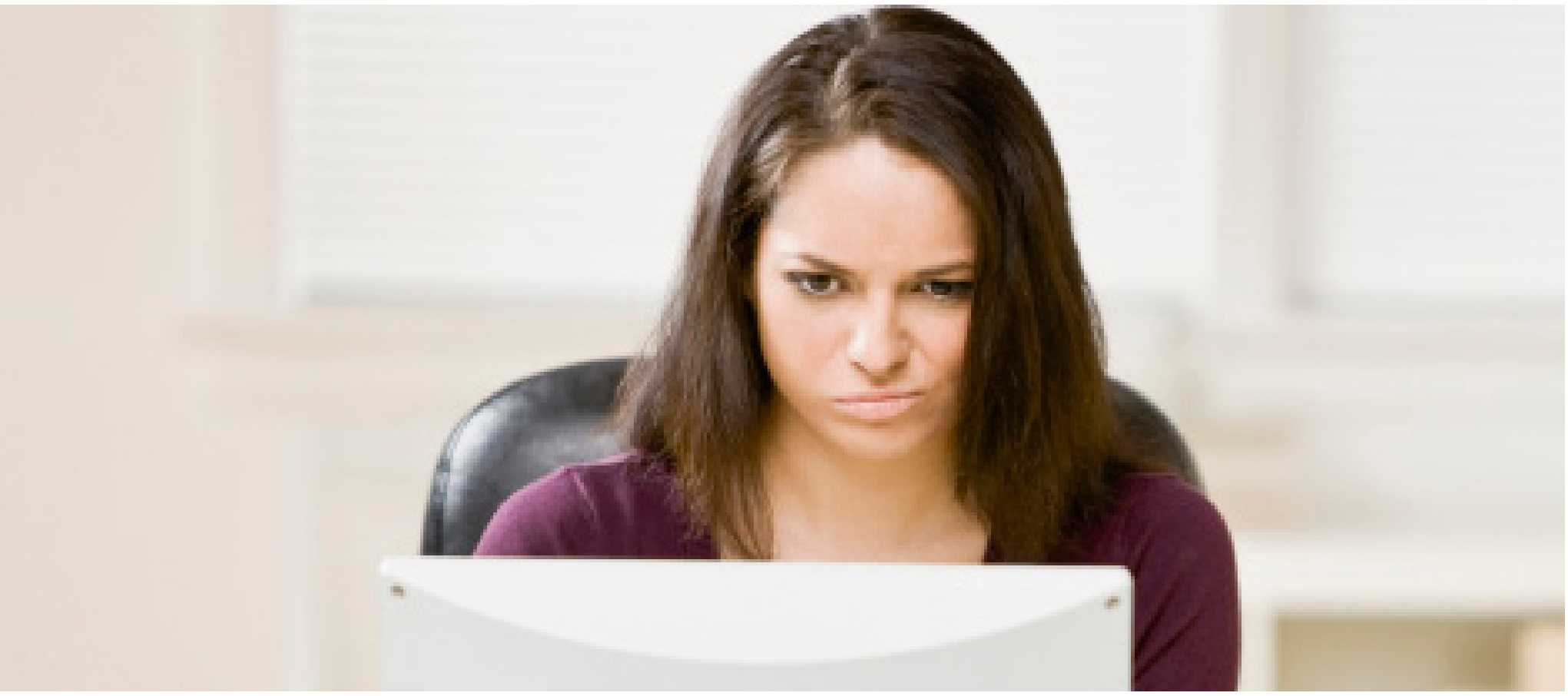
How can you tell the check is counterfeit, especially when it looks so real thanks to copying logos, using high-quality ink and paper and even replicating the watermark? The address information for the credit union is correct. The routing number is, too. The best option for you is to find the credit union's number and call it directly to verify that the check is accurate. But don't trust a phone number listed on the "cashier's check." It may also be (and probably is) fraudulent.

What happens if you cash or deposit the check? Anytime you cash or deposit a check, you are held accountable until the check clears the originating credit union. If no account exists, as in the case of counterfeit checks like these, you are responsible for any funds you withdraw or spend against the check. In other words, you have just lost your hard-earned money, which didn't come from the mystery shopping scam.

Legitimate secret shopper or mystery shopper programs do exist. To help make sure you are working with a legitimate one: avoid programs that contact you by email, require you to pay for "certification," guarantee you a job, charge you a fee, or ask you to wire money from a cashed check. Additionally, make sure you research mystery shopping and secret shopping opportunities and search for reviews and comments about the companies you find.

If you do find yourself on the receiving end of a counterfeit check that is claiming to be from a credit union, regardless of the scam, contact the credit union directly as well as the U.S. Postal Inspection Service and the Federal Trade Commission (FTC).

DOCUMENTATION



SOCIAL SECURITY CARDS FOR SALE

Think snagging your credit card statement from the trash or mail is a surefire way to protect yourself from identity theft? Well, it's a good start. However, as federal authorities in New Jersey have discovered, fraud is increasingly becoming more involved and complex.

The latest sophisticated plot, headed by Sang-Hyun "Jimmy" Park, involved a bank-fraud ring that exploited loopholes in the security around identification documents to create a series of bank, credit card and government fraud schemes. The 53 people involved in the schemes began by acquiring legitimate Social Security cards through a black market network. The cards were provided in the 1990s to Chinese nationals working in American territory.

Park's operation sold the Social Security cards to individuals for $5,000 to $7,000 each. Park also helped buyers obtain driver's licenses and raise the credit scores so they could carry out crimes that included opening bank accounts and credit cards and loans that could be cashed out and never repaid. Networks of merchants even helped out by ringing up fake credit card charges without selling actual merchandise. Profits were shared with Park and his team.

ARE YOU DEALING WITH A DIPLOMA MILL?

Education is expensive. It's so expensive that it's tempting to take shortcuts. Unfortunately, sometimes consumers turn to so-called "diploma mills." These are for-profit companies that do little more than separate people from their money in exchange for a high-priced piece of paper they call a diploma.

There is little or no actual coursework or learning that takes place. What little

there is often represents a fraction of the coursework that is normally expected of an associate's, baccalaureate or master's degree.

The problem: When you graduate, you will still have spent a bunch of money, but employers are wise to the diploma mill game. Your resume will go to the bottom of the pile.

HOW TO SPOT A DIPLOMA MILL

- **The school is not accredited by a legitimate accrediting institution.** Legitimate colleges and universities jealously guard their reputations – and their accrediting bodies do not grant accreditation to diploma mills because they do not live up to even minimal academic standards. Remember that diploma mills may even have created fake accreditation organizations to help them mask the scam.

  The U.S. Department of Education maintains a list of legitimate accrediting institutions at http://ope.ed.gov/accreditation. You can research any school's accreditation at that site.

- **The school grants academic credit for your life experience.** Most legitimate schools will grant a few credits here and there if you have significant professional experience in a given career field. They may also grant credit for military schooling. But they do not grant all or almost all of a degree based upon past life experiences.

- **There is no professorial contact.** Legitimate schools will put you in regular, direct contact with professorial staff. It's not enough just to send you a reading list.

- **Aggressive marketing.** Most for-profit institutions will do their best to get you to sign on the dotted line. Even legitimate for-profit schools have to keep the lights on. Diploma mills will be more aggressive than most. Don't give in to sales pressure. Take your time to fully research the institution.

- **Questionable Marketing Media.** Legitimate colleges generally don't advertise using deceptive or obnoxious techniques, such as e-mail spam or pop-up/under web ads. Diploma mills will also sometimes have obvious typographical errors or English usage errors. Legitimate schools proof their materials thoroughly.

- **Flat-Fee pricing.** Legit schools typically charge per credit hour or course. Diploma mills are likely to charge a flat fee for a given degree.

- **Sound-alike names.** Diploma mills have been known to use names that sound very similar to recognized and legitimate institutions. Check the name carefully. Visit the website. If the site seems thin, the education might be thin, too.

Check with your state attorney general's office. Most state AGs try to track known diploma mills that are operating within their states. If there is an enforcement record against a given institution, they may be able to warn you off or lead you to the appropriate records.

Diploma mills hurt everyone. They dilute the reputations of legitimate institutions and their graduates – while destroying the professional reputations of those who fork over their money and try to use their fake degrees to pad their resumes. If you feel you are victimized by a diploma mill, contact your state attorney general's office.

WHERE IS YOUR TAX RETURN REALLY BEING FILED?

You go into a large chain such as HR Block, Jackson Hewitt , or Liberty Tax Service to file your taxes and assume they'll be handling it on premises. Or you go into an accounting firm and figure that the person you're speaking to is the one who will actually do the work. Before making that type of assumption, ask. With Internet access, it takes nothing for the person you've delegated your tax return filing to, in turn, outsource the work to someone in India or China who will do it overnight for as little as $50.

You're not just supporting someone in a third-world country, you're also giving what *Smart Money* calls "a great gift" to an identity thief. Nothing contains as much information as your tax return — your Social Security number, income, date of birth, account numbers . . . yikes!

If that sounds like too much of a risk, ask your tax preparer a simple question: will you be preparing my return in-house or outsourcing it? If they'll be outsourcing the actual work, find out what steps will be taken to protect your personal information. Or, better yet, find another tax preparer who will keep your information in-house.

CHILD FRAUD: WARNING SIGNS

Child fraud happens when someone steals your child's identity. It can happen with Social Security numbers or birth dates. It can be done by someone you don't know. It can even be perpetrated by a relative or family friend who has credit problems of

their own.

Once your child's information is stolen, it could be used to open credit cards, take out loans or even claimed by others on taxes. In essence, someone else could completely take over your child's identity.

Some warning signs exist. Watch for these possible indications of child fraud:

- Is your child receiving pre-approved credit card offers in the mail?
- Is your child receiving bank, credit card or other financial statements in the mail? These mailings do not include any accounts you hold jointly with your child.
- Is your child receiving phone calls or letters from collection agencies?

If one of these warning signs or others has you concerned, it is important to contact one of the three major credit bureaus to look into whether child fraud is occurring.

CHILD FRAUD: REQUESTING A CREDIT REPORT

Each year, adults can request a free annual credit report from the three credit reporting agencies. It would seem that the same process could be used to request a free credit report for a child.

However, the credit reporting agencies do not knowingly maintain credit files on children. If you think someone is using your child's personal information, you will need to directly contact the agencies.

The agencies will ask for some basic information; such as the child's complete name, address and birth date. They will also request a copy of the child's birth certificate and Social Security card. As the parent, you will need to provide proof of your identity through a driver's license and a copy of a utility bill for address verification.

Once your information is received, the agencies will verify whether a credit file exists for your child. The agencies will then contact you in writing with the findings and any actions that have been taken.

In the case of suspected child fraud, it is a good thing to receive the letter that a credit file does not exist for your child.

FINANCIAL SELF-DEFENSE: DIVERSIFY!

Enron was the toast of Wall Street, back in 2000 and 2001. Even as the rest of the market was suffering from the collapse of the technology bubble, this innovative energy trading company continued to post profits, driving its stock price up to $90 per share. A Nobel Prize-winning economist, Paul Krugman, now a columnist for the New York Times, was extolling its praises.

The problem: It was all a sham. Enron turned out to be a cesspool of smoke-and-mirrors accounting. When the con was finally exposed, the stock collapsed from $90 per share to just pennies. The company went through the biggest bankruptcy in U.S. history at that time (which has since been eclipsed by Lehman Brothers), and thousands of workers – most of whom were innocent of wrongdoing – lost their jobs.

But they lost more than their paychecks: Many of them also had their retirement savings in Enron stock. When Enron collapsed, they lost not only their present income, but much of their future. Most of them will never recover from the hit.

- **Diversification.** The story of Enron is a vivid reminder of the importance of diversification. For the individual investor, diversification means spreading your savings, investments and sources of income out so no single financial setback will spell catastrophe for you and your family. You don't need to be running a pension fund to diversify. Even at the household level, there's a lot you can do.
- **Consider mutual funds.** Any single stock or bond can become worthless

nearly overnight. Enron proved it – and many more companies have gone bankrupt before and since. But when you buy a mutual fund, you are buying shares of dozens, hundreds, or even thousands of companies in some cases, through a single transaction. Any given company in that batch can go bankrupt tomorrow, and you would scarcely feel it in your portfolio. You still have market risk, though ... and even well-diversified stock mutual funds can experience wide swings.

- **Use multiple mutual funds.** You can help reduce that volatility by owning different kinds of mutual funds. For example, consider owning a diverse bond fund along with your stock funds. Hold an international fund as part of your portfolio. Hold some small company stocks along with your "blue-chip" large companies.

  You can diversify even more by including an REIT fund, which invests in real estate investment trusts, or a gold and precious metals fund. And keep something in cash, savings, money markets or CDs. Each of these fund categories tends to behave differently at different points of the economy. Some will be doing well at any given time, and some will struggle. But overall, it's unlikely that everything you own will collapse at the same time – and that's the real disaster you want to avoid.

- **Separate income from savings.** Be careful about tying your retirement money too closely to your paycheck. You can recover from losing one or the other if you have enough time. But it's very difficult to recover from both. Try to avoid investing too much of your savings into your employer stock, or even in your industry. If something happens and your industry takes it on the chin, you won't take a devastating hit to your savings and income at the same time.
- **Tax diversify.** There are taxable investments, tax-deferred vehicles such as annuities, IRAs and 401(k)s, and tax-free accounts such as Roth IRAs and cash value life insurance. Hold something in each category. That way, no matter what Congress does with the tax code in future years, you won't get clobbered with a rate increase.

AUTO DEALER FINANCE SCAMS

So, you're buying a car. You've made it past the tedious comparison shopping, you've finished the detail-oriented research and you've even endured the haggling with the salesperson. Your tongue probably tastes like that terrible coffee they use in every car dealership in America, the kids are probably getting cranky and it's pretty likely you're thinking about everything else you could have done with your weekend. But, it's almost over.

"I just gotta go in to see the finance manager, sign some papers and we're on our way home." That feeling of relief washes over you, you let your guard down and you don't even realize until too late that you're suddenly in a much higher monthly loan payment or longer term than you'd planned for. What, in the name of Lee Iacocca, just happened?

The stereotype of car dealerships usually involves a salesman with a pencil mustache and a polyester jacket who lies through his nicotine-yellowed teeth about undercoating or telling you how the used car you were looking at has only ever been driven to church on Sundays. That guy is easy to spot. If the salesperson lies to you, you have some legal protections. If you Google before you go, you'll even know most of the tricks the salesperson might roll out. What you're less protected against are the tricks that happen in the finance office. Below, we'll talk about what to look for and how to avoid dealer finance scams so you don't spend too much on your next car.

1. **Keep your wits about you.** Never let your guard down at the dealership. Every person there wants to make money off of you, and they're very competitive. Even if he or she says that they don't want or receive commission on your particular sale ("I just need to hit my quota," or "One more sale puts me at my bonus; I'll

take a loss on this one."), that person is almost certainly a very competitive person who's going to be comparing notes with his or her co-workers this afternoon.

The finance office is designed to put you at ease, so you'll lower your guard. The finance office is probably in a different part of the building, with different lighting and ambience. The offices may be appreciably nicer, with actual walls instead of cubicles, some of which may have art hanging on them. Clearly, the person you're talking to is important, having been in such a nice office for so long.

And that's what should scare you. The people in the finance office are often not financial experts by trade; after all, they don't need to do your taxes or invest your money. They only have to understand one transaction. Therefore, many dealerships will send their best salespeople to finance classes so they can have a smooth closer at the end of each transaction. Don't let the gray hair fool you; the person in front of you is just as competitive and sharp as the one on the sales floor. After all, to get this office, the finance officer had to be really fantastic at making sales.

2. **Know your credit score.** There are a lot of reasons to know your credit score before you make a large purchase, including the fact that you should check your credit report for irregularities fairly often, whether or not you're buying anything. When you buy a car, it's especially important. Finance managers like to use customer ignorance against them, and if you don't know your up-to-date credit history, then they'll smell blood in the water.

   While the most obvious example is to try to charge you more than you need to pay, you might not expect that another classic is to offer you a loan at a far lower rate than you deserve. The idea is to offer you a rate so low you can't say no, then wait a few weeks before telling you that the financing unexpectedly fell through. Don't worry, he or she will tell you, you can keep the car. There's a clause in your contract that says "subject to financing," so he or she found a different lender. The good news turns sour, however, because your new rate is through the roof, and you've already signed the contract and taken delivery of the vehicle.

3. **Don't take a loan at a rate that's too good to be true.** If you're tempted by an offer in the finance office, ask how long it'll be valid. Then, take it home and show it to your lawyer, so someone you trust can tell you if it's on the up-and-up. If you don't want to pay your attorney's rate, you can also bring it to us. We'll take a look, let you know about any potential pitfalls and we might

even be able to beat that rate or provide a better term, saving you even more money. Remember, if they say that the deal expires today (particularly on the weekend) or that you can't take your contract with you, it's almost certainly because they don't want you to take the time to think about what you're doing.

It's never a good idea to trust someone who doesn't want you to think.

4. **Walk in with an offer.** Then, walk out with an offer. The best way to get a fantastic rate on a loan for a new or used car is to finance through the credit union. We aren't looking to make a profit, we're looking to support our members. We're also trustworthy – it's why you're here in the first place, after all – so you know our great rates aren't scams. So come see us first, and you can walk into the dealership with your loan financing already approved. You'll know how much you can spend, taking the pain out of negotiating. You'll also know what interest rate you'll get and have a pretty good assurance that your monthly payment will be manageable. Plus, you'll only need to run your credit score once, so you don't have to worry about losing points from looking it up too often.

Don't let the salesperson know that you've already gotten financing, though. The dealership knows how much it wants to make on the transaction, and it doesn't care if that money comes out of the trade-in, the sale or the financing. If you know how much your trade-in is worth and you have your financing taken care of, then the only place they can make money is on the sales price. If they know that, they'll be less flexible on the sales price. Let them think that if they give in a little on the sales price, they'll be able to make it up in financing.

But you also need to be able to walk away. Just like any other part of the sale, whomever can walk away controls the deal. If the terms of the loan the dealer offers you sound great, thank them and take them with you and let's compare notes. We're here for you and we promise to burn the midnight oil figuring out what we can do to make the best deal you can get.

This might all seem a little excessive. Maybe you're good at negotiating, you've looked up all the dealer scams and dirty tricks and you can get the loan really close to what you want. You're only off by $50 or so, and if you just sign the papers you can take the car home tonight and be done with the whole process.

Remember, $50 may not sound like much, but over a 60-month loan, that's $3,000 plus interest. Who would you rather see pocket that $3,000: the dealership or your family? To put it another way: if your child racked up $50 in extra data charges on your phone bill, how would you feel? What if he or she did it every month for five years? Let's beat the finance office together.

HIGH-YIELD INVESTMENT FRAUD

Whenever the stock market takes a hit, unscrupulous individuals will try to find a way to use the misfortune of worried investors to make a quick profit. Like all of the classic scams, this one is based on the oldest premise there is: Make a lot of money, really fast, with no work.

High-yield investment fraud is most commonly found on the internet, where it's much easier to put together a website that appears trustworthy and professional than it is to create the same appearance in person. Such sites claim to provide amazing returns, sometimes as much as 40% or 50% per month, and are supported by dubious charts and testimonials from people who may not actually exist. Between a quality website, impressive charts and some meaningless investment buzzwords describing a "magic pill" of an investing philosophy, unwary consumers can be easily fooled into forking over a chunk of their savings to an investment broker who is not licensed by the SEC and makes claims the SEC would call illegal.

The clearest warning signs of these scams are easy to remember, just like avoiding them should be simple to do: Don't trust anyone who offers too-good-to-be-true returns, dismiss cutting-edge investment opportunities if they come from anyone but an investment professional with whom you've worked before, and ignore any evidence of success that can't be verified by an outside party.

Big returns are appealing. You want to retire someday, send your kids to college or start a business to get away from the morning commute, and the more money your investments make, the quicker you can do so. But it's important to trust the process. Return on investment is tied to the risk involved in spending money on that investment. The stock market offers better returns than treasury notes because it's far riskier to bet on United Airlines than on the United States. High-yield investment scams are successful because we want to believe that someone can beat the market so well and that we can have returns that are better than the stock market with risks that are lower than treasury bonds. It just doesn't happen that way.

At your credit union, we believe we've created a nice sweet spot with our savings products. No matter what your preferences are, we can fit into your investment portfolio. In times that the market does well, the money you have with us will keep you moving towards retirement, but when the market slows down, you don't have to worry about losing your financial security – because the money your entrust us with is safe.

To put it another way, the U.S. economy has traditionally done three things very well: lower prices, create jobs and price risk. The last recession was caused by doing

a poor job of pricing risk, and that hurt our ability to do the other two. But that's exactly the point. As an economy, we are so good at pricing risk that when we screw it up, it's an enormous, world-altering event. If you find someone who can price risk so much differently than every other investment professional in the world, you need to also be ready to bet that the economy is going to take a radical shift in an entirely new direction – because that's what happens when we do a bad job pricing risk.

Finally, if you want to avoid all kinds of investment scams – and the SEC, FTC and USA.gov all have many pages listing the variety and creativity of these scams – the best thing to do is remember why you bank with us. We're part of your community, not a giant multinational corporation. We share our revenue with our members, not shareholders who may not even be connected to our local community. Our kids go to school with your kids, and you can always come in to talk to us for helpful advice.

PREVENT BROKER FRAUD OR INCOMPETENCE

Even the very best brokers pick a loser every now and then. However, you may have been the victim of broker misconduct or malfeasance if one or more of the following occurs:

- Your broker failed to disclose an investment's risk to you, or even actively concealed it.
- Your broker failed to provide you with a prospectus.
- Your broker was "churning," or trading in your account primarily to generate commissions for himself.
- Your broker failed to execute a trade in a timely manner and you suffered a loss as a result.
- Your broker forged your signature for any reason.
- Your broker concentrated your investments in a few high-commission products rather than diversifying your investments appropriately and you lost money as a result.
- Your broker made trades without your knowledge or authority.
- Your broker stole money from your account.
- Your brokerage had their broker recommend you buy securities that they were rapidly selling out the back door.
- Your broker sold you B or C class shares with high trailing or deferred commissions when you clearly would have been better off with Class A shares,

or vice versa.

- Your broker sold you securities that were clearly unsuitable for you, given your risk tolerance, time horizon and objectives.

How can you prevent becoming a victim of broker fraud or incompetence? Research your broker. Every registered representative (a fancy term for stock broker registered as a securities salesperson with the Securities and Exchange Commission) must maintain a current Form U-4 with FINRA, or the Financial Industry Regulatory Authority (formerly the National Association of Securities Dealers, or NASD).

You can research your broker's license status as well as his or her disciplinary and complaint record by looking up their Form U-4 via FINRA's "Broker Check" feature. Ask for a prospectus for each investment you are considering. Look carefully at the sections discussing potential risks to the security.

Don't invest money in risky securities that you can't afford to lose. If you can't afford to lose a significant portion of your investment at any time, you may be better off in risk-free or nearly risk-free assets, such as CDs and cash.

Keep a close eye on your statements. You should recognize every transaction, unless you signed over full discretionary authority to your broker to trade on your behalf.

Understand the different share classes and how commissions work for each share class.

Keep careful records of your interaction with your broker. Keep a copy of everything you do.

Ensure your broker's firm is covered by SIPC. This is a kind of federal insurance that replaces your securities in case your brokerage fails or goes bankrupt. It doesn't typically make good on your losses – instead, it just replaces any securities your broker or brokerage may have lost or stolen, or help you regroup if your brokerage goes bankrupt.

WHAT TO DO IF YOU ARE A VICTIM OF BROKER FRAUD

The first step is to speak to your broker to see if you can identify the cause or to work it out yourselves. If you cannot get satisfaction with your broker, you may go to your branch manager. Failing that, you may want to file a complaint with FINRA, which you can do via their website, finra.org.

Most brokerage houses limit your authority to pursue a lawsuit in the court system. You may have signed an agreement to pursue any cases or accusations through a mediation process instead, which may be less favorable to you.

DEBT AND TAX SETTLEMENTS

Americans are afraid of the IRS, and because of that, debt and tax settlement scams have become more widespread and more professional-looking than ever. If you get an email or see an advertisement offering to get rid of your tax debt for "pennies on the dollar" and deal with the IRS, too, read the fine print. While it sounds like the answer to your prayers, and the company claims to know a secret or a little-known facet of the law that will wipe out that tax debt, there's probably something else going on.

The company charges a fee upfront to pay for expenses. Not only that, but it asks for information that you should NEVER share with a company you don't know and trust. The company will then go away for a little while to "discuss the matter with your tax authorities." After a short period, it may come back for other minor expenses related to your case.

At this point, it'll start to look suspicious because the IRS is still demanding payment. However, the company will no longer answer your calls and you'll be left with your existing IRS debt plus interest on top of new debt and maybe even identity theft. What seemed like the perfect, easy answer brought on a whole new set of problems.

In fact, the only way to get out of a debt to the IRS is called "an offer in compromise." It's a lengthy procedure that very rarely gets you anywhere. The IRS DOES NOT let you out of paying your debts, except in extremely rare cases. If you see an ad or get an email that looks legitimate and you really want to respond to it, check with a trusted tax advisor first.

STUDENT LOAN SETTLEMENT

More than 42 million Americans have student loan debt, with their collective debt topping $1.4 trillion. Unfortunately, these big numbers make student loan debtors excellent targets for scams.

The FTC, partnering with 11 states and the District of Columbia, has recently announced "Operation Game of Loans," the first law enforcement initiative pursuing student loan debt relief scams. This nationwide crackdown includes 36 government actions against scammers alleged to have conned more than $95 million from victims.

Already, the FTC has charged more than 30 organizations, faulting them with falsely claiming to be affiliated with the Department of Education, misleading advertising and collecting upfront fees with deceptive intent.

In a typical scam, the "organization" will promise to use the victim's money for paying down their debt, reducing their monthly payments, or forgiving their loans entirely. The scammer does none of the above and instead uses the victim's money for their own personal use.

Several of these organizations have also victimized desperate homeowners, promising to provide mortgage relief and to prevent foreclosure. Of course, the victims' payments went towards lining the scammers' pockets, making no dent in the victims' mortgages.

Here's how to protect yourself from these scams:

1. **Visit the FTC site.** The FTC has recently updated its consumer education on student loan debt relief scams. You can read up on the FTC's warnings at ftc.gov/StudentLoans. The FTC will also be hosting a live online panel in late October. The panel will include a Twitter chat with state attorneys general and a Facebook Live session with attorney experts detailing ways to avoid these scams. Check the FTC website for information about this scheduled panel.
2. **Know that there's no fast way out.** When seeking help with a loan, remember that there is never a quick way out. Only scammers will promise fast loan forgiveness.
3. **No upfront fees or shared information.** You should never have to pay for a service before it's been rendered. If you're asked to pay an upfront fee for debt assistance, that's a sign you're being scammed.

On a similar note, never share your FSA ID (the username and password used to log in to U.S. Department of Education websites) with anyone.

4. **Verify affiliation.** To appear legitimate, scammers often claim to be affiliated with a governmental body or with a private loan company. These claims are hard to prove; it's best to contact these agencies yourself.

   You can apply for loan deferments, forbearance, repayment and forgiveness or discharge programs directly through the U.S. Department of Education or their loan servicer. These applications and services are cost-free and you will never need the assistance of a third-party company. To review your options, visit StudentAid.gov/repay.

   For private student loans, contact your loan servicer directly.

3 MORTGAGE SCAMS AND HOW TO BEAT THEM

The phrase "home security" is pretty widely used and has a variety of contexts. It can mean locking doors and windows when leaving the house, setting up an alarm system, participating in a neighborhood watch or setting up automatic lights for vacations.

These are all steps homeowners take to keep the contents of their homes safe.

When it comes to the home itself, though, folks can be a lot less particular. While homeowners insurance can protect against natural disasters, there's a new threat to the cornerstone of the American dream. Scam artists are targeting desperate homeowners, trying to steal their money, personal information or even their homes.

These scams come in a variety of shapes and sizes, and each one needs a detailed response. Before you do anything with your mortgage, check to make sure your "once-in-a-lifetime" offer isn't on this list.

1. **Upfront cost refinance.** *The scam:* You get a phone call or a letter from someone who wants to refinance your mortgage. The rates they're offering are crazy low. They can cut your monthly payment by hundreds of dollars or help you pay off your mortgage in record time. All you have to do is pay a small percentage of those savings upfront.

   Of course, the company offering the mortgage is fake. You might get bills from them for the new amount, but paying them won't affect your mortgage. Meanwhile, the institution that does hold your mortgage still expects you to make your regular payments.

   How to beat it: It's illegal to charge upfront fees for mortgage refinancing.

Some institutions may try to waffle around this by calling them "document processing" fees or using some other jargon. Whatever they call it, it's against the law and is a sure sign this "lender" is really just looking for a quick payday while not delivering anything in return.

Also remember that, while rates can fluctuate over time and from institution to institution, the fluctuation is limited. If someone is offering a rate that is several percent lower than anyone else in town, be highly skeptical. Check with your Better Business Bureau to see if the company exists or if complaints have been filed against it.

2. **Hope foreclosure relief.** *The scam:* This savage scam targets homeowners who are facing foreclosure. Whether because of job loss, medical expenses or other hardships, foreclosures affect 100,000 households each month. People in desperate situations try anything they can to dig themselves out. That's when they get a phone call from someone representing Hope Services, who can connect them with government assistance to stop their foreclosure. All they have to do is make three "trial payments" into a mortgage escrow account.

   Hope Services collects the money and encourages borrowers to stop paying their mortgage. They'll actively encourage homeowners not to talk to lenders or lawyers. They'll take care of everything. As it turns out, Hope Services provides neither hope nor services. Homeowners are stuck facing foreclosure hearings without any assistance whatsoever.

   How to beat it: Anyone who tells you not to get a lawyer or talk to a lender does not have your best interests at heart. If you miss several mortgage payments due to extenuating life circumstances, call your lender. Most institutions would always rather you pay something and keep you in your home than have to go through the process of foreclosure. Keeping lines of communication open is critical to getting back on the right track.

   Also, watch out for high-pressure sales tactics. Anyone who wants you to make a mortgage decision on the spot is trying to deceive you. Mortgages are long-term arrangements and they should be considered carefully. A "money-back guarantee" is also a big red flag. Getting your money back will do you little good if you lose your house in the process.

3. **The fine print deed sign.** *The scam:* Scammers use a variety of upfront pitches. Some might offer to lower your rates or lower your mortgage payments. Others might try to rescue you from foreclosure. Still others might offer a home equity line of credit with alarmingly good terms. They may also offer to take over the deed to your house and then use their superior credit rating to secure a

lower rate, while allowing you to remain in the home as a renter. Whatever the pitch, there are a ton of forms to sign. All of them are written in indecipherable legalese.

Somewhere amid these forms, perhaps buried in the back, is a form signing the deed for your house over to the scammer. Once they have the deed, they can rent the home to someone else or sell it outright, while forcing you to vacate. Worst of all, you're still on the hook for the balance of the mortgage, since the loan is tied to you and not to the home.

How to beat it: Scrutinize every document you sign relating to your mortgage or home. Have someone with experience in these matters look over documents if you're not confident in your ability to detect these scams. Spending 20 minutes with a real estate lawyer is expensive, but not as expensive as losing your home.

There is never a legitimate reason to sign the deed of your house over to someone else unless you're selling the house. While rent-to-buy schemes aren't illegal, they very seldom end well for the renter. It won't even get you out of legal or financial trouble.

Also, be wary of anyone who claims to guarantee a halt of foreclosure. No one can make such a guarantee, and legitimate businesses would lose everything in lawsuits. The same is true with money-back promises. That's good protection when buying a blender. It's not something anyone can promise for your house.

WHEN IT'S TOO GOOD TO BE TRUE

THE TROUBLESOME TICKET: HOW TO SPOT AND AVOID A FAKE

After months of dreaming, wishing and praying, after a five-hour car ride without air conditioning, and after waiting in line for what feels like a lifetime, you've finally gotten into the concert experience of a lifetime. Beaming, you step forward and hand your ticket to the security guard at the entrance. You begin to stride forward, but he stops you dead in your tracks. He can't let you into the concert because your ticket won't scan. I'm afraid to be the one to tell you this, but you've been sold a fake ticket.

In a world where almost everything can be accessed online, live performances are a valuable experience. Unfortunately, scam artists across the globe have realized this and are turning that value against people. Users on sites like Craigslist and eBay have been selling fraudulent tickets for performances and sporting events for years. Concert or sporting event tickets can cost hundreds of dollars at face value these days, and much more than that as the date of the event approaches. Scam artists have tapped into that market big-time. All they need to do is ask you to pay online or mail your payment to a private P.O. box, and they're almost untraceable.

So, without question, by purchasing tickets online, you're putting your wallet at tremendous risk. Shelling out hundreds of dollars for a piece of paper anyone can forge is a gamble any way you look at it, but using faulty tickets can pose other dangers as well. For example, if you pay with a personal check, an experienced con artist might attempt to use the information on it to steal your identity. Even if nothing else goes wrong with the sale, if you show up to the event with a faulty ticket, you could be arrested for trying to pass it off as real.

Given the spread of online ticket exchanges, it may seem that there's no alternative to buying tickets online. The era of the box office windows may be drawing to a close, but that doesn't mean the safety it provided has gone away. So, what can you do to protect yourself? Try these six handy tips.

1. **Do your research.** For starters, find out as much background information as you can. See if you can find out exactly what a real ticket looks like, so you can spot differences in a forged one. For sporting events, most national sanctioning organizations include holograms and other hard-to-fake pictures on their tickets. When in doubt, contact the venue.

2. **Spot the spec.** "Spec" tickets are being sold speculatively. These are not tickets that the seller has in his or her possession. They are tickets the seller expects to have after they come up for sale. If you see tickets for events that haven't been released by the box office yet, this is likely how they're being sold. Steer clear, as a "spec" seller is just as likely to take your money and run as they are to give you a ticket.

3. **Make sellers do their homework.** There are ways you can strike preemptively against fake ticket scammers. Ask for a copy of the seller's invoice, proving that the tickets have been paid for in full. This is no different than asking for a receipt to prove the goods you're buying aren't stolen. For season ticket holders selling one event, you can also ask them for the ticket account number, which will always be printed at the top of the ticket.

   Also, ask the seller why they're selling. Imagine yourself as a teacher and the seller as a child who's asking for a homework excuse. Be skeptical of reasons why the seller is missing the event. No one schedules a funeral a month in advance.

4. **Deal with reputable websites.** Craigslist should be the last resort for buying tickets to events. Check reputable websites like Seatgeek, StubHub and Ticket Exchange before you dive into Craigslist. Better yet, ask your friends if they know anyone with tickets. It's always easier to deal with friends or co-workers than with anonymous strangers.

5. **Trust your instincts.** Always be wary of people who are selling tickets at face value or less. Unless prohibited by state law, many people who resell tickets will do so at many times face value. Someone with a last-second conflict will still likely attempt to get at least face value for tickets to a popular event. Think like a scalper. If you saw a ticket for sale below face value, wouldn't you snap it up, knowing you could multiply your money at the event? If a deal feels too good to be true, you know what to do.

6. **Manage the meet.** See if you can meet your contact in person. Aim to meet in a well-lit, public place. Many grocery stores and other large retailers offer their parking lots as safe spaces for all sorts of transactions and they would be excellent candidates for this one.

   As far as payment goes, a cashier's check is the safest way to pay a stranger, since it contains little personally identifiable information and doesn't require the same level of trust as a personal check. With the rise of mobile payment apps like PayPal and Square, it might be wisest to pay through one of these in order to create a digital paper trail should something go wrong with the ticket. Always inspect the ticket carefully for signs of fraud before handing over any money. If the seller doesn't agree, walk away.

No matter how high-definition the video gets or how free of ads it is, it'll never compare to the thrill of being at a live performance. That being said, even a live performance is never worth giving up your account information and funds for the possibility of being arrested at the gates. Go enjoy your concert, but never stop being wary of scam artists in the digital age.

Bonus Tip: Once you have your tickets in hand, you may want to share your exciting news on social media sites like Facebook or Twitter. That's cool. You're excited, and you should be. But also be careful not to post a picture of your ticket(s) containing all the relevant information that is unique to your purchase (such as seats and ticket serial numbers). Sophisticated scammers can replicate your ticket using that data and leave you facing a lot of questions when you try to attend the event.

THE PUPPY SCAM

"Puppy. Purebred. Free to a good home," the online ad reads. The photo of the dog looks at you with those adorable eyes.

Before you send an email for more information, beware. That ad may be part of a puppy scam working off your love of dogs in hopes of taking your money.

One type of puppy scam involves a "bait-and-switch" tactic where a cute puppy picture is posted with the ad. When payment is sent and the puppy is delivered, however, it has health problems that were not previously mentioned. Sometimes the dog is a completely different dog from the one in the picture.

The "Free to Good Home" puppy scam involves the buyer covering shipping costs, up to $500, for the dog through wire transfers or money orders. The deal is for the dog to be picked up at the airport after the money is received; however, the dog

never arrives as promised.

"Adoption fees" of more than $1,000 are also used in puppy scams. A legitimate rescue or breeder will charge fees based on age, breed, and vet care, yet no official paperwork and dated vet receipts will document these expenses.

How can you avoid these scams and still get a puppy? When you find an ad, make sure you get a local phone number and address you can verify. Watch for form-letter replies that leave off your name or other specific information. Never wire money or send money order payments to someone you don't know.

If you are interested in adopting a dog, research the SPCA, breeders or rescues in your area. Make sure you and your family meet the dog prior to finalizing the deal. Don't have the puppy shipped to you, but instead pick up the puppy directly.

Ask for references of others who have bought from this seller, breeder or rescue group. Additionally, ask for the name of the veterinarian with whom the seller works. Ask any other questions you may have about the dog. Also, a legitimate seller, rescue or breeder will take back a dog if things don't work out, so be aware when "no refunds" are discussed.

If you have been part of a puppy scam, contact the Better Business Bureau, the Internet Crime Complaint Center, which is a partnership between the FBI and National White Collar Crime Center, as well as the ASPCA.

BEWARE OF PUBLISHING SCAMS!

Are you an aspiring writer or published author? If so, you may be the perfect target for a publishing scam.

The scammers will reach out to you via email. Their pitch might look like this:

Happy House Publishing is looking for captivating stories. If you've got a great story, send it to us for consideration. All authors whose entries are printed in our collection of stories will receive $1,000 compensation. Upon submission, all works become copyright of HHP.

It can also look like this:

Are you trying to get your first book published? Professional Publishers is here to make your dream come true. For just a small fee, we'll review your book, print it and sell it on Amazon. Submit your manuscript for the chance to become the next successful author!

In the first example, the scammers are soliciting quality stories they'll publish. They'll

also enjoy all profits – you won't see a penny in royalties. Even worse, you can never reclaim your submission since the "publisher" retains all rights to submitted works.

In the second case, your book may be printed, but it will likely not be edited professionally. You'll be tricked into signing a very unfavorable contract and into paying exorbitant, unnecessary fees.

Don't get conned! Here are six signs of a publishing scam:

1. **Publisher claims exclusive rights** - Read all the fine print clearly on any contract so you're not locked into an awful deal that robs you of your rights to your own work.
2. **Reading fees** - Never pay to have your book read. If you're being charged a "reading fee," take your manuscript and run!
3. **They claim your book is perfect** - Every manuscript needs some editing. If you're told that your book is perfect as is, look for another publisher.
4. **They're faceless** - Your publisher should have an address, a phone number, names of real people who are part of the company and an updated website. If these are non-existent, and/or they refuse to allow you to meet an editor or graphic artist in person, be very suspicious.
5. **Publishing fees** - If you're asked to pay to have your book published, do careful research on your publisher. If they claim to be a traditional publishing company, you should receive an advance payment against royalties and should not be paying publishing fees. Your publisher is an investor who is buying and selling your intellectual property. Alternately, if your publisher claims to be a "self-publisher," you'll need to pay for publishing costs, but you'll own 100% of the product and profit.
6. **Amazon fee** - Scammers love preying on the technologically challenged. That's why they charge authors for listing books on Amazon – they're hoping some people don't realize that listing on Amazon is simple and cost-free.

TROUBLE WITH TECH SUPPORT SCAMS

Advanced computer technology can look like magic. Consequently, the wizardry that those with technical savvy can perform can be baffling. You might be thrilled to have found someone willing to help you out so quickly, but at the same time, you're likely confused as to how they'll go about doing it.

That confusion is exactly what some scammers rely on. The Federal Trade Commission is warning consumers about scams featuring phony tech support.

These schemes have one goal: compromise your technology to steal personal information and money.

It's important to be vigilant when browsing, and watch out for these three tech support scams.

1. **Yahoo phone support** - Data breaches have two sets of victims: those immediately affected and those victimized in the ensuing confusion. Yahoo's data breach has found a new group of the latter.

   Scammers have created several phony replicas of Yahoo help sites. These sites detail common account problems and offer a phone number for "Yahoo Customer Care" or something similar. If you call, one of several things might happen. You might be asked to pay a support fee, to allow remote connections to your computer or for your account information, including your username and password.

   Whatever the scammer's request, their "assistance" is bogus and the damage they can do is real. Yahoo affirms it will never charge for tech support, nor will its employees ask for your password or to remotely connect to your computer. While pay-for-support lines do exist, they're very rare. Never allow anyone you don't trust remote access to your computer.

2. **Spyware scanners** - In this scam, a banner ad claims to have discovered infected files on your computer. A list of suspicious-sounding file names flash past, including some that are actually on your computer. The ad will insist that you need security software and will provide a download link.

   The downloaded software can do one of several things. It could log your keystrokes so a hacker can steal your passwords; it might allow remote access to your computer and, by extension, to your personal information; or it may be "ransomware," which encrypts your computer's information until you pay a hefty fee.

   Be proactive! Don't download files from websites you don't trust. Use reliable antivirus software and a malware scanner so that you can ignore pop-ups that claim your computer is infected.

3. **Inbound tech support** - These scams usually start with a call from an unknown number. If you answer, the caller tells you he's detected a problem with your computer. You'll be instructed to provide him with remote access so he can fix it.

   Once the scammer has control of your computer, he'll do any of the things described above. It's difficult to reverse this process, and you may end up losing

your computer!

No tech support company will call about a supposed monitoring of your computer. If you get an unsolicited call from an unknown number about your computer, hang up and report the number at donotcall.gov.

Technology operates by a predictable set of rules. Learning a bit about how it works can keep you safe online.

INHERITANCE SCAMS

You've just inherited millions! Or have you? Inheritance fraud isn't new, but scammers have recently upped their game to be more convincing.

In this scam, you'll receive an email from a foreign "lawyer" or "bank official," claiming your long-distant relative has just died intestate, making you the sole heir. You'll be warned that immediate action and the payment of various fees is necessary to keep the government from seizing the money.

The email will include identifying documents from the lawyer or bank official, as well as an overseas address for the bank in which the money is supposedly being held. Recently, scammers have begun using a local address for this step.

Unfortunately, there is no inheritance involved; just a crooked scam. If you answer the email, they'll start charging you various fees which will gradually increase in size. Next, they'll ask for your checking account information so they can transfer the millions of dollars supposedly coming to you.

Sharing this information will open you to more loss or identity theft. Once the scammers have this information, you'll never hear from them again. Be on the lookout for these warning signs to help protect yourself from becoming the next victim of inheritance fraud:

1. **The initial email** - The email itself is a red flag. You'll never be contacted by email regarding a matter of this magnitude. Secondly, the email's wording will be riddled with typos. Third, if the contact's email address uses a public domain, such as @gmail.com, be cautious. Banks and reputable law firms use their own domains.
2. **Personal documents** - Is the "lawyer" sharing his own personal documents? This is a huge red alert. Nobody, especially a bank official or lawyer, would ever share personal documents with a stranger. Certainly it would not be shared online or by email. Never give account details or copies of personal documents to a stranger, especially over the internet.
3. **Bogus bank** - Check the legitimacy of the bank address provided by doing a

quick Google search. It will usually be a bogus address, or at least not an address at which a reputable financial institution exists.

4. **Overseas wire transfer** - Never agree to make an overseas payment to a stranger via money order, wire transfer, prepaid debit card or electronic currency. Once these transactions have been made, it's nearly impossible to recover the funds.

Have you been scammed? Remember to contact [credit union] and your credit card companies immediately to minimize damage. Also, be aware that you are now a likely target of other fraud, as fraudsters commonly share details about their victims.

HOME IMPROVEMENT SCAMS

Home improvement scams visit the neighborhood every summer. As many as 100,000 scammers work in the United States each year, according to recent estimates reported in Consumer Digest, and with Americans spending more than $500 billion a year on remodeling and home improvement projects, they're not going to stop anytime soon. Those scammers are very good at identifying their victims, so we need to get better at spotting them.

Here are some signs you might be working with the wrong person:

1. **He "just happens" to be in the area...** Contractors don't go door-to-door drumming up business, but one of the most common ways scammers make contact with their victims is by simply knocking on their door, explaining that they were in the neighborhood and offering to take care of a job they noticed a need for. They might claim to have leftover materials or they noticed some missing shingles on your roof when working on your neighbor's house, and now they have a great deal to offer you. By the time you realize you're not missing any shingles, the scammers will have cashed the check you gave them to buy some extra materials.

2. **He needs you to pay today...** Scammers may claim they want to make some money on the side and if the boss sees leftover materials, then they can't use them. Don't let your fear of losing out on a bargain get you into trouble.

   If your neighborhood recently had the kind of natural disaster that makes it hard to get an appointment with a contractor, it's even more likely the person you're talking to is a scammer. Government agencies refer to these people as "Storm Chasers" because they like to prey on the victims of natural disasters, often crossing the country to do so. The National Consumer Law Center reported that complaints of

contractor fraud vaulted from 150 cases in Louisiana the year before Hurricane Katrina to 6,000 cases during the following two years.

3. **You have to pay upfront...** Scammers might claim they need to charge you for materials upfront or they need a hefty deposit to get started. Don't fall for it. Professional contractors have enough credit to buy materials and usually have accounts at local hardware stores to make billing easier. If the person you're talking to doesn't have good enough credit to buy materials, they're probably not good enough at home repair to be worth your money. More than 60% of the Katrina-related victims of home repair scams said they paid upfront, according to an LSU study, because the lack of skilled contractors in the city made homeowners anxious to get their projects done.

4. **He's hard to reach...** Many of those who were robbed by home improvement scammers reported it was difficult or impossible to get in touch with their scammer after the initial visit. In many cases, the scammers told homeowners a sad story to explain their lack of cellphone or business card, taking advantage of homeowners' sympathy in order to not provide contact information.

   In this day and age, there is no reason for a person you trust to not have a cellphone, business card or a profile on social media sites like Angie's List, Facebook or Twitter. If they do have a social media presence or business card, check it out before you pay. Make sure their account has been active for more than a few months and that there are other ways to contact anyone working on your house. If they can't provide any of that, how about a reference from one of your neighbors? There are lots of ways to verify someone's identity, and with each excuse or objection, it seems more likely the person you are talking to has criminal intentions.

WHAT TO DO IF YOU THINK YOU HAVE BEEN SCAMMED

If you think you might have been the victim of a home improvement scam, let [NAME] know immediately. Call us at [PHONE], email us at [email] or report a fraud online [link]. If we find out quickly enough, we may be able to stop the check before the scammers can cash it.

We're here to protect your money. You can find out more about our security and

fraud alerts at this link: [LINK].

PREYING ON PANIC

PRODUCT RECALL SCAMS

A product recall is never pretty. Organizing refunds and exchanges for customers takes time. Meanwhile, the customers just want their product to work!

Unfortunately, many scammers prey on customers' panic, confusion and frustration. There are several tactics criminals use to steal money or information using the cover of a product recall.

1. **Discounted cellphones** - In the days after a major recall on new smartphones, thousands of those phones went up on auction sites like eBay, many selling for half their market price. It sounds like a great deal, especially when the seller promises the ability to trade it in for a phone of your choice. But buyer beware: Secondhand buyers of the phone may not be eligible for any refund program.

   Before you buy a steeply discounted product, do a quick online search to make sure there's no recall on it.

2. **Fake rebates** - Sometimes, companies issuing a recall write checks to compensate the product owners. This strategy was employed by car maker Volkswagen, in the wake of its emissions scandal.

   Again, scammers capitalize on the recall. They buy the recalled vehicles for less than the buyback price, hoping to turn a profit. Alternately, scammers posing as representatives of a company issuing a recall have pumped product owners for bank information so they could supposedly deposit the refund directly.

   When getting a refund for a recalled product, only deal with the company

directly. If a recently purchased product of yours is being recalled, be proactive and find out on your own how to get your money back.

3. **Telephone number swaps** - With large-scale product recalls, calling the company can be annoying; the company is fielding calls from thousands of buyers, leading to impossibly long hold times.

   A group of scammers took advantage of this after a major Toyota-issued recall. The scammers sent out an official-looking email instructing Toyota owners to call a number that was one digit off from the official Toyota help line. Calls to this line were put on hold with a recorded message saying that all operators were busy. The message went on to explain that there was a premium helpline available to recall participants. There was a $5.95 per minute charge attached to it, but that information went by too fast for most callers to hear. Worse yet, people who called that fake premium helpline were asked for sensitive information, such as Social Security numbers.

   Here, too, to avoid being hooked, be proactive. Call the company's phone number. You may have to wait on hold, but you'll be safe from scams.

BEWARE THESE UTILITY SCAMS

Gas, electricity and water are not purchases you regularly think about. However, if someone called and said your account was overdue and that your service was about to be shut off, you'd likely panic and do whatever they say to avoid the consequences. And that's exactly what scammers are counting on.

The Department of Consumer Affairs has warned of a scam targeting utility customers. A scammer calls and claims the potential victim is overdue on a utility bill and that someone is coming to turn the power off. The scammer will instruct the victim to go buy a prepaid debit card. The scammer asks for the number on the card and then takes its whole value. Transactions on these cards are difficult to trace, which means recovering the money is nearly impossible.

If you're targeted by one of these scams, stay calm and don't succumb to threats.

1. **Know your rights** - Utility companies don't operate like these scammers. No utility company representative would tell you that your service will be shut off in minutes unless you pay immediately. There are regulations that govern how and when service can be turned off.

   First, they're required to send a notification of termination, a letter identifying the reason, the date and how you can prevent this shut-off. This process is cumbersome,

so most companies won't send one until you're more than two payments behind.

Second, turning your service off is expensive, so utility providers will first make several attempts to contact you. Ask for a record of past attempts at contact. A utility company will gladly provide this information; a scammer will hesitate when questioned.

2. **Pay it right** - Utility companies process hundreds or thousands of payments every day using established procedures. They will never insist on a specific means of payment.

   Always choose a secured means of payment, like your credit or debit card. These cards offer fraud protection and limit your liability if something goes wrong with the transaction.

   If you're not already signed up, [CREDIT UNION] offers automatic bill payment to make paying your bills simple.

3. **See something, say something** - If you get a call like this, hang up immediately. Next, contact the FCC. Demanding money over the phone is illegal, as is making unsolicited commercial phone calls. Report violations of the no-call registry at complaints.donotcall.gov.

4. **Stay ahead** - If you've run into payment trouble with utility companies in the past, work to get ahead on your utility payments. If money is the issue, there are federal and state programs designed to help. One such program is the Low Income Home Energy Assistance Program (LIHEAP), which provides utility payment credits for low-income individuals.

   You might also look into programs which average your utility payments. This can make budgeting easier, ensuring that you can pay each bill and avoid being a target for these scams.

DON'T DRINK THE WATER! HOW TO BE ON ALERT FOR WATER PURIFIER SCAMS

For millions of Americans, warming weather and longer days mean more than just baseball and allergies. It's a great time to be rolling up your sleeves, opening up the toolbox and getting started on home improvement projects. Many consumers are beginning to pay more attention to their own local water quality.

There are many legitimate ways to improve your home's value by improving its plumbing. You could add an inline purifier, a water softener or a tankless water heater. However, not all plumbing improvements are created equal, and many

people don't think about what comes out of the tap unless it's brown or has a foul odor.

Imagine, then, two men coming to your door wearing navy blue jumpsuits. They say they're from the water company and they need to do some tests on your tap water for public safety. They pour a small quantity in a beaker and claim to be testing for lead, mercury or some other contaminant. They tell you that, if the substance they add turns red, your water is dangerous and potentially toxic. They add a few drops and swirl it around. Lo and behold, your tap water turns a menacing blood red!

Sounds scary? No worries -- these gentlemen are quick to reassure you that this is not an unsolvable problem. It'll take them a few days to get the parts together, but they can install a system to treat your water for just a few hundred dollars. If you write them a check now, they can get to work right away and have you and your family safe in minutes!

Of course, there is no real danger ... in your water. These men don't work for the water company, and the substance they added to your water was food coloring. They might install a $20 water purifier, which is available at any hardware store, to your kitchen sink, and walk away with hundreds of your dollars. You've just been the victim of a water purifier scam.

Now that you know how it works, you can take steps to help keep yourself from being a victim. Like most other scams, the advice is pretty straightforward. Ask for identification, do your own research and be proactive.

WHO ARE YOU, AGAIN?

If your life goes according to plan, and you never encounter a major plumbing disaster, you may never see an employee of the water company. Your only interaction with them will be a monthly bill. On that bill, though, is a number you can call to connect with a service manager. A quick phone call to verify the identities of the "workers" who offer to help you out should scare away most scammers.

Don't be afraid to ask anyone who comes to your door for proper identification and don't be shy about verifying that information. Anyone who represents a legitimate organization will want you to know they represent someone you trust. That will bolster their credibility and make the rest of their job easier. It's only people who are trying to deceive you who want to short circuit your research.

Water companies, like any other employer, try to keep their employment costs low. If they had so little work to do that they could send people door-to-door to test water for free, you'd be paying much more on your monthly bill than you do currently.

Also, be careful of people who claim to be "certified" by a government agency, like the EPA. The EPA doesn't endorse any specific brand of water purifier, nor would it. There are many different water filter suppliers across the country, and no single one would be appropriate for all situations. If a product bears an EPA seal, that means the company has registered its product with the EPA and nothing more.

TEST YOUR WATER YOURSELF

If you have concerns about the quality of your drinking water, there are a number of services available for putting your mind at ease. For starters, your water company is required to provide analysis and test results to members of the public. Call your water company and ask for the latest test results of the water supply if they have not already provided it to you. Take that information and compare it to EPA standards for clean drinking water.

If you have a well, many state and local environmental agencies will conduct testing for bacteria and other common contaminants for free or for a reduced price. Maintaining clean drinking water for all citizens is a public health concern, and many agencies are willing to cooperate to ensure your water passes that standard.

If you have concerns about the water supply in your house, you can order a chemical analysis of your house's tap water. There are kits for sale in many hardware stores that will test for acidity, runoff contamination and bacteria. These are the most common problems facing home plumbing systems. Many labs also offer independent chemical analysis, though these may run hundreds of dollars, depending upon the level of detail required.

FIX IT!

There are many solutions available for DIY water purification. These can be as simple as a water filter pitcher, which removes many common impurities and can help with taste and odor. If you're looking for something on a larger scale, many companies sell whole-house water filtration systems, though these can also cost hundreds of dollars.

As people become more health conscious, drinking water may become a serious issue for homebuyers. Purifiers and softeners can also help to extend the life of your plumbing and fixtures by eliminating mineral deposits before they have a chance to corrode your house plumbing. These improvements may also be worthwhile in terms of the value they add to your house.

Access to clean, safe drinking water is an important part of everyone's well-being. Don't let scammers play on your fear and destroy your peace of mind. Whether you're looking for help finding a reputable contractor or are undertaking a serious renovation on your own, stopping by [CREDIT UNION] can be a great first step.

IMPERSONATING THE LEGAL SYSTEM

Most people have limited (and unpleasant) interactions with the legal system, with traffic violations and jury duty being among the most common causes of court appearances. Neither one makes for a fun afternoon. This unpleasant association explains why people live with a certain degree of fear of the courts.

A particularly malicious breed of scammer is preying on this fear. The tactics that perpetrators of these scams use are chilling.

The message could come by phone, email or fax. The caller may manipulate the caller ID system to make the number appear as though it's coming from a law firm or federal agency. Emails and faxes may have official-looking "seals" of district courts. They may also include specific information like case numbers, presiding judges and a list of charges.

The specific charges that are typically listed vary. Yet, they usually fall into one of two categories: minor offenses and financial fraud. Minor offenses include things like skipping jury duty or unpaid traffic tickets. The financial fraud charges can range from failure to pay loans to bank and check fraud, or even money laundering.

The scammer will try to make money in one of two ways. They will either ask for money to pay the fine or demand personal information. They might claim that they need a Social Security number or other private information to investigate a mix-up. If you protest, they will threaten that the police are on the way and that paying up will be the only way to avoid prison.

Paying your parking tickets on time and going to jury duty can help you avoid the first part of this scam. With complicated financial regulations, though, you might be legitimately concerned about accidental bank fraud. You've probably heard news stories about criminal organizations laundering money through the big banks. As a credit union member, though, you have many tools available to combat this threat. Let's look at six easy ways to beat this scam and keep your money safe.

1. **Know the law.** Police do not serve warrants over email, phone or fax. As one county sheriff said, "Police officials do not serve any summons by email. Legal documents are only delivered by officers or certified mail." In other words, if you're in trouble with the law, you'll know about it. If you receive a call like this

and have concerns about your legal status, call your local law enforcement. Ask them about outstanding warrants in your name. If you have outstanding warrants, you are better off speaking to law enforcement or hiring a lawyer.

2. **Never give out personal identification over the phone to someone you don't know.** Never send money via Western Union or prepaid credit cards to people you don't know. Never discuss your financial status, except with credit union representatives or financial service professionals. Practice the same good financial habits you always do.

3. **Learn the court system.** County, city and local state courts handle all minor offenses. No one will literally make a federal case out of your speeding tickets or unpaid fines. If you receive a notice from a federal court about offenses like these, do not respond to any request that follows.

4. **If you receive one of these notices, take action!** There are several agencies you should contact. The Federal Department of Justice has an email address and phone number set up to respond to these queries. You can email n.iljuryscam@usdoj.gov or call 312-353-2284. The Federal Trade Commission has a website set up to deal with these cases as well. You can file a report at www.ic3.gov. You can also contact the Clerk of the Court for the district in which the warrant was issued.

5. **Trust your credit union.** They work hard to protect your money and preserve their relationship with you. If someone was using an account at your credit union to commit fraud or launder money, your credit union would be working hard to stop it. They'd also let you know about it. Don't take the word of a threatening stranger over your friends and neighbors.

6. **Always know your credit history.** Enrolling in a credit monitoring service with your credit union means you know with certainty what debts are yours. This service also provides protection against identity theft and other scams. As an added bonus, you can figure out what you need to do to boost your credit score. Speak with a representative from your credit union about credit monitoring services today.

WHEN THE IRS CALLS … BE SURE IT'S REALLY THE IRS

Tax season is scary enough for most people. Translating the arcane scripts of bureaucratic forms is a difficult task. And once that return is filed and out the door, most Americans would prefer to never think of it again. That sentiment is what a

new class of scam artists is counting on.

The Treasury Inspector General for Taxpayer Administration reports that more crooks are posing as IRS tax collectors than ever before. And they have taken to calling many folks at random. They use common names and bogus badge numbers to bolster their credibility. They may use your name and the last four digits of your Social Security number, which they likely obtained from a credit check or an information clearing house. They will claim you owe a large, specific amount of money. This strategy makes the con more believable. $5,000 sounds made up, but $4,987 must be right. They will insist that if you don't pay immediately, the sheriff in your state or county will arrest you.

The con artists expect to scare you. They expect your fear will overwhelm your decision-making ability, and that you will comply without much or any debate. They make their money from the fear they can create. Most victims of this scam report receiving calls from a Washington, D.C. area code (202, most commonly). If you don't answer, you can expect them to leave a voicemail identifying themselves and demanding that you call an 888 or 800 number. They may threaten that if you ignore the voice mail, they'll issue an arrest warrant in your state. They'll use legal terminology to make themselves sound legitimate. If pressed, they'll focus on the consequences more than the process.

They may also send emails that include the same threats. The con has the same end goal – the expectation that you will be too scared to investigate and will then comply immediately. These emails will almost always come from email addresses that don't end in irs.gov.

It's tempting to believe that the IRS is a heartless, ruthless organization that uses threats and intimidation to collect its pound of flesh. In actuality, IRS collectors must obey specific rules of conduct. They don't need to scare you into compliance. They can and do use the legal system. There's no way the IRS can go from pointing out an error in your return to arresting you without a court date.

There are a few key ways to tell if the contact you've received is legitimate. Watch for these signs:

1. The IRS always makes first contact with people via U.S. mail. This is so there are always accurate records of what was said to whom and when. Your first notification that you have an unpaid tax debt will not be a phone call.
2. The IRS will never ask for a wire transfer of funds or a prepaid debit card. It's rare that tax repayment will use a credit card. Most of the time, this process takes place through wage garnishment. In no case should you send cash to someone you have never met.

3. If you believe you may have a tax problem, don't panic. Call the IRS taxpayer help line at 800-829-1040. If you are, in fact, in trouble, you should call a lawyer. Throwing money at the problem can never help.
4. If you receive a call like the one described above or something similar, report it. You can call the Treasury Inspector General's scam line at 800-366-4484. If you receive an email, you can forward it to phishing@irs.gov. You can also file a report with the Federal Trade Commission at ftc.gov/complaint.

MY ELECTRIC BILL IS HOW HIGH?

Usually, you get your electric bill in the mail. This month, however, it appears in your email account. You don't remember signing up for the electronic version of the bill. You aren't even sure they have that available. You stare at the email. Wait. How did a bill that is normally $150 a month suddenly jump to $550? You stare at the email in a panic.

In another scenario, you receive a phone call from someone claiming to be from your water company. They tell you that you owe on your account or your water will be immediately shut off. You are pretty sure you paid that bill last week. If only you could find the most recent bill while also trying to find a debit card to pay the bill.

If anything like this happens to you, it should trigger alarm bells. What you're encountering may be fraud. It may come in the form of emails or phone calls, but the goal of the fraudster is the same: to steal your information.

This has happened under the guise of reputable companies such as UGI Utilities, PG&E Energy, Atmos Energy Corporation, Portland General Electric, NW Natural Gas Company, Pacific Power and Duke Energy.

If you get an email from a utility company, pay attention to the account number, the logo and the return email address. Even links within the email can actually send you to a fraudulent website that looks just like the website you would expect to see. Pay attention to the amount. Is it close to what you typically pay? Of course, consider if you even signed up for electronic bills from the utility company. If things don't look right or you just aren't sure, don't click on any links and contact your utility company immediately. It should go without saying, look up the phone number in the phone book or online – don't rely on any phone number that is printed within the suspicious email.

If a phone call comes from someone claiming to be from your utility company, consider that your service won't be turned off that instant. In other words, don't reach for that prepaid debit card. And remember, if indeed your bill is past due, you will be mailed other reminder notices. The phone call won't be the only indicator

that your bill is past due (if it really is).

If you get an email or phone call, gather as much information you can from the caller. Refuse to pay any money or provide personal information like account numbers, tax identification, etc. Call your utility provider and share the information. If it is a fraudulent email or phone call, you likely aren't the only potential victim. Any information you share with your real utility provider will help them inform their customers and protect their financial identity.

HEALTH INSURANCE SCAMS

There's a lot of confusion these days in the healthcare market. Unfortunately, scammers are preying on this confusion to con people out of their money.

Common variations of health insurance-related scams include:

- **Fake or worthless policies.** Some health insurance "companies" offer little or no real protection against costs arising from serious illnesses, but they'll take your premiums anyway. But if you should have a claim, you may find that the 1-800 number to file your claims is fake, or the company simply won't pay a covered benefit, whatever it says in the contract. Sometimes the carrier just doesn't have the cash reserves to pay a claim.
- **'Discount-club' policies.** Sometimes people buy a health "insurance" contract that seems very affordable – only to find you get what you pay for. Beware of "stripped-down" health insurance policies that amount to nothing more than prepaid health care at a limited network of providers. The consumer mistakenly thinks he or she has health insurance – but the policy provides little or no risk-transfer benefit. Meanwhile, even moderately expensive medical events remain impossibly expensive for the consumer, because the plan only offers, say, a 50 percent discount on services. Often, the list of exclusions is long. The customer winds up paying the premium, but retaining much of the risk anyway.

JURY DUTY SCAMS

Have you heard of jury duty scams? Here's the scenario...

The phone rings. You check it, expecting that call from your mother about your sister's birthday party, but instead you see a number you don't recognize. You decide to answer it and are shocked to hear what the person on the other line has to say.

"Hello, my name is Terry; I'm with the local court system. You have failed to report

to jury duty and a warrant is out for your arrest."

You rack your brain, trying to remember a letter or any kind of correspondence you may have received, but you can't think of any. Maybe it went to the wrong address?

You are eager to settle the issue, so you ask what you can do. They want to verify that it is really you, so they ask you to confirm personal information, such as your Social Security number, date of birth, etc. Then they tell you that you can pay a pretty steep fine and they'll forgive it this once. You are now a victim of identity theft.

Phone identity theft is an issue that has been around for a long time, and scammers are constantly coming up with ways to separate you from your money and your identity.

Always be cautious with anyone who wants your information. Ask for verification before providing someone with personal information and check up on information they give you.

Anything involving your account number, Social Security or credit card information is especially suspect and you should always get an official correspondence before giving someone any of this information. Ask them who you can speak to locally and tell them you will call them directly. Double-check with online sources that the phone number matches.

Above all, never give out personal information over the phone to strangers just because they have an urgent and official tone. Thieves rely on fear and intimidation to make a normally sensible person make a rash decision.

If the company is legitimate, it will not mind providing you with a way of checking into it and making sure the caller is are who they say they are. Sometimes, even something as little as putting the pressure back on them can cause them to back off. It is always important to be on the defensive. Don't take what someone from "the courts" or anywhere else says at face value!

PAYDAY LOAN SCAM

It seems like there's a new scam to warn our members about at every turn. This one is especially pernicious: Beware the Payday Loan Scam.

No, it's not the payday lenders themselves (though they can be bad enough). It's a group of criminals who try to steal your money by tricking you into thinking you are liable for a debt that doesn't exist.

How it works:

You receive a call from someone claiming to be with the "Federal Collections Department," the FBI, or some other official-sounding office. They claim you owe money on a delinquent payday loan and demand that you pay up. They will call incessantly at your home and even your workplace. They refuse to provide additional information or documentation of the original loan and may become verbally abusive when you question them.

They're banking on you figuring it's easier to pay the money to make them go away rather than resist them.

In some variants of the scam, people have been visited at home or at work by a phony process server. In other cases, the caller or fake server informs the victim that there has been a warrant issued for their arrest for failure to pay a loan.

Unless there is evidence of fraud, you will not be arrested for failure to pay a payday loan.

TAKE ACTION

If you are targeted by scammers pushing this scheme, immediately contact your local police department. You should also contact the federal government at IC3.gov. This is the Internet Crime Complaint Center set up by the Federal Bureau of Investigation and the National White Collar Crime Center.

Also, if someone has enough information on you to contact you at home and at work, your identity may have been compromised – especially if the scammers have correctly identified a financial services company with which you have done business.

In this case, it's prudent to contact your bank and credit card companies. You may also request an alert be placed on your credit bureau reports by contacting the three major credit bureaus:

1. Experian – 1-888-397-3742
2. Equifax – 1-800-685-1111
3. TransUnion – 1-800-916-8800

WHAT YOU NEED TO KNOW ABOUT RANSOMWARE

In recent years, there has been a serious increase in ransomware attacks, including infamous scams like Petya, WannaCry and Cloudbleed. While each incident has its

own specific variables, here's what you need to know about ransomware attacks.

Ransomware is evolving like an uncontrolled virus. Don't be the next victim! Here's what you need to know about ransomware:

WHAT IS RANSOMWARE?

Ransomware is a subset of malware that isolates a victim's data and then demands a payment for release. It is often embedded inside seemingly harmless software and applications. It activates as soon as the user launches the program. Devices can also be infected through email links or malicious websites.

HOW DOES A RANSOMWARE ATTACK WORK?

There are two primary types of ransomware: locker and crypto. Locker ransomware locks victims from using important device functions, like accessing a desktop or browsing the internet.

Crypto, the more common form, encrypts files using a unique algorithm and demands a ransom payment.

Cybercriminals usually demand payment in bitcoins. This form of digital currency allows you to pay for goods or services remotely, using a mobile app or a computer. Every bitcoin transaction is anonymous, making it the payment method of choice for cybercriminals.

TO PAY OR NOT TO PAY?

Experts are on the fence about this million-dollar question. Joseph Bonavolonta, the ASA in charge of the FBI's Cyber and Counterintelligence Program, claims that the FBI often advises people to pay the ransom, explaining that when more people pay the ransom, it keeps ransoms low. He also believes that most scammers keep their word and will decrypt the victim's files.

However, other FBI officials urge victims not to pay the ransom. They say there is never a guarantee of the files' return and that paying the ransom encourages more attacks.

Everyone agrees, though, that victims should seek assistance from law enforcement agencies and share the details of the attack. The law enforcement agents will tell them whether they've seen this group attack before and whether it tends to decrypt files in return for payment.

If your computer has been infected and you decide to pay the ransom, your payment can be anywhere from $200 to $10,000. Before you pay, though, do a quick search to find out if there's a decryption tool online.

If you decide not to pay the ransom, shut down your computer and disconnect from your network. Scan your computer with an antivirus or anti-malware program and let it remove everything on your device.

PREVENTION

Be proactive. Strengthen your email's spam filter, don't ever click on suspicious links, and never download mobile apps from unfamiliar application stores.

Make sure your operating system is protected with a strong firewall, spyware and sufficient, updated anti-virus software.

Finally, backup your files on an external hard drive or on a USB every few weeks. If the unthinkable happens, contact a law-enforcement agency for assistance and check for a decryption tool online. If you do decide to pay, be sure to take preventive measures against future attacks.

CHARITY SCAMS!

Sadly, hundreds of crooks hide behind the veil of charities. They'll impersonate known charities or create a bogus one, then solicit funds and pocket the cash.

In one instance, scammers abused the name of the Make-A-Wish Foundation, an organization dedicated to granting the most longed-for wishes of terminally ill children.

Here's how it went: The scammer called the victim and announced they had won hundreds of thousands of dollars in an alleged sweepstakes conducted by Make-A-Wish. The caller claimed to be representing the FTC or another federal institution. The "government official" then explained that the "winner" must pay thousands of dollars for taxes and insurance to claim their winnings.

Of course, there was no sweepstakes and the caller was no government official. In fact, on its website, Make-A-Wish asserts that it never conducts sweepstakes. The victims who wired their money over never heard from the caller again.

There are several red flags here. First, the FTC does not hand out sweepstakes prizes. Second, you should never have to pay money to claim a prize. And third, no legitimate organization will ask for such large amounts of money to be paid over

the phone.

Unfortunately, this scam is not the first of its kind and it won't be the last. Here's how to verify that you're only donating to legitimate charities:

1. **Don't donate over the phone** - It's hard to determine authenticity over the phone, and up to 95 cents of every donated dollar may actually go to the telemarketer.
2. **Be wary of sob stories** - When a caller preys on your heartstrings to the point of discomfort, you may be falling for a scam.
3. **Donate with caution after a major catastrophe** - Natural disasters, like floods, hurricanes and tornadoes, bring out the generosity in people, but they also bring out the bogus charities. When disaster strikes, you can still help, as long as you're super-vigilant and extra careful. Be wary of "Watch this Now!"videos with links for donating or other random requests that show up on your social media platforms. Instead, donate directly to the Red Cross or to another large charity you are familiar with and whose identity you can easily verify.
4. **Know the charity** - When choosing a charity, research it first. This way, when someone impersonates this organization while collecting for a cause you know they don't support, you'll recognize the scam.
5. **Read reviews** - Check for a charity's legitimacy on objective review sites like CharityNavigator and CharityWatch.
6. **Ask for info** - If a caller sounds genuine and you'd like to donate over the phone, first ask for details about the charity. If the caller is hesitant to answer or unsure in their response, hang up!
7. **Give safely** - Never wire money to an unverified recipient. Similarly, only provide sensitive information if you're certain the caller is genuine. If you're in doubt, contact the organization on your own to donate funds.

SEASONAL SCAMS

SUMMERTIME IN SCAM CITY

Scammers don't take summers off. In fact, some scams thrive during the summer, particularly those involving vacations or travel.

An increasingly common one involves hotels. You're awakened at night by a call from the front desk saying there's a problem with your credit card, so please reread the number. The scammers hope you'll do something half-asleep that you'd never do wide-awake: give out card info to a caller.

Other hotel guests find pizza delivery order forms, but when they place an order – by credit card – their identity is stolen.

Another scam involves a cabbie who unloads your bags at the airport in a rush, then speeds away – with the last bag. Sgt. Jerry MacDonald of the Las Vegas Police Department has seen plenty of this: "They'll snatch your luggage faster than you can blink."

A recent scam involves cellphones and the number 72. You receive an awful call reporting a family member's death, with instructions to call another number beginning with *72 for details (a hospital or doctor). This transfers your number to the scammer, who can give it to anyone, with you picking up the tab. Don't use *72 or any other number to forward calls to someone you don't know.

Sometimes scammers phone as cops, saying you've been photographed breaking the speed limit and demanding a hefty fine. Legitimate police officers don't do this.

Text phishing is common, too. Scammers send a text message, supposedly from your bank, asking you to visit a website that requests personal details to "unlock"

or "verify" your account. Never follow a link you're not sure about.

A new phone scam has been reported by the U.S. Citizenship and Immigration Services (USCIS): Scammers call immigrants in America pretending to be from Immigration, Refugees, and Citizenship Canada (IRCC). They threaten people with investigation or a lawsuit, throwing around terms like "affidavit" and "allegations," and tell you to pay by money transfer or gift card. The IRCC doesn't collect payments this way, and they wouldn't ask for basic info they would already own. And they don't threaten to arrest people.

David Dewey, research director at Pindrop Security, says scammers thwarted by chip-embedded credit cards have turned to mobile wallets, tapping into accounts through Apple, Samsung and Android Pay, Google Wallet, PayPal and others.

Dewey put mobile wallets to the test: He secretly copied credit card numbers and expiration dates from some colleagues, then Googled the answers to identification questions (like a colleague's mother's maiden name).

Within minutes, Dewey went to Whole Foods and bought lunch. (The colleague was reimbursed.)

"It's amazing how easily I added somebody else's credit card to my Apple Pay account," Dewey says. With new technologies come newer scams. Check your credit card statements carefully.

Finally, with new Medicare cards coming (without your Social Security number), scammers are calling, claiming to be from Medicare, and asking for your Social Security number or demanding payment for your card. Hang up, and report scams to the FTC. Medicare will never call you, and your card is free.

Whatever your circumstances, if you get a call or email asking for money or personal information – stop. Just hang up. You'll remember your summer much more fondly.

DON'T LET YOUR RIGHT TO VOTE BE SOMEONE ELSE'S CHANCE TO PROFIT! AVOIDING ELECTION DAY SCAMS

Democracy is a privilege. And Election Day is when our voices are heard.

Unfortunately, many people use voting season to make a dishonest dollar. The Federal Communications Commission (FCC) and the Better Business Bureau (BBB) are warning of an increase in fraudsters using the election as a pretense to get your money or personal information. Be on the lookout for these schemes!

1. Last-minute campaign contributions - In this scam, someone asks you for

another small donation before the election.

These funds never make it near your candidate's campaign. At best, the crook keeps your money. At worst, they have your credit or debit card information, leaving you a huge bill down the road!

In most states, voter registration information is public. A quick search of your name or address reveals your party affiliation. From there it's easy to guess your candidate preference. The scammer uses the candidate's credibility to gain your trust. Don't let them succeed!

To avoid this scam, give proactively. To donate money, seek out the candidate's website and donate there.

2. ***Voter re-registration*** - Going to vote means dealing with endless rules. Did you register to vote? Did you miss last election and aren't sure about your registration status? This uncertainty forms the basis of this scam.

   A scammer contacts you claiming your name has been accidentally removed from the voter rolls. They'll promise to correct that mistake with some information, like your address and Social Security number.

   You'll soon discover that your identity has been stolen. The caller didn't complete a voter registration form – it wasn't necessary. They just collected your information and abused it.

   Beat this scam using the same public records scammers use. A quick search on your state's Secretary of State website will reveal whether you're registered to vote.

3. ***Opinion polling*** - Everyone wants a preview of election results, leading to thousands of pre-election polls. To incentivize participation, survey companies offer rewards for participation. That's the "in" for this scam.

   A fraudster will call and walk you through a general survey. Then, they'll tell you you've earned a thank-you prize. You only need to pay a small "processing fee" using a major credit card or give them your account information so they can directly deposit the "prize."

   There is no prize, and there's probably no poll. Scammers are using the pretext of a poll to gain access to your personal information.

   Never give any personal information in a call you didn't initiate, and never trust anyone who asks you to pay a fee before they give you a prize.

   Whoever you vote for, it's your right to make your voice heard. Don't let criminals prevent you from doing your civic duty!

PROTECTING YOURSELF FROM COLLEGE FOOTBALL SCAMS

When football season is upon us, ticket scams start hitting college football fans hard and fast. It's important to know how to get to that game without losing half your savings in the process.

You can skip bootlegged merchandise at the game to avoid accidentally buying counterfeit goods. You can park in official places to avoid fake parking attendants. Those are easy scams to detect and dodge. Spotting phony tickets is harder.

Almost all the phony ticket sales are made online through sites like Craigslist or eBay. The seller writes a bit about how excited they were about using these tickets but had to make other plans at the last minute. They might even offer to sell the ticket for less than it's worth, because it's such short notice. You read this, buy the ticket immediately and wire them what they ask for. Depending upon how much effort the crook wants to put into the operation, one of two things could happen: you'll never get that ticket or hear anything from them again, or you might be lucky enough to get a realistic-looking fake ticket that'll be turned away as soon as you get to the gate.

If you want to save your money, check out the following three tips.

1. **Watch for red flags** - Read through the seller's blurb about the ticket. Does it have the same tone as those "Prince of Nairobi" emails? Is the seller lacking proof that they actually have these tickets, such as a picture of the tickets in question? If they do have pictures, do those tickets fail to match up with the venue, the date, the stated seating, etc.? Has the seller asked you to wire money to them?

   If the answer is yes to any of the above questions, it's almost definitely a scam. Take the information you've gathered and report it to the website administrators.

2. **Keep yourself protected** - If the scammer was clever enough to trick you, and you end up losing your money, there are a couple things you can do. If you paid them through a third-party service, such as Paypal, you can cancel your transaction within a few days and get your money back. The same is true of many debit and credit cards that offer buyer protection services. Call your issuing company to find out if you can stop payment because of fraudulent or undelivered goods.

3. **Do your homework -** The only way to be 100% certain you're not being scammed is to buy the tickets at full price from the venue. Anything less than

that is a gamble either way. Your best bet is to have as much contact with the seller as possible.

Start a conversation over email that goes back and forth for a little bit, asking them to verify every last detail about the sale. If you can, you might even want to call them by phone or agree to meet them in person. Just in case it is a scam, you'll want to have all the information you can get to report them to the police and your credit card company.

Nothing beats the thrill of seeing a live football game. Do that safely and securely by using common sense and keeping an eye out for suspicious sellers. Then, there'll be nothing for you to worry about but the score.

KEEP YOURSELF SAFE DURING THE HOLIDAY SEASON

Every year, we hear about the same holiday safety tips – don't drive tired, don't drive drunk, assume every other driver is drunk or tired, etc. Those are all good ideas to keep in mind year-round. Occasionally, we'll hear one that's specific to the season, like how frying turkey in the driveway is as dangerous as it is delicious, and it's also not something to try while drinking or overly tired. Unfortunately, this time of year is also one of financial dangers, many of which you won't hear about on the morning news or read about in the paper. Take some time, read our tips and hopefully you won't be a holiday victim.

- **Keep an eye on your surroundings** – Crowded malls and shopping centers are a savory opportunity for pickpockets. You're expecting to get bumped and won't notice one more jostle in a day full of them. If you do recognize you've been robbed, the thief can probably get away into the crowd, disappearing like a needle in a haystack. Purses should be worn across the body, wallets kept in the front pocket or inside a closed jacket. Consider leaving the house with the bare minimum, such as your driver's license or ID, health insurance card and debit card – which offers fraud protection and security features not available with cash.
- **RFID, RFID, RFID** – Today's pickpockets don't need to take your wallet to cause you problems, because many modern debit and credit cards emit RFID signals with personally identifying information. If any of your cards have a chip, then you need to account for them. Don't leave them at home, because they offer superior protection at the register. Check our RFID wallet guide for some tips [link]. In a pinch, you can wrap chipped cards in two layers of aluminum

foil, which will offer you protection from high-tech pickpockets, but you may get some bewildered stares or questions from folks at the register.

[skip the next paragraph/bullet if not offered by the CU]

- **Consider using Apple Pay or Samsung Pay** – Tokenization is the single safest way to spend money at any time of year. A malicious reader stuck into a cash register's card reader won't get you, RFID skimmers won't get you, and if you don't bring your wallet, no one can steal it. (Although they can still nab your phone, so watch out.) One important distinction to remember, though, is that not all Samsung Pay transactions are tokenized, so you only have as much protection as a regular card. The general rule is that any register that doesn't support Apple Pay's technology also doesn't support the tokenized version of Samsung Pay.
- **Don't leave checks in the mailbox** – At some point, we all learned not to use those colorful envelopes that tell thieves which cards might have checks in them, but we never learned the next step: Don't put checks in the mailbox at all. It's not hard for thieves to grab stuff out of the outgoing mail, whether it has the power company's name on it or is shaped like a holiday card. Drop all checks into a big blue mailbox, bring them into your post office branch or hand them to your postal carrier in person. By the way, this tip should be followed year-round, and you might want to consider setting up our online bill pay feature to minimize the number of checks you write, as well. Find more info: [link].
- **Understand the dangers of every form of payment** – Every form of payment has its dangers. Cash is portable and untraceable, so it's a target for thieves. Cards without EMV chips are in danger from skimmers built into the card reader at registers (like what happened at Target). EMV cards can be skimmed by people with specialized equipment who bump up next to you. All cards, cash and mobile phones are in danger of being stolen. Some experts are even saying that check fraud will be the most dangerous type of identity theft over the next five years. Even if you attempt to return to agrarian-era bartering, an enterprising thief could run off with the cow you were going to trade for an Old Navy gift card.
- **Take a breath, recognize the dangers and take reasonable precautions.** Do you know what kind of fraud protection you have on each of your credit cards? Any card about which you're unsure needs to stay home until you find out. Unsure about the cyber security of a small boutique? Bring cash.
- **Check out our security features at [link].** We offer a wide variety of fraud protections and cutting-edge cybersecurity for all of our cards and online bill

pay features, so if you have any doubts, just bring your debit card or a credit card with the credit union's logo on it.

- **Bring your own bag** – Shopping bags are a great way for stores to advertise, but they also advertise to thieves. "This overburdened, overtired, potentially unwary individual is carrying goods from all of these stores," the bags say. "Some may even have receipts in them and might have been paid for with cash." Don't make it easier for thieves. Instead, bring a tote bag that zips up if you have one, or your canvas grocery bags if you don't.
- **Take a trip to the car** – Carrying too much is asking for trouble. It makes you less mobile, you're less likely to feel someone remove an item from your bags, and even if no one hassles you, it's a good way to end up with back pain. If you're enduring a marathon trip to the mall, take time every few stores to take your purchases out to the car. Keep receipts in your wallet and take pictures of the bags you put in your trunk (where thieves can't see), so even in the worst possible scenario, your car insurance can cover the loss of your shopping from a car thief.

  Plus, you'll have less to carry, you'll get some exercise and the cold air can help you clear your head to decide if you need to purchase anything else. Not a bad way to keep from overspending!
- **Buy yourself a holiday drink from the coffee shop** – You're probably safer if you're alert, but that's just an excuse. Holiday coffee drinks are delicious, you want one and we just gave you an awesome excuse to justify the everyday luxury of a peppermint mocha to yourself. You're welcome.
- **January is coming, be ready** – If you're going to binge on holiday shopping in December, you'll need to purge in January. Keep all of your receipts and do an extra-careful reconciliation of your accounts in January. Be ready to spend a few afternoons making phone calls to make sure every charge is correct and accounted for. Make sure to check your credit report in January as well. While you're checking your credit and your accounts, take the opportunity to start the new year off right. You have your financial information gathered already, you have your credit report in front of you and your W-2s are starting to show up, so it's time to do three things:
  - **File your taxes.** Don't get mad at us, it's not our fault. We're only reminding you to do it early because you'll already have most of what you'll need, so getting your homework done on Friday will give you the rest of the weekend off.
  - **Rework your debt.** You have every one of your credit card and other

account statements in front of you, so it's time to make some calls. For your higher interest cards, it's time to pay them down, transfer the balances or negotiate a lower rate. This is easier if you've got some cash in hand, possibly from the tax refund you now know you're getting. You can also take this time to explore using your home equity to eliminate some of the high-interest cards. Get more information here: [link].

- **Set up a Christmas Club for next year.** Alright, you just saw how much money you spent this holiday season. Next year, resolve to do it all without taking on unnecessary debt. You'll save a ton of money and a ton of stress. The best way to do that is with one of our Christmas Club accounts. Use this year's budget as a guide and follow the tips on our Christmas Club page to set one up now. Next year will be a breeze. Link here: [link].

And that's it. It sounds like a lot, but it's really taking the same level of vigilance you would use for normal shopping and increasing it to correspond with the increased spending of the season. For a good rule of thumb, maybe we should just establish the "three-Mariah" rule: Once you hear Mariah Carey's "All I Want for Christmas is You" for the third time on any day, you have to go home – you've either spent too long at the mall, or your brain has been turned into holiday slurry and you can no longer be trusted to remain vigilant. Three Mariahs and you're out.

THE 12 SCAMS OF CHRISTMAS

The holidays are a time of family togetherness and celebration. Scammers know you're distracted, busy and emotional. That's why their schemes are so devilish. They get their own twist around Christmas time.

In the interest of keeping things in the holiday spirit, let's look at 12 scams of Christmas. Don't get taken in by these or similar schemes. Otherwise, you might be footing the bill for 12 drummers drumming and all the rest!

1. **Mobile malice** - Be wary of "season-themed" apps that perform frivolous functions, yet demand top-level security access. An app that makes it look like there's snow on your background image doesn't need to send or receive texts. Such an app might send premium text messages and leave you holding the bill.
2. **E-card danger** - Everyone with an email address will send these little flash programs. Scammers have designed some with malicious code. They can install data leaching programs on your computer and do untold damage. Don't click

links in emails unless you know the sender. Even then, if it looks a little out of the ordinary, it probably is. They may have already fallen victim and it would be good to let them know.

3. **Fake packages** - You'll be receiving unexpected packages this season. Scammers know this and will send realistic-looking delivery failure notifications. They expect you to follow up with them and reveal personal identification information! Head to your local post office or call the parcel delivery service to check with a clerk before you hand over information on the internet.

4. **Hotel "Lie"-Fi** - The FBI issued a warning to this season's travelers about a malicious pop-up at hotel chains around the country. This scam requests people install a foreign program before connecting to a hotel Wi-Fi network. This foreign program turns out to be data-stealing malware. Remember, internet connections you don't own or control can easily be used against you. Before you use the internet at a hotel, ask yourself if it's worth the risk. If you do need access, be wary of what you're installing – there shouldn't be a need to install anything.

5. **Festive spam** - We've all gotten used to filtering out spam in our email. Now prepare yourself for it to take on a more holiday-oriented theme. Messages will suggest that off-brand Rolex watches and cheap pharmaceuticals would make excellent gifts. Be careful, though, because these companies might just be in the market for your personal information.

6. **Bogus gift cards** - There's a bonanza of savings to be had buying gift cards through second-hand retailers. Be careful, though, because many of these retailers might be a front for scammers. Gift cards may be invalid, used or forgeries, and you'll be left holding the bill.

7. **Fake charities** - These crop up every time there's a major disaster, but they also show up at the holidays. Leaflets and phone calls from organizations with familiar-sounding names will soon appear. To be safe, don't give to any charity with whom you didn't start the contact. Do your research, and give to charities whose values align with your own.

8. **Must-have gift scams** - There will soon be an "it" gift. You'll know it by the high demand, low supply and hugely inflated prices. Almost on cue, websites will pop up offering the rare widget at unbelievably low prices. This is a scam – the advertiser doesn't have the product and is only using the offer to harvest personal information or bilk you of your hard-earned money through sites like Craigslist or eBay, where they will seek payment through PayPal and never send the item you purchased.

9. **Christmas catfishing** - "Catfishing" means pretending to be seeking a romantic

partner on the internet to dupe people. Scammers take advantage of the loneliness the holidays can evoke to trick people out of gifts or worse. As tempting as it is to believe in love stories at Christmas, keep your feet on the ground and practice safe internet dating. A good rule of thumb: If you're single at Halloween, stay that way until after New Year's.

10. **Holiday vacation scams** - If it's cold and miserable where you are, it's always tempting to go someplace tropical for a few weeks. If you're thinking about getting away, be careful of unrealistic prices or "too-good-to-be-true" travel offers. Scammers have been setting up phony travel sites to harvest personal information. Only book through reputable websites.

11. **Devious Christmas games** - If you're facing a five-hour flight and a three-hour layover, it's fantastic to have a distracting mobile game to pass the time. Be careful, however, not to download the wrong one. Mobile games can harvest data from your phone or steal password information. Always do a quick search to check the validity of the app you're downloading and read the permissions carefully. A fun game should never ask for permission to send texts or send information to third parties.

12. **Free USB Tricks** - Be careful with unsolicited gifts of "free" USB thumb drives. Security firm McAfee warns that many of these devices come pre-loaded with malware. Such scams often target company computers, so ensure you only use approved hardware on your work network. USB storage is cheap enough that you can pass on the freebies.

GOING AWAY FOR THE HOLIDAYS? DON'T ANNOUNCE IT ONLINE ... UNTIL YOU'RE BACK

As if you didn't have enough to worry about, what with making travel arrangements and packing, if you're going away for the holidays, don't announce it on Facebook, Twitter or any other social networking site.

Scanning the newspaper for funerals and weddings for opportunities to break into homes while people are otherwise occupied is an old trick for thieves. Social networking sites are just a new spin on that. And while most sites allow you to restrict who gets your info, there are no restrictions on who your friends share it with.

So warn your kids not to discuss upcoming travel plans with friends or share any personal information online. Use the feature that allows you to restrict who gets your information. Watch what you and your children post, ensuring that you don't

give away information that could cause a break into your home, or to your identity.

As with all forms of identity theft, or just plain old theft; it's better to be safe than sorry.

AVOIDING CHRISTMAS CHARITY SCAMS

It's the season of giving – and for criminals it is the season of the taking. Every year, dozens of new "charities" conspire to rip off well-intentioned givers. They also wind up starving legitimate and efficient charities of desperately needed resources as well. In the end, it's not just the giver who's ripped off; the real victims are the needy and the would-be beneficiaries of the causes that were targeted.

So how can you make sure your dollars are going to your preferred causes – and are being spent responsibly and allocated efficiently?

Have a giving plan. Many times, criminals can thrive because people don't really have a system or discipline in place to manage their charitable giving. They give on an ad hoc basis, often on impulse, and with no research into the organization.

Research your charities. This is a process called due diligence. If a charity wants your money, you are absolutely justified in investigating it. How reputable are they? How efficient are they? Does 95 percent or more of your donation actually make it to those who need it? Or does the charity have an unreasonable amount of overhead? How much does the executive director make? Is it reasonable for a charity of that size? One resource you can use to start investigating a charity is CharityNavigator.org.

Determine a charitable giving budget and stick to it. You know what you can afford. Don't go over that budget – at least not on impulse. Give with your heart – but use your head.

Don't give on the street. Many street collectors are scammers. You're OK buying Girl Scout cookies from the neighborhood children in front of the supermarket. But you're getting some good cookies for your money. Don't put cash in some collector's bucket without doing some due diligence.

Get a receipt. Legitimate charities can give you a receipt, which you can use to take a tax deduction. If you take the tax deduction, you can give more. No receipt? No deal.

Ensure the charity is a legitimate 501(c)(3) tax exempt organization. To get the official IRS list, download Publication 78 from the Internal Revenue Service at IRS.gov.

Write a check. Don't give cash. This establishes a paper trail.

It's not enough just to give. People can give and give, but without some controls on their money, their giving might not benefit anyone but crooks. The needy are left out. The whole point of giving is to make life better for the people who are most in need. Take these steps and the needy will be getting the maximum bang for your charity buck.

DON'T LET CHRISTMAS SEASON BE OPEN SEASON ON YOUR PERSONAL INFORMATION!

Every year has a new "it" toy that must get under the tree. These toys fly off the shelves, spawning an incredibly inflated secondhand market.

One of the more recent is Hatchimals – those adorable stuffed animals in cloth shells. There's an element of surprise until the toy "hatches" and its true form emerges, adding to the thrill.

Unfortunately, scammers are always capitalizing on parents' desires to make Christmas memorable for their children. Scammers have been known to set up fake Facebook pages, Instagram sites and Twitter profiles offering "giveaways" to people who follow them and/or download a "fan app." There are no such giveaways, though. Worse yet, the fan app may turn out to be a piece of malware to steal personal information and transmit it to the criminals.

If you're hunting for this year's "Hatchimal," these tips will keep you safe:

1. **Never download anything you don't need** - When people are tricked into installing something on their computer, they can unknowingly send personal information to a scammer. Before you click any downloadable link, ask yourself:
   - Do I know the company that produced this software?
   - Do I trust the person who sent the link?
   - Do I need this software for my daily life?

   If the answer to any of those questions is "no," close the browser immediately. If you doubt the safety of a piece of software, don't download it.

   These rules apply for every device you use. In scams during recent years, the perpetrators intentionally targeted mobile users. Your phone has as much personal information on it as your PC does; so safeguard both!

2. **Double-check when shopping online** - Many scammers have taken a more conventional route: They promise goods and take the payment, then don't

deliver the goods. While this scam is common all year round, the holiday-shopping insanity makes more people more vulnerable.

More insidiously, scammers have been posting "black market" toys. Factory defects are sold at many times the retail prices, even on reputable websites like Amazon. To avoid this scam, check reviews for the account. If someone's selling a new toy but they've never sold anything before, it's likely they're running a scam.

3. **If you must shop second-hand, try to deal locally**. Never send payment through unsecured means, like a cashier's check or wire transfer. Meet your buyer in a public place, and always inspect the goods before paying.

4. **Read the reviews before the hype** - Despite the popularity, many parents who've purchased the year's "it toy" are disappointed. The toy doesn't live up to the hype and kids lose interest.

Ask your children what they really want for Christmas; it may be something entirely different. Find something they'll really treasure. They, and your pocketbook, will thank you!

Don't forget that building great holiday memories doesn't cost a dime. You just need to spend time together! Happy Holidays!

AND EVEN MORE SCAMS...

BEWARE OF PHISHIN G SCAMS!

The Federal Trade Commission (FTC) has warned of a recent upsurge in phishing scams involving credit union brands.

In all phishing scams, the scammer poses as a legitimate business or service provider where the victim may have familiarity. In this case, they claim to represent your credit union.

The fraudsters use social engineering, capitalizing on social norms to inspire trust and manipulate unsuspecting people.

The scammers usually communicate via email, but they may also use mediums like phone calls, text messages or social media. They convince the victims of their legitimacy by providing personal details about the victim that have been found online.

Next, the victim is lured into providing more information by the promise of compensation, or by claiming the victim needs to verify or update their account. Once the scammer has the information, they can empty the victim's accounts, track their online activity and/or steal their identity.

Alternately, the scammer may lead a victim into clicking on links that are embedded with spyware. The links go to a website that looks just like [credit union's] site, but is actually bogus. Since the victim thinks they're browsing [credit union's] site, they generally won't hesitate to input usernames and passwords.

You can recognize these messages as scams by remembering that your credit union will never ask for sensitive information through insecure channels.

Unfortunately, hundreds of people are falling prey to phishing scams. Don't be the next victim! Here are four tips to help you protect yourself:

1. **Ignore suspicious emails** - If you receive an email from an unidentifiable source, ignore it. Don't reply to the email, click on any embedded links or open attachments. Similarly, never "friend," or otherwise accept communications with a stranger via social media. As a general rule, it's best not to share any personal information over the internet.
2. **Alert [credit union]** - If you think you've been contacted by a scammer that's impersonating [credit union], let us know! It's best to forward the original email you received. If you've already deleted it, though, send us an email with every detail you can remember.
3. **Report all suspicious activity** - File your complaint at ftc.gov. You can also visit the FTC's Identity Theft website at consumer.gov/idtheft to learn how to minimize the fallout of a possible identity theft.
4. **Strengthen your computer's protection** - Efficient antivirus software will prevent your computer from accepting suspicious emails. If your software doesn't update automatically, be sure to update it manually on a frequent basis.

   A strong firewall prevents scams and viruses by making you invisible on the internet and blocking all communications from unauthorized sources.

   Similarly, the settings on all of your social media outlets should be as private as possible. Finally, all suspicious email addresses should be added to your computer's blacklist as quickly as possible.

With good precautions and steps toward prevention, you can keep yourself safe from phishing scams.

STUDENTS BEWARE: SCAMMERS PREY ON LEARNERS OF ALL AGES

As if college wasn't stressful enough, here's another thing for students to worry about: being on high alert for scams.

For many young people, college is the first taste of financial independence; scammers prey on this naivete. Also, the expense of college gives students financial pressure, which becomes ammunition for scammers.

Read on to discover three tricks criminals use to steal your money, and how to increase your personal safety.

1. **The Federal Student Tax.** Taxes are complicated for college students. With so much uncertainty, students are vulnerable to misinformation.

This vulnerability is exploited in a scam targeting college students. The scammer calls or emails, impersonating the IRS and claiming the student didn't pay the "federal student tax." The student is instructed to pay immediately, and is threatened with fines, penalties or even jail time.

Obviously, there's no such thing as a federal student tax. Additionally, the IRS never contacts anyone for the first time by phone or email; they only use certified letters.

The best defense against this scam is to get tax help. Many organizations exist to help students navigate their taxes; these will protect you from tax scams.

2. **Paper mills** - It's 3 a.m., your paper is due in several hours, and you're desperate for help. Then you find a site willing to sell you a paper. It's not cheap, but you enter your credit card number and cross your fingers.

   The paper turns out to be substandard, mostly copied from obvious sources. It contains numerous errors and has little to do with your chosen topic. You definitely will not get a good grade on the paper.

   Worse yet, a month later, mysterious charges appear on your credit card bill. The paper-writing company sold you a failing paper, and then stole your identity!

   Naturally, you can avoid this problem by doing your own writing. Most colleges have writing centers available to help you write your essays.

3. **Scholarship fees -** Many scammers use tuition expenses to lure their victims, promising scholarships as bait. These scholarships are ultimately useless, and generally turn out to be a ripoff.

   In one such scam, a company will offer to sell you a list of hard-to-find scholarships. Since they're obscure, you'll think you have a better chance at getting them. In truth, most of these scholarships are for specific institutions or have exceptionally narrow requirements. Worse yet, the information on these lists is publicly available.

   Alternately, you may be contacted by a scholarship agency offering you a generous scholarship. They've had a shortage of applicants and so you only need to pay a "processing fee" to supposedly secure your future. The scholarship, though, will go to "another applicant" — if it exists at all.

Keep yourself safe by being proactive. Look for opportunities yourself to ensure that what you're applying for is legitimate.

Finally, as you move forward, try to think critically about what you're telling people. If someone can make money off your information, they'll find a way to do so. The

only way to protect your information and that of your family's is by being vigilant.

PHONY WEIGHT LOSS PRODUCTS

More than two-thirds of Americans are either overweight or obese, and scammers hope to profit from the desperation many of us feel to lose weight.

Weight loss scams are nothing new. In fact, the FTC has been prosecuting false diet claims since 1927. Further, the word "diet" comes from the ancient Greek word "diatia," meaning Plato might have been dealing with diet scams while he wrote "The Republic." In the 21st century, the internet has greatly accelerated the speed and impact of scammer successes by gaining access to wide audiences and making it easy for them to reap large profits.

The variations are many and the tactics are just as varied. Since 2005, the FTC has brought 82 cases against scammers for using false or unsubstantiated claims about weight loss products. Surely there are many others that have gone under the radar or are lacking evidence for prosecution. That's why awareness is a valuable means for guarding yourself. Diet experts and government agencies offer some warning signs to help consumers avoid these types of scams:

The product claims you will lose more than one pound per week. Diet experts believe about one pound per week is the ideal rate for healthy weight loss. Any product that claims it can shed weight faster is probably too good to be true.

The product advertises you can lose weight without diet or exercise. It's not fun to hear, but if you really want to lose weight, a diet and exercise are the only proven and healthy paths.

Be alert if it claims you can lose weight from a specific part of your body, that a single factor is preventing your weight loss, or any advertisement using the words "miracle," "scientific breakthrough" or "secret formula."

The images on the site are obvious stock photos or appear altered. If you aren't sure if the images are authentic, use Google images to perform a reverse-image search. Google can show you all the places using a specific picture. The method for doing this varies based upon your web browser. Just search "Reverse Image Search Google" to quickly find the instructions that will work best for you.

Google the name of the product and add the word "scam" to the search query. Simply searching for "weight loss scam" returned the following products in just a few seconds: HCG Diet Direct, Sensa Products, LeanSpa, L'Occitane, Lobster powders and creams, caffeine underwear, double shot pills, Healthe Trim and many others.

WHO CAN YOU TRUST?

Medical research progresses every day and even well-intentioned diet experts can find it difficult to determine if any specific product works. TV's Dr. Oz recently testified in front of the U.S. Senate about the difficulties he has experienced in keeping up with dietary science. He even has encouraged viewers to interpret his advice as if he were a celebrity rather than a doctor.

Whether Dr. Oz encourages misinformation or is the victim of forces outside his control, the green coffee bean supplements scammers have been peddling skyrocketed in popularity after appearing on Dr. Oz's TV show, while the guest promoting them settled with the FTC for $9 million.

If you can't trust famous doctors, you might then turn to friends for diet advice. That's why many recent email scams have used Americans' faith in their loved ones against them by hijacking email addresses to make it look like the scammers' pitch was coming from a close friend or family member. In addition, these emails send readers to false versions of respected news websites, giving their false claims an air of objectivity, because even people who might not trust Uncle Fred's diet tips might accept claims made by famous journalists. Here are some additional tips for combating those deceptive practices:

Always confirm that someone you really know sent you the email before you pay any money or volunteer any personal information.

Even if a site shows the logo of a major network, that doesn't mean it's legitimate. Check out the other headlines the page links to. Take a look at the ads on the page. Are all the ads directing you to weight loss products or other similar businesses?

If a "reporter" tells you about their first-hand experience with the product, be skeptical. If the claims seem incredible, be even more doubtful. Reporters don't usually try medical products for a story and they are even less likely to do so for a long period of time.

If a major news network were to subject a reporter to experimental medical treatments, they would most likely put the segment on television and do a lot of pre-story promotion. Weight loss offers a very dramatic visual, after all. If you don't see the reporter describing the product on video, or if the video doesn't look like an expensive, major-network production, it is probably fake. Scammers will take images and names from authentic news sources and use them without regard to legality, so confirm you are actually seeing the reporter talking about the product that's on the video.

If you're still unsure about a product or offer, question everything. What name did the reporter use in the video? Search for it online to make sure he or she works for that network. Look up the product and see if it's for sale at a legitimate store. Call the friend who sent you the email. Ask your doctor.

If you are attempting to shed pounds for whatever reason, remember there are many healthy ways to do so. Some are relatively inexpensive, while others can put a heavy strain on your wallet. Being armed with awareness of the tricks and tactics will help you be alert and less susceptible to falling for the latest magic pill a scammer claims will get you to your ideal weight without the work.

3 COMMON TELEMARKETING SCAMS – AND HOW TO AVOID THEM

The annoyances presented by telemarketers are so common they've become go-to topics in sitcoms and stand-up comedy acts. Everyone laughs about how annoying telemarketer calls are because we all know and share the frustration of having our meal times interrupted or our family conversations disturbed by a ringing telephone. More than a running joke, though, these annoyances can pose a real threat to your financial security.

There's no good way to avoid getting a call from these companies, either. The FCC's Do Not Call list complaints site saw 3.7 million complaints from people who received unsolicited calls last year despite being on the list. Only about 600 companies have faced penalties or fines from the FCC. Even worse, if you make a transaction with a company, they can cold call you for up to three months if you've made an inquiry and up to 18 months if you've made a purchase.

These irritating calls seem to be a fact of modern life. The best thing you can do is be polite in saying "no" and ask them not to call again. However, when they turn from sales to scam, extra attention may be required. Let's take a look at three common scams, how to detect them and what you can do to fight back.

1. **The Fake Charity** - *How it works:* You get a call asking for your help dealing with a recent catastrophe. It will be ripped from the headlines and pull at your heartstrings – a hurricane in the Gulf Coast, an earthquake in the Philippines or a refugee crisis in Uganda. The cause is just a smokescreen.

   The scammer has set up the charity and hired his own organization to run advertising and promotion. He will use that organization to collect somewhere between 90% and 95% of the funds raised. The tiny fraction leftover will be donated to a legitimate charity and written off as a charitable contribution by

the scammer.

The worst part about this scam is it's completely legal. The people who set up these fake organizations know the tax code and exactly how far they can push the scam. By the time anyone investigates the "charity," it's already shut its doors. The scammer moves on to the next crisis.

In the best case, these scammers will merely take your money. In worse cases, they may sell your contact information to other scammers. They may even use your payment information to steal your identity.

How you can find it: Savvy scammers will set up a legitimate-looking website for their fake charity, so a simple search won't help. However, searching websites like Guidestar (guidestar.org) can help you sort out legitimate charities from scam organizations. Legitimate charities report information to the website, including what percentage of the funds they raise goes to overhead costs. Honest charities will never mind if you do your research.

How you can avoid it: Be proactive in your charitable contributions. Don't wait for a telemarketer to make a pitch about suffering in the world. If you want to give money to a cause, do some research and find an organization that aligns with your values. That way, you can tell anyone who calls, legitimate or not, that you already gave.

2. **Yard Sale Help** - *How it works:* You're trying to sell some stuff you don't need, like an old car or an antique desk, on a community website like Craigslist. You put your phone number on the ad so buyers can get in touch with you for answers to any questions. It's been up a few days, and you're starting to get discouraged.

   Then, a company calls and offers to put you in touch with a buyer. They want a percentage of the sale price as a commission. They want it upfront, but if the deal falls through (they say) they'll refund your money.

   However, the truth is that there is no buyer, and there is no refund. You're out the money you've spent on this bogus service and you're no closer to selling your stuff.

   How you can find it: Watch out for vagueness in the message – if you're selling a truck, be careful of people who want to help you sell your "vehicle." Frequently, vague messages are used to avoid changing the telemarketing script. Similarly, don't do business with services like this outside your community.

   What you can do about it: Selling things yourself can be very stressful. Be sure to give yourself as much time as possible to complete the transaction and always get an offer in writing before committing to sell. If time is really short,

consider selling vehicles or other large products to scrap yards or through consignment shops. Legitimate organizations will pay you to sell your things at a markup. No one in this business asks for money upfront.

3. **Senior Alert Scam** - *How it works:* One of the demographic groups who still has landline phone service in large numbers is senior citizens, and telemarketing scammers know this. Earlier this year, the Better Business Bureau issued a warning about telemarketers advertising a personal alarm system for seniors. The pitch began by describing a dangerous situation like a break-in or a medical emergency. This was done to create a sense of urgency and easily relatable panic.

   The scam offers a free personal alarm system, ordinarily worth thousands of dollars. The senior is only responsible for a small monthly fee, usually around $30. To reassure you, the scammer will cite endorsements from familiar-sounding organizations, like the Retired People's Association (not, to be clear, the American Association of Retired Persons (AARP), with which you're familiar).

   No alarm ever comes, and mysterious credit card charges start showing up. In truth, there was no alarm. The call was just trying to get credit card numbers for identity theft. The company doesn't really exist. It's just a front for a scam.

   How to identify it: Watch out for any sales tactic based on creating fear. Scammers know that people value their safety more than anything else and will frequently make bad decisions just to regain that sense of security. Also be careful of any organization that won't send information for you to consider or is withholding business details. Pay close attention to the names of organizations the telemarketer is citing.

   What you can do about it: Do not give your credit card information to anyone offering a free service. If it's free, they don't need it. If it's not, they're only telling you it's free to fool you. Instead, try to get as much information about the organization as possible: a name, an address, a primary telephone number or a website. Then, take that information to the Better Business Bureau and the Federal Communication Commission.

While we may never be rid of the scourge of telemarketing, we can take steps to make sure we lose as little as possible to scammers who use it.

No matter what's being peddled, your refrain should always be the same. No thank you, stop calling, and hang up. Document the times and dates you receive these calls and don't be afraid to contact the FCC, the BBB and your state's Attorney General.

If you're concerned about keeping yourself safe from scams, consider credit monitoring from [CREDIT UNION]. The same institution you trust for all your financial services can also help improve your credit and keep you safe from identity theft. Call or stop by [CREDIT UNION] today to see if credit monitoring can improve your financial peace of mind.

IDENTITY THEFT: GHOSTING AND THE OBITUARY

When a loved one passes away, the last thing on your mind is identity theft. However, you should be aware of "Ghosting" – when the identity of the deceased person is stolen.

"Ghosters" can find information about deceased persons through a number of sources. One is a hospital database, if the thief has an accomplice who works at a hospital. Another source is the Social Security Death Index. Unfortunately, you don't have much control over access to these sources.

One source you do have control over is the deceased person's published obituary. Often, this published remembrance of the person contains important personal information: birthdays, current addresses, hospital names, mother's maiden names, places of employment and the names of those who are left behind.

"Ghosters" can use any of this information to start building a new, albeit stolen, identity. In some cases, "ghosters" will even break into the deceased's home during the printed time of the funeral.

When you print the obituary, think through what information should be publicly available and what could be printed and handed out specifically at the service. By simply thinking through these items, you may be protecting your loved one's memory and identity from a would-be "ghoster."

In addition, a few simple phone calls made by the family immediately after the death of a loved one could help prevent this form of identity theft.

The three credit reporting agencies, TransUnion, Equifax and Experian need to be notified. You'll also want to ask for a "deceased" alert to be added to the deceased's credit report.

The Social Security Administration and Department of Motor Vehicles also need to be informed about the death. Additionally, you will want to call all lenders, creditors and financial institutions holding an account in the deceased person's name. If you decide to close an account, ask that it be coded as "deceased account."

These phone calls may require follow-up paperwork, which usually involves sending

the death certificate. Make sure you don't send the original death certificate. Instead, have plenty of copies on hand. Make sure you use certified mail when you mail the death certificate. After the phone calls and follow-up paperwork are done, you'll want to continue to monitor the credit report of your deceased loved one for any potential "ghosting" issues for up to 12 months. Doing so will prevent the deceased's assets from going to an unscrupulous identity thief.

PROTECTING YOURSELF

First, ensure that your agent, the company and the plan are all licensed to sell health insurance in your state. You can do this by calling your state's Department of Insurance Regulation, Department of Financial Services, or an equivalent. If you don't know how to contact regulators in your state, visit the National Association of Insurance Commissioners.

Also, beware of slick salespeople who claim that they are with the federal government, or that participation in their plan is "mandatory" under the Affordable Care Act.

Furthermore, don't fall for an agent's claim that they don't need to be licensed by the state because they fall under federal auspices. Even Medicare Supplement plans are sold by state-licensed insurance agents.

For more information, visit NAIC.org, Insurancefraud.org, or the Federal Trade Commission.