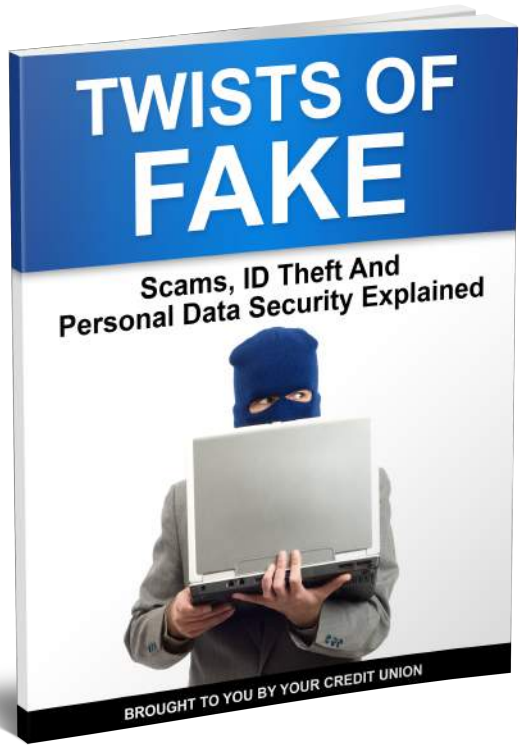
TWISTS OF FAKE

Scams, ID Theft And Personal Data Security Explained

BROUGHT TO YOU BY YOUR CREDIT UNION



TWISTS OF FAKE

New and time-tested threats to your identity

Welcome to the scammer's worst nightmare: this eBook!

Within these pages, you'll find tips on identity theft prevention, information on the most popular and prevalent scams, methods for safeguarding your personal information and much more.

Read it now, and save it for further reference. Here at your credit union, we want to help you maintain your peace of mind and financial security!

TABLE OF CONTENTS

An Ounce of Prevention

High Tech - Low Morals

Who Is This?

More You Oughta Know

AN OUNCE OF PREVENTION

E-STATEMENTS: SAFER THAN PAPER STATEMENTS?

With identity theft on everyone's minds these days, it's not hard to see why e-statements are something you might hesitate to sign up for. After all, cyberspace is kind of big and scary and full of shady characters, right? Who knows how many people could get their hands on your credit union statements if you opt for e-statements?

Actually, probably a lot less than the number of people who could get their hands on your paper statements.

Your paper statements can be lost, stolen or somehow accessed in a way that your e-statements cannot. When you're ready to dump them, paper statements should be shredded or destroyed in some other fashion. E-statements, on the other hand, really can't be accessed by anyone who doesn't have access to your service. Shredding is not a problem. Add in the ease of accessing them when you want to review or look something up, and you're better off with electronically delivered statements than a paper copy that could end up in the wrong hands.

KEEP YOUR SOCIAL SECURITY CARDS SECURE

Don't keep your Social Security card in your wallet. Many people do this and it is a huge mistake. If your wallet is stolen, the thief will have instant access to the most important identification you have. Instead, keep your Social Security card in a safe place at home, and commit the number to memory. Bring it with you only when absolutely necessary.

IDENTITY THEFT PREVENTION: SHREDDING

You know the importance of shredding junk mail and credit card offers. But have you thought about what might be in your own home that an identity thief could find useful?

Credit card bills, bank statements, canceled checks, receipts, credit reports, insurance policies, travel itineraries, used airline tickets, utility bills, credit and identification cards or badges, pay stubs … the list could go on but you probably get the idea. Anything that has your name and/or any other personally identifying piece of information could provide an opportunity if obtained and used by an identity thief.

Just like junk mail and credit card offers, household paperwork should be considered for shredding. Anything that expires should be immediately shredded. For everything else, don't shred the bill until your payment clears your account or until your receipt matches your bill.

Of course, not everything should be shredded. Keep anything with long-term implications, such as paperwork that is related to taxes, home improvements, business expenses, and marriage licenses, birth certificates, or receipts for large purchases.

One recommendation is to keep bills for at least a year and then annually determine what to shred and what to keep. If you have specific questions about what you should shred or keep, contact your accountant or financial advisor.

SECURE YOUR SOCIAL SECURITY NUMBER

One of the easiest ways to steal someone's identity is to steal their Social Security number, since it potentially links to a lot of other sensitive information about the individual. Hence, your Social Security number is the number one item to protect.

Don't carry your Social Security card in your wallet, and don't write the number on checks. If your Social Security number is used as your driver's license or insurance policy number, ask to have it changed. Also, never give out your Social Security number via phone or e-mail.

Sometimes it is necessary to give out your Social Security number. For example, your employer and financial institutions need it for wage and tax reporting purposes. Your Social Security number will also be needed by anyone who needs to do a credit check on you. However, many businesses just want your Social Security number for their general record keeping. Therefore, whenever someone asks for your Social Security number, ask them the following questions.

- *Why do you need my Social Security number?*
- *How will my Social Security number be used?*
- *How do you protect my Social Security number from being stolen?*
- *What will happen if I don't give you my Social Security number?*

You can then make an informed decision whether or not to share your Social Security number with the business. Remember, it's up to you.

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 too much 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.

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.*

HANDLE IT AT ONCE

There's an acronym for the correct handling of mail, so it doesn't clog up the house and important documents don't get lost in the muddle. OHIO stands for Only Handle It Once. In regard to identity theft, we're going to have to change that to HIAO: Handle It At Once.

Before dumping any mail that contains personal or financial information, shred it. Don't leave mail in your mailbox overnight, and don't let it pile up if you're going away for a weekend. You can call your local post office when you're going away and ask them to hold your mail for you. If you get very sensitive information, consider opening a PO box in your post office.

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 Web site 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.

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.

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?

- *Appoint a privacy officer in your company and invest in training.*
- *Develop a company privacy and data security policy, and put it in the employee handbook. Have each employee sign an acknowledgement.*
- *Conduct background checks on new hires.*
- *Go into all your employees' copies of Outlook and turn off Autocomplete.*
- *Consolidate all sensitive information onto a single server and password protect that server.*
- *Password-protect all sensitive files. These are any files that include personally identifiable personal, medical or financial information.*
- *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.*
- *Increase your company's liability and errors and omissions insurance coverage.*
- *Invest in a good shredder and ensure your employees use it. Identity thieves commonly go through trash to find sensitive information.*
- *Don't tolerate employees leaving valuables unsecured.*
- *Create a culture that emphasizes the value of confidentiality.*
- *Implement strict controls on the use of your company's credit and debit cards, as well as business checking accounts.*

- *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.*
- *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.

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 went 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.

FAX MACHINES

Planning to trash your fax machine or sell it on eBay? CBS News investigative reporter Pam Zekman has discovered some alarming reasons why you may want to reconsider.

With identity theft continuing to rise, it may not be all that surprising that even a seemingly innocuous fax machine may put you at risk. What Zekman found is that plain paper fax machines that use thermal carbon cartridges retain copies of all faxes the machine receives. Zekman reports that, upon purchasing two thermal fax machines on eBay, both cartridges were full of personal information, including addresses, Social Security numbers and financial account numbers.

"Beyond a shadow of a doubt, there's documents stored within all plain paper fax machines," says Intercon CEO Brian Brundage. Intercon Solutions, an electronic recycling firm, provides a safe means for disposing of your machine while protecting sensitive information. Upon receiving the machine, they break down the electrical equipment to its core material for recycling.

FAKE JOB LISTINGS

While you're searching online for that next job, someone else is posting fake job ads for the intention of obtaining your personal information … and yeah, that's identity theft.

Protect your identity from these fake job ads. Never include your Social Security number on your resume. The same is true for your driver's license number. If a company is interested in hiring you, it won't require that information until much later in the hiring process. The exception being jobs requiring a background check, such as for law enforcement and certain government agencies.

If you come across a job ad that interests you, research the company before applying. You can do this through the Better Business Bureau and the State Attorneys General websites. Both of these authorities keep files about U.S. companies and complaints. Also check out the company's own Website to validate its authenticity.

Verify the relationship between your contact and the employer. Is that person an employee or a third-party head-hunter? Does their e-mail address point to the company's Website address? Is the contact's phone number located in the same area code as the company's phone number?

If you think a job ad or contact's behavior is questionable, report it to the site where you found the ad, whether it is directly with the company or through an online job site.

ONLINE SAFETY

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

1. If your personal information – your name, email or home address, phone number, account numbers, or Social Security number is requested, make sure find out how it's going to be used and how it will be protected before you share it. Check for indicators that the site is secure such as a lock icon on the browser's status bar or a website URL https, the "s" stands for secure. Teach your children not to give out your last name, home address, or phone number on the Internet.
2. Read companies' security policies.
3. Don't respond to e-mails that are urgently asking you to update or validate your account information. Often such e-mails will direct you to a website that looks like the real one, but is really a fake. Don't click on the link. Rather, contact the company you are dealing with directly. Legitimate companies will not ask you for sensitive information via e-mail.
4. Protect your passwords, and be original in the passwords you use. They should not all be identical, and they should not reflect your user name.
5. Make sure to install and use antivirus and firewall protection
6. Use parental controls on your computer. Remember parental controls are a supplement but not a substitute for parental supervision.

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.

- *Store any bank and check information in a secure place. This includes checks, deposit slips, canceled checks and statements.*
- *Never leave bank information in your vehicle.*
- *Reconcile your bank statement when you receive it and be alert for any potential fraudulent activity.*
- *Unless it is needed for tax purposes, shred any canceled checks, statements, deposit slips and ATM receipts.*
- *Don't list your Social Security number, driver's license or telephone numbers on your checks.*
- *Use permanent blue ink to write your checks.*
- *When writing your checks, don't leave any spaces that could be changed, such as the payee or amount.*
- *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.

MEDICAL IDENTITY THEFT

You safeguard your financial information: your checkbook, your credit card, your Social Security number. But do you safeguard your health insurance information?

Medical identity theft happens when someone else uses your information to receive health benefits or reimbursements. This can impact not only your financial health but also your medical health.

Unfortunately, you may not be aware that someone is using your medical identity until you are denied coverage for a pre-existing medical condition you actually don't have. You might also receive bills that related to services you never received.

How can you prevent medical identity theft?

- *Ask for a copy of your medical records in case something is later changed.*
- *Ask your insurance company for an annual list of payments made for your medical care.*
- *Protect your insurance card.*
- *Ask if your doctor's office really needs your Social Security number.*
- *Review any "explanation of benefits" letters you receive from your insurance company.*
- *Review your credit report for any unpaid medical-related bills.*

If something related to your medical identity and health insurance doesn't make sense or seems out of the ordinary, call your insurance company immediately.

IDENTITY THEFT INSURANCE

You can buy insurance coverage for your car, your home, and your jewelry. But did you know you can also buy Identity Theft Insurance?

It won't protect you from becoming an identity theft victim, nor will it cover the loss of money that results from identity theft. What it will cover are expenses that are related to restoring your identity. This could include phone calls, copies, mailing costs, legal bills and lost wages while you resolve the issue.

Identity Theft Insurance coverage usually ranges from $20 to $100 each year. It can be added as a rider to a current homeowner's policy or purchased as a stand-alone policy. Before you purchase coverage, however, check on the deductible amount. It can range from the low hundreds into the thousands. Also, carefully read what the policy does and does not cover, since each insurance company differs.

Don't forget to check with your credit card company before buying an Identity Theft Insurance policy as well. Some credit card companies offer the same type of protection and coverage for free.

HIGH TECH - LOW MORALS

BETA BOTS, MALWARE AND SCAMS

"Do you want to allow the following program to make changes to this computer?" The message box, which is named "User Account Control," looks legitimate. It even boasts the "Microsoft Windows" name. However, one click of "yes" and you will have just given permission to allow "the Windows Command Processor" to modify your computer settings. While that doesn't sound like a problem, the program is a version of malware that will take over your computer.

This specific malware is known as "Beta Bot." Malware is software that comes in the form of worms, Trojans or viruses and takes over your computer to steal private information and create chaos. In the case of Beta Bot, the malware targets financial institutions, online payment platforms, social network sites and e-commerce sites with the goal of stealing your sensitive data to log in to such sites.

Additionally, Beta Bot blocks your computer from being able to go to websites that would otherwise provide security features. It even disables anti-virus programs on your computer. Beta Bot has also evolved since it was created and now can redirect you to specific websites instead of those with antivirus programs you are trying to download. Fake banking transactions, downloading files, and logging stolen data are all part of the chaos it creates.

The hard part is that sometimes the malware appears to be genuine software. Such is the case with Beta Bot and its use of the "Microsoft Windows" name. How then do you know if Beta Bot is trying to take over your computer when that message box pops up? Did you request the prompt to appear? Are you already making modifications to your system's configuration? Consider these questions when a message box such as this pops up. It may be safer to click "No" instead of "Yes."

It is also important to make sure your antivirus software is up-to-date and regularly run a full system scan on your computer. Also, make sure you run an anti-malware program and have firewalls in place. If you can't download the updates, consider putting the anti-virus updates on a USB drive and running it on the infected computer. And as always, keep tabs on your financial accounts to be on the lookout for any suspicious transactions.

BEYOND THE PASSWORD – WHY WE NEED BETTER COMPUTER SECURITY

There was, perhaps, a time when standard passwords were adequate security measures for most computer applications. Now is not that time.

Crooks are able to decipher passwords in many fashions. They use remote "sniffers" to record keystrokes. They cause you to download computer viruses that record your keystrokes or sniff out your password and cookie files before transmitting them back at their lairs. They look over your shoulder at cafes when you're logging in (123456789 is pretty easy to spot … as is "qwerty.")

In some cases, they can just guess. If your children's names are on Facebook, or your pet's names, those are often enough for them to pry into an account. The word "password" is a lousy password. "Password1" isn't much better.

In other cases, crooks can use "brute force" computer programs that will try tens of thousands of number and letter combinations in an effort to break into your account. Today's computers are more powerful than ever and some can break a standard password in mere minutes.

The stakes are higher than ever, too. Americans have more information hanging on a single password. One email address and password can get a hacker into your checking account, your retirement savings accounts, your Facebook and Twitter. If they get into one account, such as a PayPal account, they can then raid your PayPal, your bank or credit union account, and probably many other accounts. Throw in a PIN (it's not your birthday, is it?) and things can get pretty bad pretty quickly.

The financial services industry, including credit unions, is constantly looking for ways to make your financial information more secure, without making your account too difficult for you to access yourself. Security vs. access is a very difficult balance to strike, but it's one we must always consider and improve upon.

As we do so, here are some things that you can do to help ensure your safety:

- *Don't use the same account login or password on multiple accounts.*
- *Don't keep all your assets in a single account. Separate them and ensure they aren't linked, so if a thief were to gain access to one account, they cannot gain access to the others.*
- *Use long passwords rather than short ones.*
- *Use special characters and mix up upper-case and lower-case letters.*

- *Consider giving unguessable answers to security questions. Hackers can figure out what city you were born in. Unless you type in "ogre."*
- *Create a "utility" email account that you don't use publicly. This is the address you should give site operators to send password reset information. You might keep one email address for correspondence, for example, and one to receive financial and personal statements.*
- *Be careful about sharing email accounts with family members. Even spouses, children and parents have been known to abuse them.*

Ultimately, keeping your passwords and IDs safe is your responsibility. Banks and credit unions may not be responsible for losses if you are careless with your PIN or if you neglect to report a known security breach. If you believe your account has been compromised, notify your financial institution immediately. The faster you report it, the faster the damage can be limited.

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 who you don't see every day.

Scammers have recognized these sites as ideal places to strike. A Better Business Bureau report from March 27, 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 e-mail 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 e-mail and click the link, which directs you to a fake login site that looks like the Pinterest log in page. You log in with your user name 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 log in

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.

Also, 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.

You should 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 you your email inbox. You never know who might be on the other side.

IDENTITY THEFT AND TECHNOLOGY – INCLUDING SOCIAL MEDIA

A recent study put together by The Javelin Group has some disturbing findings: The incidence of identity theft was up 13 percent, 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 percent of social media users publicly shared their birthday.*
- *63 percent shared the name of their high school.*
- *18 percent shared their phone number.*
- *12 percent 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?

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

- *Keep documents that list Social Security numbers off of your laptop, or encrypt that data if you do store there.*
- *Keep private information private. If any company uses specific information about you to verify your identity – your mothers' 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?

Now a more popular way (according to Nielsen Online) to keep up with people than email, sites such as Facebook and Twitter are growing rapidly. Facebook has hundreds of millions of active users, and Twitter is also growing rapidly.

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 home page 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 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.

ONLINE SCAMS

Word is out about the 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 doesn'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, 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 (bank 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 often printed on the check*

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

- *The nature of the process ensures that 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 log in 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 traditional banking.

IDENTITY THEFT: STORING PASSWORDS

Once you have created your passwords for your online accounts, you need to find a way to easily and securely store these passwords. One thing you don't want to do is write passwords on a piece of paper and put it in your wallet, on your computer or even in your desk. If you do have passwords written down, put that list somewhere safe.

Another option is to put your passwords on a portable storage device you can take with you. This could be a CD, a zip disk, or a flash or thumb drive. Don't keep your password information directly on your computer, however, unless you have the files encrypted.

The "remember me" or "store password" feature found on many online sites makes it easy to log into your accounts without having to recall your password. If you are using a public computer, however, do not use this function as it can leave your accounts vulnerable to the next computer user.

An online search on "password manager" shows various programs and tools specializing in safely storing passwords. Before you use any of them, review the program's specifics to make sure it meets your needs and answers any further security concerns.

IDENTITY THEFT: CREATING PASSWORDS

Think of all the passwords you have to create. There are ones for your debit card, your computer, your voice mail and your many email accounts. Don't forget about the passwords for your online share draft account and numerous online credit card accounts. Each password is supposed to protect your personal information that, if in the wrong hands, could lead to identity theft. How can you create a password that will adequately protect your information and hopefully prevent an identity theft attempt?

- *Use letters, numbers and special characters in your passwords. For example, instead of "l" use "1" instead of "a" use "@" and instead of "s" use "$."*
- *Don't use information that is personal, such as Social Security numbers, names of spouses or children, birthday or anniversary dates.*
- *Don't use whole words.*
- *Don't use repeated or sequential letters and numbers.*
- *Use a different password for each account.*
- *Review each site's password requirements. Some require uppercase or lowercase passwords. Some even require a specific number of characters or numbers in passwords.*

These tips may require you to be a bit more creative when making your passwords but that might just be enough to prevent an identity theft attempt.

THE IMPORTANCE OF ANTIVIRUS SOFTWARE

Are you using antivirus software? There is a good chance that you are, because in today's environment, spam, viruses and hackers are rampant. And your computer is at risk … unless you are protected. Are you?

It's not enough to install your software once. Make sure it's up to date, and that it's actually protecting you. Update it regularly and scan your computer for issues every week-or more often.

Another thing to keep in mind is that not all antivirus software is created equal. Ask around, check out ratings, and see what's out there. An excellent pick is Trend Micro (www.trendmicro.com) which you can purchase online and download instantly.

HOW 'SPOOFING' CAN HAPPEN FROM LEGITIMATE WEBSITES

"Spoofing" refers to a website that claims to be a certain type of business or charity, when it is really a fictitious business that's out to gain a victim's credit card number or personal information.

Spoofing doesn't just happen from unsolicited emails, the growing crime of identity theft by spoofing can happen right from a website that you know and trust. How? Advertisers and links to third party sites try to pose as legitimate businesses. Sometimes the ads appear to be the original site you signed on to, and then you are prompted to fill in your information again. As you click on the ad, you are actually navigating away from the page and entering your information on the fraudulent site.

To avoid becoming a victim of a spoof site, always check the address bar when navigating around on links and advertisements. You can also view the web address of a link before actually clicking on it by right-clicking with your mouse on the link. If the web address is something different from the site you intended to go to, you can then be cautious about entering information. When in doubt – don't! You can enter the site directly by the known address and sign on there. If it's a website you are curious about, you can check the web address on www.betterbusinessbureau.com and do a little "background check" before doing business with the unfamiliar website.

PEER-TO-PEER SOFTWARE AND FILE SHARING

While you may just be using that Peer-to-Peer software (P2P) to share MP3 files with other computer users, cyber-criminals are searching to find access to your personal computer files through that software as well. Once P2P is downloaded, it allows for file sharing between users. These files can include music, movies, and software. Napster is an example of P2P software as well as Limewire, Morpheus, Gnutella, Gnutella2 and BitTorrent.

While the P2P software should only give access to designated files, it can give access to all the files on your computer. Cyber-criminals are searching online for this open access to your computer files, which can include bank records, health records, tax files, passwords, and any other personal information you store on your computer. The searches are done using terms that might be found in those files, such as "credit card," "password," and even "stop payment."

Once your file with personal information is found through P2P access, that cyber-criminal has found a new identity to steal and use. If you have P2P software installed, review the installation and configuration of the software to make sure you know what files are being shared through the software. Another option is to have separate computers; one for your personal information and another solely for P2P software and file sharing. If that is not possible, you can also look into encryption programs for your personal information. If you aren't sure if you have P2P software downloaded, review your computer's programs and do any online searches of unfamiliar program titles. It is important to make sure any necessary P2P software is working properly to protect you from identity theft attempts.

NEW ONLINE SCAMS: PHOTO SHARING, PHONY WEBSITES, AND ESCROW SERVICES

The Federal Trade Commission is alerting the public about a new scam that uses photo sharing to infect computers with harmful malware.

In the latest variation, a stranger will advertise something for sale on a website – a car for example. They don't offer any pictures on the original ad, but say they will send pictures on request.

When you email the advertiser requesting more information, they will reply and attach a file that they tell you is a photograph. But when you open the file, it actually contains a virus or other malware that infects your computer.

In another variation of the same scam, con artists send a link to a dummy website that looks like the first website – except its 100 percent run by the perpetrators. They may have you use an "escrow service" and lead you to believe that the service is run by Craigslist, Backpage or whatever other website you were using originally. They also run the tech support line and everything else about the dummy site. You send your money to the escrow service and they are supposed to hold the money until you confirm delivery of whatever they were selling. But in the scam, the escrow service doesn't exist. Instead, your money is gone, you never receive the goods or services, and you never hear from them again. You will have a very hard time recovering any money that you send to these scam artists. You will also generally not have any recourse against the original legitimate website.

In yet another variation, the scammer will run an online auction. You will lose the auction, but the scammer will contact you and say the original purchaser fell through and ask if you would still like to make the purchase.

Don't worry, he's contacting everybody. And anyone who sends him money will be stung by the scam.

TO PROTECT YOURSELF, FOLLOW THESE TIPS:

- *Check URLs carefully, and do not click links these advertisers send you via email. Type them in yourself.*
- *Use only well-established escrow services that you can independently verify.*
- *Beware of sham car dealerships selling cars online for prices that are too low to be believable. Always check out the dealership independently to ensure it is reputable and established.*

- *Update your anti-virus software, and scan emails before downloading any attachments.*
- *If you believe you have been targeted by Internet scammers, report them at www.ic3.gov, the Federal Trade Commission's anti-scamming site.*

TARGET DATA BREACH: WHAT YOU NEED TO WATCH OUT FOR NOW

Scammers are an opportunistic lot. The schemes and ploys to get your money and identity over the Internet are always evolving and responding to real-life occurrences. It's part of why they're so successful; the people behind them use every kind of trick they can to convince you they're someone you can trust with your personal information.

It's no surprise, then, that Target's data breach and ensuing customer correspondence created a number of rip-off spoofs. Target's data breach has left consumers feeling exposed and vulnerable, and uncertain of whom to trust. Regardless of what appearance a potential scam takes, there are a few questions to ask yourself any time you receive an unsolicited email asking for your personal information.

1. **Do you recognize the email address?**

   A lot of scammers make their money on their victims' lack of attention to detail. It's remarkably easy to get an email address like "target.co" which, on first glance, might appear to be genuine. Common email user names can also be easily spoofed, so look for emails from user names like "abuse" or "security." When in doubt, you can always go to the company's website and look for a link like "contact us." Comment or email the company and inquire to find out what email addresses they use to contact customers. It may take a few days to get a response, but no company ever minds your help in catching people who are using their good name to defraud customers.

2. **Does this look like the kind of content a company like the one that's contacting you would produce?**

   Target is a multimillion-dollar and multinational corporation. The emails it sends to customers are going to be, at the very least, spell-checked, and probably use official logos, slogans, and other images wherever possible. They're also likely going to be digitally signed by a real person who will likely have at least some online presence. Remember, for companies, emails like this are a tool of advertising as much as they are a way to communicate. Look for grammar, spelling, and punctuation errors, blurry or otherwise unprofessional looking images, and vague or unnamed signatures. All of these are sure-fire ways to spot fraudsters.

3. **Is the information that's being requested necessary?**

Target did, in fact, offer a year of free credit monitoring to help people who may have been exposed to fraud by their data breach. In order to obtain it, you need to obtain an access code for a 3rd party credit monitoring website. At no point does anyone with legitimate business interests benefit from being emailed your credit card number, Social Security number, or account number. If you are asked to provide any of this information in an email, you are looking at a scam. The service that Target is offering is also free, so there is no need to give them your credit card number. Moreover, anyone who requests your credit card number without a secure web form is probably attempting to steal it. You can recognize secure web forms by the prefix HTTPS (as opposed to "HTTP") before the web address.

4. **Does the offer sound too good to be true?**

This is what makes the Target scam so dangerous. The retailer did make a mistake with your data and is therefore offering something for nothing to make it right. In general, though, anyone who offers you a significant amount of money in exchange for a trivial or insignificant service is likely trying to trick you. The scam works because your brain focuses so heavily on the reward that you stop critically evaluating the risk. This is also why scammers will push fantastic rewards with short time frames. Human beings tend to make poor decisions when forced to do so impulsively, and scammers know this. That's why they want you to act now, before you've had a chance to do your research. Legitimate offers will never come with very short time frames.

5. **Do I need the service that Target is offering?**

If your credit union or credit card company has already issued you a new card, chances are you're safe. You should keep an eye on your statement for the next several months to watch for unauthorized charges, and dispute them quickly. You can also get a free 3-bureau credit report once per year from www.annualcreditreport.com. You will have to provide some personal information and answer a few questions about your background for identity verification, but seeing this report will let you know if new accounts have been opened in your name. Your credit union may also offer a variety of financial monitoring instruments, and speaking with a representative there can help make sure they know to watch out for suspicious activity on your account.

It's natural to feel uncomfortable after finding out your personal data has landed in someone else's hands. Don't let that feeling trick you into making poor financial decisions. Practice the same online safety procedures you always do and be skeptical of everyone who wants your personal information. No one who wants to do legitimate business with you will be upset or angry if you want verification that they are who they say they are. Stay vigilant, and stay safe!

SMARTPHONES AND IDENTITY THEFT

The Washington Post ran a story about mobile phones, such as the BlackBerry and Palm Treo, 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 www.WirelessRecycling.com for instructions on how to delete what's there. Once on the site, click on online tools/cellphone data eraser.

STOLEN CELLPHONE

Recently, 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 whom 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 just released a report on a new trend in crime. According to the report, 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 have made it even easier for thieves to sell stolen hardware. Demand for smartphones in the booming second hand 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 reselling 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 new 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 ear buds 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 this week which would require every smartphone in the US 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 and 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 ear buds 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. In fact, the directors of the Thrift Savings Program – a popular defined contribution benefit plan for federal employees and military members – recently posted an alert on its website:

There are a number of mobile applications that reference the Thrift Savings Plan and may prompt you for your TSP account credentials. These applications are NOT sponsored by the TSP. The TSP cannot endorse any information or advice provided by third-party applications. More important, providing your TSP account credentials to third-party applications may jeopardize the security of your account.

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 number. 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 county. 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.

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:

1. *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.*
2. *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.*
3. *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.*
4. *Be cautious about the services you subscribe to.*
5. *Be wary of urgent messages that request personal information.*
6. *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.

WHO IS THIS?

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, DC area code (202, most commonly). If you don't answer, you can expect them to leave a voice mail 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 e-mails 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 e-mails will almost always come from e-mail 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 US 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 e-mail, you can forward it to phishing@irs.gov. You can also file a report with the Federal Trade Commission at ftc.gov/complaint.

EMAILS AND PHONE CALLS FROM UTILITY PROVIDERS

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 is happening to customers in Pennsylvania, Texas, Oregon, Florida, and Oklahoma. It 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.

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 indicated 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.

IDENTITY THEFT RELATIONSHIP SCAMMERS

While dating sites are a legitimate way to meet people, there are scams you need to be aware of.

A common scam is the use of military photos and profiles to attract upstanding women who are seeking reliable boyfriends. The scammers give the women a false sense of security by wooing them with phone calls, presents and poems. Once the women feel special, requests for small amounts of money start. The women are first asked for a few hundred dollars for medical bills, or to pay for their "boyfriend" to visit them. Once the women start sending money, the requests increase in size until some women have lost significant amounts of money. Some of the women have even become engaged and sent money to pay for weddings and rings. Many of these scammers are believed to be based overseas.

Men have also been drawn in by third world women seeking boyfriends in the West. Men from the USA, the UK and Germany have all been scammed this way. Once the men have fallen in love with the beautiful women, often receiving pictures of the "family" and loving phone calls, they are asked for small amounts of money to pay for medical emergencies or similar expenses. Then they are asked to send money for a plane ticket, with the expectation that their fianc'e or girlfriend is flying over to meet them. Many men have stood in airport lounges, wondering where their money has gone.

The bottom line is, be cautious when using a dating site. It may be a good idea to never get involved financially until you've actually met the person.

HEALTH INSURANCE SCAMS

There's a lot of confusion these days. As the federal government moves toward the implementation of the Affordable Care Act (or "Obamacare," in common parlance), consumers are looking everywhere they can for information or advice concerning their health insurance.

Unfortunately, this makes them vulnerable to sales pitches from health insurance scam artists. 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.

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

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 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

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 www.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:

Experian – 1-888-397-3742 P.O. Box 9556 Allen, TX 75013	Equifax – 1-800-685-1111 P.O. Box 740241 Atlanta, GA 30374-0241	TransUnion – 1-800-916-8800 Trans Union Consumer Relations P.O. Box 2000 Chester, PA 19022-2000

THE PAYDAY LOAN COLLECTION SCAM

Scammers have become increasingly bold of late, evolving from telephone or Internet-only scams to showing up at the victim's home or workplace, demanding money to repay a debt you don't owe.

Typically, the victim receives a phone call from someone claiming the victim is behind on a payday loan or check advance loan. The caller tells the victim to pay immediately or face legal consequences.

The callers may represent that they are with the FBI, or the Federal Legislative Department or other official-sounding agencies. Or they may claim to be with a law firm, that's collecting on behalf of major payday lenders.

The con men will repeatedly call the victim at work and home. They refuse to provide further information about the loan, and may become agitated or abusive when questioned or challenged on the phone.

In at least two cases, the scammer turned up at the victim's place of employment, pretending to be a process server, serving notice to appear in court unless the victim handed over money.

In one variation of this scam, the caller claims that there are outstanding warrants for the victim's arrest, either for nonpayment of the fraudulent debt, or for hacking. In both cases, the caller presses the victim to pay a fine online to clear the record and cancel the warrant.

If someone targets you and demands that you pay a debt you don't owe, here's what you can do:

- *Contact your credit union, banks and credit card companies.*
- *Contact local law enforcement if you feel you are in danger.*
- *Contact the three major credit bureaus and request an alert be put on your file.*
- *If you have received a legitimate loan and want to verify that you do not have any outstanding obligation, contact the loan company directly.*
- *File a complaint at www.IC3.gov*

To prevent being a victim, keep close tabs on your credit report. You can review a free copy of your credit report once per year by visiting www.annualcreditreport.com, or by calling 1-877-322-8228. Know what you owe and to whom! That way, no scammer can take you by surprise, or convince you via fraud that you owe money when you don't.

BEWARE OF MILITARY-RELATED ROMANCE SCAMS

Con men have been preying on lonely hearts since ancient times. But today, the Internet makes it much easier – you don't even have to act. The U.S. Army's Criminal Investigations Division is warning that some of these crooks are taking advantage of Americans' sympathy and support for our troops abroad to separate lonely women from their money.

Even this has been going on for years. Here's how the scam works: A con man puts up a profile or answers a woman's profile on a dating website. Over the course of a few emails (he's almost never available on the phone or via Skype), he lets you know he's an American, serving in Afghanistan or on a Navy ship or embassy post.

Some days or weeks go by and you chat or email nearly every day as you grow closer and closer to your correspondent. When the con man thinks you have fallen in love, he'll let it slip that he has some leave time coming – and says he wants to visit. You get excited. But as the long-anticipated day approaches, he springs a trap: He's trying to get out of Afghanistan or some other country, but customs won't let him out unless he pays a transfer tax of thousands of dollars. But he can't access his bank account from where he is. He begs you to wire the money via Western Union to his bank account so he can come to see you.

In some cases, they will send you a form on ostensibly military stationery. The form often has basic English spelling and grammar mistakes.

Most people would smell trouble at that point. Unfortunately, some don't.

One report found that romance scams sting Americans for as much as $100 million per year. The average victim loses over $5,000 per incident before she wises up. These figures are almost certainly under reported, since victims feel a great deal of embarrassment, on top of dashed hopes and heartbreak.

Yes, there are many honorable men and women in the military, and they do on occasion use dating sites. But the scammers are out there too. Here is how to spot fraudsters:

- *They send you a leave application or deposit form with basic spelling or usage errors.*
- *The forms are in an amateurish font, such as Comic Sans.*
- *They ask you to send any money by Western Union.*
- *They ask you to send money, period.*
- *They can never meet with Skype or speak on the phone.*

- *They are traveling through Ghana, Nigeria or any other African country.*
- *They can't or won't write you from an email address that ends in ".mil" rather than ".com."*
- *The unit doesn't turn up in a Web search, or if it exists, the unit is not deployed where your "friend" says it is.*

To protect yourself, share some of the correspondence with a veteran you know – preferably of the same service. A scam that is tough for a civilian with no military experience to spot may be obvious to someone who knows how the military works.

You can also visit online resources such as RomanceScams.org. Victims and near-victims share their experiences there and you can compare notes. If you do get scammed out of money, you can file a report with the Federal Trade Commission (FTC.gov), though it is very difficult to collect damages from abroad once you get stung.

THE RENTING FORECLOSURES SCAM

The collapse of the housing market has bought about a new scam, as thousands of foreclosure houses now lie unoccupied. A criminal will find a likely house and call a locksmith, stating that they have locked themselves out. Once they are in the house, they change the locks so they now have control of the house. The next step is to put up a "For Lease" sign outside, which rarely attracts suspicion from the neighbors in the current housing meltdown.

The scammers advertise it for lease or rent on Craigslist. Unsuspecting tenants are shown around the house and quoted a low rent, because the owner is "desperate to get rid of" the house. The criminal takes a deposit from the unsuspecting viewer, then hands them a bogus lease and a set of keys.

From there, the scam then goes one of two ways: either they continue to show the house and take deposits in exchange for keys, leases and a move-in dates over a couple weeks time; or they let the unsuspecting tenant take occupation of the house 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 wanting to know why they are living in the house.

Either way, the tenant has lost many hundreds of dollars and is without somewhere to live or any way to contact their "landlord".

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.

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."

IDENTITY THEFT: GHOSTING AND PREVENTION

"Ghosting" is identity theft committed against a deceased person. But 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, Trans Union, 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.

THE FACEBOOK SPANISH GRANDMA SCAM

Be careful what you post online. There's no end to the number of variations on cons and scams that criminals can concoct to separate the vulnerable from their money. One recent scam that has already stung a number of people is The Spanish Grandma Scam. Here's how it works:

Con men will gather data from your Facebook profile – and other online sources – to learn as much about you as they can. They will build a dossier – mapping out your known family connections, such as vacations together, and try to get to know you as much as possible.

Once that's done, they will contact an elderly relative, pretending to be you. Here's the story: They tell your grandmother that you were vacationing in Spain, and you hit a telephone pole with your car, and they arrested you. You need grandma to wire $2,000 immediately so you can get out of jail.

If grandma's not sure about their identity, they start peppering her with personal information she thinks no one but you would know: Your visits to her house, information about your parents, your aunts, uncles, anything. Eventually, grandma relents and wires the money. They'll also get her to swear not to tell anyone – you'll just pay her back as soon as you get home. That stops her from calling your parents and finding out you never left.

But the scam doesn't stop there: If grandma's convinced, they will call her again. This time, the judge is forcing you to make restitution for the cost of the telephone pole. Another $1,746.73, or some other oddly specific number. And then they'll call again, a day later, again posing as you, and claiming to be at the airport, where Spanish customs officials are refusing to let you leave the country unless she wires another $1,577. And so on until grandma either says she doesn't have the money or catches on to the scam.

To protect yourself, watch what you put on Facebook and elsewhere on the Internet. Alert your grandmother and other family members to the scam. And once you've alerted them, don't hit any telephone poles while on a trip to Spain!

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.*

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.

MORE YOU OUGHTA KNOW

OBAMACARE: BE AWARE OF FRAUDS AND SCAMS

While you are working to understand the Affordable Healthcare Act, also known as Obamacare, and its implications for your family, scammers and con artists are also working hard. They are working hard to gather your personal information and use it for their benefit. Obamacare scams have occurred over the phone, through emails and fake websites, perpetrated by con artists posing as government employees and Obamacare "navigators." How can you be on guard while you also navigate what Obamacare means for you and your family?

The most important aspect to prevent fraud that's related to Obamacare scams is to understand the law. The more you understand, the less scam artists can feed off your fear or lack of understanding. For example, current scams using fear include: "Sign up now. There are only 20 spots remaining" or, "If you don't buy it, you could go to jail." Neither are accurate depictions of the law. The number of spots in Obamacare is not limited and the penalty for not having healthcare is only $95 for the first year.

Estimates suggests that over 700 fake or misleading Obamacare websites exist on the Internet. However, the only legitimate website to find state and federal exchanges is www.HealthCare.gov . Even if the other fake websites don't steal your personal information, they could corrupt your computer with malware.

Don't give your personal information to random callers; this includes account information, Social Security numbers or even agreeing to wire money or buy prepaid cards. Any cold calls or emails should be considered fraudulent and reported to authorities. Additionally, any counselors or navigators who are working with Obamacare won't charge a fee for their help. If someone offers to help you, even for a small fee, assume it is a scam. Just as an official website exists, the official number for questions about Obamacare is 1-800-318-2596.

If you are on the receiving end of suspected fraud or scams related to Obamacare, contact the Federal Trade Commission (FTC). If a business is involved, contact the Better Business Bureau (BBB) as well. And if you have given out personal information and later realize it is a fraud related scam, contact your credit union and the three major credit bureaus so you can watch for future suspicious activity on your account.

ID THEFT: CATFISHING

A college football star became involved in it. An MTV show revolves around it. A documentary made its name known. Catfishing: where someone uses an online scam, hoax, assumes a fake identity or borrows a real identity to make you think they are someone else.

Whether catfishing is illegal depends upon why the scam was done and where. For example, in Washington state, Texas, New York and California, it is a crime to pretend to be someone else while online. In California, you also have to show intent to harm, intimidate, threaten or defraud. Crimes committed through catfishing can include profiting off of a disaster, luring children or any other illegal purpose.

Anyone with a legitimate online presence can be susceptible to catfishing. While this may be a scary thought, you can protect yourself from becoming a catfishing victim. Start by arming yourself with information:

- *Do you know your local and state laws regarding social media? Do you know the privacy policies of the social media websites that you use?*
- *If any of these laws or policies is violated, know how to report them to the appropriate officials or representatives?*
- *Do you have a social media account, including but not limited to Facebook, Twitter, LinkedIn? What personal information do you disclose on those networks? Does that information really need to be available online? What are your privacy settings on these accounts?*
- *What do you find if you Google your own name? This isn't about being vain but seeing what shows up in results: pictures, videos, location, employer, bio or any other personal information. Does the information you find make sense to you? Is your picture identified as someone else? If you can Google it and find it, so can anyone else. One way to monitor this more easily is to set up free Google Alerts to email you whenever your name shows up online.*
- *Be aware of your online contacts. Don't blindly trust online interactions with strangers.*

Most importantly, think about the information you are sharing online. Would you share that information with a stranger in a checkout line at the grocery store? Would you really want a friend of a friend of a friend, who is really a stranger to you, to know your information? In order to protect yourself from being a catfishing victim, be proactive in your online presence.

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!

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 associates, 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.

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.

PHISHING

Long ago, identity thieves had a harder time of it. They had to actually steal something like your wallet to get your information. A sophisticated identity thief in the 21st century will try phishing. That's phishing, not fishing, but the victims are caught on a hook just as surely as if they were a hapless fish in the lake. Yet, if the fish knew what lay beyond the juicy worm on the hook, they wouldn't get caught either. To avoid phishing, you have to be informed.

Phishing is defined as the act of sending an e-mail that impersonates a legitimate company or organization. The e-mail address is often very close to the real corporate e-mail, except for a few minor URL differences. In this e-mail, the sender falsely claims to be representing an established, legitimate organization. Posing as the legitimate company, the e-mail directs the user to a website where he will be asked to immediately "update" or "verify" personal information. The user is usually told there is a problem with his account, or warned of possible account fraud. He might be asked to provide credit card, Social Security, or bank account numbers that the real organization already maintains. Though the website might be set up to look just like the real thing, it is in fact bogus. Before he knows it, his identity is stolen.

You don't have to be a computer programmer to avoid phishing. You just have to use your common sense and stay up-to-date. Here are just a few tips:

- *Treat any unsolicited e-mail requesting personal/financial information as guilty until proven innocent. Most major companies will not ask for sensitive information in an e-mail. Don't reply or click on the link. If you have reason to believe it is legitimate, contact the organization itself via phone or a website that you know is real. Don't use the phone number provided in the e-mail.*
- *Don't enter a website via an e-mail link, rather type the address in the address bar.*
- *Use different passwords on different websites. If you believe you might not be on the actual site, try typing in a fake ID and password. The real site wouldn't let you through, the phishing site will.*
- *Review your account statements frequently.*
- *Make sure to read the privacy policy of any website before giving them your information and check that they have secure data encryption. What to look for is a closed lock on the bottom right of the browser window, not the web page. Double clicking on the lock will reveal the company's security certificate. The name on the address bar and the certificate should match. If they don't, you know the page is a fraud. Your other clue is the https:// in the URL vs. the common http://. The 's' stands for secure.*

- *Maintain up-to-date anti-virus, anti-spyware and firewall protection software. Some software comes with anti phishing protection that can determine whether a website is legitimate.*
- *Block pop-ups. You can never be too careful.*

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.

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 mush 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!

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.

IDENTITY THEFT: FRAUDULENT CHARITIES AND NATURAL DISASTERS

Whenever a natural disaster happens, a scam will surely follow – usually said to be collecting donations for a charity that doesn't exist. While you may feel generous to help with the efforts, you do need to be wise and make sure your donations are truly helping the victims.

One of the ways fraudulent charities request donations is through e-mails that are really phishing scams trying to get your personal information. When you receive an e-mail asking for a donation, read it carefully and ask yourself some questions. Did I agree to be on this organization's mailing list? Have I supported this organization before?

Even if you are familiar with the charity, don't click on any website links or use the phone number that's provided in the e-mail. Instead, search online for the organization's website and contact information. Then, you can review the charity's site and learn how it uses donations. You might also contact the charity directly.

You can also use the Internet to research current scams that are related to natural disasters. Additionally, it is important to apply these same precautions to any donation requests or posts on Facebook or Twitter.

AVOIDING CHRISTMAS CHARITY SCAMS

It's the season of giving – and for criminals it is the season of 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?

1. **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.
2. **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.
3. **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.
4. **DON'T GIVE ON THE STREET.** Many street collectors are scammers. You're okay 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.
5. **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.
6. **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.
7. **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.

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 stockbroker 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, www.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.

BEWARE OF UNLICENSED CONTRACTORS

It happens all too often – someone with a pickup truck and a smile will knock on your door, mention something at your house that needs work, and will offer to do it at a cost that seems almost too good to be true.

Frequently, they'll tell you they were working in the area anyway, which is part of why the job will be so cheap. But it pays to do a bit of research. Here's why:

LIABILITY. Legitimate businesses carry two kinds of insurance that protects both themselves and you, the customer:

- ***LIABILITY INSURANCE***. *If the contractor or his employees cause damage to your property, or a neighbor's property, they will generally carry insurance or have posted a bond to ensure that they can make good on any damages. Sure, you can file a lawsuit and maybe win a judgment. But having a judgment and collecting on it are two different things. A licensed contractor will generally have enough insurance coverage to ensure you will be made whole in case of any kind of claim.*
- ***WORKERS COMPENSATION***. *Unlicensed contractors typically don't provide worker's compensation coverage to their workers. Most states require this coverage, which covers any medical costs incurred by workers injured on the job, as well as some disability benefits. If a worker gets injured on the job, and this insurance isn't in place, that worker could sue both the employer and you, the property owner, for damages.*

JAIL TIME. It's true: In some jurisdictions, using unlicensed contractors not only jeopardizes your own finances – it's actually a crime.

SCAMS. Most unlicensed contractors mean to actually do the work. But one common scam goes like this: The scammer will begin work, then ask you for money "to go buy materials." Then you give the contractor the money, and you never see them again. Or there may be an injury, for which you as the property owner are expected to provide compensation. The injury could be legit … or it could be part of the scam.

Worse yet, unscrupulous contractors could begin work, tear your roof open, for example, and then demand much more money than agreed upon to close the roof back up again. Had you used a legitimate contractor, you would have recourse to your state licensing boards for unethical work or breaches of contract. Legitimate contractors don't want to lose their license, and so will work very hard to satisfy you as a customer to prevent racking up a track record of complaints.

How to Avoid Them

The simplest thing to do is ask for their license number. If they can't give it to you, or claim to be "working under someone else's license," then don't let them touch a thing.

Also, ensure the contractor gets a permit for any construction projects or anything that involves digging. Legitimate contractors will normally arrange for the permits themselves. If they ask you to get the permit, consider that a red flag. It may be they are no longer welcome at the permit office – or they don't have the cash to get a permit. Either way, it doesn't bode well.

The Bottom Line

Using licensed contractors is a smart move in a variety of ways: It encourages and supports the legitimate, law-abiding businesses in your community. You can generally expect a better quality of work. It encourages employment in your community, as unlicensed contractors are more prone to hire illegal workers. And it protects you against unwanted liability when things don't go as planned.

DOOR-TO-DOOR SCAMS

You hear a knock on your door. You aren't expecting anyone. You open the door to find someone trying to sell you something. While that salesperson may seem polite, honest and legitimate, he or she could be trying to steal your identity along with your money.

When a "random" person knocks on your door, common sense dictates that you don't let them enter your home and that you don't answer the door at night. Even if you do answer the door, you don't have to talk to them; you can simply ask them to leave.

If the salesperson and the item for sale seems legitimate and you're interested, ask for a business card or a brochure to review over the next couple of days or to share with your spouse before making a decision.

After you have that business card or brochure, research the product and company. You can research online and/or call your local township, city or county offices to make sure this person and company can legally sell door-to-door.

Of utmost importance: Do not give any cash, checks or credit card information to the salesperson while he or she is at your door. Also don't fill out any "request for information" forms. Once you do this, the salesperson may sell your information to others, resulting in you being bombarded with junk mail and other annoying solicitations.

If you are concerned about a door-to-door person that might be fraudulent, contact your local police department.

PYRAMID SCHEME INVOLVING LICENSE PLATE NUMBERS

In 2010, a new scam was introduced as an "opportunity" – collecting your neighbor's license plate numbers. This was mostly championed by two companies, Narc Technologies, Inc. (now known as Crowd Sourcing International) who want to use the database to help the law enforcement agencies with auto repossession, and Data Network Affiliates who want to help underprivileged children.

After paying an upfront fee, and in some cases, being charged monthly, participants are paid a few dollars for basic number plate collection. The real money comes in when they recruit family, friends and, presumably, neighbors to join. It's a typical MLM (multi-level marketing scheme) structure, and the Better Business Bureau has received countless complaints about these companies. The only one who profits from this setup is the company, collecting a small fortune in setup fees from those who hope to make money from the deal. Lessons learned: if it sounds too good to be true, it usually is. Do your research, ask around, and don't part with a single dollar bill-and certainly not with your personal information-unless you verify that it's a legitimate firm. One of these companies signed up over 90,000 "associates" in just three months, so the hype is there. Don't fall for it.

‘GREEN DOT’ CARDS ARE CONVENIENT – BUT BEWARE OF SCAMS

You’ve probably seen “Green Dot” pre-paid debit cards at outlets like Walmart and CVS. You can buy a card worth, say, $50, and use it anywhere that takes credit cards. The “off the rack” cards are not rechargeable. But you can get a permanent card that you can recharge – for a fee, of course.

These cards are not good substitutes for a regular checking account at a good credit union – or even at a higher-fee bank. The ongoing fees for recharging your card – up to $4.95, compared to free direct deposits and online transfers at most traditional financial institutions – can really add up if you use these often. But in some circumstances, they come in handy for convenient gifts. Some people also use them for online purchases – to conceal their real credit card numbers from possible scammers.

All financial products have their place. Unfortunately, scammers are targeting the unwary – and dragging Green Dot and other similar services into the crime.

The Power Bill Scam

One scam goes like this: The unsuspecting victim receives a call from someone claiming to be from the local power company. The scammer tells them that the power is about to be shut off. To avoid the shut-off, they’re instructed to buy a pre-paid Green Dot card, and then call another number to pay online.

The utility companies have nothing to do with this. The scammer is long gone with the money – and you won’t get any credit for payment on your power bill!

The Bogus Grant Scam

Another scam uses a powerful lure, according to Scambusters.org – a website devoted to exposing frauds and scams. The mark receives a check in the mail-often for thousands of dollars-along with a letter informing them that they’ve received a grant. They frequently camouflage themselves as government agencies or religious organizations. The letter instructs them to deposit the check, and then transfer a “finder’s fee” to a Green Dot account. The mark deposits the check, sends money back to the scammer, who, naturally, disappears. Meanwhile, the check bounces, and the victim is out whatever he sent to the scammer – with a returned check fee for good measure.

The bottom line: Use caution whenever you send money to anyone you know. Do your homework. And you know what they say about things that sound too good to be true.

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.,