Some Current Scams

1. **The Nigerian Scam**
2. **Fake Calls from Government Agencies**
3. **They Want Your Number**
4. **Buyer Beware**
5. **Job Search Scams**
6. **The Grandmother Scam**
7. **Cramming**
8. **Credit Card Wireless Skimming**
9. **IRS-Impersonation Telephone Scam**
10. **The “Ring and Run”scam**
11. **Webcam spies**
12. **Contractor Scams**
13. **Microsoft Technical Support Scam**
14. **Hostageware or Ransomware**
15. **Purchase Confirmation Scams**
16. **Credit Card & Debit Card Skimming**
17. **Credit Card Support Scams**
18. **Caller ID Spoofing**
19. **Phony Charities**
20. **Phony Sweepstakes Giveaways**
21. **College Students Work Scams**

The Nigerian Scam

One of the most enduring scams is the so-called "Nigerian" or "419" scam; named for the country where it originated.

There are many variations on this scam, but they all basically follow the same pattern below:

How to spot this scam:

- You receive an e-mail from a person, or someone claiming to be a representative of someone has inherited a very large sum of money.
- You may even receive a check in the mail for a large amount of money in which you are instructed to keep a large portion of it and to send a small percentage after depositing it in your bank account.
- A legal obstacle exists which does not allow the person from receiving the money directly.
- The correspondence offers to make you wealthy if you assist in processing the beneficiary's new found wealth through your own bank account.
- The request instructs you to send a small amount of money (it could be several thousand dollars in bribe money) to foreign government officials in order to release the funds.
  - In exchange for your assistance, you are promised millions.
  - One variation of the scam is a claim that you have won a large sum in a lottery (that you never entered).

What to do if you receive a Nigerian Scam e-mail or phone text message:

- Do not send money – it is a scam.
- Do not cash any unsolicited checks – you will be responsible for the funds when the check is found to come from an empty or non-existent account.
- Do not respond to the e-mail or provide any personal information.
- Never provide social security number, credit or debit card, bank account or routing information to anyone unless you know who you are speaking with and you initiated the call.
- Contact http://www.ic3.gov , or https://www.ftccomplaintassistant.gov/#crnt&panel1-1 and file a complaint.

Fake Calls from Government Agencies

One of the most recent ongoing scams is one in which telephone scam artists call and pretending to be with and agency that many people seem to fear, the Internal Revenue Service (IRS). The caller might also claim to be with the police, FBI, or other government agency.

The caller might say that you either owe them money or that you have a refund due from them, or have an outstanding warrant, etc. in an effort to trick you into divulging personal information. These crooks can sound very convincing and can be very intimidating on the phone.

And, they may even know some information about you, and can "spoof" or alter the caller ID to make it look like the IRS, or other government agency is calling you. The scammers may also use fake names and fake badge numbers. If you don't answer, they might leave an "urgent" callback demand.
These telephone scams are being reported throughout the country.

How to Spot the Scam

- The caller demands immediate payment and might ask for a credit card number or debit card number, or may ask for your social security number, date of birth, etc...
- The IRS will not call you without first having mailed you official correspondence.
- Someone who claims to be a law enforcement officer who will not give you the opportunity to verify who they are.
- They threaten to have the police or other law-enforcement agency have you arrested for not paying or giving them information demanded.
- http://www.fbi.gov/news/pressrel/press-releases/internet-alert-scammers-sending-fake-fbi-e-mails-seeking-personal-information

How to Protect Yourself:

- Tell the caller that you will speak with them once you are able to verify who they are.
- If they attempt to pressure you for information – hang up.
- Do not contact the phone number or internet address given to you by the caller.
- Call the phone number listed in the phone book or on the internet for that agency.
- Do not give the caller any personal information.
- Report the call to your local police or to http://www.ic3.gov .

They Want Your Number

We have all been told repeatedly not to give out our credit card, debit card or social security number, but there are other numbers that scammers are after as well.

Your **date of birth**, along with other personal information such as place of birth, schools attended, etc. can be used to create a new identity for a criminal – yours.

Your **social security number** is used for financial transactions, by banks, the internal revenue service and the social security administration to identify you and benefits that you are accumulating. However, way too many other institutions ask for your social security number when they have no legitimate reason to know it. Guard it carefully or you may find someone else enjoying your social security retirement checks.

Health insurance account numbers may not seem very important until you realize how much your premiums cost and how important they are when medical care is needed. It is estimated that health care fraud costs the US tens of billions of dollars each year. Another factor to consider is the potential health risks to you if someone else is using your account and medical information; you may be given the wrong medication or treatment.

Many of us rely on **PIN codes** to enable us to use our debit cards, some credit cards, and more. Unfortunately many of us use the same number combination for everything, which makes it much simpler for hackers and thieves.

Your **bank account number** helps you to access money you may have in a bank or credit union. Unfortunately, if you are still using paper checks, this information is printed right on the front along with the routing number for that account.

Your **drivers license number** can be used to create a duplicate counterfeit document. Have you ever wondered why a motel or hotel needs to swipe the magnetic strip on your license? The strip contains much more information than any front desk clerk will ever need about you – unless they are going to sell the information.

With the advances in technology, it takes more and more effort to keep this information safeguarded from criminals. But an important first step is to not make this information available to anyone who does not have a legitimate need for it. And, more importantly to keep as much personal information off of your social networks as possible.

Buyer Beware

Scams are as old as humankind, but technology has helped crooks come up with new ways to rip people off. And people continue to fall for offers that are just too good to be true.

The basic cautions continue to apply:

If it sounds to good to be true, it probably is.

If someone is trying to pressure you into buying something now – back away and think before you buy.

Limited time offers, often are not.

Prices that seem too low, should inspire you to do some comparison shopping before a purchase..

Many scammers use what Dr. Robert Cialdini calls "reciprocity"; they will offer you "a favor", special discount, or gift to help earn your trust or instill a sense of obligation in you to repay the favor.

Be cautious of situations where someone works on your emotions to try to get you to help out and donate money to a seemingly legitimate cause.

Job Search Scams

It is very easy for someone looking for a job or seeking better career opportunities to fall prey to job scammers.

An example of this are the many desperate job seekers who fall for the “work from home” scams. While it is true that many legitimate companies allow their established staff to “telecommute”, an ad offering work from home should be looked at with suspicion.

Not only are younger job seekers becoming victims, but a growing number of senior citizens and retirees are falling for many of these scams as well.

Things to consider if you are job hunting:

- Be suspicious of job ads that say that “no experience is necessary” but offer you an attractive salary.
- Don’t fall for the scam which offers to provide you a list of high paying jobs for a fee.
- Legitimate employment agencies who recruit and screen job candidates for employers have their fees paid for by the recruiting employer, not the job seeker.
- If you see an ad for a job listed for a legitimate company, go to the company’s website first to see if a job vacancy exists and is actually listed on their site.
- An unsolicited e-mail offering job opportunities that seem too good to be true is probably spam and may contain malware.
- Be cautious of links to a company website that looks professional, but lacks any real details such as where they are located, or how to contact them.
- Most legitimate employers are looking for people with specific job skills and work experience.
- The majority of jobs are still found through networking; telling people who you know that you are looking for a specific type of job.
- If you are asked to send or mail money to apply for a job – Don’t!

The Grandmother Scam

You are a grandparent, and you receive a phone call or an e-mail from someone who says, “Grandma , I’ve been arrested in another country, and need money wired right away to pay my bail. Please, don’t tell my mom or dad because they’ll get mad!”

This is known as “the grandparent scam”. Scammers prey on the elderly, taking advantage of their affection and concern for grandchildren.

The grandparent scam is not new, and has actually been around for some time. The FBI’s Internet Crime Complaint Center (**IC3**) has been receiving reports about it since 2008. But the scam and scam artists have become more sophisticated. Because of the easy access to information on the internet and on social networking sites, a criminal can often uncover personal information about their intended target.. This makes their scam more believable.

For example, the real grandson may post on his social networking site that he’s a photographer who often travels to Costa Rica. When contacting the grandparents, the phony grandson will say he’s calling from Costa Rica, where someone has stolen his camera equipment and passport.

How this scam works:

- A grandparent receives a phone call (or sometimes an e-mail) from a “grandchild.” If it is phone call, it’s often late at night or early in the morning when most people aren’t thinking clearly. The person claims to be traveling in a foreign country and has gotten into trouble, like being arrested for drugs, getting in a car accident, or being mugged…and needs money wired ASAP. And the caller doesn’t want his or her parents to know.
- Sometimes, instead of the “grandchild” making the phone call, the criminal pretends to be an arresting police officer, a lawyer, a doctor at a hospital, an embassy official, or some other person.
- Military families have also been victimized: after seeing a military member’s social networking site, a criminal will contact the soldier’s family, sometimes claiming that a problem came up during their military leave that requires sending money.
- While it’s called the grandparent scam, **criminals also call claiming to be a family friend, a niece or nephew, or another family member.**
-

What to do :

The losses in these type of cases may be substantial for any individual, usually several thousand dollars per victim, but usually don’t meet the FBI’s financial thresholds for

opening an investigation. **And, our advice is to avoid being victimized in the first place:**

- **Resist the pressure to act** - stop and do some research first.
- **Try to** contact your grandchild or another family member to **determine whether or not the call is legitimate.**
- **Ask** the person on the phone **for other personal details** that only the actual family member would know.
- **Never wire money based on a request made over the phone or in an email**….especially to another country. Wiring money is like cash - once you send it, you can't get it back.

Cramming

Cramming is the act of illegally placing unauthorized charges on a telephone bill. The Federal Communications Commission (FCC) estimates that tens of millions have been the victims of cramming.

Crammers rely on confusing telephone bills to trick consumers into paying for services they did not authorize or receive, or that cost more than the consumer was told.

How cramming works:

Cramming often happens when phone providers allow retailers or service providers to place charges on their customers' phone bills; allowing a telephone to be used like a credit or debit card account number for vendors.

Crammers may place a charge on a person's phone bill using nothing but an active telephone number, which can be obtained from a telephone directory.

Wireless customers should be especially vigilant because **s**martphones allow consumers to shop online from wherever they are and charge purchases to their phone bills.

Charges for services that are explained on your telephone bill in general terms such as "service fee," "service charge," "other fees," "voicemail," "mail server," "calling plan," and "membership" without a clear explanation of the services provided **might be cramming**.

What you can do to protect yourself:

• Carefully review your monthly phone bill, just as closely as you review your credit card and bank statements.
• Ask yourself the following questions as you review your telephone bill:

1) Do I recognize the names of all the companies listed on my bill?
2) What services were provided by the listed companies?
3) Does my bill include charges for calls I did not place or services I did not authorize?
4) Are the rates and line items consistent with the rates and items that the company quoted to me?

• When in doubt, ask questions. You might be billed for a call you placed or a service you used, but the description listed on your telephone bill for the call or service may be unclear. If you don't know what service was provided for a charge listed on your bill, ask your phone provider to explain the charge before paying it.

Credit Card Wireless Skimming

Did you ever think that ID theft would be so common that you would be buying a pair of jeans to help keep you from becoming a victim of Identity theft? A new company will be marketing a pair of pants that "uses special lining in its front and back pockets to block radio-frequency identification (RFID) and near-field communication readers, which are used to scan for credit cards."

Many of the newer generation credit cards contain a RFID chip in them which makes buying more convenient for the buyer, and much less trouble for scammers to obtain the credit card information. The information on these cards can be read while still in your purse or pocket with a simple reader that can be purchased on the internet.

How this works:

- The credit card has an embedded RFID chip that contains all the information needed to complete a purchase.
- Usually, a customer passes the card near a device that allows it to read the financial information for the purchase; examples are places like Starbucks, Jack in the Box, and others.
- The information is automatically entered at the point of sale and the purchase is completed.
- The same information can be retrieved (while in a wallet or purse)by a criminal using a device that reads the card from a distance away. Y
    - You could be sitting at a table sipping a latte while a criminal is reading and recording the information on your credit card.
- The information can then be used to create duplicate cards or to sell to oversee buyers.

How to protect yourself:

- If possible, ask your financial institution for a card without a RFID chip.
    - However, some of the newest RFID protected credit cards also have a PIN associated with them; that is necessary to use them. Ask your bank or credit union.
- If you already have one of these cards buy an RFID protective sleeve, or wallet.
- Be aware that the RFID protection diminishes as the materials integrity breaks down with use.
- Check your monthly credit card statements carefully for any unauthorized purchases.

IRS-Impersonation Telephone Scam

One of the most current, ongoing scams is an aggressive phone scam targeting taxpayers, claiming to be a call from employee of the Internal Revenue Service (IRS). The scammer can sound very convincing when they call. They will usually "spoof" (alter) the phone number appearing on your caller ID to make it look like the IRS is calling.

Victims are told they owe money to the IRS and it must be paid promptly through a debit card or wire transfer. If the victim refuses, they are threatened with arrest, deportation or suspension of a business or driver's license. Often, the caller becomes hostile and insulting.

Or, victims may be told that they have a refund due to try to trick them into sharing private information.

If you don't answer the phone, scammers will often leave a message saying that it is urgent that you call them back; usually telling you that a warrant has been issued for your arrest, you have taxes owed or you are due back a large refund..

- The IRS will never call to demand immediate payment.
- They will not call about taxes owed without first having mailed you a bill.
- The IRS will not demand that you pay taxes without giving you the opportunity to question or appeal the amount owed.
- Nor, will they require you to use a specific payment method for your taxes, such as a prepaid debit card.
- They will not ask for credit or debit card numbers over the phone.
- Legitimate agents will not threaten to bring in local police or other law-enforcement to have you arrested for not paying.

How to Protect Yourself

- If you receive a similar call, and doubt whether it is the IRS – contact your local IRS office (the phone number can be found in a phone directory or on the internet.
- Do not share any personal information, give out credit card or other financial information over the phone.
- Write down the home number appearing on your caller ID, hang up, and report the call to the local IRS office or FTC complaint center:
- http://www.treasury.gov/tigta/contact_report_scam.shtml
- https://www.ftccomplaintassistant.gov/#crnt&panel1-1

The "Ring and Run"scam

A scam that continues to repeats itself in various forms is one in which criminals target victims simply by calling them.

The victim receives a call from an out of area phone area code which rings once making the recipient call the number out curiosity. And, sometimes the caller lets the phone to ring just long enough for the victim to answer after which the caller hangs up.

How this scam works:

- The victim receives a call in which the caller hangs up, or sounds distressed on the other end before the hang-up.

- The recipient of the call phones the number back, many times out of curiosity or concern.

- Most of these call originate from area codes 809, 284, 649, 473, and 876, which are international area codes.

- Sometimes, the number can be “spoofed” to appear to be a local number.

- Calls to some of these area codes may exceed $20 for the first minute; don’t call back.

How to protect yourself:

- If you receive a hang-up call – **don’t call them back**.

- There is no reason to call back missed calls from unrecognized numbers.

- If the call is something important, the caller will leave a message or text you.

- Don’t let curiosity cost you.

Source: Forbes Magazine: 2/2014

Webcam spies

The same technology that allows us to stay in touch with family and friends also allows criminals to monitor our every move. The webcams that helps us to communicate face-to-face over the internet, can be used by criminals to monitor our office and even our bedroom.

Criminals have been using the ability to hack into individual webcams (and microphones) to target individuals with customized scams using personal information gathered via their camera and microphone.

Here is how it works:

- The hacker turns on a person’s computer, tablet, or home security camera and microphone, after finding one with a default (manufacturer’s) password, or an unsecured one.
- Sometimes the hackers embed malicious code in an e-mail attachment, allowing them to control the webcam and microphone.
- In several cases, the hacker posed online as a young woman’s friend or sister and sent messages with attachments asking if the victim wanted to see a scary video.

- The hacker collects video or captures (sometimes compromising) images of the victim for later use in an extortion scheme.
- Some of these videos are posted on the internet for all to see as is the case with thousands of webcam feeds hacked recently by Russian hackers.
- Some victims were coerced into sending explicit photos of themselves after viewing what the hackers had downloaded.
    - In one case, the hacker attached a pornographic picture of the victim in an e-mail and demanded sexually explicit video of her in return for not telling her parents about the pictures he had downloaded from her computer.
- This is also a very easy and disturbing way for predators to spy on children without detection.
-

How to Protect Yourself

- Be sure to change your wireless camera's default password right away.
- Create a password that uses a combination of capital and lower case letters, numbers, and special symbols.
- Cover your camera when it is not being used.
- Look for the indicator light on your webcam.. Laptops with internal webcams usually have an LED indicator. If you use an external webcam, detach it from the USB port when not in use.
- If possible, do not keep computers with webcams in a bedroom.
- Turn your computer off when it is not in use.
    - Many of the reported victims chatted on social networks so much that they never turned off their machine.
- If your system has been compromised and you have received extortion threats, contact law enforcement for assistance.

Contractor Scams

Beware of contractors who swindle unsuspecting victims out of their money by promising to make repairs to homes damaged by winter storms, earthquakes or floods, but who are nowhere to be found once they have been paid.

Some of these "contractors" may advertise on Craigslist or knock on your door offering painting, home repair, tree trimming, gutter cleaning, or other professional services.

Often these contractors are not licensed, insured or up to industry standards in the quality of the services that they offer.

Senior citizens are sometimes targeted by fake contractors who will knock on their door offering services and distract them. While a cohort enters their home and steals whatever is of value; often entering (and leaving) through an unlocked back door or window.

What to look for

Ask to see their CSLB (Contractors State License Board) license; a state contractor license is required for work that totals $500 or more (in combined labor and material costs).

Ask for a written bid for the services that are being offered.

Any contract should include the three-day notice of cancellation required by federal law for contracts signed in the home. Never sign a blank contract.

In California, contractors cannot ask for deposits of more than 10% of the total cost of the job or $1,000 -- whichever is less -- unless the contractor has a special bond.

A licensed contractor will have a CSLB license that looks like a credit card with their contractors license number on it.

You can verify a contractors license online at: https://www2.cslb.ca.gov/O…/CheckLicenseII/CheckLicense.aspx or call 800-321-2757.

- Be very suspicious of any contractor demanding that you pay them in cash for their services.
- Be especially wary of any contractor whose vehicle has out of state plates.
- If the contractor has employees, he must also have workers compensation insurance; ask who their insurance carrier is.
- If they don't have this insurance you may be liable for costs associated with any injuries to the contractor's employees incurred while working on your project. Carefully inspect any work performed before making a final payment.

Microsoft Technical Support Scam

A scam that has been going on for several years doesn't seem to be going away seems very real. It begins with a friendly sounding voice, often with a foreign accent, announcing that they are a representative from Microsoft. "We've had a report from your internet service provider of a serious virus problems from your computer," the caller continues to explain.

The person then continues with the charade trying to convince you that your computer has critical errors in its operating system. Soon they will be remotely accessing and controlling your computer.

How the Scam Works

- You receive a phone call from someone claiming to be from Microsoft, or they may even claim to be from your own internet provider.
- They may even call you by name and use your correct address.
- The person claims that your computer has serious errors that they will help you fix.
- They may direct you to a logging program on your computer that may show some errors to convince you that they are legitimate.

- The so-called technician then asks you to log onto a website where you will be able to download software that "will help you fix the problem".
- The download is actually a program that will allow them remote access to your computer.
- Once the software is downloaded, they can control your machine anytime.
- Most of these calls have originated from India, but could come from the US.
- Microsoft tech support will not call you unless you contacted them first.
-

What to do if you receive one of these calls:

- Realize that it is a scam.
- Don't engage the caller in conversation as they can quickly win your confidence.
- Do not go to any website that the unsolicited caller asks you to .
- And, never download software that you did not intend on downloading .
- Record the phone number for use in reporting it and blocking it.
- Contact http://www.ic3.gov , or https://www.ftccomplaintassistant.gov/#crnt&panel1-1 and file a complaint.

Hostageware or Ransomware

One of the most malicious scams is the use of "ransomware" or "hostage ware" that will lock up your computer when you open an infected attachment or go to a malicious site. It will usually not allow you to use your computer until you have paid, given up some sensitive personal information, or clicked on a link and downloaded another virus.

Here is how it works:

- The malicious application is spread through e-mail, attachments, infected sites, or instant messaging.
- The scammers who originated the ransomware want to scare you into clicking on an infected link, providing personal information or sending a payment.
- They may intimidate you by having a message appear on your screen that may say:
- "Your computer has been infected with a virus. Click here to resolve the issue."
- "Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a $100 fine."
- "All files on your computer have been encrypted. You must pay this ransom within 72 hours to regain access to your data."
- They may even resort to using a message on your screen with an FBI or other government agency logo, that appears all too real.

What to do:

- Disconnect your machine from the internet.

- Use your computer anti-virus software emergency disk.
- Try to restart your computer in safe mode and attempt to locate the latest application download and delete it.
- You may need to use your emergency recovery disks to recover use of your computer.
- Always keep your operating system, backups, and anti-virus software up-to-date · With the latest reported version of ransomware, "VirRansom", you may have to reformat your entire machine.
- You may have to rely on having a knowledgeable computer professional assist you in some cases.
- Report it to http://www.ic3.gov

Purchase Confirmation Scams

With Cyber (Monday) Week just ending, holiday-shopping is in full gear. This is the time when scammers, thieves, fraudsters and malware writers work their hardest at snagging the unaware. Chances are that you have been seeing "order confirmation" messages landing in your e-mail inbox – and there is a very good chance that most, if not all of them, are scams, trying to trick you into opening them and dumping malware onto your computer.

How this scam works

Those seemingly realistic messages, allegedly from some well known retailers like Target, Home Depot, Costco or other major retailers trick you into opening them, knowing that you didn't order anything.

By responding to the message, or clicking on the link in the realistic looking purchase confirmation, you wind up loading malware onto your machine that will steal sensitive information from your computer including contact lists and passwords.

It can also serve to enslave your computer into sending junk e-mail from outside sources to those on your e-mail contact list and beyond.

What to do

The smartest thing that you can do with a message that you are suspicious of is to delete it immediately without opening it.

Credit Card & Debit Card Skimming

Criminals are increasingly using available technology to skim financial and personal information from automated teller machines, credit card readers at gas station pumps and department store checkouts.

Blue-tooth enabled skimming devices are enabling criminals to wirelessly capture credit card information without their physical presence to retrieve the data. These devices are nearly impossible to detect and can easily be purchased online.

Law enforcement authorities have confirmed millions of dollars skimmed in just a one year period. How much has actually been stolen and from whom is unknown.

How this scam works

A blue tooth enabled skimmer / transmitter is installed in the card reader of a gas station pump, ATM, or store point of sale machine. The device is small and virtually undetectable, unless it is closely inspected.

How to Detect a Skimmer

• Inspect the card reader and the area near the PIN pad for any suspicious devices or equipment tampering.
• If you are using a debit card, try to conceal your PIN while entering it.
• Use a credit card instead of a debit card whenever possible, as most debit cards do not have the fraud protection that credit cards do.
• Use gas pumps that are in plain view and not in concealed or out of the way locations.
• Inspect the card insertion device and pin pad to see if they are loose or can come apart.
• Avoid using gas pumps where the tamper safe seal is broken or appears to have been tampered with.

Credit Card Support Scams

If you travel like many of us do, you may have had your credit card deactivated at one time or another by your card company's security department. This happens when purchases out of your ordinary buying habits or out of your normal geographic area suddenly appear on their radar.

However, it can be easy to fall for fake messages claiming that your card has been deactivated. This scam is an attempt to get you to share banking information such as your account, social security, credit card or routing numbers with criminals on the other end.

How it Works:

- You receive a text message or automated phone call claiming that your credit or debit card has been deactivated. The message tells you that all that you have to do to reactivate it is to call a customer service number and confirm some information. The message might read: "Your credit card has been put on hold, call customer service at X-XXX-XXX-XXXX."
- You dial the number in the message, and you are put on hold. A message instructs you to enter your 16 digit credit card number. Don't do it! If you do, you will have fallen for a common credit card fraud scam.

How to Spot This Scam:

- Call your bank or credit union directly or go to their website. Find the correct phone number on the back of your credit or debit card and call to confirm the status of your card. Don't call the phone number given in the text message.

- Ignore instructions to respond to the text message. This is used by scammers to confirm that they have an active phone number.
- Did you sign up for text messages alerts? Be aware of how your bank or credit union communicates with you; anything out of the ordinary could be a scam.
- Forward the texts to 7726 (SPAM on most keypads). This will alert your cellphone carrier to block future texts from those numbers.

Caller ID Spoofing

Scammers are using caller **ID spoofing** to impersonate the phone numbers of local businesses, your neighbors or even the police!

How the Scam Works:

Your phone rings, and you may recognize the number as a familiar one. It may be from a neighbor, a local business, or even the police department.

You answer the phone, and realize that it is a robo-call. Victims have reported several different phishing scams. In one version, a recording asks you to verify your credit card number under the pretense of lowering your interest rates.

With more and more people rejecting phone calls from numbers that they don't recognize, scammers are beginning to pose as familiar businesses, government organizations, or local people. Scammers purchase lists of phone numbers and use spoofing technology to trick potential victims into picking up their phone.

What to do if a scammer calls:

- Hang up, don't press any buttons and, if you receive a voice mail message, don't call back.
- Returning the phone call may give the scammer information that he can use.
- Don't trust your Caller ID. Scammers have the ability to display any number or organization name that they choose on your Caller ID screen.
- Never give out any financial information. If you didn't initiate the call, do not provide bank account, credit card or Social Security numbers over the phone unless you have thoroughly verified the caller.

Phony Charities

The holiday season is a common time to receive solicitations from charities that claim to be collecting donations for any number of causes. It may take the form of a mail solicitation, an email, social media post, or even collecting door-to-door.

Just because the solicitation claims that it is collecting money for a certain cause, doesn't mean the funds are really going there. Charity fraud varies from outright scams to misrepresentations about how much of the donation actually goes to the stated cause.

How to Protect Yourself from Phony Charities:

- Mistaken Identity: Watch out for the use of name confusion. Many so-called charities include virtually the same words in different order or slightly different form in their name as legitimate ones.
- Charity Description: Look for a clear description of the organization's programs and mission on its website. If it says it is helping orphans, does it explain how (adoptions, shelter, health care), and where this work is being done?
- Time Deadline Donation Decisions: Be very cautious of fund raisers who employ pressure tactics in their fund raising efforts. Don't be pressured to make an immediate on-the-spot donation. Charities should be willing to accept your donation whenever you wish to send it.
- Check with Reliable Sources Before Giving: You can go to http://give.org to access information that summarizes management, reporting results, finances and appeal accuracy for many charities. You can also go to http://va.gov/vso/where you can find a list of Veteran Service Organizations (VSO) information about Military Service Organizations can be found at http://militaryonesource.mil

Phony Sweepstakes Giveaways

Emails posing as **business giveaways** are a popular way to transmit malware or phish for banking or other personal information. Be careful of any unsolicited email that promises free gift cards, discount coupons or other too-good-to-be-true gifts. Once downloaded, malware can hunt for banking and other personal information on your computer, putting you at risk for ID theft.

How to Spot a Scam:

- Watch for these signs that your email is likely a fake:
- Hover your cursor over links to check their source. Place your mouse over hyper-linked text and the true destination will appear.
- Don't believe what you see. scammers often copy a real business' colors, logo and even email address.
- Be wary of unexpected emails that contain links or attachments. Do not click on links or open attachments in emails from unsolicited sources
- Check the offer with a quick web search. If a business is really offering a promotional giveaway, they should be advertising it on their website and elsewhere. A quick search on Google will often reveal that this offer isn't real.
- Watch for poor grammar and spelling. Scam emails often are riddled with typos.
- Ignore calls for immediate action. Scam emails try to get you to act before you think by creating a sense of urgency. Don't fall for it.

College Students Work Scams

College students across the United States have been targeted to participate in work-from-home scams. Students have been receiving e-mails to their school accounts recruiting them for payroll and/or human resource positions with fictitious companies.

The “position” simply requires the student to provide his/her bank account number to receive a deposit and then transfer a portion of the funds to another bank account.

Unbeknownst to the student, the other account is involved in the scam that the student has now helped perpetrate. The funds the student receives and is directed elsewhere have been stolen by cyber criminals. Participating in the scam is a crime and could lead to the student’s bank account being closed due to fraudulent activity or federal charges.

Here’s how the scam works:

- The student is asked to provide his/her bank account credentials under the guise of setting up direct deposit for his/her pay.
- The scammers will add the student’s bank account to a victim employee’s direct deposit information to redirect the victim’s payroll deposit to the student’s account.
- The student will receive the payroll deposit from the victim’s employer in the victim’s name.
- The student will be directed to withdraw funds from the account and send a portion of the deposit, via wire transfer, to other individuals involved in the scam.
-

Consequences of Participating in the Scam:

- The student’s bank account will be identified by law enforcement as being involved in the fraud.
- The victim employee has his/her pay stolen by the scammers utilizing the student’s bank account.
- Without the student’s participation, the scam could not be perpetrated, so he/she facilitated the theft of the paycheck.
- The student could be arrested and prosecuted in federal court. A criminal record will stay with the student for the rest of his/her life and will have to be divulged on future job applications, which could prevent the student from being hired.
- The student’s bank account may be closed due to fraudulent activity and a report could be filed by the bank.
- This could adversely affect the student’s credit record.