STC Fraud News

AUGUST 2019

Scams are on the Rise!

Scam artists are constantly looking for ways to steal money. We put together a list of scams we are seeing now along with some tips to avoid them. As always: if you ever need help deciding if something is legitimate or not, call our Fraud Hotline at (814)530-1013 or our People First Call Center at (800)972-1651.

Trending: Scams

Social Security: We have received many reports of people receiving phone calls supposedly from Social Security. The caller tells you that there is fraud associated with your social security number and they have frozen your SS benefits. They will ask you for personal information to "verify" your identity which may include your SSN and bank account information.

What to do: Hang up the phone and do not call them back if you get a voicemail. This type of scam can result in your identity being compromised. Social Security will not call you if there is ever a problem, they usually communicate through the mail. Whatever you do, DO NOT give out your information! If in doubt, you can always contact your local Social Security office as well.

Publishers Clearing House: You receive a call or a letter stating you won their jackpot prize! In order to receive your winnings, you need to send some money to pay for "taxes and fees". People have sent cash, wire transfers and multiple checks to other individuals resulting in a loss for the victim. In some cases, they may send you a smaller check and instruct you to deposit or cash the item and send funds back.

What to do: IGNORE IT! These are always a scam. You never have to pay taxes and fees up front and any checks they send you are fraudulent. Hang up the phone, get rid of the letters and never deposit random checks you receive in the mail.

Microsoft Tech Scams: You receive a phone call from someone claiming to be Microsoft, because they have detected a virus or malware on your computer. They need to remote into your computer in order to fix it. They may also tell you there is a fee involved and they need your bank account information or even your online banking credentials to debit the fee.

What to do: Hang up the phone! Microsoft (or Dell, Apple, HP, Facebook, or any other tech company) will not call you to tell you there are problems with your computer. The scammers goal is to get into your computer, compromise whatever information you have on it (Saved tax returns, personal documents, emails etc). Once they are in, they install viruses and malware onto the PC. Some of these are sophisticated enough to track your keystrokes and watch your computer. The next time you login to pay your bills, your credit card accounts, work documents etc. they are watching and obtaining all of you usernames and passwords. Some scammers have even initiated fund transfers and wire requests using the victim's online banking accounts.

Online Loan Scams: This type of scam usually begins with a person who is searching online for loans. The lender may advertise that they do not do a credit check, they offer same day funding etc. Without doing further research, the victim enters all of their personal information into the website to get approved for the loan. Once approved, in order to receive funding they ask for your online banking credentials. The scammer logs into your online banking and deposits a check, which is always fraudulent. They may ask you to send a portion of the funds back after you receive the deposit in order to prove that you will repay the loan.

What to do: Research any lending company BEFORE giving out information. Be aware! After researching, the lender may seem legitimate but it is possible the website you are using is fake! A sure way to avoid this scam is to go to a bank to obtain a loan. Red Flags for this type of scam: Asking for your online banking credentials, asking you to send back money before obtaining the loan, advertising no credit checks in order to get funding.

Trending: Scams Cont.

Online Friend/Social Media Scams: You start receiving messages from someone you may have known for a while, but haven't talked to lately. The "friend" seems to know a lot about you and begins communicating frequently. Eventually, this "friend" tells you a story that will tug on your heart strings and requires financial help (maybe they were in an accident, behind on bills, need help paying for Christmas gifts for their children etc.) You decide you want to help them out, so you send them some money. The "friend's" story may dig deeper and they keep asking you for more money, but the person on the other end isn't actually who you though it was and you just sent money to an impersonator. You may also see the opposite. Maybe you have a friend contact you and know a little bit about your situation, maybe they know your car broke down, you lost your job etc. and they say they want to help you. They may send you a check, wire or ask for your online banking credentials to deposit funds.

What to do: Don't fall for it! These are always scams and the victim is always left losing money. If they send you money, the check or wire is always fraudulent. Often it is actually stolen funds from another victim. Once the other victim realizes they have been scammed, they report the activity to their bank and dispute the transactions. The items are then returned to your bank and if you already spent the money or even sent some back to the scammer, you are now responsible for paying back those funds. Never give your account information or online banking credentials to anybody!

Another form of the online friend scam targets veterans: You may receive a sudden phone call, email, or message from one of your buddies you served with in the military. They give you a story about how they are losing their home, going through a tough time or had a horrific accident and need money. Military members support each other and it may be hard to believe but this is a HUGE scam! The person you are speaking with is not the person you served with, it is an impersonator. Do not send money!

The Bottom Line

This is not a complete list of scams. Criminals are always looking for ways to steal money so always be on alert! Don't give out any personal information (name, address, phone, social security number, date of birth), your online banking credentials (user name and password), or your bank account information. Don't accept funds from anyone you don't actually know. Even if you have known someone for years, if you don't actually see them and speak to them in-person it could be a scam. Don't send money to other people, businesses, or anyone promising you money. If you receive something you are not sure about, CALL YOUR BANK! They can help you verify if something is legitimate before giving out information, or help you if you already fell for a scam.

If you would like to learn more about scams, identity theft, and fraud prevention, call us to schedule a Fraud Outreach Presentation! We present different topics to church groups, non-profits, senior centers, civic groups etc, and you do not need to be a customer!

Help us spread the message about scams, Call Angie Rowland in Marketing to schedule an event at (814)443-9370.