**Fraud Prevention**

**Common Scams:**

* **IRS Impersonation Scams**
  + Facilitated via phone or email from a person claiming to be from the IRS.
  + Impersonator will attempt to convince the victim that they are behind on their taxes and may even threaten arrest by local law enforcement unless payment is received.
  + They may even ask for personal information including social security number, date of birth, address, etc.
  + Keep in mind that the IRS does not contact you via phone or email to make any notifications or demands. You will most likely receive any contact from them via mail/letter.
  + Resource: <https://www.irs.gov/uac/tax-scams-consumer-alerts>
* **Foreign Lottery Scams**
  + Facilitated via mail with letter informing the victim that they are winners of a lottery that they never bought a ticket for. The letter may also inform the victim not to tell anyone of their winnings or they would be disqualified.
  + Usually accompanied by a counterfeit or fraudulent check with the goal of having the victim negotiate the check and send funds back to either pay taxes or fees for the winnings.
  + Once negotiated the check would be returned and any funds used by the victim are not recoverable.
  + Keep in mind that it is illegal for US citizens to win a foreign lottery.
  + Resources: <https://www.fbi.gov/news/stories/2006/august/lotto_scams080906>, <https://postalinspectors.uspis.gov/the-inspectors/foreign-lottery.html>
* **Sweepstakes Scams**
  + Facilitated via mail or email offering the victim a chance to enter a sweepstakes but requiring an entry fee. They may even ask the victim to make small purchases to increase the chances of winning.
  + Keep in mind that legitimate sweepstakes require no fee or purchase to win. They also must disclose in their mailings “No purchase necessary”, rules, name of sponsors, & terms and conditions.
  + Victims should verify the company’s reputation with the Better Business Bureau where the company is located.
* **Craigslist or Care.com Scams**
  + Facilitated using craigslist, care.com, or related websites. Victims normally are selling an item or advertising a service on these websites.
  + Victim selling an item or service will receive check payment from buyer for well over the asking or listed price. The excess funds are to be used for shipping or to pay for movers to pick up the item.
  + Once the check is negotiated and funds are spent, the check will return and the victim is at a loss for the funds.
  + Keep in mind to deal locally as most Craigslist scams are from people not in your area. Never wire funds to pay for an item you’re buying. Sellers trying to scam buyers often are very vague when they respond to your inquiries about an item. This is because they may be using generic responses to maintain a large number of scam nationwide.
  + Resources: <https://www.care.com/c/stories/2717/carecom-and-scams-how-to-avoid-babysitting/>, <https://www.craigslist.org/about/scams>
* **Sweetheart/Romance Scams**
  + Facilitated via dating or social media websites where the victim is befriended online and the relationship evolves into a romance.
  + Common aspects of this scam include the girlfriend/boyfriend being deployed or overseas and are in need of some financial help to solve a problem restricting them from being able to visit the victim. Sometimes it is to pay customs or because they have lost their passport.
  + The scammer will never stop asking for money. There will always be another issue that requires additional funds be sent to help. Many times they will leave their victims in debt.
  + Keep in mind that should you be scammed in this manner, you should first report the instance to the site where you first made contact with the scammer.
* **Microsoft/Tech Support Scams**
  + Facilitated via phone call or pop-up on your computer. The scammer will be impersonating an employee with Microsoft or another tech support company.
  + They indicate to you that your computer has a virus and they need remote access to your computer in order to fix the issue.
  + Once remote access is provided the scammer has access to all of your files and any personal information on the computer.
  + After they “fix the problem” (which was actually them installing malware on your computer) they will request payment for their services by credit card or by having you login to your online banking.
  + If you login to your online banking while they are remoted in to your computer, they now have access to your personal information and banking credentials.
  + Keep in mind that you will not receive calls from tech support unless you have paid for such a service. Even then, be cautious with allowing remote access to your computer. You can always independently contact your tech support provider if you are suspicious.
  + Resource: <https://www.consumer.ftc.gov/articles/0346-tech-support-scams>
* **Phishing Scams**
  + Most commonly facilitated via email impersonating a legitimate business and indicating an issue that needs to be fixed. The email requests that you click on the link embedded in the email.
  + Once you click the link, you are directed to a bogus website where you are directed to enter personal information. Simply clicking on a link or opening an attachment may also open your computer up to viruses and malware installation.
  + Keep in mind that if you are familiar with a company that you received an email request from, call and verify the email is from them before continuing. Enter sensitive data in secure websites only.
* **Mobile Banking Fraud**
  + Facilitated via phone, email, or any other contact medium with the intent of persuading their victims to disclose their online banking credentials.
  + Once disclosed, the scammer will log into their online banking using the mobile phone application and will made a check deposit using the mobile deposit feature.
  + The fraudster will then instruct the victim to visit their local bank or ATM and withdrawal funds to send to them in some manner. This is usually done via wire or MoneyGram.
  + The check will return after and if funds have been sent the victim is at a loss.
  + Keep in mind that you should never disclose your online banking credentials, especially to those you don’t know or have never met.
  + Resource: <https://www.snapmunk.com/mobile-banking-fraud-defense/>

**Helpful Tips to Avoid Falling Victim To A Scam**

* If it seems farfetched it probably is.
* Research the situation
* Contact local law enforcement agencies or financial institutions for help
* Protect your personal information
* Do not send money to someone you have never met in person
* Ask questions
* Should you fall victim to a scam – contact law enforcement, credit bureaus, social security, and all of your financial institutions.
* You can find a lot of helpful information regarding scams at [www.ftc.gov](http://www.ftc.gov)