Financial Crimes Prevention

1. It should be assumed that your personal information is not private. Unless you have been living without utilites, no internet connection, no financial institution accounts, and have been paying for everything for your entire life in cash, then more likely than not, your information is available to (if not already in the hands of) a criminal. This happens because we all willingly give our information to companies and governement entities, for legitimate reasons, but those organizations then retain our information. Those organizations are then attacked by criminals to steal that data. This has happened countless times all around the world, and will continue to. It is just a part of the 21st century, and there is no need to panick about it. There are countermeasures. The best defense to not becoming a victim of a scam is simply to be educated.

2. Scammers often try to deceive potential victims into being scammed using a veriety of methods. Remember, they likely have at least some of your personnaly identifying information (PII), so they will try to incorporate that into their stories to make themselves seem more legitimate because you assume that only someone legitimate would know your PII:
   A. They will often claim to be someone from the governement or a company (likely one you area already associated with).
   B. They may speak quickly and try to control the converstaion. They overload victims with information to confuse them.
   C. They will lie, especially about sensitive topics like loved ones in need or danger, to create a sense of urgency and panick, which is distracting.
   D. They may pretend to be part of the IT unit at a company you do business with and claim that there is an issue with your account and try to convince you to give them remote access to your computer to fix an issue.
   E. They may claim to be from a charity seeking donations.
   F. They may claim to be part of a company with a too good to be true offer for you to invest for substantial and quick returns on your investment.
   G. They may try to become romantically involved with you to convince you to "help them" financially.
   H. They may send you malicious emails that contain malware links or documents, which if opened can infect your computer, reading your activity in the background or producing pop-ups to aid in the IT scams.

These are just a few examples of common scams, but the underlying principal of a scam is always the same, <u>deception</u>!

Preventative Tips

1. **JUST SLOW DOWN!!!** Don't make quick decisions; don't assume they are telling you the truth; don't send money until you verify what is being told to you. Don't let them tell you what to do. *A tell-tale sign of a scammer is they may become hostile if you begin to challenge what they say.*
2. If someone you don't know calls, texts, emails, or mails (traditional mail scams are not as common – don't use "suspicion" as an excuse not to pay your bills!) you and claims something happened or that you need to do something (especially if they start to talk about money) there is a good chance it is a scam. If they are claiming to be a representative of the government or of a company/organization, especially if you already have a relationship with that entity, *then hang-up and contact that entity on your own via a form of communication that you know is legitimate.*
3. If someone tells you to go get a bunch of gift cards and, by any means, instructs you to get the card information to them, **IT IS A SCAM!** The same goes for wiring money.
4. If someone asks you to remote into your devices or to click on a link (unless they are someone you know who is actually performing IT service for you), **IT IS A SCAM!**
5. Mail is stolen more often than we would like to admit. Cash in an envelope is potentially cash in a crimnal's pocket. Checks are often stolen from the mail and altered. *If you don't have to mail money or checks, don't!*
6. If you don't need to actively use financing, consider locking your credit reports (TransUnion, Equifax, Experion).

Again, these are just a few examples of preventative tips, but the underlying principal is always the same, slow down, be thoughtful, and be defensive!

The world is very interconnected now, and all of our personal information might as well be considered public, but even with that being the case, the percentage of people who get scammed (although a lot) is still a tiny portion of the the total population. You don't need to lose sleep over this, but you do need to prepare for it to be ready to protect yourself when the need arises. That means don't wait until after there is a need to attempt to protect yourself. Preparation is key.