Staying ahead of the Scammers

Every week, I receive calls that state, "I have been scammed." Most of the time it is a wrong click on an errant email or text. However, more recently, it is more sinister as people are being impersonated at banks or investment institutions. Imagine someone trying to open an account in your name and they have all of your personal information to do so. The good news is, the banks, credit unions, non-profits, and investment companies are on high alert and often call the real customer to verify potential transactions that are falsified. Most of the times, the perpetrator does not get very far, but it is still unnerving, and many can still cause harm. Here are a few tips to keep your private information safe.

Phishing Emails can arrive, in some cases, daily to your work or personal email. The following list is from trusted government source of what to look out for:

1) If the sender is promising a high reward of some kind - most likely it is not real
2) If the email indicates a high sense of urgency- most items are not urgent and can wait
3) Watch out for Mystery emails asking you to click 'for a surprise'
4) Strange tone in the email, does not sound like a friend or family member
5) Sender's Address is out of order: spelling, senders name vs. name within the email address, do the detail in the 'From In-box match the person that sent it, is it someone you know at all? If not, delete. . . just do not click for sure
6) Unsolicited attachments. Does the URL match the company that you know?
7) Ask around to see if others received the same questionable email

Fake Texts are now prevalent. In AARP for September 2021, they point out a few items to look out for:

1) Personal texts that include your name suggesting a relationship that does not exist
2) Texts from a company that uses emojis (companies do not us emojis)
3) Texts with obvious spelling mistakes
4) Websites that are not linked to the company that sent it
5) Texts in all CAPS
6) Texts sent time from another time zone/ another country

7) Texts requesting confirmation of an account number, cell, email, or other private piece of information. Think, do you have an account there? Were you expecting this text?

Emails or tests from unknown senders -when in doubt, Do Not Click On It! Most people think that clicking on these items only refers to the elderly. Studies have shown that even IT professionals in cybersecurity are still prone to 'clicking on' enticing emails. This happens to everyone, and it is not IF but when it will happen to you.

"**Breach" letters**. Unlike the categories above, you may also have received legitimate 'breach' letters from either your health insurance carrier, your bank or credit union, store credit card, or other service provider intended to notify you whether your information has been compromised or not.

1) If you receive such a notification with assurance, your information was not compromised, no action should be necessary.
2) If you receive such a notification and have been informed that your information has been compromised, I recommend you step up being vigilant as mentioned below. They may send out a letter and include an offer a free credit monitoring for one year, I recommend that you take it, if you don't already have a system in place.

In general, my precautionary recommendation is to be vigilant:

1) Monitor your bank, investment, and credit card activity at least weekly. You may want to run the free Annual Credit report you are entitled to make sure nothing on there that should not be. The website to do this is: https://www.annualcreditreport.com/index.action
2) If you want to take it one step further than just a checkup, then freeze your credit might be necessary. You can be assured that no one will be taking out credit in your name: buying a house or car in another part of the country. If your house is paid off and you pretty much never need to apply for 'new' credit, freezing your credit may put you at ease.

Lastly, if you decide to freeze your credit, make sure to keep good records! First, you will need to freeze the credit with all three credit bureaus (one does not notify the other two). Experion, Equifax, and Transunion all have their own systems. Secondly, the credit companies give you a PIN # specific for unfreezing and freezing your account. The login systems for freezing and refreezing can be different then logging into one of the credit bureaus to see your credit score. The last thing that is important, is to keep the date that you froze the account. An example would be, if you are turning on the electricity on a new home you are buying, the utility company may ask, "What day did you freeze your credit?" This can be annoying if you do not have the date from five years ago! This information can also come up if you decide to switch phone carriers. Any new 'pulls' on the credit report will call for an unfreeze on your credit. Again, the challenging thing of unfreezing, is this has to be done on all three credit bureaus. This is a decision you really need to think about before doing!

There are additional resources available at your bank or credit union. Please, be vigilant as you protect your information, and remember when in doubt, try to avoid unnecessary clicks!

Sincerely,

Andrew D. Wade, CFP®
President