STC Fraud News

May 2019

The Ins and Outs of Scams– Part 1

When dealing with Fraud situations, the most common question asked is How? How did a scammer get that information? How can I protect myself? How can I avoid this type of thing in the future? How do we educate customers/employees/friends and family members about fraud and how to avoid it?

I wish the answer was easy and simple, unfortunately, it's not. This is Part 1 of a 3 newsletter series that will go over the ins and outs of scams and fraud. This month, we will cover how scammers can get information on potential victims. June's newsletter will feature fraud that may be attempted after your information is obtained… we will be visiting both old and new scams we have seen targeting the people in our area! Last but not least, in July we will discuss how to protect yourself and how to share the information with your family & friends to protect themselves as well. We will also cover what to do if you or someone you know has already fallen victim to a scam.

In no way is this a complete list…scammers work day and night to find new ways to get information but the more you know, the more you can do to protect yourself and those around you!

Data Breach: Any company that houses consumer information could be an attractive target for scammers. You may remember in 2017 when Equifax was breached. Can you believe that more than half of the 148+ million people that were affected STILL have not checked to see if they were a victim? Think about Equifax for a minute, it is a credit bureau which means it is not a service we really "opt in" to. Whether we want it or not…almost everyone has a credit file (even you children and grandchildren!) Think about all of the information the credit bureau may have… Full name, address, phone number, Social Security number, previous employers, all of your current and previous loan/credit card information, previous addresses & phone numbers and in some cases, driver's license and debit/credit card information. This breach was a GOLD MINE for scam artists. The information that was breached was most likely sold to other scam artists on the Dark Web. Most people don't realize that the effects from that breach could last for years to come. Scammers will keep the information and possibly begin using it years down the road, after most people forget that their identity was stolen and maybe ease up on protecting themselves!

The Internet: There are some best practices to limit your exposure online; keep your social media accounts private, don't click on links in emails, watch for pop ups on websites. At the end of the day, your information is most likely out on the internet whether you know about it or not (and whether you like it or not!) . There are websites that gather public information and social media information and compile it for anybody to see. When I searched for my own name, it came up with information over 10 years old. The information included my maiden name, previous addresses, phone numbers and some employer information. Occasionally, do a google search with your own name and you might be surprised at the results.

If the websites offer the opportunity to opt out and remove your information– use caution though, you shouldn't have to provide additional personal details or pay anything in order to do so!

Phishing: Scammers are constantly "phishing" for information. According to Merriam-Webster phishing is defined as: a noun: a scam by which an Internet user is duped (as by a deceptive e-mail message) into revealing personal or confidential information which the scammer can use illicitly. While this definition is accurate, phishing scams can also be done over the phone or even by mail. Most people feel confident that they would never fall for a phishing scam…but how do you know what is phishing and what is legitimate? What if you get a phone call stating they are from your bank, electric company, credit card company or car insurance representative and give out information without realizing it? What if you get an email that looks to be from a friend or coworker with a link that leads to a fictitious website? What if you get a letter in the mail appearing to be from Social Security or the IRS and you fill it out and mail it back, but it turns out it was a scam? Scam artists are relentless in their attempts to obtain your information- be on the lookout!

Social Media: Do you frequently take quizzes (ex. Which Smurf are you? What car fits your personality? What profession should you be in?) Do you answer questionnaires friends or family members tag you in (ex. What was the name of your elementary school? What town did you grow up in? What was your first pet's name?) Every question you answer on social media could potentially give a scam artist the keys to stealing your identity. Think about it, most of the questions in those quizzes are similar to the out of wallet security questions you are asked when you are trying to unlock different accounts like your online banking, credit cards or utilities.

Continued on page 2...

Social Media Cont... If the scammer was able to obtain your personal identifying information from the Equifax Breach, completing these quizzes might just give them the rest of the information they need to fully steal your identity. So next time you see a quiz to find your spirit animal, think twice before clicking on it! Most of the apps used to take those quizzes store that information that can be used weeks or months after you take the test! Another thing to watch for is duplicate profiles. Have you seen people posting a status saying "If you get a second friend request from me, don't accept it! I've been hacked!" Most likely, that person was not actually hacked however, a scammer made a duplicate profile to attempt to "friend" unsuspecting people. The scammer may attempt to message different people in an attempt to see if they can form a relationship and eventually, ask for money or scam them in some way. Another tip? Don't automatically accept everyone who sends you a friend request! Be aware, there are fake accounts out there and if you allow them in, they may try to scam you. It may start out with them liking all of your pictures or making little comments but could turn to something suspicious.

Other: Think about all of the other things you may have done that could potentially expose your information… Did you fill out a warranty card and mail it back for a new car seat, highchair, freezer or mattress you bought? Do you respond to surveys on the bottom of a receipt after you went shopping? How about the hotel or restaurant review you did online? These types of things seem innocent enough but many of these companies sell your information to third parties, which means another possible compromise point for your information. Do you donate to charitable organizations that call you? Use caution! Many scam artists impersonate your local police, fire departments and emergency services in order to try and get you to donate. Most often, they will ask for a credit or debit card for payment and in the meantime, possibly make small talk to get you to reveal little details that could give them enough information to call your bank or credit card company and impersonate you. Another scary (and creepy…) way scammers get information, is to review obituaries to piece together family information, where you live, your spouse/children/grandchildren names and sometimes the next of kin becomes a target because they may have received a life insurance payout.

I realize this is a lot of information and some of it can be a bit scary and overwhelming to think about. Fraud experts now say it is not a matter of IF you will become an identity theft victim…it's WHEN. The bottom line is, sometimes protecting your information is out of your hands but the more you know about identity theft fraud, the better you can limit your risk, and be prepared to react if you unfortunately do become a victim. Don't forget to watch next month for Part 2 where we will discuss different scams (there are a lot of them!) we see impacting people in our area!

If you believe you may be a victim of a scam, call Somerset Trust Company's Fraud Hotline for assistance!
(814)530-1013