Information Security Update  October, 2021

I hope this communication finds you healthy and reasonably happy. Covid is still part of our lives but it has definitely begun winding down and that makes me happy.

I’ve always thought that we humans are a social animal and I think the last 18 months has caused some of us to perhaps feel that something was lacking in our lives. Hopefully we can now start the process of reconnecting with friends & family and getting back to some semblance of what I consider normal.

Before we get to the real subject of this newsletter, I did want to mention that Duo, our multi-factor authentication application, recently updated their interface. One of the changes they made was to swap the location of the “Approve” and “Deny” buttons displayed on your phone.

Pay attention when approving or denying access. If you receive an unsolicited Duo prompt on your phone, make sure you click the deny button!

Now on to the real purpose of this newsletter –
**How easy is it to steal from you and what can you do to minimize the risk of becoming the victim of online theft?**

Allow me to try and answer those two questions for you.
The anatomy of online theft.
In this narrative, I will write about two fictional people that we will call "Sam" and "Mike".

Sam is an ordinary, average guy with an ordinary, average digital presence. He has an email account, an Amazon account, an account with his bank, a few social media accounts, several accounts for newspapers/news sites, a Google account and various accounts at websites interest him interest. These may be websites about his favorite hobbies, educational sites or entertainment sites such as TikTok.

Since Sam is an ordinary, average guy, he can’t remember the passwords to all those sites so he uses the same password for all of them. One website that he recently created an account on was a site that offers humorous “memes” called "FunnyMemes.com". He used his email account as his ID and his usual password.

Several weeks later, Mike, a ne’er-do-well with some knowledge of how websites work, is poking around on the FunnyMemes.com website and he discovers an exposed database that contains ID’s and passwords. He downloads the data and finds Sam’s email address, averageSam@any-email.net and password.

Mike goes to the any-email.net website and enters Sam’s email address. He uses the password he found on FunnyMemes.com and since Sam uses the same password for everything, Mike is able to log in to the any-email website as Sam. Mike now has full access to Sam’s email. Mike goes through Sam’s inbox and finds several recent emails from Amazon.

After spending time poking around in Sam’s inbox and reading all his private emails, Mike decides to go to Amazon.com and see if he can access Sam’s account. He enters Sam’s email address and password, gaining access to Sam’s Amazon account.

Mike is now in his happy place. He has just stumbled upon a cache of goods that he can plunder but first he has to make sure he can get away with it.

Step one – Mike logs back in to any-email.net as Sam and adds a rule to Sam’s email account. The rule says, "If any email comes in from Amazon that contains the words ‘gift card’, forward it to ‘mike@badguy.org’ and delete it from Sam’s inbox."

Step two – Mike logs back in to Amazon as Sam and makes a purchase. He buys a digital Amazon gift card for $100. Amazon charges the $100 to Sam’s credit card and sends the gift card code to Sam’s email address. Upon arrival in Sam inbox, any-email.net follows the rule Mike just added. It automatically forwards the email with the gift card information on to Mike and deletes it from Sam’s inbox.

Mike just got $100 from Sam and Sam has no idea he’s been robbed. He never saw the email from Amazon so the only way he’ll know about the gift card is when he gets his monthly credit card statement.

If we assume Mike did this at the beginning of the month and Sam doesn’t get his credit card statement until the end of the month, it’s a pretty good bet Mike can steal several hundreds, if not thousands, of dollars from Sam before Sam even knows there is a problem.

And yes, everything I just typed happens all the time. There are bad actors out there that steal hundreds of thousands of dollars a month. They do it because it’s easy.

And while this scenario is bad, what is worse is that Mike could also gain access to Sam’s bank account, his retirement account, his Social Security account, etc.
Protect yourself.
Us information security folks like to tell you to protect yourself by using different passwords for each account you create.

That is a ridiculous recommendation on our part.

It is difficult at best for the average human to do that. No one can remember every password for the dozens of accounts we all have.

What if I said you should have at least six different passwords? Would it be easier for you to remember six passwords?

With that in mind, here is my modified password recommendation:

1. A password you use at work.
2. A password you use for your email account(s).
3. A password you use for your financial (banking, brokerage, credit card, etc..) accounts.
4. A password you use for your shopping account(s).
5. A password you use for your social media (Facebook, twitter, etc..) accounts.
6. A password you use for low-risk websites that require you to create an account.

In my example, if Sam had used separate passwords for each of those six account types, Mike would never have been able to log in to Sam’s email or his Amazon accounts. The only thing Mike would have access to would be low-risk entertainment accounts like FunnyMemes.com.

As a final note, and I can’t emphasize this enough, if any of your accounts offer multi-factor authentication, take advantage of that. If someone does get your password, the second authentication factor will be the only thing preventing them from logging in as you.