CM WEALTH ADVISORS

PERSPECTIVE

Cybersecurity and the Family

By Douglas Smorag November 2019

You and your family are online. Whether you like it or not, this makes you visible around the world. There are currently over 10 billion internet connected devices and it is estimated that one in 15 people will become a victim of identity theft…and that includes your children.

Knowing what to look for can significantly reduce the risk of a cyberattack. This ***PERSPECTIVE*** will attempt to give you some direction to help keep you and your family safe from attack.

Phishing Scams are Increasingly Sophisticated

Email phishing scams are 92 percent of cybersecurity issues…92%! We rarely get the email from exotic places asking for money now; instead, the hackers come at us pretending to be someone we trust…or fear. Banks, Amazon, cell phone companies, UPS, the IRS and even Medicare emails are being spoofed. Here is what to watch for:

1) Any email asking for private information such as passwords, account numbers, sensitive information, etc.…and I mean **ANY,** do not respond to these emails. If you think they may be real, call the organization or go directly to their website to check. Do not call the number in the email, and NEVER click on a link in an email unless you are certain where it will take you.

2) Another warning sign is unusual language, typos or strange wording (as if the sender does not know English). This includes emails from actual friends whose email account may have been hacked.

3) If a friend's email account is hacked, the hacker is certain to send emails to the entire contact list. When you get an unexpected email and it asks you to click on a link or open a file (like a video), call your friend to check if they really sent it. It is much harder to impersonate a voice or steal their phone.

4) Lastly, and staying with the thoughts in the first three above, it is unwise to click on a link or open an attachment through email or social media without talking to the person who sent it. That attachment could be harboring malware that can take you weeks, or even years to recover from.

Internet Connected Devices and Sensitive Information

With cyber-connected devices of all types (door bells, refrigerators, baby monitors, etc.) there are numerous new ways for a cyberattack to take over your entire system. That cyber-connected baby monitor is a great idea…until it isn't. The usual cybersecurity guidelines still apply to this equipment, including strong passwords, multifactor authentication, security updates and others. Always do your best to avoid using public Wi-Fi (coffee shops, restaurants, hotels) as those networks are NEVER secure.

Ultimately you need to ask yourself if it is necessary for the device to be connected to the internet. If it does, it is wise to put the device on a different network than your main computer. The last thing you want is someone to hack into your baby monitor's video system!

Your Child's Identity

The news media is full of stories about senior citizens falling for various scams, but the reality is kids are more likely to be affected by identity theft. Why? Because from the time they get a social security card (right after birth) until they are 18 years old, they do not look at their credit report. That allows the bad guys to take out credit in your child's name without much notice, racking up big debt in the meantime.

How do you stop this? First, pull a credit report on your child (which are free annually) to make sure everything looks right. Second, and probably most importantly, is to put a credit freeze on all your children's accounts with the three major credit bureaus. This free tool is one of the easiest ways to prevent your child's identity theft by stopping anyone from accessing their credit report. Since most new accounts cannot be approved without the report, it makes it much harder for identity thieves to use their information.

The three national reporting agencies are:

1. Equifax® - www.equifax.com – 800-685-1111
2. Experian® - www.experian.com – 888-397-3742
3. TransUnion® - www.transunion.com – 888-909-8872

A credit freeze does not affect your credit. It also does not affect your credit score. It remains in place until you ask the credit bureau to lift the freeze. If you are applying for credit (for an auto loan, etc.) it would be helpful to find out which agency they are using because you must call to lift the freeze. It may take an hour to lift the freeze.

Oversharing on Social Media

So, you are on a great vacation, taking a lot of pictures, and figure you want to post them on Facebook/Instagram or other social media to show everyone how much fun you are having. You might as well hang a sign on your front door that says, “Please rob my house”.

It is fine to have public social media pages but do your best to avoid sharing personal information…especially vacations. And do we really keep in touch with or need 1,000 friends? Remove the people you don’t know, strengthen your security settings relative to who sees what, or just stop posting personal information.

Also keep in mind that every time a social media site like Facebook does a security update, there is a pretty good chance that they will reset your security settings to a weak default setting, so check these settings regularly. You may also want to set up multifactor authentication on sites that allow it. Multifactor authentication includes such things as a combination password and finger print or code sent to your cellphone.

For Those That Travel

Travelers make easy, unsuspecting targets. Everyone should be aware that there are hackers everywhere trying to take advantage of you, and they love to prowl the hot destinations like Las Vegas, Disneyland, New York City, Paris.

You’re at a hotel and want to catch up with a few work emails. You pull out your iPad and look for the hotel wi-fi (that’s secure isn’t it?). You see these options: Hotel-wi-fi, Hotel-Guest, Guest. Pick the wrong one, and you could be falling into a trap laid by a hacker waiting to steal all the information you have. It is extremely easy for the crooks to set up phony hotspots and wait for you to log on, which would allow them to see everything you are doing, like getting into your bank account, or working on a proposal for your biggest client.

So, what do you do? The easiest is to bring your own personal hotspot. Most cell phones and carriers allow you, with the touch of a button, to turn your phone into a roaming hotspot. Then you just pick your own phone out of the wi-fi list that shows up on your device. In the alternative, if you must use public wi-fi, use a clean device, which is a device without any personal information on it. This way, even if the hacker gets in, there is nothing to steal.

Don’t Tell Apps Your Secrets!

Many cellphones and mobile apps, without your knowledge, gather data and personal information on a continuous basis. Information such as your location, shopping habits, web sites you like to visit and other personal information. What do these apps do with this information? A lot, including but not limited to sharing the information with other companies, including advertisers.

When you download an app, they may ask your permission to track your location and other data. Do they really need the data? Does your solitaire app really need access to the inner workings of your phone, your GPS, your contact list and the internet? Does it need access to your microphone? Your camera?

How do you protect yourself from bad apps? Research the app before downloading it. Read the reviews. Do a quick internet search to find possible consumer complaints, lawsuits and privacy violations. Pay attention to what your children are downloading because games are particularly vulnerable to privacy violations. You do not want the bad guys listening in or watching you through a phone or portable device because some mobile game allowed it to happen.

It is also very important to keep your software up-to-date because many updates contain security fixes. Hackers look for devices that have not updated their software or apps.

Final Thoughts

It only takes a few minutes for your data to be compromised and only a small percent of hacks are discovered quickly. Two-thirds of attacks take months to reveal themselves, and you usually find out from a third party (like your bank). This may seem like a lot of effort, but it is much easier to prevent an attack than it is to detect one and reverse the damage that occurs.

If you run into a problem and think your system has been compromised, please call Karrie Turczynskyj (216) 831-4040 or Doug Smorag (216) 831-4105 at CM to help you walk through the first steps to recovery.

Safe surfing!