Ulliance
Enhancing People. Improving Business.

The Life Advisor
Improving the lives of the people we help.

October, 2019

How To Be Safe Online

Cybersecurity is a booming industry. For a great many of us, just about every aspect of our life – family, work, social, financial – touches on technology in some form or fashion. We share about our personal lives on Facebook, Instagram, Twitter, and other platforms. Many of us do our banking online – if not exclusively, then at least in terms of having our bank app on our phone and/or checking account balances online via the bank website. And many of us field emails and phone calls as part of our daily job, with a number of workplaces providing some kind of remote access (work cell phone, remote VPN, etc.) for this information at any time.

For these reasons, we need protection. And while there is computer virus/malware protection we can purchase, and volunteer benefits like IDShield we can opt in to help protect us, there are some things we can do by ourselves, with minimal technical know-how, to ensure that we are being a little safer online.

Recognize that there is no such thing as privacy online.

Even if you delete your browsing history, even if you use a "private" or incognito browser, there is no absolute privacy. It is best to act online as though every website you visit, every keystroke you make, and anything you post could be made visible to anyone in the world with an internet connection at any time. It's especially important to be cognizant of this if you use a work computer. Be aware of your company's technology and (if applicable) social media policy. Most company policies specify that work property, including computers, is only to be used for work-related reasons. Your company's IT department likely has the means to look at everything you look at while at work – so be cautious, be wise, and be safe.

Be cautious when prompted to "register this computer/device."

Bank websites and other financial institutions (student loan vendors, 401K and retirement plan providers) will often automatically prompt you to "register this computer [or device]." Unless you are on your own private computer or tablet at home, *do not* register the computer or device you are on. You may have to answer additional security questions by not registering, but better safe than sorry. Unless you are the *only* person who has access to the computer/device, don't register it with the website.

Use complex passwords.

Coming up with passwords is frustrating for many of us, especially as more and more websites require more and more complex passwords (e.g., upper- and lower-case letters, at least one number, and at least one special character). But complex passwords are a better safeguard against hackers than simple passwords, easy-to-guess passwords, or passwords based on a name or place. Use upper - and lower-case letters, numbers, special characters, and do not use the same password for multiple systems. Also, remember to change your passwords on a regular basis – workplaces which utilize password access to work computers often require employees to reset their password every few months. You might also consider looking into a password management system - a web-based database that manages your passwords for you, but keep in mind even these systems have their vulnerabilities.

Alert your IT department if you receive any suspicious emails.

Our IT team here at Ulliance will send frequent annotated emails to illustrate how "phishing" works. Phishing is the term used to describe gaining access to confidential information by impersonating someone online. If you receive an email that *looks* like it may have come from your boss or a peer, but it doesn't look like the usual emails you receive, notify your IT department immediately. Hackers have gotten much more sophisticated in their ability to disguise themselves. You especially want to be cautious of emails that request confidential information. Again, alert your IT department if you receive these sorts of messages.

Don't share more information than necessary.

Enough said. If you can opt out of providing private and/or sensitive information, do so. Be cautious when asked to provide this information anywhere online, and do *not* provide the information to any source you are not familiar with.

Captain Cyber Security says:

Treat your passwords like your underpants!

- Change them often.
- Don't leave them lying around.
- Don't share them.