Personal Cybersecurity: What to Do

CYBER CRISIS was written primarily to raise your consciousness about the personal impact of some of the internet concepts and conditions that may seem far removed from the smartphone in your hand, or from your tablet, computer, or gaming device. However, I would be remiss if I did not offer some "how-to" advice in the form of fundamental cyber safety tips. (As with almost everything in the realm of personal online safety, there are many and varied opinions about what should be part of the routine.)

Personal Cybersecurity Basics

- Use anti-virus and anti-spyware protection for your computers, tablets, smartphone, and even gaming devices.
- Software, operating system, app, and browser security updates are frequent and essential. Download the latest online safety updates and patches when advised by a trusted vendor to do so.
- Load security software that protects kids from clicking on links and sites that could be harmful.
- Configure your home Wi-Fi network to require a unique password for authentication.
- Back up your critical files so that if you are hacked, you may still have access to uninfected versions.
- Monitor your financial accounts, credit card, and credit information, for any unusual activity that could indicate a hack of your personal data.

An excellent resource for personal privacy tips (written in plain English) is offered by TRUSTe, a provider of privacy management solutions. https://www.truste.com/consumer-resources/personal-privacy-tips/. I highly recommend reading it.

Passwords

- Always use passwords and change them often. Put the next date to change your passwords on your calendar. Be sure that everyone in your family, social and work groups do so as well.
- Use complex passwords, including a mix of letters and numbers. A password generator can do this for you. Here is one example, courtesy of Norton: https://identitysafe.norton.com/password-generator#
- Use different passwords for your major online accounts, including banking, health care, government-operated sites and social media.
- Make password management easy on yourself by using a password manager. If you do this, all you have to remember is one password: the one that unlocks the digital vault of your passwords. Here are some ideas: http://www.pcmag.com/article2/0,2817,2407168,00.asp
- For your most important accounts, use two-factor authentication (easier than it sounds). It typically involves receiving a numerical code sent by SMS to your smartphone, to be used along with your password. Here is more information for your consideration. https://www.onionid.com/blog/2-factor-authentication-a- primer/

- Remember to sign out when finished with sites where you must sign in.

Email

- Do not open email messages if you do not recognize the sender. Delete them.
- Never click on links in or attachment to emails, texts, or other internet-borne communications that you do not have a good reason to trust.
- Use a secondary, “spam” email address for enrollment on sites that you believe will want to add you to their email lists (most) and likely send you spam or unwanted advertising.
- Don’t send private or sensitive email over public Wi-Fi networks (e.g., the one at your local coffee shop). Also, avoid banking or shopping online from public computers.

Social Networks

- See the Passwords section above!
- Take advantage of social network privacy-enhancing capabilities and options, and proactively manage them. Under Settings or Options, filter how people can search for you, make comments, see photos tagged with your name, and learn how to block people. Revisit these settings periodically so as to take advantage of the latest options.
- Only accept new invitations you receive on social networks if you know or can qualify the person as trustworthy.
- Minimize your personal information sharing. What you share will become part of your online reputation and precede you in many future situations.
- If you have determined to not be a part of a particular social network any longer, go to the trouble of officially terminating your account and deleting your content.

Browser Security and Privacy

Internet browsers have a variety of privacy-enhancing capabilities and options that can be a crucial part of your online protection. Here are links to view the privacy options for some of the major browser providers:

- Internet Explorer / Microsoft http://www.microsoft.com/privacy
- Chrome / Google https://www.truste.com/consumer-privacy/personal- privacy-tips/
- Safari / Apple http://www.apple.com/safari/features.html#security
- Firefox / Mozilla https://support.mozilla.org/en-US/kb/settings-privacy- browsing-history-do-not-track

If you want or need more information, you already know how to get it: Google, Bing and a host of other search engines and websites will take you there. If you want a different, more advanced, or technical approach, simply Google the term “online safety”—about 930,000,000 results will come up. Even just grazing the first few pages of these results, or entering more specific terms, will take you directly to considerably more information than space here permits.

CYBER CRISIS – It’s Personal Now by William Keiper is available on Amazon: https://goo.gl/Otnomc