Cybersecurity for the Confused, i.e., All of Us

Sheldon Greaves, Ph.D. – 25 April 2019

This is a summary of measures you can take to enhance your security online.

Basic Precautions:

1. **Secure your passwords**.
   Visit "Have I Been Pwned?" (https://haveibeenpwned.com/) to see if your passwords appear in major password lists.
   Visit "How Secure Is My Password?" (https://howsecureismypassword.net/) to experiment with possible new passwords.
   Use a different password for each of your accounts. If any accounts offer Two-Factor Authentication, use it.
2. **Set New Passwords for Your Home Network**.
   Ask your ISP provider how to change the password on your cable modem, and any other routers or repeaters in your network.
   Set up a "guest" network on your home Internet connection to limit access to your personal machines.
3. **Secure all Internet of Things (IoT) Devices**
   Change the default passwords on your devices.
4. **Always perform updates when they become available.**
   This applies throughout your system; operating systems, applications, etc.
5. **Install good anti-virus software on your computer and mobile devices.**
   Be careful to use just one software package to avoid competing protection protocols.
6. **Set up regular file backups.**
   Ideally, this should include both cloud-based and local hard drive backups.
7. **Beware of Phishing!**
   Don't click on links or download attachments from suspicious emails. Check first!
8. **Freeze Your Credit**
   Also check with your bank and other financial institutions to learn about their anti-fraud measures. Do the same with your credit cards to see what kind of coverage they have in the event of fraud.

Privacy Tips:

- Use web browsers with a Virtual Private Network (VPN).
- Check the "Do Not Track" option in your browser settings.
- For social media accounts, review your privacy settings and use the highest level that you can.
- If you use SMS/text messaging, use an app that features end-to-end strong encryption.
- Use search engines that don't collect information on your searches such as https://duckduckgo.com or https://startpage.com
- Request removal of your profile from info sharing sites. This article explains how to do that: https://medium.com/@tamaragane/how-to-remove-your-information-from-sites-like-mylife-77f89aff1aff
  - *Note: there are a lot of these kinds of "personal information" sites out there, and this article only covers the major ones. You will need to do some sleuthing to find others.*
- *Get involved*: support legislation that protects personal privacy and net neutrality.

A Brief Glossary of Cyber Security Terms

Cloud	A technology that allows us to access our files and/or services through the internet from anywhere in the world. Technically speaking, it's a collection of computers with large storage capabilities that remotely serve requests.
Software	A set of programs that tell a computer to perform a task. These instructions are compiled into a package that users can install and use. For example, Microsoft Office is an application software.
Domain	A group of computers, printers and devices that are interconnected and governed as a whole. For example, your computer is usually part of a domain at your workplace.
Virtual Private Network (VPN)	A tool that allows the user to remain anonymous while using the internet by masking the location and encrypting traffic.
IP Address	An internet version of a home address for your computer, which is identified when it communicates over a network; For example, connecting to the internet (a network of networks).
Exploit	A malicious application or script that can be used to take advantage of a computer's vulnerability.
Data Breach	The moment a hacker successfully exploits a vulnerability in a computer or device, and gains access to its files and network.
Firewall	A defensive technology designed to keep the bad guys out. Firewalls can be hardware or software-based.
Malware	An umbrella term that describes all forms of malicious software designed to wreak havoc on a computer. Common forms include: viruses, trojans, worms and ransomware.
Virus	A type of malware aimed to corrupt, erase or modify information on a computer before spreading to others. However, in more recent years, viruses like Stuxnet have caused physical damage.
Ransomware	A form of malware that deliberately prevents you from accessing files on your computer – holding your data hostage. It will typically encrypt files and request that a ransom be paid in order to have them decrypted or recovered. For example, WannaCry Ransomware. For more information on Ransomware, check out our free Ransomware Guide.
Trojan horse	A piece of malware that often allows a hacker to gain remote access to a computer through a "back door".
Worm	A piece of malware that can replicate itself in order to spread the infection to other connected computers.
Bot/Botnet	A type of software application or script that performs tasks on command, allowing an attacker to take complete control remotely of an affected computer. A collection of these infected computers is known as a "botnet" and is controlled by the hacker or "bot-herder".
DDoS	An acronym that stands for distributed denial of service – a form of cyber attack. This attack aims to make a service such as a website unusable by "flooding" it with malicious traffic or data from multiple sources (often botnets).
Phishing or Spear Phishing	A technique used by hackers to obtain sensitive information. For example, using hand-crafted email messages designed to trick people into divulging personal or confidential data such as passwords and bank account information.

Soruce: "16 Cyber Security Terms That Everyone Who Uses A Computer Should Know"
https://www.cybintsolutions.com/16-cyber-security-terms-that-you-should-know/