Internet Risks

Because the Internet has become such an integral part of everyday life, it is easy to forget that our connection can leave us vulnerable to an array of cyber attacks. Anti-virus protection is a necessity, but software updates cannot always keep pace with the latest evolving threats. To help minimize online risk, the following software also needs to be updated: Adobe products, such as Acrobat, Reader, and Flash Player; browsers used to access the Internet, such as Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, and Apple Safari; Oracle Java, a program that enhances the Internet experience by powering features such as real-time chatting, gaming, and e-commerce; and finally, device operating systems such as Microsoft Windows, Apple Mac OS X and iOS.

Malware

Malware is a term for malicious software intentionally designed to disrupt computer operations, gather sensitive information, or gain access to private computer systems.

Spyware

Spyware is a term for applications that send information from a computer to a third party without the user’s knowledge or permission.

Social Engineering

Social engineering is a method of hacking that relies on human interaction and deception to bypass security procedures and obtain confidential information. Social engineering is often accomplished through a scam email or text message encouraging the recipient to click a link in the message. The embedded link will either direct the user to a website where they are prompted to enter personally identifiable information, or begin to download malware.

Social Media

Social media are on-line publications or websites designed to facilitate social interaction, often in real-time. Examples include Facebook, Twitter, LinkedIn, and YouTube. Information posted to social media sites can give cyber attackers valuable details that can help them design a sophisticated social engineering attack.

Scraping

Scraping, also called screen scraping, is the process of taking information posted on a social media or web site and using it to breach the owner’s accounts or commit fraud involving identity theft. Due to the growth in social media sites such as Facebook, it is becoming a popular method for cyber criminals to easily obtain information for fraudulent purposes.

Internet and Social Media Best Practices

* Use firm-approved software and browsers, and lock your computer when away to ensure others can’t access the Internet in your absence.

(Continued)

* Pop-up windows are often associated with spyware and clicking a link or button in a pop-up window might launch a spyware installation. When closing a pop-up window, click the Close button, X, in the title bar of the window rather than a Close button or link in the pop-up box to reduce the chances of installing malicious software.
* Only download programs in compliance with firm policies and guidelines and be wary of ‘free’ software.
* Contact the Information Technology department regarding suspicious dialog boxes related to running or installing software. If you think your computer might be infected, contact the appropriate person immediately.
* Review the Terms of Use for all social media sites in which you participate and use privacy settings on social media sites to control what information is visible to the public.