CITADEL
INFORMATION GROUP, INC.

A Personal Guide to Staying Safe Online

Distrust and Caution are the Parents of Security … Benjamin Franklin

Cybercriminals want your bank account and credit card numbers so they can take your money and use your credit while stiffing you or your bank with the bill. They want your social security number so they can apply for credit in your name, stealing your identity. They want your medical id so they can have medical care in your name. They want control of your computer so they can use it to commit other cybercrimes. All the more so if your computer is connected to your corporate network.

Cybercriminals want to take control of your computer. This control lets them install rogue programs on your computer, turning your computer into a *zombie* under their control—the cyber-equivalent of *Night of the Living Dead*. These control programs make money by stealing your information, sending spam, displaying pop-up ads, and committing sophisticated computer crime.

Defense Strategy 1: Keep Cybercriminals Off Your Computer

a. **Keep Systems Patched:** Software manufacturers issue program updates containing *patches* to fix known vulnerabilities. Set *Microsoft Windows* and *Office* to automatically update. Turn on automatic updates whenever you can, including Adobe Acrobat and iTunes. Make sure you manually update programs that don't update automatically. Pay particular attention to Flash and Java, as these are particularly vulnerable. Subscribe to Citadel's FREE *Weekend Vulnerability and Patch Report*.

b. **Limit Exposure:** Create separate accounts for all family members. This is done in the *Windows Control Panel*. Set all user *account types* to "Limited" rather than "Administrator." An Administrator account should only be used when doing systems work. This makes it harder for cybercriminals to install malware on your computer.

c. **Protect Your Desktop:** Install a *reputable antivirus / antispyware product* & keep it up-to-date. Sophisticated cybercriminals can get past basic antivirus/antispyware software. Antivirus is necessary. You need it. But it is not sufficient.

d. **Secure Your WiFi:** If you have a wireless network, encrypt it with WPA2 encryption and use a strong password. Otherwise anyone near you can eavesdrop on your communications and piggy-back on your connection.

e. **Stay Away from P2P Networks:** Don't run Peer-to-Peer or other file sharing programs, such as *Kazaa*, *Limewire* or *BitTorrent*. These networks provide strangers access to your computer.

Defense Strategy 2: Don't Become a Social Engineering Victim

a. **Don't open unusual or unexpected email attachments, not even from people you know**. It's easy to send an email so it looks like it came from someone else. Also, how do you know your friend's computer hasn't been taken over? *Distrust and caution*.

b. **Don't follow links in unexpected or unusual emails**. While a SPAM filter can help, you must be on guard for emails that get past your SPAM filter. *Distrust and caution*.

c. **Don't click on web-site ads or pop-ups offering to scan your computer for free**. Cybercriminals love to take advantage of people's fear of getting a virus. Instead of scanning your computer, these programs will infect it. *Distrust and caution*.

Defense Strategy 3: Be Careful On-Line

a. Never send your Social Security Number, bank account numbers or credit card numbers in unencrypted email.

b. Use different strong passwords [12+ characters, upper & lower case, numbers, characters] for all eCommerce websites. Use a program like *Keepass*, *RoboForm*, or *Lastpass* to securely manage online passwords. And make that master password at least 15+ characters.

c. Use *Two Factor Authentication* when available. This provides an important extra layer of security should your password be compromised.

d. Only buy on-line from merchants using SSL, which means the website address begins with https://. Look for the "lock" on the title bar of *Internet Explorer* or on *Firefox's* upper-left corner.

e. Use a credit card rather than a debit card when shopping on-line. Link PayPal to your credit card, not your bank account. Federal law limits your credit card exposure to $50. There is no corresponding limit if you use a debit card (even though many banks cover debit card fraud).

Defense Strategy 4: Protect Your Information Away from Home

a. Use your operating system's built-in encryption to encrypt the hard drive of your laptop, protecting it with a strong 15+ character passphrase. If you lose the laptop, the information is still safe.

b. Keep WiFi and Bluetooth turned off except when you are using them.

c. Never use a public computer, Kiosk, or public Wi-Fi for online banking, shopping, to access sensitive information, or for anything that requires a password. Since you don't know how secure these are, prudence requires you to assume they are insecure.

Defense Strategy 5: Watch Your Credit

a. Subscribe to a basic credit monitoring service (AAA California offers members a free service)

b. Regularly review your bank, credit card, investment accounts, and medical explanations of benefits for fraudulent activity.

c. Check your credit report regularly. You can get a free annual credit report from each of the 3 bureaus. https://www.annualcreditreport.com/index.action.

d. For more tips, including freezing and locking your credit, see http://citadel-information.com/2014/12/sony-hackers-personal-information-can/.

Defense Strategy 6: Better Safe Than Sorry

a. Always think about the information you are giving out.

b. Stay up-to-date with our *Cyber Security News of the Week* and our *Weekend Vulnerability & Patch Report* available Sunday. Sign up for FREE at www.citadel-information.com

c. When in doubt, don't.

d. If you want to be sure, just ask: info@citadel-information.com.

Citadel Information Group

Delivering *Information Peace of Mind* ® to Business and the Not-for-Profit Community

© Copyright 2017. Citadel Information Group. All Rights Reserved.