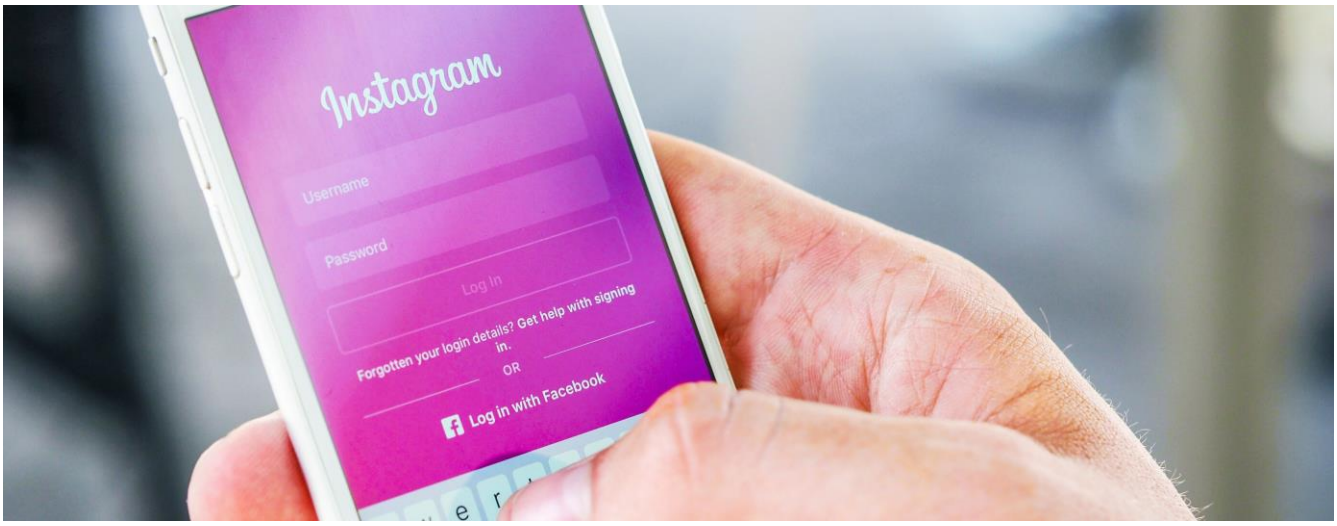
# SECURITY AWARENESS NEWSLETTER




## DO NOT USE THE SAME PASSWORD FOR EVERYTHING

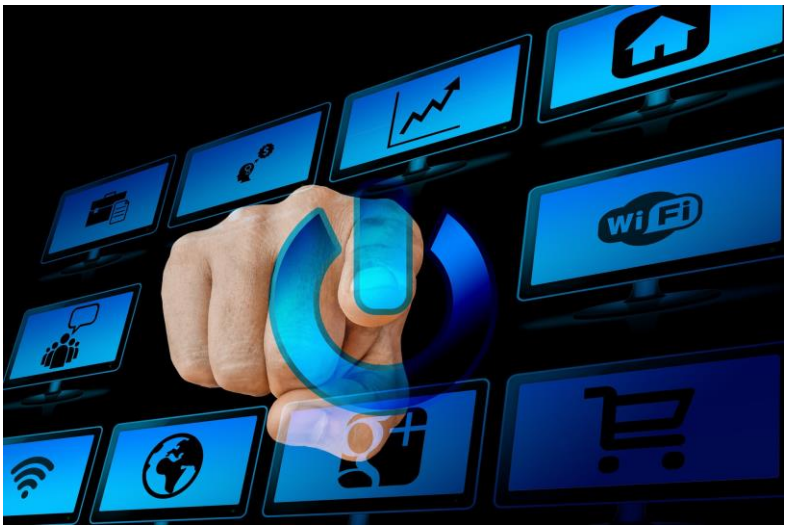
An attendee of a training program for a new software package to set up login accounts mentioned using the same password for everything to make it easy to remember. As a security professional, I said that this was a bad idea because, if the password was disclosed, the "bad guy" would have the keys to all their information. The attendee scoffed and told me it did not matter because the password was a word from a foreign language. The person then sat down to create his account on the computer that was attached to the overhead projector. He typed his password into a non-masked field, exposing it to everyone in the room. My security advice was proven true.

## BEWARE OF USB FLASH DRIVE'S AUTOPLAY FEATURE

A white hat hacker broke into a bank and left 20 USB tokens lying around the parking lot of the bank for employees to find. When they plugged in the USB token, the Trojan backdoor was installed on the employees' computers and the hacker was into the banks network! Some employees claimed they were being helpful — trying to find the token's owner, others were curious about the token's content, still others thought they had scored a huge USB token and tried unsuccessfully to reformat the token. Unfortunately the new "U3 Technology" on these tokens prevented a hidden partition from being deleted, and it contained a remote access Trojan which installed itself by emulating a cdrom and using WinXP's Cdrom autoplay feature.

CYBER ZONES
Cyber Security Services

SECURITY AWARENESS NEWSLETTER




# Four Tips to Help Keep Your Computer Secure

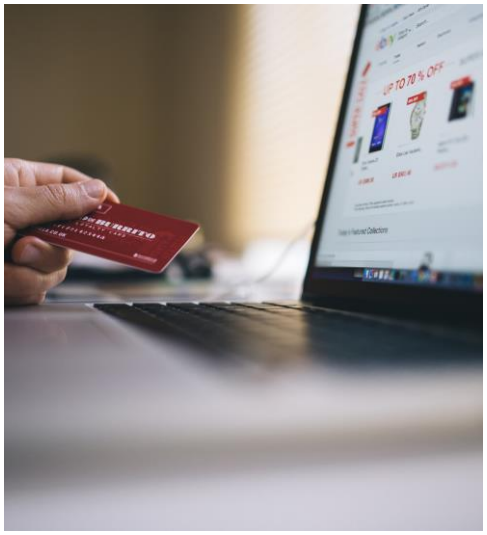
1. Anti-virus. A reliable, effective anti-virus program with the latest updates. Both licensed and free anti-virus software are available. Whichever you use, make sure it scans incoming and outgoing emails for malware.
2. Anti-spyware. Reliable effective anti-spyware is a must for securing your computer. Both licensed and free anti-virus software, such as Windows Defender, are available.
3. Two-way Personal firewall. Two-way personal firewall software monitors network traffic to and from your computer and helps block malicious communications.
4. Anti-Keylogger software. Anti-Keylogger software products, like AntiLogger and Keyscrambler Personal, help prevent what you type on your computer, especially sensitive information such as the usernames, passwords, and financial information you use in making online transactions,

# Wireless Hotspots...limit activity to web surfing only

A hotspot is an open wireless network that is available (open) to everyone. An example would be the wireless network at your favorite coffee shop. These networks hook computers into the public Internet — handy but dangerous. Because wireless hotspots are for open use, they don't provide much protection for your data.

When using a wireless hotspot try to limit activity to web surfing only. You should also disable peer-to-peer networking, file sharing, and remote access.

Always use a good personal firewall and of course make sure all your software including your operating system (like Windows) is up to date and patched. You should never use hotspots for online banking, bill paying, or for making purchases that require you to give out confidential information such as a credit card number.



***Only deal with reputable companies that you know and trust***

***At the very least be sure the company has a physical address and phone number. If you haven't done business with the company before, visit the Better Business Bureau online (http://www.bbbonline.org) and do some research. Check the company's website for feedback from previous customers.***