Computer Security Tips for Cyber Monday

What could be more convenient than shopping on-line right from your laptop, desktop or mobile phone on Cyber Monday? There are no jostling crowds of shoppers and no long lines to stand in; no snarled traffic or nasty weather to contend with. But on-line dangers abound, including risks of identity theft, retail fraud, phishing scams, phony charitable organizations looking for "donations," and various other cyber-attacks, any of which could turn a holiday shopper into a computer crime victim.

Here are some "cyber" security tips that can help you to avoid some of these inherent risks when using the internet and while shopping on-line during Cyber Monday and throughout the year:

- *Use anti-virus software.* Installing anti-virus software and updating it regularly are among the best defenses against cyber-attacks. Never open e-mails from anyone you don't know. To be even safer, scan attachments with anti-virus software before opening them.

- *Install a firewall.* A firewall is a software program that examines information coming into and leaving the network and only allows authorized traffic to go through. You decide what content is permitted and which should be blocked. Firewalls can also prevent unwanted access to your network.

- *Stay current with software updates and security patches.* Download fixes as soon as they are available and always back up your data. Security apps and browser extensions that block pop-ups and detect malware will give you added protection.

- Because many people shop on-line by using their mobile phone instead of, or in addition to, their personal computers, it is recommended that you *enable "timeouts" on your mobile phone*, in the event that your phone is lost or stolen. This would entail enabling a lock screen password that you would use to "unlock" your phone after it had

automatically timed-out after a set, but brief, duration of time when the device is on, but isn't in active use.

- *Create and use strong passwords.* Passwords are essential to maintaining network security and protecting personal information from prying eyes. Poor passwords are often the weakest link in internet security: they provide an easy way for hackers to access your digital device so as to unleash a virus or to access sensitive material.

- *Log off when you are done for the day.* Your computer system is most vulnerable when connected to the internet.

In addition to taking the "concrete" computer-security measures recommended above, it also is important to develop and maintain a proactive mindset and a sensibly cautious mental attitude when navigating the internet, and to do so *before* any trouble crops up. Even if the very best security software is loaded on your computer, and you've signed-up for the most comprehensive identity protection service around, you'd still be quite prudent to adopt an approach to cyber security akin to the "defensive driving" attitude that should come into play when you're behind the wheel of a motor vehicle.

- *Be skeptical and don't believe everything you read online.* Take appropriate precautions and try to verify the authenticity of any information before taking any action.

- *Beware of online scams.* Avoid suspect emails, as these may be phishing scams aimed at obtaining your personal information. No matter how enticing the sales pitch, don't click on pop-up ads: "x" them out when they pop up. In these and almost every other trick-of-the-trade, if a deal seems too good to be true, it probably is!

- Before placing your order on-line, always check to make sure that *there is an "s" after the "http"* in the address bar of your Web browser. By looking for and finding the "https" in the URL, you can be reasonably assured that your personal information is being entered on a secure website.

- *Check the privacy policies of the on-line sites you visit.* Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam.

- *Keep the amount of personal information that you post on-line to a minimum.* Do not post personal information that could make you vulnerable to ID theft. Seemingly common information could prove valuable to an experienced identity thief or hacker. Banks, credit card companies and other financial institutions many times use personal information, such as a customer's birthday, address, or mother's maiden name for security questions to validate identity in order to access customer accounts.

- *Do not divulge your credit information or Social Security number* to unauthorized individuals. Keep your credit cards physically secured when they're not in your immediate possession.

When shopping on-line:

- When shopping on Cyber Monday or at any other time – and whenever you make use of personal information, such as account numbers, while on-line - *make sure that the Wi-Fi network you use is secure.* Hence, rather than using the Wi-Fi networks available in public places like airports and coffee shops - where there is no guarantee of internet security and there is a high risk of susceptibility to hackers – do your shopping at home, or at a location whose Wi-Fi network security can be assured.

- *Patronize companies that you are familiar with and trust*. If you've never heard of a company, do some on-line research and check the company's background. And before you purchase something, make sure that you've researched the item so as to be sure that you are purchasing a quality product: Shop with trusted brands that can guarantee the quality of their products and offer a valid warranty in case you end up with a defective product or an infected digital device.

- When making your on-line purchase, it is recommended that you *use a credit card instead of a debit card, or a wire or bank transfer*. Credit cards have built-in safeguards to protect you against identity theft. And by using a credit card, you have a better chance of getting your money refunded if you happen to end up with product that is defective or fraudulent.

- Better yet, rather than using your "usual" credit card, consider paying for merchandise that is bought at on-line stores and auction sites with *single-use, disposable credit cards,*

also known as virtual credit card numbers. These are offered by some (but not all) banks and they provide an additional layer of protection when shopping on-line. The virtual credit card number usually has a dollar amount and a timeframe that you set yourself. And it can be a smart choice when you want to purchase things online from an unfamiliar website, because they protect your real credit card account number from identity thieves

- *Save all of your sales receipts; print out and retain the confirmations from your online purchases*. By starting a file folder to keep all of these receipts well-organized and in one place, it will be easier for you to verify credit card and bank statements as they come in, which could provide a real organizational advantage for you during the hectic holidays!

- Carefully *review your bank and credit card statements* for irregularities. *Regularly check your credit report* with one of the three major credit agencies (*Equifax, Experian,* and *TransUnion*).

If you suspect that you have become the victim of identity theft, fraud or any other type of criminal act, *take quick action in response*! Report all suspicious activity to your financial institution(s) and law enforcement, and quickly implement the self-protective response measures recommended by trusted professionals, industry and institutional experts, and by law enforcement personnel, in order to limit present and future damages and losses, and to speed recovery and a return to normalcy.

Once again, I hope that you have found these tips and reminders to be useful, especially if you plan on taking advantage of the abundant bargains that will be offered on Cyber Monday. Being cyber-security savvy while on-line will help to minimize your exposure to cyber threats and on-line risks, so that you may more easily shop on-line with confidence.

Please do not hesitate to contact me, the Area Vice President or the Branch Manager serving your Securitas account, if we can answer any questions or, in any way, further promote Securitas' partnership with you. Thank you.

Richard K. Avery CPP
President - Northeast Region
Securitas Security Services USA, Inc.
O:☏ (617) 568-8701
F:🖷 (617) 568-8814
Toll free 1 800-225-6146