Seven Cybersecurity Myths Busted

(NAPSA)—It's a common occurrence these days—one of your friends recently had an online account hacked but doesn't have a clue how it happened. We've all heard tech advice from a tech-savvy sister or the IT guy at work, but what's the truth? When it comes to online security, it's sometimes difficult to discern between perception and reality.

Online threats are changing and becoming more sophisticated. In 2012, we saw constant and continued innovation from cybercriminals. For example, there were more online attacks taking advantage of previously unknown security gaps than any year before; attacks continued to spread across an increasing number of popular social networks, and cyber and industrial espionage is now a reality.

With a constantly changing online world and security landscape, it seems most people are still confused about existing threats and their impact, as well as what they can do to protect themselves. Luckily, Symantec—maker of Norton security software—recently released its annual Internet Security Threat Report, which shines a bright light on the topic and helps clarify some common misconceptions around cybersecurity:

Myth #1: Viruses and other malicious software ("malware") only affect computers and laptops.

Reality: Mobile malware, which affects smartphones, tablets and other mobile devices, increased by 58 percent last year. This malware can steal information such as phone numbers and e-mail addresses (32 percent of the time), or use the phone's GPS to track the user (19 percent of the time).

Myth #2: I can't get a virus or be attacked on popular social networking sites.

Reality: Many well-known social networks, including several of the newest ones, are prime targets for scammers, with 56 percent of social media attacks involving fake gift cards and survey scams.

You can protect yourself from cybercriminals.

Myth #3: Apple products aren't susceptible to viruses and online attacks.

Reality: While hackers still primarily target PCs, more than 600,000 Mac computers were infected by one attack last April; just one example that no operating system is safe from online threats.

Myth #4: Free antivirus software on my computer provides complete protection.

Reality: "Ransomware" (which cybercriminals use to lock you out of your computer unless you pay their "ransom"), is one example of the trend toward increasingly vicious malware, which is known for being harder to undo, more aggressive and more professional than other malware. This malware requires protection beyond what basic, free antivirus software can offer.

Myth #5: It's easy to tell if a site is fake—typos or foreign characters are dead giveaways.

Reality: Many spoofed sites today look exactly like the websites of legitimate brands, down to the smallest details. Additionally, the number of fake sites that imitated social networks more than doubled in 2012.

Myth #6: My computer won't get infected since I don't visit risky sites.

Reality: Sixty-one percent of malicious sites are actually legitimate websites that have been compromised and infected with malicious code. Business, technology and shopping websites were among the top five types of sites hosting infections.

Myth #7: I'll know right away if my computer is infected.

Reality: Cybercriminals today rely on stealth—the longer they're on your machine undetected, the more damage they can do. Your computer could even be part of a "botnet"—a network of remotely controlled computers that send spam e-mails or participate in widespread attacks—and you might not even know it.

Protecting yourself doesn't have to be complicated. By continuing to educate yourself about online threats, taking advantage of available security resources and following the simple tips below, you can protect yourself against cybercrime.

- Use complex and unique passwords for each site, including upper- and lowercase letters, numbers and symbols.
- Stick to trusted websites when possible. When purchasing items online, check for security marks on the site before entering in your payment details.
- Limit your sensitive transactions when using public Wi-Fi networks or use a Virtual Private Network ("VPN"). Wi-Fi networks can allow other people to more easily snoop on your activity.
- Never click on links or open attachments from people you don't know. Also, if you receive a strange message from a friend, take a moment to verify it—it's possible his or her e-mail or social networking account was hacked.
- Make sure you protect all your devices with a comprehensive security solution, like Norton 360 Multi-Device.

For more information, go to www.symantec.com/threatreport.