Diligence Is Key For Student Safety In Cyberspace

(NAPSA)—If you're like many people, you've asked yourself: "Who would want to hack me? There are a lot more lucrative targets out there for cyberthieves, right?"

That's just the kind of easy attitude that cyberthieves are looking to take advantage of— people who are lackadaisical about online security and careless with such hardware as cell phones, tablets and laptops.

"Hackers love it when they hear that someone thinks they can fly under the 'security radar'," said Ron Woerner, director of Bellevue University's cybersecurity programs. "That's the exact person they want to go after because they're complacent or not caring about their cybersafety."

Students, running among classes, jobs, social activities and family obligations, can be easy targets. There are a few simple rules and guidelines that can help keep students safe in the cyberworld.

"If you take a lot of these basic steps, it goes a long way," Woerner said. "We see a lot of students who are technology users but don't really understand how the technology works."

• **Under lock and key**—Or if you like it, you should have put a password on it. Or better yet, use multifactor authentication. "Many online sites are now providing multifactor authentication. This allows users to easily secure their accounts with the standby password [something you know] tied to a second factor: something you have [a physical token, chip, fob or phone], something you are [your voice or fingerprint] or somewhere you are [your home location]," Woerner said. "Adding this second factor provides you with added security and will save you the hassle of having to change your password when the security is invariably breached on the site."

Students can protect their online privacy with a few simple steps.

• **Look both ways before crossing—or connecting**—Free Wi-Fi may seem like the greatest thing since sliced bread, but there are some vulnerabilities that come with it. The network might expose your information to other users or data-gathering software may be built right into the network. Using a virtual private network can help guard against such breaches. There are a lot of free VPN services available including CyberGhost VPN and VPNBook.

• **No really, lock it up**—People generally think of cybercrime as some sort of nefarious software lurking on a website but a lot of it occurs by losing your device. If your phone, tablet or laptop has been stolen, then there goes all the information you've stored on it. So keep a watchful eye on your hardware. For those times when you can't, many devices have a special security slot designed to link with a sturdy cable lock.

• **Know when to say when**—Don't be too social on social media. Sites such as Facebook, Twitter and Instagram can be a great place to share important life events, but make sure to keep sensitive information off them. Investigate the privacy settings on each site to ensure that only your friends can access your postings. Be cautious when using an app such as Foursquare that might alert prying eyes to when your home or apartment is vacant.

• **Install a security suite on all devices**—Security software can help you avoid damage or at least keep it to a minimum if you land on a website with evil intent or inadvertently click on a phishing expedition.

These tips should enable you to study safely by making use of tools that are already readily available. Mix in a little common sense and you're good to go.

Learn More

For more on cybersecurity, visit www.staysafeonline.org/ncsam. For information on turning an interest in cybersecurity into a career, visit www.bellevue.edu/cybersecurity, call (800) 756-7920 or follow Bellevue University on Twitter @BellevueU.

Note to Editors: *Although October is National Cyber Security Awareness Month (NCSAM), this article can be of interest to your readers at any time.*