Cyber Safety

Don’t Be A Hack: Cybersecurity Expert Provides Tips To Prevent Social Media Hacking

(NAPSA)—Each year, 9 million people fall prey to cyberattacks, according to the Federal Trade Commission. Data breaches wreak havoc on one’s personal and financial lives and can cause headaches for years to come. Unfortunately, you or someone you know has already likely been hacked at some point—and if you haven’t, now is a good time to make sure you’re fully protected.

Hackers use a variety of means to capture personal data, from keystroke logging and phishing e-mails to credit card or other financial information theft. While you can protect yourself by changing passwords and verifying where an e-mail originated, consumers need to take less obvious steps to protect themselves.

Dan Konzen, Phoenix college campus chair for University of Phoenix College of Information Systems & Technology, and a cybersecurity expert, teaches others how to protect themselves online by performing live hacks of social media sites, starting with information they thought was secure.

“Social media sites like Facebook lead users to believe their information and data are secure through a few self-selected security settings,” said Konzen, who co-founded his own cybersecurity company.

“The best way to protect yourself is knowing what information is available online and how to reduce access. Consumers think because they have a password on an account, they’re protected. But today’s cybersecurity criminals can often get around basic passwords and uncover personal information like addresses and GPS coordinates on things like a photo.”

Konzen often performs live hacks to show people just how easy accessing blocked or hidden information can be. He offers the following tips for people to protect themselves:

iPhone apps, Google searches and most any online activity can be tracked and used to find personal information.

1. Use VPN networks and Tor browsers on public networks when available.

2. Use websites like www.agilebits.com/onepassword or guerrillamail.com to protect passwords and e-mail addresses. And make sure passwords are more than eight characters long and contain numbers and symbols.

3. Remember that nothing posted online is truly hidden, secure or private—and that doesn’t pertain only to the Internet; information from apps, smartphones and tablets can also be accessed. Take extra steps to keep financial information, passwords, e-mail addresses and other personal information secure.

“We can’t just turn off our phones and never use electronics again; that’s not realistic,” Konzen said. “You need to be aware of what is being put out there and make sure all your data is secure.”

For people interested in additional ways to protect their online identity, or interested in courses on cybersecurity, many colleges offer cybersecurity degree programs. According to the Bureau of Labor Statistics, cybersecurity jobs are expected to grow 37 percent by 2022. University of Phoenix, for example, offers associate’s, bachelor’s and master’s degrees and a number of certificates in cybersecurity on campus or completely online. For more information, visit www.phoenix.edu/colleges_divisions/technology.html.