20 Tips to Improve Your Campus’ Cybersecurity Smarts

Here are tips campus administrators can use to protect against cyber attacks.

By Barbara Shaw · January 20, 2015

A popular magazine features a monthly pictorial of fashion’s winners and losers called “Dos and Don’ts.” Unsuspecting people going about their everyday routines are photographed on the street wearing outfits that are ruled either fashion-friendly “Dos” or fashion faux pas “Don’ts.” The fashion offenders’ identities are subtly obscured by a black bar across their eyes, while their style missteps are aired in an associated caption.

Though I’ve never been caught off-guard with a style citation from the fashion police, I must admit that I have been caught with my defenses down in the usage of my PC. I was sitting in an office seminar with colleagues a few years ago when the session took a break. Heading off to grab a quick refill on my beverage, I returned to find my PC rendered locked and unresponsive to my login credentials. As it turns out, one of my security-conscious colleagues sought to teach me a lesson about leaving my PC unsecured, even for a few minutes. It was annoying, but it was a good lesson learned. Besides learning not to sit next to him again, I’ll remember to never leave my PC unsecured, even in known company.

RELATED: How to Confront the Cybersecurity Challenge

Take Good Care of Your Cyber Hygiene

There is a lot of great information about cybersecurity and what we have come to understand as “cyber hygiene.” Cyber hygiene refers to steps users can take to improve their cybersecurity. One of the first times I encountered the term was in a discussion about information security best practices with Darnell Washington, CEO of SecureXperts. I asked him for a list of cyber “Dos” and “Don’ts,” and here are his top 10 recommendations (in no particular order):

1) **DO** make sure that when you connect to a wireless connection, you are connecting to the proper network, otherwise known as SSID.

2) **DON’T** assume that because the name may sound similar that it comes from a trusted source.

3) **DO** use passwords that include a mix of upper and lower-case letters, including special characters.

4) **DON’T** use names/numbers of your dog, family members, street address and birthday.

5) **DO** take advantage of dual or multifactor authentication. Many Web sites now offer securities beyond just a username and password, such as a token, smartcard, PIN, or even user-selected security images that you will recognize upon login.

6) **DON’T** use username and password only when other options are available.

7) **DO** maintain a list of passwords in a safe place, and change them at least quarterly.

8) **DON’T** keep the same passwords without changing them.

9) **DO** keep your corporate passwords separate from your personal passwords.
10) DON’T keep reusing your personal password for your company password, or vice versa.

11) DO make sure that your computer has the latest patches and virus signatures loaded.

12) DON’T assume that the virus detection software works perpetually with computers.

13) DO use cloud data systems to upload and share nonconfidential data.

14) DON’T trust friends, family and associates with using your personal computer when you are not present.

15) DO back up data onto removable media and store in a safe place.

16) DON’T assume someone else has the responsibility to maintain and protect your data.

17) DO check E-mails carefully to ensure that the source header is from a valid address.

18) DON’T fall prey to clicking a link to malicious Web sites that load malware into your computer.

19) DO establish a relationship with a reputable cybersecurity firm. Ask questions in advance about policy and procedures to keep your company safe on the Internet.

20) DON’T wait until you are confronted with an incident to seek advice.

As fashion trends and critics come and go, we can expect the fashion police will continue to issue their harmless citations. Fortunately, the chances of your being photographed with odd outfit selections by a national magazine are fairly remote. Unfortunately, the chances of your being caught violating one of these cyber “don’ts” is much more likely. While ready-to-wear missteps may cost you little more than some temporary humiliation, malware incidents can cost you plenty.

*Barbara Shaw, CPLP, is Director of Education at PSA Security Network. Shaw earned the Certified Professional in Learning and Performance credential from the American Society for Training & Development (ASTD) Certification Institute.*