Coding for Cybersecurity / Mr. Hansen
5/2/2018

Name: _____
www.modd.net, click on Cybersecurity!

PLUS-UPS for your cybersecurity

None of us is perfect, and we can all use a little more cybersecurity in our lives. You already know not to trust public WiFi or even hotel WiFi. (See, for example, www.wikipedia.org/darkhotel for more information.) But here are some more things to check.

P

Passwords are passé, but we still need them. Remember, length beats complexity, so consider using pass phrases instead of passwords. Use an obfuscation technique to meet complexity requirements. Example: 1th1nKmy$oN1$AgreaTtenn1$playeR. Oh, and about those "password reset questions" you're supposed to answer—don't ever give true answers. (Sarah Palin learned her lesson the hard way.) That city you were born in? It's Blomgrozzville. Write down the answers in your password book.

L

Links and attached files in emails . . . **DON'T CLICK**! Exceptions are permitted for password-reset links *that you requested* and file attachments *that you requested* (from a coworker, say) and are expecting. All others: Delete with extreme prejudice.

U

Use a *unique password* for each online persona you have (Facebook, Amazon, online banking, etc.). This is probably the hardest requirement of all. Use a password book to record your less-often-used passwords, and guard that book carefully. If you trust a software application to store all your passwords, that is another option, but be careful.

S

Spoofing/spearphishing is a real danger, especially if you or someone in your family is a high-value target. Never trust the purported identity of an email or text-message sender without some additional proof, such as a partial account number or a reference to a conversation you recently had. Example: Vance Wilson spoofing/phishing scam.

U

Up to date! Keep your OS and application software up to date, and stay up to date on other trends as well. Example: 2FA (two-factor authentication) instead of simple passwords.

P

Physical access to your device is a problem, with or without password protection. The threat includes not only device theft but surreptitious data theft, installation of keyloggers, etc. *If someone else has physical access, it's not really your device.*

S

(Systems people only.) Remember to *salt* your authentication verifiers. If you have a table of hashed passwords, the passwords should be salted before hashing in order to defeat rainbow-table attacks. Yes, salting is supposed to be a standard practice in 2018, but there are still a few holdouts. If those organizations are not already pwned, they will be in the near future.