MALWARE AND OTHER MALADIES

Ransomware is malware that encrypts your computer files to prevent you from accessing your data until you pay a ransom for the decryption code. In May 2017, a global cyberattack spread ransomware called "Wannacry" to countless computers in over 150 countries, shutting down Britain's National Health Service, FedEx, and Spain's telecommunications systems.

The majority of the victims were using Windows 7 and had neglected to keep their operating system up to date. Microsoft updated Windows 7 (as well as Vista and 8) in March to fix the vulnerability, but many users ignored the update. Others were using Windows XP, a 16-year-old operating system that Microsoft stopped supporting some time ago. Apparently, the malware didn't infect Windows 10 or Apple's MacOS.

Unlike hacking, when someone "breaks in" to a computer, malware is often installed unwittingly by the user who downloads the software in an E-mail attachment of uncertain origin. Last year, I wrote two Newsletter articles on computer security: "Phishing" in January and "Hacking" in October.[1] Phishing lures you into responding to what appears to be a legitimate request for your user name and password from your Gmail account or Medicare. The E-mail might explain, for example, that you need to verify your account information. Most of the recent hacking events in the news started as phishing expeditions that snagged unwary users into giving up their usernames and passwords.

However, the requestor isn't Gmail or your Medicare, but a clever phisher who will then use your credentials to log into (hack) your on-line accounts and steal information. Unless you look at the actual E-mail address, which could be something like reply_to@zidmaderdegsh.com, you'd never know it wasn't legitimate.

Wannacry spread through corporate computer networks, and didn't affect many private (home) users. However, the Wannacry episode should be a reminder to keep your computer safe. Here's how:

[1] Both are available from the PSRC website in the Newsletter section.

1. Make sure your version of Windows and MacOS is always up to date (for Windows 10, go to Settings ➔ Update and Security; for earlier versions, go to Control Panel ➔ Windows Update).
2. Do the same for your virus protection system, such as Windows defender, Avast, Norton, etc.
3. Install Malwarebytes antimalware software. The manual version (you have to initiate the scans) is free. For $40/year, it will run automatcally.
4. If you're still using Windows XP, consider moving to Windows 10 (about $100).
5. Never provide your username or password in response to an unsolicited E-mail request (or over the phone). Legitimate companies don't ask you for this information out of the blue.
6. Don't open E-mail attachments from people you don't know or if the E-mail looks suspicious. (e.g., Beware of an E-mail that reads, "I thought you'd like to see this.")

If you have any doubts about your computer security, visit the PSRC computer lab on Tuesdays from 1 until 4 p.m. and Fridays from 10 a.m. until noon.