Computer Viruses

Dale Willenborg gave a presentation on Computer viruses on March 16. He works for MITRE Corporation at Offutt AFB, but is not a computer security expert.

The greatest dangers for computer viruses and infections are from visiting sites that prompt you to download something, opening e-mail attachments, from clicking on links in an email, and from responding to pop-up alerts on your computer. These actions can cause software to be downloaded to your computer that can either collect personal information from you, to allow someone to take over use of your computer, or to just delete everything off your computer.

Presenting too much information about yourself on facebook or other social networking sites can be used by criminals and other devious people. Be user to restrict access to your social networking sites to only those people you give permission to.

Internet and computer fraud is a rapidly growing business, including:

- Auction and E-Commerce Fraud
- Credit Card Fraud
- Divorce Schemes
- Fake Diplomas and Degrees
- Identity Theft
- “Nigerian” Letter Scam Advance Letter Scheme
- “Work at Home” Schemes

To avoid email spam and viruses:

- Filter spam.
- Don’t trust unsolicited email.
- Treat email attachments with caution.
- Don’t click links in email messages.
- Install antivirus software and keep it up to date.
- Install a personal firewall and keep it up to date.
- Configure your email client for security.

Phishing (pronounced fishing) email is crafted to look as if they’ve been sent from a legitimate organization or friend. These emails attempt to fool you into visiting a bogus web site to either download malware (viruses and other software intended to compromise your computer) or reveal sensitive personal information. If the email is sent and viewed as HTML, the visible link may be the URL of the institution, but the actual link information coded in the HTML will take the user to the bogus site. For example, a phishing email has a visible link such as: http://www.yourbank.com/accounts/

but the actual link is to a bogus site like: http://itcare.co.kr/data/yourbank/index.html

Hovering your mouse over the link will show the bogus link.

Trojan horse email offers the promise of something you might be interested in—an attachment containing a joke, a photograph, or a patch for a software vulnerability. When opened, however, the attachment may do any or all of the following:

- create a security vulnerability on your computer
- open a secret “backdoor” to allow an attacker

- future illicit access to your computer
- install software that logs your keystrokes and sends the logs to an attacker, allowing the attacker to ferret out your passwords and other important information
- install software that monitors your online transactions and activities
- provide an attacker access to your files
- turn your computer into a “bot” an attacker can use to send

There are actually companies that sell programs which can attack your computer with a virus. The Blackhole Exploit Kit and is responsible for 30% of computer attacks. A Russian cybercriminal organization, operating under the pseudonym ‘Puanch’ is responsible for the Blackhole Exploit Kit and the Cool Exploit Kit. Affordably priced at $50 a day, $500 a month, or $1,5000 a year, Blackhole is cheap and within reach of most attackers. The Cool exploit kit on the other hand is anything but cheap.

Use your best judgment to keep your computer and yourself safe. The best rule to use is “If something seems to be too good to be true, it probably is.”