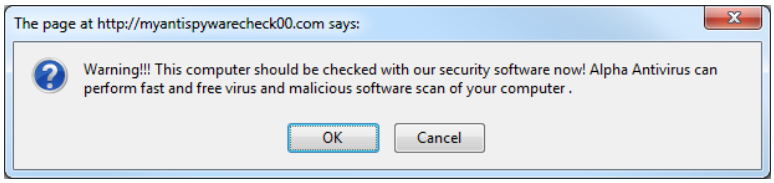
Wireless Access: Do's and Don'ts

ANTI-MALWARE PROGRAMS

- Always keep your firewall, anti-virus, and anti-spyware products up to date!
- There are many good commercial products available, such as:
  - Norton
  - McAfee
  - Kaspersky
  - Vipre
- There are several free options as well, including:
  - Zone Alarm
  - AVG

ANTI-ANTI-MALWARE PROGRAMS

- Beware of *insecurity software* – you're browsing along, and suddenly you see something like this:



- Clicking on buttons such as *OK* or *Click here to fix the problems* may load malware onto your computer; some of this malware may force purchase of the infiltrator's product before it can be removed.

HOME WIRELESS

- If you use a wireless router in your home, make sure that it has encryption enabled.
- Encryption hides your data from prying eyes.
- Common forms of encryption for wireless routers:
  - WEP
  - WPA2

LAPTOP USAGE PRECAUTIONS

- Create passwords for all of your accounts – this prevents others from easy access to your data.
- Create a non-administrator account for guest users – this prevents them from installing software on your computer.
- When you walk away while your laptop is in use, lock the keyboard – Windows Key + L.

WIRELESS WHEN TRAVELING

- Disable file sharing on your computer
  1. Go to Control Panel → Network …
  2. Look for options related to printer and file sharing.
  3. Turn off printer and file sharing.
- On newer versions of Windows, you are asked to specify the network type the first time you connect to it.
  - Home network – most open.
  - Work network.
  - Public network – most restricted
- When you are presented by your computer with a list of wireless networks that are available:
  - Avoid connecting to ad-hoc networks – most trustworthy connections are infrastructure networks.
  - Know the name of the wireless network you should be using – if your computer presents you with multiple wireless networks from which to choose in an airport, hotel, or restaurant, ask a staff member which network you should be using; networks with names such as "Free Airport Wireless" may be baited traps!

BROWSER TIPS FOR TRAVELING

- Be cautious when entering passwords and personal information (for example, credit card numbers) in a Web browser.
  - Look for a closed padlock icon at an appropriate location on the Web browser window (but not in the Web page).
  - Look for a URL that begins with https://.
- Sometimes one needs to access the Internet from a computer at a bank, in a computer lab, or at the public library.
- One danger is that someone may have installed a keylogger onto the computer – this is a program that captures all keystrokes for that computer for later download.

BROWSING ON PUBLIC COMPUTERS

- Here are some browsing tips for public computers:
  - Firefox-on-a-stick – Download the portable edition of the Mozilla Firefox browser, and install it on a pocket USB drive.
    http://portableapps.com/apps/internet/firefox_portable
  - Use bookmarks to access sensitive sites – do not type the URLs.
  - Let the password manager in Firefox remember your passwords so that you do not have to type them.
- But remember! This solution is only as secure as your flash drive!

SECURE YOUR LAPTOP OR FLASH DRIVE DATA

- One of the problems with laptops and flash drives is that they can be stolen or lost.
- For private data, a good solution is the open-source product TrueCrypt (http://truecrypt.org). This product allows you to:
  - Create an encrypted volume.
  - Hide the encrypted volume.
  - Encrypt an entire partition.
  - Encrypt the system partition.

OTHER ADVICE ON NETWORK USAGE

- Don't give out personal information! Avoid sharing too much information on sites such as FaceBook.
- If you are paranoid, consider subscribing to a VPN (virtual private network) service.
  - Be aware that such service may slow down your Internet access somewhat; but this may be an acceptable price to pay if you want the added security.
- If you're really paranoid, consider using GPG (Gnu Privacy Guard) with Mozilla Thunderbird and Firefox.
- Be cautious of P2P (peer-to-peer) services unless you trust the particular service or site you are accessing.
- Malware is rampant on some of these sites:
  - Viruses – infect your computer and can cause all sorts of problems.
  - Trojan horses – hidden within useful files, they open the door for hackers to enter your system.
  - Cuckoo eggs – files that are not what they claim to be.
- P2P includes such services as BitTorrent, Kazaa, and Limewire.