

VCU School of Medicine Security Best Practices

Internet is a bad neighborhood we all live in, follow these tips to help secure your data...

1. Strong Passwords

Always protect your systems and data with strong passwords or passphrases

- *Use a combination of letters, numbers, unique characters*
- *Never leave your password laying around*
- *Use multiple layers of passwords*
- *Consider the use of passphrases where permitted*

2. Antivirus

Always have VCU approved and up-to-date anti-virus software installed on your computer

- *Get Sophos at <http://www.ts.vcu.edu/security/virus.html>*
- *Also available for your home computer if you are employed by VCU*

3. Firewall and Anti-Malware

Supplement the up-to-date anti-virus with an up-to-date and reputable firewall and anti-spyware software

- *Windows Firewall: **Control Panel** → **Security Center** → **Windows Firewall***
- *Spybot S&D*
(<http://www.safer-networking.org/en/download/index.html>)

4. Updates

Make sure automatic updates is turned on for your computer, and your computer's operating system (Windows, Mac OS) and other software packages are up to date.

- *Windows Automatic Updates*
- *Microsoft Office*
- *Quicktime*
- *RealPlayer*

5. Network Storage

Store all confidential and sensitive business data on VCU or VCUHS centrally managed servers. Such information may include personal identifiable information such as Social Security Numbers, credit card account numbers or even VCUCard numbers.

6. Backup

Make multiple backups of your most important data.

- *Use of external hard drives, USB drives*
- *Consider encryption of sensitive and important data*

7. Email awareness

Be suspicious about emails and email attachments.

- *Do you know the sender?*
- *Are you expecting an email from this person?*
- *Is this email asking for your personal information*
- *Does it sound too good to be true?*

8. Website awareness

Avoid going to less reputable and suspicious websites.

- *Was this a link from a suspicious email?*
- *Consider encryption of sensitive and confidential data*
- *Does the site sound legit?*
- *Is the spelling of the website correct?*
- *Does the website prompt you to install something?*
- *Be aware of “Free” things*
- *Check site against google ranking*

9. Other infection sources

Be aware of other means of infection:

- Instant Messaging
- Skype and its cousins
- GoToMyPC.com and its cousins
- Chat rooms
- Peer-to-Peer (P2P) networking
- Facebook and Myspace
- Poorly configured machines (Windows file and printer share etc.)
- Wireless Keyboard and Mice
- Bluetooth devices

10. Physical security

Be aware of the “social engineers” among us

- Lock your computer when you step away from it.
- Lock your office when you step out.
- Shut off your computer every night unless told not to.
- Be aware of strangers in your area.
- Be aware of over friendly individuals and do not offer sensitive information
- Keep an eye out for anything abnormal

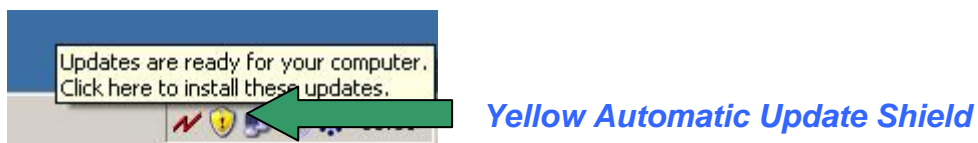
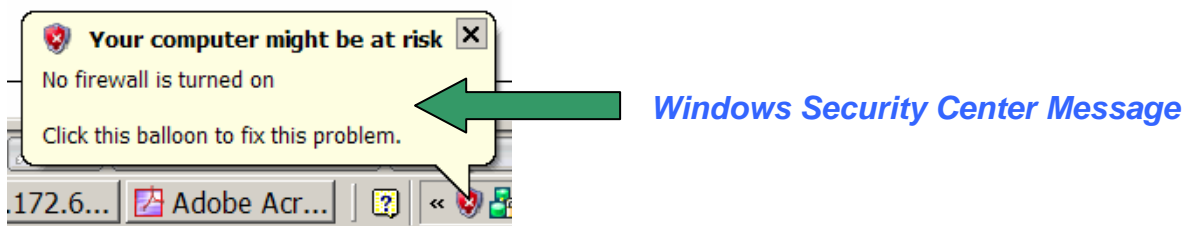
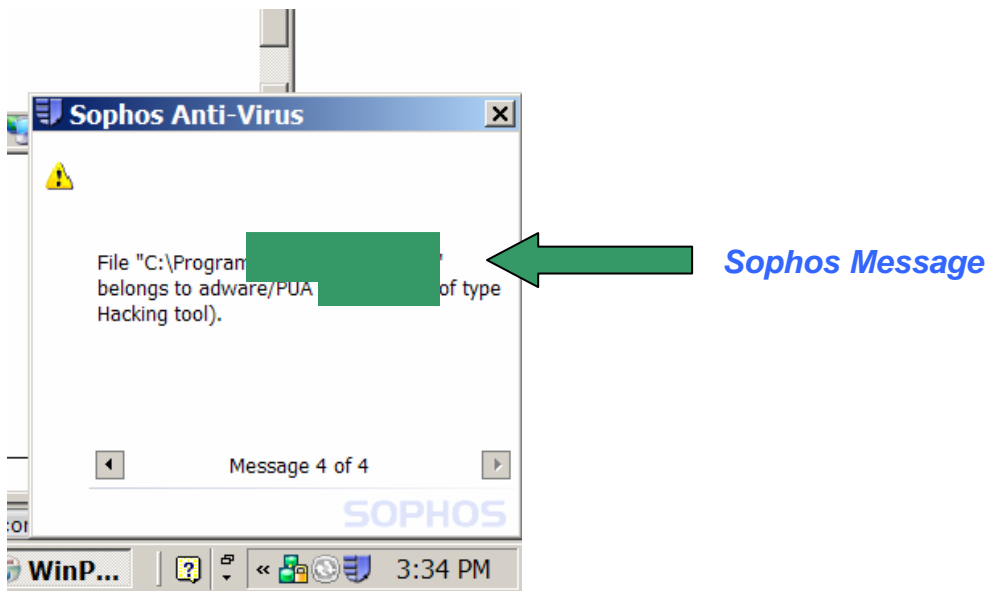
Security must be achieved at all levels in the organization. Keep these 10 rules to protect yourself from the bad guys and help make us a secure organization.

For more information on Security standards, please visit SOMTech standards page at:

http://www.medschool.vcu.edu/technology/somtech_standards.html

Recognize these icons and messages

- Natively, Windows will not warn you against viruses. Recognize the Sophos, Automatic updates, and Windows Security Center messages. (See images below) Ignore other messages prompting for security related issues.



Phishing

- VCU will never send emails asking for any of your passwords.
- Microsoft never sends out emails prompting you to update your machine.
- Your bank or any other financial institutions are not likely to send you emails inquiring your authentication information (user names and passwords).
- Legitimate businesses do not typically ask for your personal information or user credentials through email.
- Never give out your personal or authentication information over the phone, unless if you can verify the caller's identity or you initiated the call. You never know who is on the other end of the phone.

Wireless

- Wired connection is **always more secure** than wireless. Do not access sensitive or confidential data over a wireless network, especially an un-trusted one (Starbucks, My neighbor's network, etc.)
- Wireless network security (Things to watch out for)
 - If it is not your own wireless network, then it is not trusted.
 - If your own wireless network is not properly secured, then it is not trusted.
 - If you can get on the wireless network with no authentication, then anyone else, including an attacker can also get on the same network.
 - If the wireless network do not have a lock icon beside it, then by all means, **DO NOT CONNECT TO IT**
 - If a wireless network shows up as a "computer to computer" network, **DO NOT CONNECT TO IT.**



Figure 1. Computer to Computer network icon

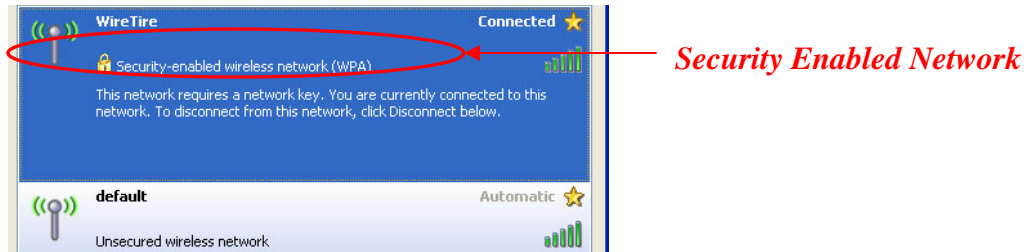


Figure 2. Security Enabled network VS. Unsecured Network

- Wireless network best-practices:
 - Always set a strong password or passphrase to your wireless router.
 - Avoid using WEP.
 - Use WPA-PSK as a minimum encryption standard for your wireless traffic
 - If using PSK, assign a strong password or passphrase.
 - If possible, place all wireless network IP addresses in a separate subnet.