

## It is *Our Shared Responsibility* to stay safe online.

“Our Shared Responsibility” is the theme of National Cyber Security Awareness Month 2009. This promotes the message that all computer users, not just industry and government (or the IT Department), have a responsibility to practice good “cyber hygiene” and to protect themselves and their families at home, at work and at school.

### What can I do to help protect myself and the network?

1. Use strong Passwords and change them periodically
  - a. What are the characteristics of a strong password?
    - i. At least 8 characters long
    - ii. Includes a combination of upper and lower case letters, numbers and special characters
  - b. How do I create a strong password that I can remember?
    - i. Make up a sentence about something that makes you feel good
    - ii. Use the first letter of each sentence to create the password
      1. Substitute numbers for words (4 for ‘for,’ 8 for ‘ate,’ etc.)
      2. Add special characters in place of words (& for ‘and,’ @ for ‘at,’ etc) or for emphasis
      3. Capitalize some extra words to mix it up
    - iii. Type out the password four or five times while saying the sentence out loud – this will associate it in your memory

#### EXAMPLE:

‘Vermont Law School is number one in environmental law’ becomes: VLSi#1iEnvLaw!

2. Keep software updated
  - a. Periodically check to be sure the **Symantec Antivirus** software has updated definitions
    - i. Double click on the diagonal yellow shield at the bottom right of your screen by the clock
  - ii. If the Virus Definitions File version is more than a week old, click ‘LiveUpdate’ to run the updater for the software
- b. Restart the computer at your earliest convenience if you get a message that your computer needs to be restarted to complete a **Windows or Microsoft Update**
- c. Choose to install **Java updates** when you see this icon and message:



- d. Do Not install other updates from popup messages – contact the HelpDesk first to verify
3. Avoid clicking on suspicious links in email or online
    - a. If you receive a suspicious email, forward it as an attachment to [BadEmail@vermontlaw.edu](mailto:BadEmail@vermontlaw.edu) for review

- b. Think twice about clicking on links posted on Facebook or other social networking sites
  - i. Many types of **malware (malicious software)** are spread through infections of other people's accounts – their 'account' posts a link to your wall and the link downloads the infection to your computer
  - ii. Never choose to install an updated version of Flash, a video codec or anything else that pops up when you click on these links
    - 1. Go directly to the software installation page and check to see if you really need the update
    - 2. Contact the HelpDesk if you are not sure
  
- 4. Report suspicious files or popups
  - a. If you receive a file that you think may be infected, forward it to [BadEmail@vermontlaw.edu](mailto:BadEmail@vermontlaw.edu)
  - b. If you see a window pop up saying that your computer is infected, STOP!
    - i. DO NOT CLICK ON ANYTHING, even to close the window or say no to an installation
    - ii. Back up anything you are currently working on by clicking on the application button down in the taskbar (Word, Groupwise, etc.)
    - iii. Restart your computer
    - iv. Call the HelpDesk for further instructions
  - c. If you see a popup message saying that your Firewall is turned off, report this to the HelpDesk
  
- 5. Keep your data backed up
  - a. If you have backed-up copies of your data, you can recover much more easily from a computer infection
  - b. What are my data backup options?
    - i. Anything stored on our network drives (J: and K:) are backed up by the IT Department
    - ii. Your 'My Documents' folder should be in your J drive, or in your iFolder if you have one
      - 1. Check with the HelpDesk if you are not sure
    - iii. iFolder is automatically backed up on our servers
      - 1. This is a technology that we are implementing in stages across campus
      - 2. Double-check that you can access your files by logging into your online File Access at <https://ifolder.vermontlaw.edu/NetStorage/>
    - iv. Anything stored on your desktop or on the C: drive is NOT BACKED UP

Resources for more information:

### **Stay Safe Online**

Home Page: <http://www.staysafeonline.org/>

Page for Higher Education Administrators: <http://www.staysafeonline.org/content/for-administrators>

### **Department of Homeland Security**

National Cybersecurity Awareness Month: [http://www.dhs.gov/files/programs/gc\\_1158611596104.shtm](http://www.dhs.gov/files/programs/gc_1158611596104.shtm)

**LooksTooGoodToBeTrue.com** is a Web site funded by the Federal Bureau of Investigation (FBI) and the United States Postal Inspection Service. The site offers tips and defenses on how to avoid Internet scams:

<http://www.lookstoogoodtobetrue.com/index.aspx>