6. Surf Smart

Frequency: **CONSTANTLY**

Don't follow web links:

Some hackers are taking advantage of vulnerabilities in web browsers by writing code that breaks into PCs when a web page is viewed. To prevent such a problem:

- Be careful to what pages you surf. Never follow links sent to you from someone you don't know.
- Keep your browser software updated.
- At home, consider using a browser other than Internet Explorer (Mozilla's Firefox, for example).

Don't be caught Phishing:

Phishing attacks use "spoofed" emails and fraudulent websites designed to fool you into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By copying the logos of well-known banks, online retailers and credit card companies and placing them in the emails they send, phishers are able to convince up to 5% of recipients to respond to them.
Here's what you can do to minimize these kinds of problems:

- Be suspicious of any email with urgent requests for personal financial information. Banks will never ask for your password. See http://www.antiphishing.org for more information.
- Don't use the links in an email to get to any web page. Instead, call the company on the phone, or log onto the website directly by typing in the web address in your browser.
- Avoid filling out forms in email messages that ask for personal financial information.
- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your web browser.
- Regularly log into your online accounts.
- Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate.
- Ensure that your browser is updated and security patches applied (See Windows Update).

Cyber Safety

To protect yourself and your computer, you should:

1. Run a current anti-virus software.
2. Update your Windows operating system regularly.
3. Run an ad/spyware detector.
4. Delete email attachments that you are not expecting without opening them.
5. Minimize your spam.
6. Use a firewall at home (DSL and cable users).
7. Surf smart.

How we help:

1. We maintain intrusion detection, anti-virus, and spam filtering software for the university and have dedicated security staff to identify and respond to any incidents.
2. We provide a variety of desktop tools including anti-virus and anti-spyware for all CSU computers.
3. We provide access to free downloads for security tools including anti-virus and anti-spyware for use on personal PCs.

Rev. 05/14

STUDENTS, FACULTY & STAFF

Cyber Safety

Because technology is suppose to help you

engaged learning™

Cleveland State University
Information Services and Technology

1. Anti-virus

Frequency: **DAILY**

One of the most important ways to protect your computer is to have anti-virus software that is up-to-date and running. Anti-virus software protects computers from known viruses by checking all incoming email attachments and files you download, read or execute. If a file on your computer is found to contain a virus, it is quarantined before it can infect your machine.

Keeping your computer virus-free is very important. We recommend you download Microsoft Security Essentials at http://windows.microsoft.com/en-us/windows/security-essentials-download.

You can set your virus scanner to automatically update itself daily as long as your PC is turned on and has an Internet connection for the selected time. You can also update most anti-virus products manually.

2. Windows update

Frequency: **DAILY** (Automatically)

Windows, the Microsoft operating system, is often found to contain flaws or bugs. Sometimes these flaws are severe enough to allow a hacker to take control of your computer. To eliminate this problem, Microsoft periodically issues updates to Windows.

It is very important that you apply these updates or patches regularly to your computer. Fortunately, Windows is easily updated to eliminate known flaws. The best way to do this is through the automatic download/install feature built into Windows. Simply go to *Start, Control Panel,* and *Windows Update* for Windows 7. Select *Change Settings* and then select *Install updates automatically*.

2. Windows update (cont'd)

To check Windows update on demand, go to *Start, All Programs,* then select *Windows Update.* Then click on *Check for Updates*.

On this page, Microsoft runs a program that checks your machine's Windows programs and recommends updates that you can choose to install. Please be patient, the process of analyzing your system to discover what patches are missing may take a few minutes.

The process of updating your machine is fairly straight forward once you've gone to the *Microsoft Update* webpage. Just follow instructions that appear on the screen.

If you have any questions or problems on upgrading your operating system software, please contact the Help Desk at 216-687-5050.

4. Don't be curious! Delete email attachments without opening them

Frequency: **CONSTANTLY**

Only open email attachments you're expecting. Most viruses are spread via email and virus writers are getting very good at tricking people into clicking on attachments. So, if you receive email from a relative, a close friend or someone you know which contains an attachment and you're not expecting it – DON'T OPEN THE ATTACHMENT!!! If you receive an email with an attachment from your bank, school, software vendor, etc., and you're not expecting it – DON'T OPEN THE ATTACHMENT!!!

Virus emails always lie about who they're from. While a virus email may look like it came from the person that's designated in the header's 'From:' field, this is never the case.

4. Watch out for and minimize Spam

Frequency: **CONSTANTLY**

Spam is unsolicited commercial email and is problematic for most email users. Spam can result in literally hundreds of unsolicited emails a day AND spam may include viruses in attachments. Here are some rules to keep spam at a minimum.

To minimize spam:

- Don't give out your email address; be miserly with it.
- Don't put it on web pages or other public forums where it can be 'harvested' by spammers.
- Don't give it to sales people.
- Don't reply to spam email asking to be taken off their list even if they say they'll take you off, unless it's from a reputable company.
- Don't voluntarily sign up to receive information via email unless you really, really, really, want it (and understand you may consequently get other unsolicited email).

Once your email address is on a spammer's list, it'll never be removed. If you would like to reduce the amount of spam you receive, try running an email client, which has built-in spam elimination logic.

5. Use a Firewall

Frequency: **CONSTANTLY**

If you are using a DSL or cable connection to the Internet at home, purchase a firewall or turn on the firewall that comes standard on most DSL or cable routers. A firewall is a piece of hardware, or a software program that examines data passing into your computer or network and discards it if it does not meet certain criteria.

We recommend that you use the built-in firewall in Windows 7. Go to *Start*, *Control Panel*, and click on *Windows Firewall*. Select *On* and *Don't Allow Exceptions*.

If you don't want to use a firewall, then we suggest that you turn off your PC when not in use OR disconnect it from the Internet (unplug the cable or modem).