

Good Security Practices

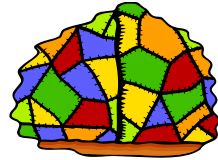
Its all within your hands



What Solutions Should be Used?

- ▶ As threats have materialized on the Internet, security practices and solutions have been developed to respond to the threats. Included in these are the following:
 - Patching operating systems and application software
 - Antivirus and anti spyware software
 - Good e-mail security practices
 - Firewall software
 - All software should be licensed and approved by EIT staff
 - Logging in as *Administrator* only when required
 - Backup your data and secure your desktop when away
- ▶ We will look at these areas and others in an effort to inform you what software and other practices you should be using to improve security.

Operating System Patching



- ▶ At regular intervals, vendors identify and address vulnerabilities in their software.
- ▶ Solutions for these vulnerabilities are known as patches.
- ▶ It is important to install these patches as soon as possible.
 - Windows patches can be obtained from the following website:
<http://windowsupdate.microsoft.com/>
 - If you have Automatic Updates active, you will be notified when patches are available for installation. See this link about activating automatic updates:
<http://support.microsoft.com/kb/306525>

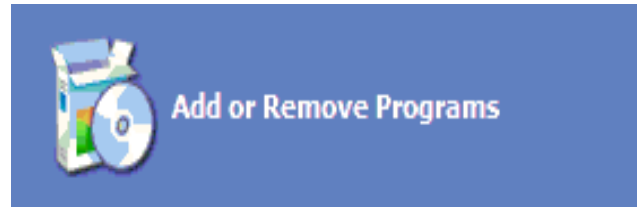
Patching Applications

- ▶ Applications also have vulnerabilities that need patching at regular intervals.
 - Updates for Microsoft Office can be obtained from the following website:
 - <http://office.microsoft.com/en-us/downloads/FX101321101033.aspx>
- ▶ Check with the vendor for the software you have installed to make sure it is current.

Good Password Practices

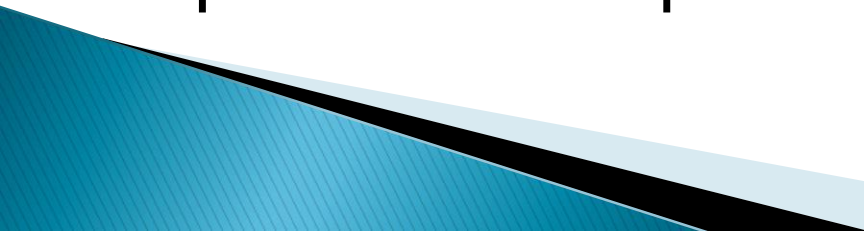
- ▶ All logon IDs and accounts should have unique userids and passwords
- ▶ Use complex passwords that are at least 8 characters in length
 - Passwords should contain upper and lower case characters, numbers and also special characters.
 - Change passwords at least every 180 days
 - Use a password vault for storing userids and passwords.
 - EIT password recommendations – <http://eit.tamu.edu/passwordinfo/passwords.htm>

Remove Software and Applications You No Longer Use

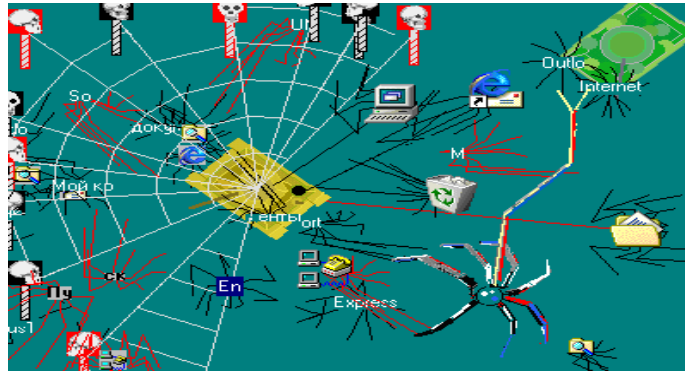


- ▶ Software that is no longer used should be removed because it also presents a security risk.
 - Hackers know what vulnerabilities exist in older versions of software and these products present prime targets.

Use an Anti-virus Application

- ▶ Viruses and malicious software are used by hackers to take advantage of unpatched operating systems and applications.
 - ▶ Using an anti-virus application can greatly reduce the chance that your computer system will be infected by malicious software.
 - ▶ If you are not able to purchase an anti-virus product, EIT might be able to supply one to you.
 - ▶ Some links to free (for home use) anti-virus products are provided on the next slide.
- 

Free Anti-virus products

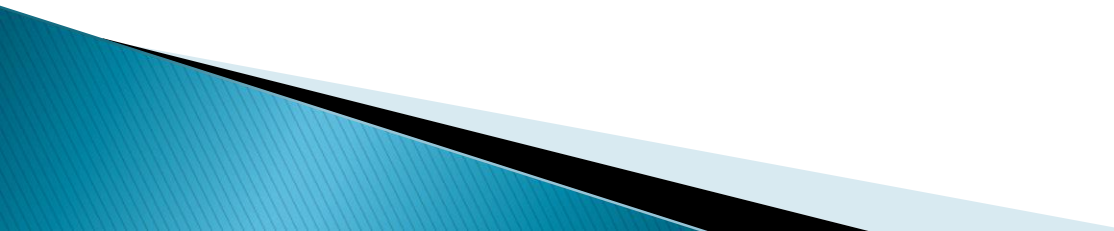


- ▶ Here are some links to free anti-virus products
 - <http://free.grisoft.com/>
 - http://www.avast.com/eng/avast_4_home.html
 - <http://www.pandasecurity.com/homeusers/download/ads/>
 - <http://www.clamwin.com/>

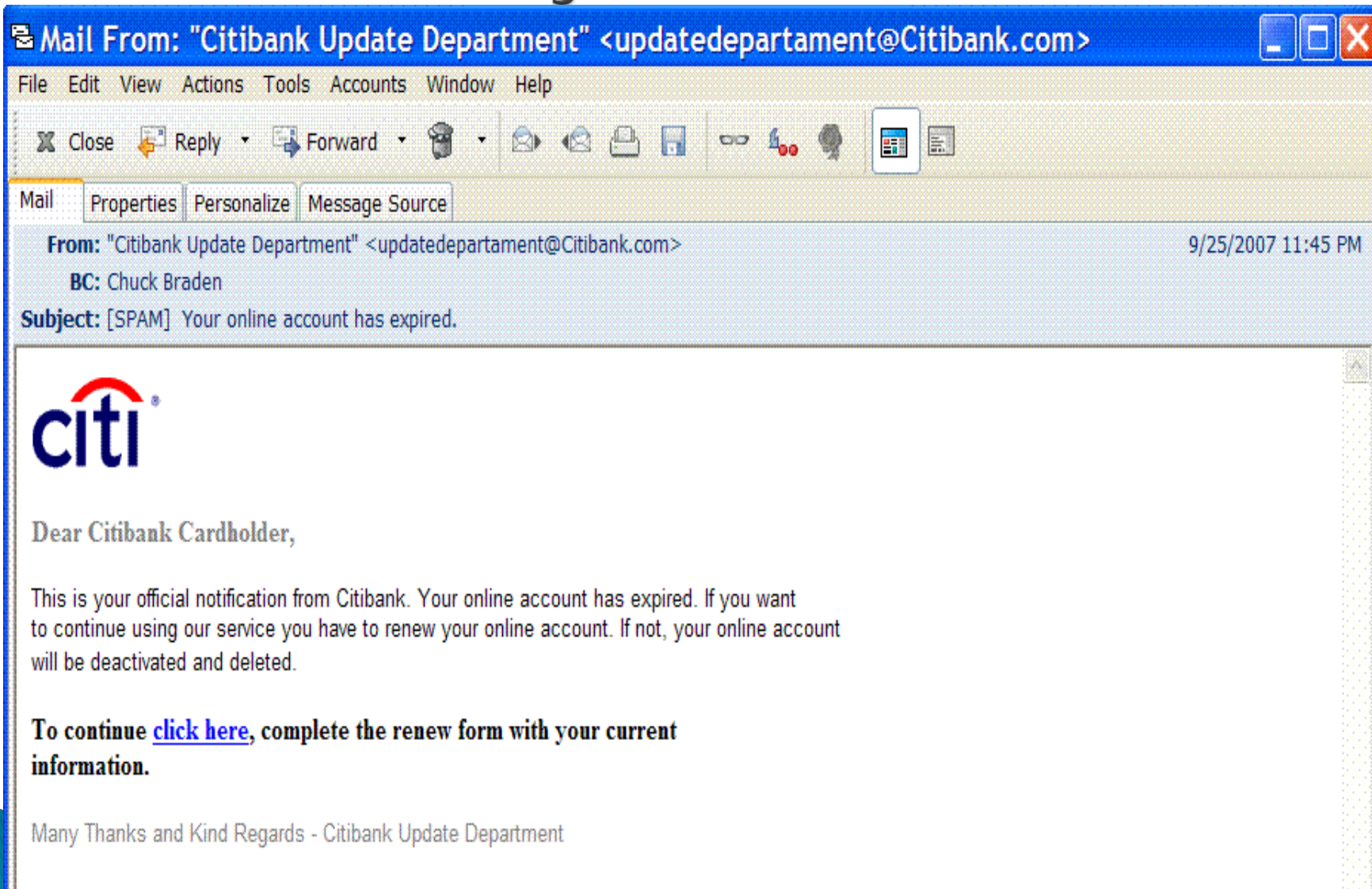
Use an Anti-Spyware product

- ▶ The best FREE Anti-Spyware product is Spyware Doctor. It is available as part of the Google pack at the following URL –
http://pack.google.com/intl/en/pack_installer.html
- ▶ Windows Defender is a good anti-spyware product but is much less likely to find some of the malware that Spyware Doctor does.
 - <http://www.microsoft.com/athome/security/spyware/software/default.aspx>
- ▶ Spybot Search and Destroy is a free (for personal use) Open Source application that detects spyware that exists on the computer
 - <http://www.spybot.info/en/index.html>

Don't Click on Links that are in Emails

- ▶ As e-mail viruses have become less successful, hackers have begun to look to other methods for infecting machines.
 - ▶ SPAM is sent to a large number of recipients directing them to a website that contains malicious software.
 - ▶ If you receive an e-mail from a business or someone you don't know, the best solution is just to delete the message.
- 

A classic example of a e-mail that should just be deleted



What you would have seen if you went to the site in the citibank email

The screenshot shows a Mozilla Firefox browser window with the title "Object not found! - Mozilla Firefox". The address bar contains the URL "http://www.gujo.ne.jp/www.citibank.com/index.php". The browser's menu bar includes "File", "Edit", "View", "History", "Bookmarks", "Tools", and "Help". The browser's toolbar shows navigation buttons (back, forward, home, stop, refresh) and a search bar with "Google". The browser's status bar shows several tabs: "Getting Started", "Latest Headlines", "DIR - Search results fo...", "April2007Agenda.pdf (...)", and "check.asp".

The main content area of the browser displays an "Object not found!" error page. The text on the page reads: "The requested URL was not found on this server. If you entered the URL manually, please check the spelling. If you think this is a server error, please contact the [webmaster](#)."

Below the error message, the text "Error 404" is displayed. At the bottom of the page, the URL "www.gujo.ne.jp" and the server information "Apache/2.2.0 (Fedora)" are visible.

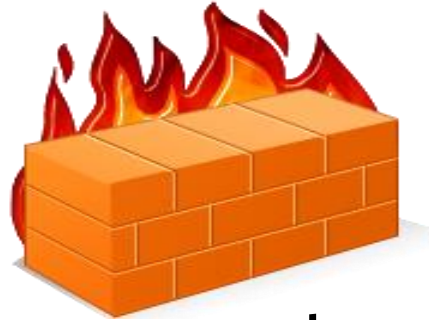
A "Suspected Web Forgery" warning dialog box is overlaid on the right side of the browser window. The dialog box has a red "X" icon in the top right corner. The text inside the dialog box reads: "This page has been reported as a web forgery designed to trick users into sharing personal or financial information. Entering any personal information on this page may result in identity theft or other fraud. [Read more »](#)". Below this text, there is a blue link that says "Get me out of here! Ignore this warning". At the bottom right of the dialog box, there is a link that says "[[This isn't a web forgery](#)]".

Don't open Email attachments unless you are expecting them



- ▶ Email attachments can frequently contain viruses or other malicious code (like key stroke loggers). For that reason, it is a good practice to not click or open attachments from individuals you do not know.

Use a Software Firewall Application



- ▶ Software firewalls prevent your system from being targeted by other systems that are not patched or have been infected by a virus.
- ▶ Windows XP version SP2 comes with a firewall that prevents exposure to many types of vulnerabilities. To activate the Windows firewall, see this link:
 - <http://support.microsoft.com/kb/283673>

Use a Web Browser Client that is Resistant to Common Vulnerabilities

- ▶ Firefox from Mozilla is much more resistant to the common vulnerabilities than Internet Explorer.
 - EIT recommends that all customers use the Firefox web browser when using the world wide web.
 - You can download Firefox from <http://www.mozilla.com/en-US/firefox/>

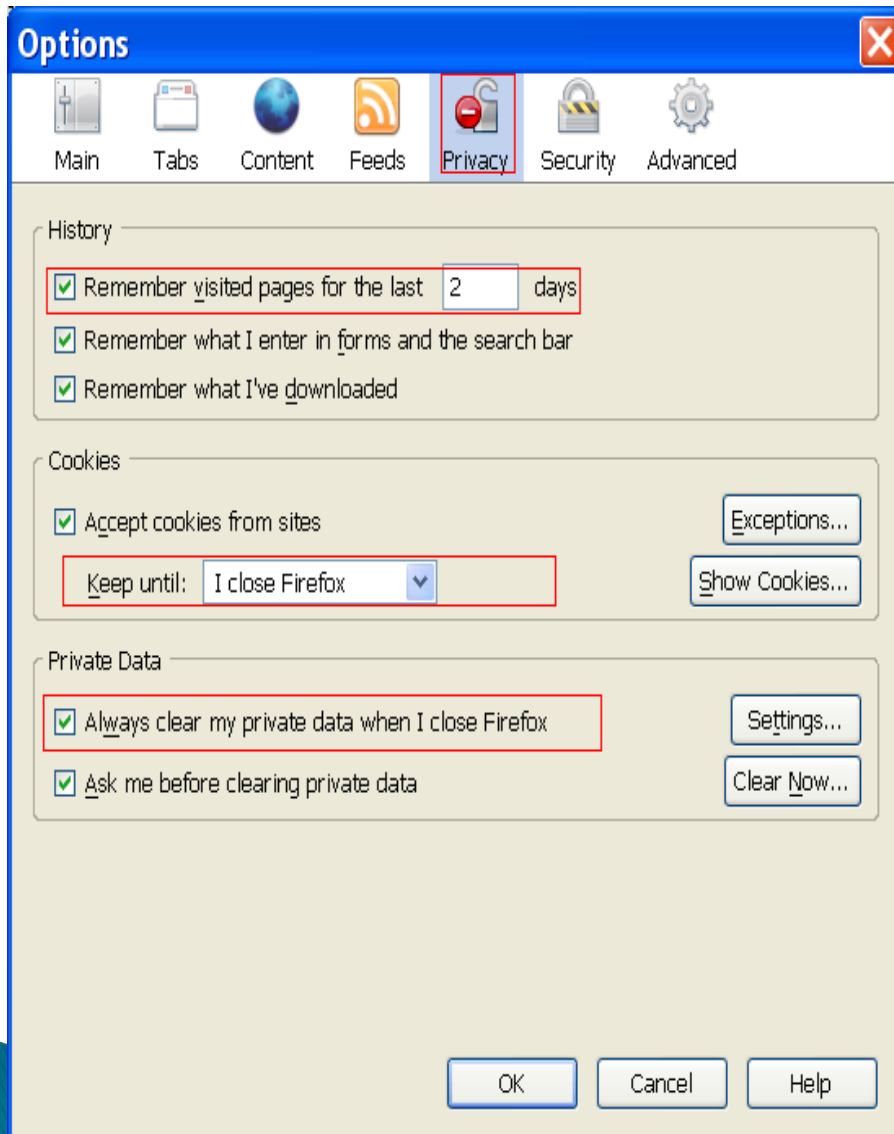
Use caution when visiting websites that are not associated with Texas A&M

- ▶ Malicious websites are now the most common method of infection
 - Even when anti-virus software is used, malicious software can still infect your system if you visit a website that has malicious code placed there.
 - Recent statistics from an anti-virus vendor indicate that about 50 percent of infected websites have malware (or malicious code) present.

Setup your Web Browser Correctly

- ▶ Select the options setting under the tools tab to change the configuration of your web browser
 - The following screen shows the preferred settings for web browsers.

Options Settings on the Tools tab



The screenshot shows the 'Options' dialog box with the 'Privacy' tab selected. The 'Privacy' tab icon is highlighted with a red box. The 'History' section has three checked options: 'Remember visited pages for the last 2 days', 'Remember what I enter in forms and the search bar', and 'Remember what I've downloaded'. The 'Cookies' section has 'Accept cookies from sites' checked, with a 'Keep until' dropdown set to 'I close Firefox'. The 'Private Data' section has 'Always clear my private data when I close Firefox' checked, and 'Ask me before clearing private data' also checked.

Options [X]

Main Tabs Content Feeds **Privacy** Security Advanced

History

- Remember visited pages for the last days
- Remember what I enter in forms and the search bar
- Remember what I've downloaded

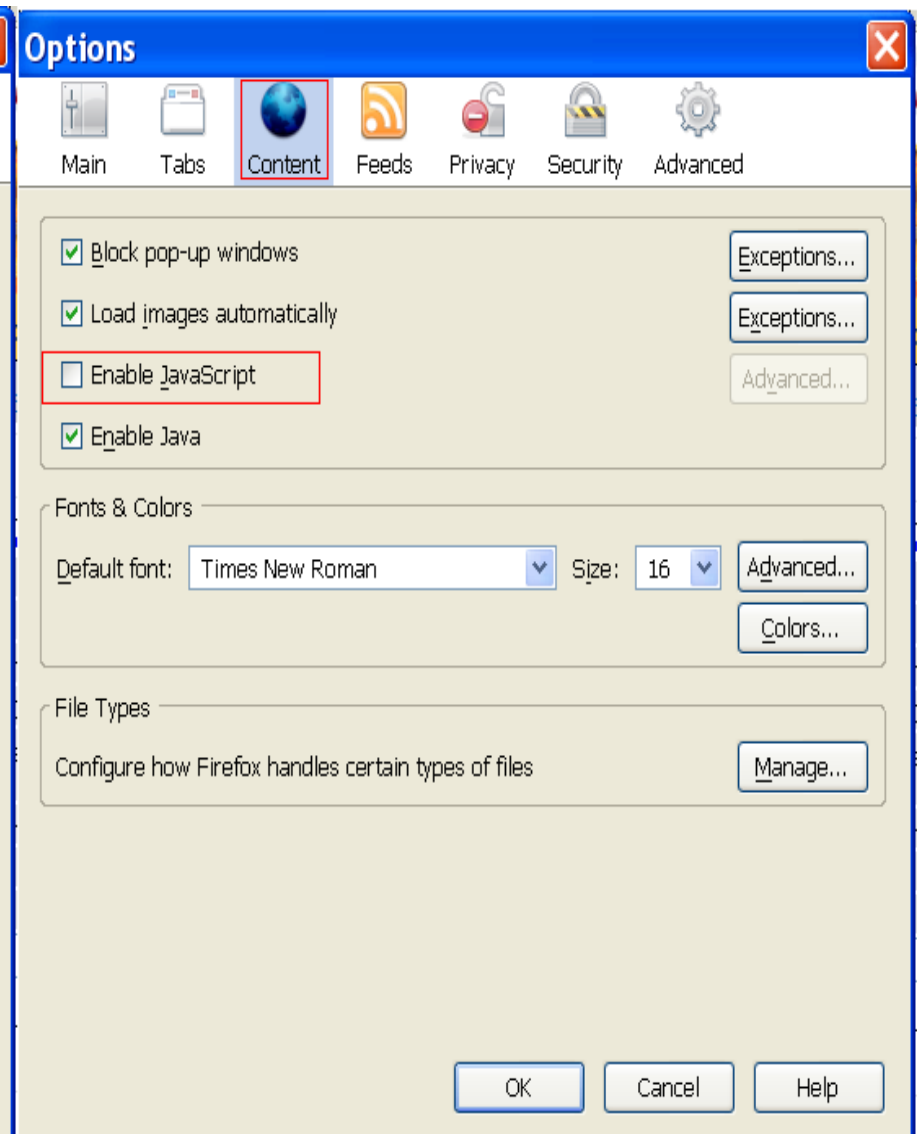
Cookies

- Accept cookies from sites [Exceptions...]
- Keep until: [Show Cookies...]

Private Data

- Always clear my private data when I close Firefox [Settings...]
- Ask me before clearing private data [Clear Now...]

OK Cancel Help



The screenshot shows the 'Options' dialog box with the 'Content' tab selected. The 'Content' tab icon is highlighted with a red box. The 'Block pop-up windows' and 'Load images automatically' options are checked. The 'Enable JavaScript' option is unchecked and highlighted with a red box. The 'Enable Java' option is checked. The 'Fonts & Colors' section shows 'Default font' set to 'Times New Roman' and 'Size' set to '16'. The 'File Types' section has a 'Manage...' button.

Options [X]

Main Tabs **Content** Feeds Privacy Security Advanced

- Block pop-up windows [Exceptions...]
- Load images automatically [Exceptions...]
- Enable JavaScript [Advanced...]
- Enable Java

Fonts & Colors

Default font: [Advanced...]

Size: [Colors...]

File Types

Configure how Firefox handles certain types of files [Manage...]

OK Cancel Help

Good Web Surfing Practices

- ▶ Vendor suggestions for minimizing the exposure to cross site scripting hacks
 - Use more than 1 web browser
 - Use one web browser for common surfing activities and another for when you logon to a website that you will use to purchase items.
 - Reduce your history settings to a very short duration.
 - Some of the cross site scripting hacks can read your history file and determine what sites you have visited.
 - Always close the window for the site you have authenticated to before you navigate away to another site.

Don't install software you are not licensed to use



- ▶ System Regulations require all copyrighted software to have an appropriate license—
<http://tamus.edu/offices/policy/policies/pdf/21-99-10.pdf>

If the software you use is not public domain (also known as freeware), make sure you have all the appropriate license agreements in your possession.

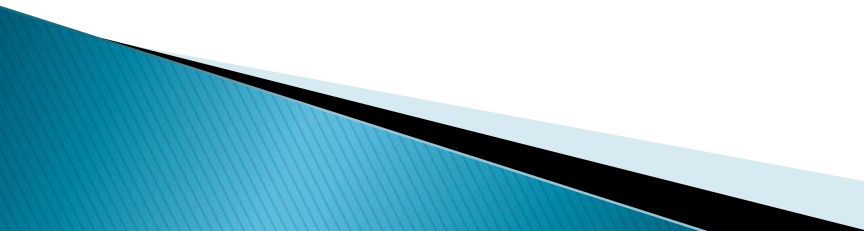
Don't install peer-to-peer (also known as filesharing) software unless it has a business purpose.

- ▶ While peer-to-peer products such as Napster, KaAaA, and BitTorrent provide ways to collaborate on projects, they also provide ways to share unlicensed software, copyrighted files and also expose your computer to security risks. Do not install peer-to-peer software applications unless you have a business requirement for the service.

Do not install software (such as instant messaging) that has not been approved by EIT staff

- ▶ Instant messaging products provide convenient ways to communicate with co-workers and friends. However, it also can expose your computer system to vulnerabilities.
- ▶ Use only the Instant Messenger products identified by EIT. These include:
 - GroupWise Instant messenger – http://download.novell.com/index.jsp?sourceidint=hdr_download
 - Gaim – <http://sourceforge.net/projects/gaim/>

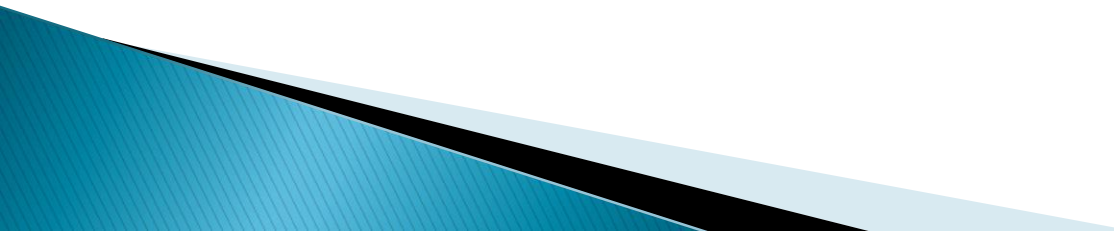
Properly Dispose of Media Containing Confidential Information

- ▶ Don't leave output on the printer for extended periods
 - ▶ Shred all documents (or media) containing confidential information
 - Credit Card Numbers
 - Social Security Numbers
 - Customer or staff phone and address lists
 - Be sure to destroy any post-it notes that contain information that could be used by unauthorized individuals.
- 

Social Engineering Practices

- ▶ Be prepared to challenge unfamiliar individuals who are in the area.
- ▶ Inform your supervisor if you are contacted by e-mail or phone and the other party wants to be provided some information they should already have or even something they should NOT require (such their logon ID or **YOUR** password)
- ▶ If you find a CD or DVD or USB storage device, do not place it in your computer to check the contents. It could contain malware.

When you don't need administrator access, login with a general Windows account

- ▶ Most of the vulnerabilities in Windows require that the user be logged in as an Administrator ID for the vulnerability to be exploited.
 - ▶ If you are logged in as a power or general user, most hacking attempts will not be successful.
- 

Backup your data



- ▶ All computer system will loose data at some point. The solution is using a regular backup process.
 - Options include backing up your important files to a CD or even a separate harddrive or partition on your computer.
 - You should also keep the backup copy in a safe place.

Lock your computer when you are away from the keyboard



- ▶ When you are not using your computer and will be away from the keyboard you should lock the desktop.
 - This can be done by pressing ctrl-alt-delete.

Laptop Security

- ▶ Its not the computer itself that is the target, it's the data.
- ▶ Use something other than a laptop carrying case.
- ▶ Encrypt the data on the harddrive
- ▶ When you are away from your hotel room, vehicle or office, you should place the laptop out of sight.
 - Other laptop security practices are available at
 - http://i.t.com.com/i/tr/downloads/home/10things_slowe_secure_laptop2.pdf
 - <http://www.informationweek.com/shared/printableArticle.jhtml?articleID=203102748>

Wireless Laptop Security

- ▶ When possible, use a wired connection
 - When you are using a wired connection on your laptop, disable the wireless adapter.
- ▶ Only use a wireless access point that is provided by the hotel or conference organizer
 - The conference organizer should provide you an access point SSID and access key.
- ▶ Use only wireless connection that has encryption enabled (such as WPA)
- ▶ Wireless best practices can be found at:
 - <http://blogs.techrepublic.com.com/security/?p=364>
 - http://articles.techrepublic.com.com/5100-1009_11-5876956.html

Report Security Incidents to Either Your Local Support or securityhelp@ag.tamu.edu




- ▶ It is important that all security incidents be rapidly reported and investigated.
 - If you suspect you are involved in a security incident, please report it as soon as possible.
 - Reporting the condition could minimize the impact to others.


Web Links to Content Mentioned in this Presentation

- ▶ EIT Security Practices site
 - <http://eit.tamu.edu/security.shtml>
- ▶ Safe Web site browsing –
 - <http://www.microsoft.com/protect/computer/advanced/browsing.mspix>
- ▶ Peer to peer information –
 - <http://www.microsoft.com/protect/yourself/downloads/filesharing.mspix>
 - <http://www.us-cert.gov/cas/tips/ST05-007.html>
- ▶ Backup resources –
 - <http://ifolderdemo.novell.com/iFolder/>
 - http://www.microsoft.com/windowsxp/using/setup/learnmore/bott_03july14.mspix

Presentation Summary

- ▶ Patch your operating system and applications regularly
 - ▶ Remove software you no longer use
 - ▶ Use Anti-virus, software firewall and Anti-spyware products
 - ▶ Use caution when:
 - Clicking on links in e-mails and attachments
 - Visiting websites other than those associated with Texas A&M.
 - ▶ Don't install software not licensed or approved by EIT staff
- 

Presentation Summary continued

- ▶ Install and use anti-virus, anti-spyware and a software firewall products.
 - ▶ Use only licensed and approved software
 - ▶ Use a web browser other than Internet Explorer
 - ▶ Don't use an 'administrator' ID when its not required.
 - ▶ Backup your data
 - ▶ Lock your computer desktop when you are away
 - ▶ Secure your laptop
- 

Who to Contact if You Have Questions

- ▶ If you have any questions about the content in this presentation or other security issues, you can send e-mail to the address below:
 - securityhelp@ag.tamu.edu