



Northeastern University

Office of Information Security and Identity Services

July 2009

Computer and Information Security Guide

Version 071409.1040

*This document is also available online at the Information Services Website:
http://www.infoservices.neu.edu/get_help/content/ITSEC_packet_for_fall09.pdf*



Northeastern University

Office of Information Security and Identity Services

June 2009

Computer and Information Security Guide

Dear Members of the University community...

Welcome to Northeastern. The safety and security of the computing environment is essential to the learning and business functions of the University. All the while, information security threats are all around us. Viruses, worms, spyware and bots can stop computers cold, invade privacy, interfere with work, drain computer resources, steal information, and cause inconvenience. Inattention to basic security and privacy concepts can cause inconvenience, financial loss, and a variety of other serious and costly consequences.

Un-patched computers, those with missing or out-of-date antivirus software, those with missing, weak, or easily-guessed administrative passwords, open file shares, guest accounts, spyware, or out-of-date operating system and/or application software are highly vulnerable to compromise. Compromised computers often become slow and unstable, damaging data, betraying sensitive information, infecting healthy computers, and disrupting your work and that of others. In many cases, compromised computers eventually become unusable and must be re-imaged, resulting in inconvenience, lost time, and in some cases, loss of critical information.

Security is a shared responsibility. To assist the community in understanding how to safeguard against information security threats, the Office of Information Security and Identity Services offers this Computer and Information Security Guide. This year's guide includes these sections:

- **myChecklist for Computer and Information Security**
- **Checklist for Protecting your myNEU Account**
- **Router/Wireless Access Point Security Requirements and Recommendations**
- **Notice to the University Community: Management of Copyright Infringement Complaints**
- **2009 General Computer and Information Security Recommendations**
- **Managing Your Electronic Reputation**

This guide is also available on the Information Services website at

http://www.infoservices.neu.edu/get_help/content/ITSEC_packet_for_fall09.pdf

Thanks for doing your part to help keep the Northeastern computing environment a safe, available and effective workspace. If assistance is needed, please contact the IS Service Desk at x4357, or Information Security at itsecurity@neu.edu.

Yours in security,

A handwritten signature in black ink, reading "Glenn Hill".

Glenn C. Hill, CISSP, IAM, CPP

Director, Information Security and Identity Services



Northeastern University

Office of Information Security and Identity Services

myChecklist for Computer and Information Security

Step	Actions	Check <input checked="" type="checkbox"/>
1	<p>Got a new computer ? Before connecting a new computer to the internet for the first time, learn how to do it safely: http://www.us-cert.gov/reading_room/before_you_plug_in.html http://www.microsoft.com/athome/security/update/newcomputer.mspx</p>	
2	<p>Got Antivirus ?...Obtain, install and update antivirus software. Download Symantec antivirus FREE by logging into your myNEU account. Note: If using a personally-owned computer for University business, contact the IS Service Desk (x4357) for assistance in obtaining antivirus software.</p>	
3	<p>Get Automatic Software Updates. Update your operating system and application software. Next, configure your computer to automatically download updates. Microsoft products: http://www.microsoft.com/athome/security/update/default.mspx Apple products: http://www.apple.com/support/downloads/ Other products: Please consult the website for your supplier or manufacturer.</p>	
4	<p>Got Spyware Protection ? Protect your privacy ! Keep spyware off your computer. Pest Patrol: http://www.pestpatrol.com SpyCop: http://www.spycop.com Lavasoft: http://www.lavasoft.com/ Note: The listed products are for information purposes only. Northeastern University makes no warranties or representations as to the fitness, suitability or efficacy of these products.</p>	
5	<p>P2P File Sharing and Copyright Checkup</p> <ul style="list-style-type: none"> • Delete illegally-downloaded materials before connecting to any NU network. • Read user documentation and privacy policies before using p2p software. • Assure sensitive/copyrighted materials are not being shared from your computer. • Read more about file sharing at http://www.musicunited.org/, and www.campusdownloading.com • Read the Notice to Students and the University Community on Management of Copyright Infringement Complaints, included with this guide. 	

Continued on next page...



Northeastern University

Office of Information Security and Identity Services

myChecklist for Computer and Information Security

Step	Actions	Check <input checked="" type="checkbox"/>
6	<p>Manage Your Security Settings and Backup</p> <ul style="list-style-type: none"> -Change the administrative password on your computer. Make it hard to guess. -Keep your administrative password to yourself. -Keep all computer and system passwords to yourself. Never use another's password. -Remove un-necessary user accounts from your computer. -Remove guest accounts. Turn off file-sharing features. -Turn off un-necessary services such as web, FTP, etc. -Use a built-in or personal firewall. -Backup critical data often. >Use a "usb" drive, zip disk or other storage device. >Use built-in backup features of your operating system, if available. >Consider making more than one backup copy. >Store backups in a safe place. 	
7	<p>Subscribe to Security Alerts</p> <p>Get breaking computer security news automatically. http://www.us-cert.gov/cas/signup.html</p>	
8	<p>Stay Informed. Be ready to act.</p> <p>Maintain awareness of computer security events and news in television, print and internet media. If advisories are issued, seek information and take protective actions immediately.</p> <p>Microsoft link: http://www.microsoft.com/athome/security/online/default.msp</p> <p>Check out the latest threats and how to prevent/fix infections on the NU security alert dashboard: http://www.infoservices.neu.edu/get_help/symantec_norton_alerts.html</p> <p>Watch the myNEU portal for announcements. http://myneu.neu.edu</p>	
9	<p>Be ready to connect once on campus.</p> <p>Before arrival, purchase a CAT5E or higher 25 foot Ethernet cable. These cables can easily be obtained at most nationally-known hardware stores, computer stores and online vendors. For those who may arrive without a cable, cables are available for purchase from the NU Bookstore, and/or the ResNet Resource Center. Note: Even if you plan to use wireless service, an Ethernet cable is your passport to the wired network in the event of wireless service interruptions.</p>	

Continued on next page...



Northeastern University

Office of Information Security and Identity Services

myChecklist for Computer and Information Security

Step	Actions	Check <input checked="" type="checkbox"/>
10	<p>Become "Security Streetwise"</p> <p>Protect your accounts and digital devices:</p> <ul style="list-style-type: none"> -Never share your passwords. Never use another's password. -Make your myNEU password and password reset challenge answer complex and hard-to-guess. -Protect your laptop by using a security cable. -Never leave computing devices unattended, not even for a moment. <p>Protect your privacy and online safety:</p> <ul style="list-style-type: none"> -Keep personal information to yourself. http://www.epic.org/privacy/consumer/ -Use discretion before sharing your picture or personal information. -Make informed decisions around use of social networks. -Don't give personal information in response to e-mail or web forms. -Don't respond or reply to spam. Delete it instead. -Don't respond to phishing. http://www.antiphishing.org/ -Guard identification, credit cards, passports and sensitive documents. -Be careful what you throw away. Shred sensitive information promptly. <p>Attend Security Awareness Training. Visit www.infoservices.neu.edu for class schedules.</p>	

Special Note about Becoming Security Streetwise...

PHISHING – DON'T TAKE THE BAIT !

During the year, you may receive many e-mail messages asking for your user name and password to various electronic accounts. These messages often look official, and sometimes include logos and other information to make the message look legitimate. The messages may even carry the name of a person you know to be trusted, such as a University official or another well-recognized name.

These messages are known as "phishing", and represent attempts by bad actors to gain access to your electronic account(s).

ALL such messages are fraudulent, and are never sent by Northeastern University or any other legitimate business.

NEVER reply to any message seeking your username and/or password. Instead, immediately delete the message.



Northeastern University

Office of Information Security and Identity Services

Checklist for Protecting your myNEU Account

Your myNEU account is your passport to a world of information and electronic services. To help protect your account from unauthorized access, follow these steps:

Step	Actions	Check <input checked="" type="checkbox"/>
1	<p>Change your myNEU password. Choose a password that is strong and hard to guess. Make sure your password is at least 8 characters long, with at least...</p> <ul style="list-style-type: none"> • one uppercase character • one lowercase character • one numeric character <p>For example: Weak password: droopyjaw Better password: droopyjaw5 (note use of a number) Stronger password: DroopyJaw5 (note use of a number + uppercase) Even better password: Droopy\$Jaw5 (note use of "\$" character)</p> <p><u>Do not use these examples for your myNEU account.</u></p>	
2	<p>Choose a password reset challenge question and answer where the answer is nonsensical, and where only you will understand the relationship between the question and the answer. The password reset challenge answer is case sensitive, so use case to help deter guessing.</p> <p>For example: Challenge question: what is my secret shame ? Challenge answer: eating YELLOW flowers</p> <p>Challenge question: What are the marks of the beast ? Challenge answer: PINK elephants with shoes</p> <p><u>Do not use these examples for your myNEU account.</u></p> <p>Never use any of the following for passwords or password reset challenge answers</p> <ul style="list-style-type: none"> • common words, dictionary words, phone numbers, sequences of numbers • name of family member, favorite color, drink, song, performer, pet name, car brand, etc. 	
3	<p><u>NEVER</u> share your myNEU password or password reset challenge question. Doing so compromises your account, can result in identity theft, and is a violation of the Appropriate Use Policy.</p>	
4	<p>Change your myNEU password and password reset challenge answer frequently. Consider every 90 days or more frequently.</p>	

Continued on next page...



Northeastern University

Office of Information Security and Identity Services

Router/Wireless Access Point Security Requirements and Recommendations for ResNet June 2009

This section of the Computer and Information Security Guide describes required and recommended security practices to be used with privately-owned routers and/or wireless access points connected to ResNet ports in those areas of the University where connection of these devices is allowed. At the current time, privately-owned routers and/or wireless access points may be connected in any location which is not blanketed by NuWave wireless networking service. For example, International Village is blanketed by NuWave wireless network service, and therefore, use of privately-owned wireless access points/routers in International Village is not expected to be permitted.

NOTICE

Owners/operators of routers and/or wireless access points are solely responsible for the security and access control for their devices, and are liable for the actions of anyone accessing ResNet through their device(s). For more detailed information on these responsibilities, please read the Appropriate Use Policy, located at <http://www.infoservices.neu.edu/aup.html>

Requirement or Recommendation	myNotes <i>Use this space for your notes...</i>	Check <input checked="" type="checkbox"/>
1 STRONGLY RECOMMENDED Keep all documentation supplied with your equipment. You will need information from these documents in order to register your router and/or wireless access point on ResNet, and in instances where you contact the manufacturer for troubleshooting or warranty support.		
2 REQUIRED Register your desktop or laptop computer first, then register other devices. After registering, the desktop or laptop computer, it is recommended to reboot the router/wireless access point.		
3 REQUIRED ALL devices connected to ResNet, including computers, XBOX, PlayStation, routers or wireless access points MUST be registered on ResNet in the legal name of the owner, using the factory-assigned MAC address of the device. Operation of unregistered devices, provision of false or misleading information during registration, or MAC address alteration (spoofing) violates the Appropriate Use Policy, and may subject the violator to suspension of service and/or referral to the Office of Student Conduct and Conflict Resolution. 3A) If your device does not have a built-in web browser, it MUST be brought to the ResNet Resource Center to be registered.		

Continued on next page...

Router/Wireless Access Point Security Requirements and Recommendations June 2009 – (continued)

Requirement or Recommendation	myNotes <i>Use this space for your notes...</i>	Check <input checked="" type="checkbox"/>
<p>4 RECOMMENDED Select an appropriate installation location for your device(s). Choose a location that does not create safety or security hazards, and that limits the spread of your wireless signal. For example, do not mount a wireless access point in a window. Rather, choose a location on an inside wall, under a desk, or near the floor. If your device features a security slot, purchase an appropriate locking cable, then secure one end to your device and the other end to an immovable fixed object.</p>		
<p>5 STRONGLY RECOMMENDED Change the default administrator password that came with your router/wireless access point. You will use this password when configuring your wireless access point. Choose a hard-to-guess password, and keep it to yourself. Never give the administrative password for your device to another person.</p>		
<p>6 REQUIRED Change the SSID (service set identifier) from the default value to a value that will help the University locate your wireless access point in the event your device interferes with University-provided services. A suggested format is your building name and room number, for example: WAP-WVE-0105.</p> <p>Note 1: Ensure you use the room number to which you are assigned. Falsification of SSID information in an effort to mislead is a violation of the Appropriate Use Policy, and may subject the violator to suspension of service and/or referral to the Office of Student Conduct and Conflict Resolution.</p> <p>Note 2: Never use the SSIDs "NUwave", "NUwave-guest", or any variants of an SSID using the letters "NUWAVE" or "NUwave-guest". These SSIDs are reserved for University use only. Unauthorized use of University-reserved SSIDs may subject the violator to suspension of service and/or referral to the Office of Student Conduct and Conflict Resolution.</p>		

Continued on next page...

Router/Wireless Access Point Security Requirements and Recommendations June 2009 – (continued)

	Requirement or Recommendation	myNotes <i>Use this space for your notes...</i>	Check <input checked="" type="checkbox"/>
7	<p>REQUIRED – TAKE SPECIAL NOTE ! If your wireless access point is using 802.11b/g, set your wireless access point to use only channels 1, or 6, or 11 for this version of 802.11.</p>		
8	<p>STRONGLY RECOMMENDED Enable MAC address filtering. This allows you to specify which computing devices may connect to your wireless access point. To use MAC address filtering, obtain the wireless card MAC address of those devices you wish to admit to your wireless access point, then enter the MAC address(es) in the appropriate screen of your router/wireless access point management software.</p>		
9	<p>REQUIRED Do not hard-code DNS settings in your router or wireless access point. Use only DNS settings provided automatically by the University.</p>		
10	<p>STRONGLY RECOMMENDED Turn OFF your wireless access point and all computing devices when not in use. This practice helps minimize exposure of your devices to hackers, and contributes to creating and maintaining a green campus.</p>		

Continued on next page....

Router/Wireless Access Point Security Requirements and Recommendations June 2009 – (continued)

Requirement or Recommendation	myNotes <i>Use this space for your notes...</i>	Check <input checked="" type="checkbox"/>
<p>11 REQUIRED</p> <p>11A) Set your router/wireless access point to obtain a DHCP address from Northeastern. Look for words like "Automatic Configuration", "DHCP client", and "Internet Connection Type".</p> <p>11B) Domain name should be set to "neu.edu".</p> <p>11C) MTU size should be "automatic", or up to 1500 if automatic is not an option on your access point.</p> <p>11D) Set your wireless access point as a DHCP server, and to give out IP addresses in one of the following ranges:</p> <p>10.0.0.0 - 10.255.255.255, or 172.16.0.0 - 172.31.255.255, or 192.168.0.0 - 192.168.255.255</p> <p><u>Never set your device to give out IP addresses other than those shown above.</u></p> <p>11E) If your router/wireless access point features a time zone setting, use the "Eastern" time zone.</p> <p>Set your router/wireless access point to give out only the minimum number of IP addresses needed at any one time. For example, if you need to allow five people to connect to your wireless access point at any one time, set your wireless access point to give out only five (5) IP addresses.</p>		
<p>12 REQUIRED</p> <p>Do not set your router/wireless access point to act as a bridge.</p>		
<p>13 STRONGLY RECOMMENDED</p> <p>If feasible, set your wireless access point to use either 802.11a or 802.11g mode. Do not use 802.11b or 802.11n "only" modes, since these modes can cause interference to other wireless devices.</p>		

Continued on next page...

Router/Wireless Access Point Security Requirements and Recommendations June 2009 – (continued)

Requirement or Recommendation		myNotes <i>Use this space for your notes...</i>	Check <input checked="" type="checkbox"/>
14	STRONGLY RECOMMENDED Set your wireless access point to use encryption such as WPA or WPA2, and be sure to change the default key to something hard to guess, and that only you will recognize. The key should be random, and at least 20 characters in length. Give the key to those whom you wish to allow to connect to your device. Change the key often, especially after allowing one-time users such as visitors to access ResNet through your device.		
15	REQUIRED Use AP-mode or Infrastructure setting on the wireless access point. Ad-hoc mode should <u>NOT</u> be used on access points or workstations.		

Wireless Access Point Manufacturer Web Sites

For more information about commonly-available wireless access points, please refer to the website recommended by your manufacturer. The following websites may also be valuable for information purposes:

- <http://www.linksysbycisco.com/US/en/home>
- www.netgear.com
- <http://www.apple.com/>
- www.hp.com
- <http://www.trendnet.com/?todo=home>

NOTICE

Approval to install privately-owned routers/wireless access points applies at this time to ResNet only. Use of privately-owned devices such as hubs, switches, routers, wireless access points and all other non-University installed and owned networking equipment on NuNET is permitted only as may be agreed in writing between a department and the Information Services Division. For more information, please refer to the Appropriate Use Policy at <http://www.infoservices.neu.edu/aup.html>

Router/Wireless Access Point Security Requirements and Recommendations June 2009 – (continued)

Example Set Up Notes Linksys/CiscoWRT610N Dual Radio Wireless Access Point

NOTE: Other makes and models of wireless access points should have similar options.

Basic Setup

1. Force the WAP to use DHCP to procure an IP address from Northeastern. Look for worlds like Automatic Configuration, DHCP Client, and Internet Connection Type.
2. Use a unique HOST NAME. The recommendation is to use the Building Abbreviation followed by your assigned suite Number, i.e. WVG-1204. It should be UNIQUE.
3. Domain Name should be neu.edu
4. MTU Size should be AUTOMATIC or up to 1500 if AUTO is not an option. Larger than 1500 will cause packets to be dropped. Smaller may cause performance issues due to fragmentation.
5. ENABLE the DHCP server on your WAP. All the default values should be ok.
6. Set the Time Zone and adjust for Daylight Savings Time, if desired. As of Fall move-in, Boston is in the Eastern time zone, or GMT -5.

Wireless Setup

7. Select SSIDs that are unique. It is suggested to use a unique HOST NAME as in step 2 above. If your wireless access point supports both 5GHz and 2.5GHz on the same device, you will potentially have two SSIDs. Append a 5.0G or 2.4G on the end of the HOST NAME to make your SSIDs unique.
8. If you have a 5GHz radio in your WAP, you can support 802.11a and 802.11n. Mixed Mode will support both.
9. If you have a 2.4GHz radio in your WAP, you can support 802.11b and 802.11g, as well as a subset of 802.11n. Mixed mode will support all three. You can disable support for 802.11b if you like, unless you wish to connect some 802.11b devices to your WAP. Be advised that even one 802.11b device will slow down all other connections on your WAP.

Wireless Security Setup

10. Use WPA2-Personal or AES encryption if supported. Failing that, use WPA-Personal or TKIP. Please avoid using WEP security, as it features no practical security, and can cause your WAP to become exposed to shutdown in the event of conflicts or security exposures.
11. Using WPA-Personal (TKIP) or WPA2-Personal (AES) encryption will require the use of a shared key. When utilizing WPA2-Personal, some WAPs have a mixed mode which allows you to use either TKIP or AES. If you have some older devices, you may wish to allow either mode.

Continued on next page...

Router/Wireless Access Point Security Requirements and Recommendations June 2009 – (continued)

Example Set Up Notes (continued) Linksys/CiscoWRT610N Dual Radio Wireless Access Point

Security Settings

13. If your WAP has a firewall built-in, enable it. Be advised that for your protection, ResNet does not accept incoming connection requests from outside the University network. Therefore, all incoming traffic you see will be local to the University. Should you encounter problems, disable the firewall to troubleshoot.

14. FTP Server – If available, consider disabling. Use MyFiles on the myNEU portal instead.

Device Administration

15. Alter the default password to be something hard to guess, and Disable Remote Management. Be aware that once local management via Wireless is disabled, the WAP can only be managed via a wired port.

16. Know how to get back to factory defaults, via the GUI and via powering down the WAP. Learn reset procedures.

17. Periodically verify your WAPs firmware is current. Instructions should be found in the manufacturers paper or electronic documentation/website. CAUTION: Errors made during firmware updates can render your WAP inoperable. When updating firmware, print out and follow update instructions carefully.

Wireless Printing

18. Wireless printing, while being commercially available, isn't always as reliable as desired. If your printer has a network (Ethernet) port, it is recommended to connect it to a wired port on your WAP. Alternately, a printer may be connected to a USB or parallel interface on your PC. A Print Server typically has a USB port as well. Plug the Print server into -WAP, and the printer into the Print Server. If possible, use the same vendor for both the WAP and Print Server.

Commonly-used wireless device models (For Information Purposes Only)

Two commonly-used and generally available wireless access points are the Cisco/Linksys WRT54GL, and the Cisco/Linksys BEFSR41. Please note, the University makes no warranties nor endorsements of any kind with respect to these devices.

WRT54GL (wireless access point and router combination)

<http://www.linksysbycisco.com/US/en/products/WRT54GL>

BESFR41 (wired router with four port switch)

<http://www.linksysbycisco.com/US/en/products/BEFSR41>



Northeastern University

Notice to Students and the University Community Management of Copyright Infringement Complaints

Amended 6/10/09

In early 2007, the Recording Industry Association of America (RIAA) changed its strategy regarding copyright infringement complaints. This strategy may impact you. The University is also required by law to notify you of additional information about copyright infringement, so we feel it is important to share the details of the RIAA's strategy and additional information.

Downloading and/or sharing of copyrighted content such as movies, music or software without permission, whether through peer-to-peer networks or any other method, without permission of the copyright holder or their designated agent, is both illegal and a violation of Northeastern University's Appropriate Use Policy (<http://infoservices.neu.edu/aup.html>) which applies to all members of the university community. Engaging in such activities may subject the violator to severe penalties, including but not limited to impoundment of computer equipment, substantial fines, and orders to cease activities. Engaging in the activities described above may also result in severe penalties at the University level.

While the University does not monitor content, the Recording Industry Association of America (RIAA) and other organizations actively do so via the Internet, and, on occasion, issue complaints to internet service providers, including the University, whose subscribers are alleged to be engaging in these activities. Generally, at the time of the complaint, the RIAA or other complainant is only aware of the network address of the computer from which copyrighted material was alleged to have been shared and not the identity of the individual community member. Additionally, the RIAA and other external organizations do not have access to Northeastern's networks, systems, nor confidential information, including individual community member's personal information stored on university systems.

When the University receives a formal complaint, the Office of Information Security investigates and takes appropriate action, including outreach to the community member and recommends how affected users may regain compliance with law and University policy. Any time before, during, or after this process, the complainant may seek to subpoena University records to establish the identity of the person tied to the computer address cited in the original complaint. If the University receives such a subpoena, the individual whose records are sought is notified and given an opportunity to object to the release of their information. The person may at their own expense seek legal representation in an effort to quash the subpoena. If this effort is not successful within the time frame demanded in the subpoena, the University must release the requested information to the complainant.

The new RIAA strategy includes a new document known as a "settlement letter", which cites the computer address of the alleged offender, and requests the internet service provider to forward the letter to the user who is alleged to have infringed RIAA copyrights. The letter informs the user they have forty (40) days to contact an RIAA legal representative or face being sued in Federal Court. The letter also features a web link (URL), where the user may pay to "settle" the matter using a credit card. These letters, as currently defined, are neither legal documents nor formal complaints to the university and do not compel the university to take any specific action.

Members of the university community who chose to violate copyright protections and university policy are personally responsible for their actions. Accordingly, the University will not be a party to these actions nor to "settlement" discussions in these matters. Upon receiving a "settlement letter", the university will not disclose the identity of the community member in question to the RIAA nor will the university retransmit the 'settlement letter' to the community member. To summarize, community members (students, faculty, and/or staff) engaging in illegal downloading or file sharing using Northeastern networks and/or systems are doing so at their direct, personal risk and are solely responsible for any and all potential consequences of their actions.



Northeastern University

Office of Information Security and Identity Services

2009 General Computer and Information Security Recommendations

Read and comply with the Appropriate Use Policy (AUP)

<http://www.infoservices.neu.edu/aup.html>

Physical Security

- Lockdown PCs, laptops, flat panel displays, printers and other high-value items.
- Never leave mobile/portable devices unattended.
- Lock doors to rooms and workspaces when not in use.
- Lock desks and file drawers when unattended.
- Do not allow unknown persons to use your computing devices.
- Shred un-needed materials containing sensitive or confidential information.

Passwords

- Define a strong administrative password on your computer, and keep it to yourself.
- Change the administrative password often.
- Define strong passwords. Use a combination of letters and numbers. Don't use dictionary words.
- Avoid writing passwords down.
- Change all passwords frequently.
- Never share passwords.
- Never check the "remember my password" box in dialog boxes.

Your personal privacy

- It is not necessary to share everything about yourself with others.
- Keep sensitive personal information to yourself.
- Trust is earned. Look to establish trust first, then consider sharing, but with discretion.
- Don't be afraid to say "I'd rather not share that information."
- When someone asks you for personal information, don't be afraid to ask them:

>what items of information are you collecting ?

>why are you collecting the information ?

>how will the information be used ?

>with whom will the information be shared ?

>how will the information be protected ?

If the person asking you for information cannot answer all the questions quickly and concisely, refrain from giving out your information.

- Protect your e-mail address.
- Avoid configuring personal information into your web browser software.
- Configure your web browser software to clear personal information when quitting the browser.

Respecting others' privacy

- Don't share others' personal or confidential information.
- Use of web cams or other technologies to capture, transmit or record video and/or audio in locations where a reasonable expectation of privacy exists may violate the Appropriate Use Policy. Never engage in this activity unless permission has first been obtained from all persons to be depicted and/or recorded.

Continued on next page...



Northeastern University

Office of Information Security and Identity Services

2009 General Computer and Information Security Recommendations (continued)

Antivirus and firewall software

- Install and maintain anti-virus and firewall software on every computer you own.
- Schedule automatic virus definition updates.

E-mail

- Don't click on or open unexpected messages or attachments, links or messages from unknown senders.
- Don't open messages with unrecognized subject lines.
- Never reply to unsolicited e-mail or web forms.
- Never click on an unsolicited web link.
- Never respond to a request for your password. All such requests are fraudulent.

Protecting your identity

- Protect your Social Security Number, driver's license number, and passport number, as well as documents on which these numbers appear.
- Don't write down PIN numbers. Do not carry your Social Security Card.
- Avoid giving out personal information unless you initiated the transaction.
- Protect your wallet or purse from loss or theft.
- Collect paper mail promptly from your mailbox.. Shred confidential information before discarding.
- Check banking and credit card statements for accuracy. Report suspicious transactions immediately to your financial institution.
- Check credit report regularly. Report errors or unusual activity immediately to the relevant financial institution and all three credit reporting agencies:
Equifax: <http://www.equifax.com/home/>
Trans-Union: <http://www.transunion.com/>
Experian: <http://www.experian.com/>

Confidential Information

- Never discuss confidential information in public places.
- Keep your desk clear of sensitive information.
- Secure sensitive information in locked containers.
- Shred unwanted/unnecessary papers.

Instant Messaging and Audio/Video Chat

- Never accept unsolicited downloads/offers.
- Never discuss confidential information on chat.
- Never use IM or IRC to authorize transactions or payments.
- Be mindful of the privacy rights of others who may be range of your video and/or audio chat.

Spyware/Trojan Horse/Keylogger detection

- Consider installing and maintaining spyware/Trojan/keylogger detection software on every computer you own.
- Avoid performing sensitive transactions on public workstations or open (hotspot) networks. When on campus, consider using NuWave Secure wireless service.

Continued on next page...



Northeastern University

Office of Information Security and Identity Services

2009 General Computer and Information Security Recommendations (continued)

Operating System and Application Software

- Keep original copies of installation media & license keys.
- Register for product updates.
- Monitor manufacturer websites for updates.
- Use "auto update" features of operating system and application websites.

Data Management, Backup and Storage

- Backup critical data daily. Use myFiles, USB stick or other method of your choice.
- Store backups in a safe location.
- Delete unnecessary files on a regular basis.

Making your computer less attractive to unauthorized users

- Lock your devices down. Use security cables.
- Before leaving your computer, always logout.
- Turn computing devices OFF when not in use.
- Don't write passwords in, on or around computer or keyboard.
- Consider storing laptops and other high value portable gear in locked drawers/containers.

Traveling with mobile devices

- Secure all mobile devices using locking cables.
- Never place a laptop in checked baggage.
- Avoid carrying a laptop in a "computer case". Instead, use a less-conspicuous carrier.

Online shopping and auctions

(Sources: E-Bay, FBI Internet Fraud Center, Federal Trade Commission)

- Deal with only reputable merchants. Check seller feedback before buying.
- Check website URL's carefully. Make sure you have the correct site.
- Before supplying sensitive information to a web page, look for the "https://" in the URL.
- Pay by credit card, never with a bank wire.
- Consider avoiding sellers who demand Western Union payment.
- Don't be lured off an auction site to complete a transaction. Consider using the site's authorized escrow service, especially for expensive items.
- Before sending money, communicate with seller via email and phone, if possible.
- Print records of all merchandise descriptions, transactions and communications with sellers.
- Never respond to email or websites asking you to confirm information such as name, password, or credit card number.

Continued on next page...



Northeastern University

Office of Information Security and Identity Services

2009 General Computer and Information Security Recommendations (continued)

Signs and symptoms of computer compromise

If a combination of these signs and symptoms are present on your computer, please contact the ResNet Resource Center or IS Service Desk for assistance.

- Unexpected disk activity when computer is not in use.
- Unexpected files appear. Expected files disappear.
- Disk space utilization is higher than expected.
- Computer is unusually slow or sluggish.

Your Credit Report

It is recommended to check your credit report at least once yearly. All consumers are entitled to one free credit report per year. At the time of writing, the URL to order this report is:

<https://www.annualcreditreport.com/cra/index.jsp>

CAUTION ! When typing the above URL into your web browser, please do so carefully. Many imposter sites exist with spellings very close to the official URL shown above.

Unauthorized Interception of Electronic Communications

Unauthorized interception of electronic communications may constitute a violation of Federal law. Never engage in this activity.

Copyright Resources

US Copyright Office home page:

<http://www.loc.gov/copyright/>

US Copyright FAQ

<http://www.loc.gov/copyright/faq.html>

Computer Security Resources

Microsoft: <http://www.microsoft.com/security/>

Apple: <http://www.info.apple.com/>

Symantec: <http://www.symantec.com/>

CERT: <http://www.cert.org/>

NU Information Security Resources

If you have questions about information security, please contact the Office of Information Security at itsecurity@neu.edu.



Northeastern University

Office of Information Security and Identity Services

Managing Your Electronic Reputation

Online expression has become a component of individual reputation, where even years later, electronic expressions can be easily discovered, possibly leading to a variety of unanticipated consequences.

Consider making your electronic reputation a powerful and positive force for your life and for your future. Here's how:

When expressing yourself online, consider...

- You own and are responsible for what you say.
- What you say online will likely be captured and stored **forever**, somewhere in cyberspace.
- What you say can be forwarded and republished without your knowledge or consent.
- What you say is virtually impossible to remove from cyberspace once it's out there.
- Others are likely to search for you online, and they will likely find your expressions.
- What they see might affect their impressions of you, and could affect decisions made about you.

Tips for managing your electronic reputation...

- Never use electronic expression to make a threat or to strike out at others.
- Think before speaking, then speak as if the world were listening.
- Consider and respect difference.
- Be mindful of the rights and feelings of others.
- Think about how others might perceive what you say.
- Express yourself in ways that support the life goals to which you aspire.
- Not sure what to say or how to say it? Ask for help.

Have Questions ? **Need Help ?**

If assistance is needed with matters of electronic expression and reputation, contact your advisor, professor, supervisor, or itsecurity@neu.edu