



**Northeastern**  
UNIVERSITY

Office of Information Security and Identity Services

## **Information and Computer Security Reference Materials**

**May 2008**

**Please read and keep for reference.**

This document is also available on the [www.infoservices.neu.edu](http://www.infoservices.neu.edu)



Office of Information Security and Identity Services

**Viruses, Worms and Bots can stop your computer cold.  
Spyware makes your secrets known.  
An unprotected computer is an open door for attackers.**

**Don't be a victim.  
Take steps to protect your computer NOW !**

Viruses, worms, spyware and bots can not only stop your computer cold, but they also interfere with legitimate work, invade your privacy, drain resources, steal your information, and can cause inconvenience for all members of the University community.

**The threat is real.** Unpatched computers, those without updated antivirus software, those with missing or weak administrative passwords, open file shares, spyware, or out-of-date software are especially vulnerable to viruses, worms and other exploits. These "compromised" computers often become slow and unusable, damaging your data, betraying your secrets, and disrupting your work and that of others. In many cases, compromised computers simply stop working, and must be re-imaged, resulting in inconvenience, wasted time, and in some cases, data loss.

**This packet provides information that will help you reduce exposure to information security threats. The packet contains these sections:**

- myChecklist for Computer and Information Security
- Checklist for Protecting Your myNEU Account
- General Computer and Information Security Recommendations
- Notice on Management of Copyright Infringement Complaints
- Policy on Unsanctioned Network Expansion Devices
- Managing Your Electronic Reputation



Office of Information Security and Identity Services

## my Checklist for Computer and Information Security May 2008

Step	Actions	Check <input checked="" type="checkbox"/>
<b>1</b>	<p><b>Got a new computer ?</b>            Before connecting a new computer to the internet for the first time, learn how to do it safely:  <a href="http://www.us-cert.gov/reading_room/before_you_plug_in.html">http://www.us-cert.gov/reading_room/before_you_plug_in.html</a>  <a href="http://www.microsoft.com/athome/security/update/newcomputer.mspx">http://www.microsoft.com/athome/security/update/newcomputer.mspx</a></p>	
<b>2</b>	<p><b>Secure your home computer.</b>  <a href="http://www.us-cert.gov/reading_room/HomeComputerSecurity/">http://www.us-cert.gov/reading_room/HomeComputerSecurity/</a></p>	
<b>3</b>	<p><b>Got Antivirus ?...Obtain, install and update antivirus software.</b>            Download Symantec antivirus FREE via your myNEU account.</p>	
<b>4</b>	<p><b>Get Automatic Software Updates</b>            Update your operating system and application software. Next, configure your computer to automatically download updates.            Microsoft products:  <a href="http://www.microsoft.com/athome/security/update/default.mspx">http://www.microsoft.com/athome/security/update/default.mspx</a>            Apple products: <a href="http://www.apple.com/support/downloads/">http://www.apple.com/support/downloads/</a></p>	
<b>5</b>	<p><b>Got Spyware Protection ?</b>            Protect your privacy ! Keep spyware off your computer.</p> <p>Pest Patrol: <a href="http://www.pestpatrol.com">http://www.pestpatrol.com</a>            SpyCop: <a href="http://www.spycop.com">http://www.spycop.com</a>            Lavasoft: <a href="http://www.lavasoft.com/">http://www.lavasoft.com/</a></p> <p><b>Note:</b> 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>	
<b>6</b>	<p><b>P2P File Sharing and Copyright Checkup</b></p> <ul style="list-style-type: none"> <li>• Delete any illegally-downloaded materials <b>before</b> connecting to the University network.</li> <li>• Read/understand user documentation and privacy policies before using p2p software.</li> <li>• Assure sensitive or copyrighted materials are not being shared from your computer.</li> </ul> <p>• Read more about file sharing at <a href="http://www.musicunited.org/">http://www.musicunited.org/</a>, and <a href="http://www.campusdownloading.com">www.campusdownloading.com</a></p> <ul style="list-style-type: none"> <li>• Read the University position on Management of Copyright Infringement Complaints, included with this packet.</li> </ul>	

Step	Actions	Check <input checked="" type="checkbox"/>
7	<p><b>Manage Your Security Settings and Backup</b></p> <ul style="list-style-type: none"> <li>-Change the administrative password on your computer. Make it hard to guess.</li> <li>-Keep your administrative password to yourself.</li> <li>-Keep all computer and system passwords to yourself. Never use another's password.</li> <li>-Remove un-necessary user accounts from your computer.</li> <li>-Remove guest accounts. Turn off file-sharing features.</li> <li>-Turn off un-necessary services such as web, FTP, etc.</li> <li>-Use a built-in or personal firewall.</li> <li>-Backup critical data frequently. Use a "usb" drive, zip disk or other device.</li> <li>-Store backups in a safe place.</li> </ul>	
8	<p><b>Get Subscribed to Security Alerts</b></p> <p>Get breaking computer security news automatically.  <a href="http://www.us-cert.gov/cas/signup.html">http://www.us-cert.gov/cas/signup.html</a></p>	
9	<p><b>Stay Informed. Be ready to act.</b></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.  <a href="http://www.microsoft.com/athome/security/online/default.aspx">http://www.microsoft.com/athome/security/online/default.aspx</a></p> <p>Check out the NU security alert dashboard:  <a href="http://www.infoservices.neu.edu/get_help/symantec_norton_alerts.html">http://www.infoservices.neu.edu/get_help/symantec_norton_alerts.html</a></p> <p>Watch the myNEU portal for announcements.  <a href="http://myneu.neu.edu">http://myneu.neu.edu</a></p>	
10	<p><b>Become "Security Streetwise"</b></p> <p><b>Protect your accounts and digital devices:</b></p> <ul style="list-style-type: none"> <li>-Never share your passwords. Never use another's password.</li> <li>-Make your myNEU password and password reset challenge answer complex and hard-to-guess.</li> <li>-Protect your laptop by using a security cable.</li> <li>-Never leave cell phone, PDA, Blackberry or other digital devices unattended.</li> </ul> <p><b>Protect your privacy and safety:</b></p> <ul style="list-style-type: none"> <li>-Keep personal information to yourself. <a href="http://www.epic.org/privacy/consumer/">http://www.epic.org/privacy/consumer/</a></li> <li>-Use discretion before sharing your picture or personal information.</li> <li>-Make informed decisions around use of social networks.</li> <li>-Don't give personal information in response to e-mail or web forms.</li> <li>-Don't respond or reply to spam. Delete it instead.</li> <li>-Don't respond to phishing. <a href="http://www.antiphishing.org/">http://www.antiphishing.org/</a></li> <li>-Guard identification, credit cards, passports and sensitive documents.</li> <li>-Be careful what you throw away. Shred sensitive information promptly.</li> </ul> <p><b>Attend Security Awareness Training.</b> Visit <a href="http://www.infoservices.neu.edu">www.infoservices.neu.edu</a> for schedules.</p>	



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 simple steps:

Step	Actions	Check <input checked="" type="checkbox"/>
1	<p><b>Change your myNEU password.</b> Choose a password that is strong and hard to guess. Make sure your password is at least 8 characters long, with the following additional features:</p> <ul style="list-style-type: none"> <li>• contains at least one uppercase character</li> <li>• contains at least one lowercase character</li> <li>• contains at least one numeric character</li> </ul>	
2	<p><b>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 answer.</b> The password reset challenge answer is case sensitive, so use case to help deter guessing.</p> <p><b>For example:</b>            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><b><u>Do not use these examples for your myNEU account.</u></b></p> <p><b>Never use any of the following for password reset challenge answers</b></p> <ul style="list-style-type: none"> <li>• common words, dictionary words, phone numbers, sequences of numbers</li> <li>• name of family member, favorite color, drink, song, performer, pet name, car brand, etc.</li> </ul>	
3	<p><b><u>NEVER</u> share your myNEU password or password reset challenge question.</b></p>	
4	<p><b>Change your myNEU password and password reset challenge answer frequently.</b></p>	



Office of Information Security and Identity Services

## 2008 General Computer and Information Security Recommendations

Read and comply with the Appropriate Use Policy (AUP)

[www.infoservices.neu.edu](http://www.infoservices.neu.edu)

### 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.
- Don't allow unknown persons to use your computer or mobile devices.
- Shred un-needed papers containing sensitive or confidential information.

### Operating System and Application Software

- Keep original copies of all installation media & keys.
- Monitor manufacturer websites for product updates.
- Register for product updates.
- Use "auto update" features of operating systems.

### 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.
- Avoid checking the "remember my password" box.

### Antivirus and firewall software

- Install and maintain anti-virus software on every computer you own.
- Schedule automatic virus definition updates.
- Use built-in or personal firewall software on every computer you own.

### Instant Messaging and Chat

- Never accept unsolicited downloads/offers.
- Avoid discussing confidential information.
- Never use IM or IRC to authorize transactions or payments,

### 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.

### E-mail

- Don't open unexpected messages or attachments, or messages from unknown senders.
- Don't open messages with unrecognized subject lines.
- Never reply to unsolicited e-mail.
- Never click on an unsolicited web link.

### File Sharing/Peer-to-Peer

- Comply with copyright law.
- Read and understand privacy policies before using P2P applications.
- Never allow guest or anonymous access to your computer.
- Download only trusted files or applications.
- Be mindful of bandwidth use.

### Data Management, Backup and Storage

- Backup critical data daily. Use myFiles on myNEU.
- Store backups in a safe location.
- Delete unnecessary files on a regular basis.

### Your personal privacy

- It's not necessary to share everything about you with others. Keep personal information to yourself. Use discretion before sharing.

### Making your computer less attractive to unauthorized users

- Lock down. Use security cables.
- Before leaving your computer, always logout.
- Turn computer OFF when not in use.
- Don't write passwords on computer or keyboard.

### Traveling with mobile devices

- Secure all mobile devices.
- Never place laptop in checked baggage.
- Avoid carrying laptop in a "computer case". Instead, use a less-conspicuous case such as a padded gym bag.

## 2008 General Computer and Information Security Recommendations

Read and comply with the Appropriate Use Policy (AUP)

[www.infoservices.neu.edu](http://www.infoservices.neu.edu)

### 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.

### 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 promptly.
- Check credit report regularly. Report errors or unusual activity promptly.
- Consider mailing bill payments from public mailboxes instead of residential mailboxes.

### Privacy

- Protect your e-mail address and personal information.
- Avoid configuring personal information into your web browser software.
- 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 depicted and/or recorded.

### 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.

### 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 Center 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.

### Unauthorized Interception of Electronic Communications

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

**2008 General Computer and Information Security Recommendations  
Additional Resources**

Read and comply with the Appropriate Use Policy (AUP)  
[www.infoservices.neu.edu](http://www.infoservices.neu.edu)

**Copyright Resources**

**US Copyright Office home page:**

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

**US Copyright FAQ**

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

**Copyright Basics**

<http://www.loc.gov/copyright/circs/circ1.html#noc>

**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 e-mail the Office of IT Security at [itsecurity@neu.edu](mailto:itsecurity@neu.edu).

**Notice to Students and the University Community  
Management of Copyright Infringement Complaints  
4/4/07, Amended 9/11/07**

On February 28, 2007, the Recording Industry Association of America (RIAA) changed their strategy regarding copyright infringement complaints. Since these changes may impact you, we feel it is important to share the details of these changes.

Downloading and/or sharing of copyrighted content such as movies, music or software without permission of the copyright holder or their designated agent is both illegal and a violation of Northeastern University's technology Appropriate Use Policy (<http://infoservices.neu.edu/aup.html>) which applies to all members of the university community.

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 aware only 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 then, 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.



Office of Information Security and Identity Services

## **Policy on Unsanctioned Network Expansion Devices**

While adding wireless routers, switches, hubs or other unsanctioned network expansion devices may be an attractive alternative to ordering ports or using University-sanctioned wireless services, use of unsanctioned devices can disrupt network service to classroom, research, residential and administrative venues. In addition, unsanctioned devices expose the University network and its data to virus, worm and denial of service attacks. For these reasons, the Appropriate Use Policy prohibits connection of personal, private or departmental switches, routers, wireless access points or DHCP-serving devices to centrally-managed network segments, except only as may be agreed to in writing between the device owner and Information Services.

University-sanctioned ports and NUWave wireless services feature reliability, backed up by centralized support and maintenance. These solutions are best when considering network expansion. For more information about the NUwave expanded wireless project, please visit <http://infoservices.neu.edu/wireless>

Members of the community who are considering network expansion are kindly asked to consider the service offerings listed above, as well as the Appropriate Use Policy, which may be read at <http://infoservices.neu.edu/aup.html>

For help with Appropriate Use Policy questions, please contact [itsecurity@neu.edu](mailto:itsecurity@neu.edu). For general assistance, please contact [help@neu.edu](mailto:help@neu.edu)



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.
- What you say can be forwarded and republished without your knowledge.
- What you say can be difficult or impossible to remove from cyberspace.
- Others are likely to search for you online.
- What they see might affect their impressions of you, and decisions made about you.

### **Tips for managing your electronic reputation...**

- Never use electronic expression to threaten or 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.

### **Have Questions ? Need Help ?**

If assistance is needed with matters of electronic expression and reputation, contact your advisor, supervisor, or [itsecurity@neu.edu](mailto:itsecurity@neu.edu). We're here to help.