Office of Information Security and Identity Services

Information and Computer Security Reference Materials

May 2007

This packet contains important information about protecting your computer and electronic experiences here at Northeastern.

Please read and keep for reference.

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 this fall.
Take steps to protect your computer NOW !

Viruses, worms, spyware and bots can not only stop your computer cold, they also interfere with legitimate work, invade your privacy, drain resources, steal information, and cause delays and inconvenience for students and staff alike.

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without updated antivirus software, those with missing or weak administrative passwords, open file shares, spyware, or out of date software are especially vulnerable to viruses, worms and other exploits.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 the work of others. In many cases, compromised computers stop working entirely, and must be completely re-imaged, resulting in inconvenience, wasted time, and in many cases, data loss.

Office of Information Security and Identity Services

my Checklist for Computer and Information Security
May 2007

☑ Step 1..Got a new computer ?
Before connecting a new computer to the internet for the first time, learn how to do so safely:
http://www.us-cert.gov/reading_room/before_you_plug_in.html
http://www.microsoft.com/athome/security/update/newcomputer.mspx

☑ Step 2.. At home
Secure your home computer.
http://www.us-cert.gov/reading_room/HomeComputerSecurity/

☑ Step 3.. Got Antivirus ?
Obtain, install and update antivirus software on every computer you own.
http://www.symantec.com
Admitted, returning students, and arriving freshmen: Download Symantec antivirus FREE via myNEU.
Arriving freshmen: FREE Symantec CD included in your dorm room packets.
Returning faculty: Get FREE antivirus software at InfoCommons in Snell Library. Bring a blank CD with you.

☑ Step 4.. Get Automatic Software Updates
Update your operating system and application software. Next, configure your computer to download automatic updates.
Microsoft products: http://www.microsoft.com/athome/security/update/default.mspx
Apple products: http://www.apple.com/support/downloads/

☑ Step 5.. Got Spyware Protection ?
Protect your privacy ! Sweep and keep spyware off your computer.
Pest Patrol: http://www.pestpatrol.com
SpyCop: http://www.spycop.com
Lavasoft: http://www.lavasoft.com/

☑ Step 6.. File Sharing and Copyright Checkup

Check file sharing settings. Observe copyright laws.

• Delete all illegally-downloaded materials **before** connecting to the University network.
• Make sure your hard disk and sensitive documents are not being shared through built-in file sharing or P2P.
• Once connected, download and share copyrighted materials only in compliance with copyright laws.

• Windows file sharing settings are described at:
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/filesharing.mspx

• Read more about file sharing at http://www.musicunited.org/, and www.campusdownloading.com

• NEW FOR 2007…Read the University position on Management of Copyright Infringement Complaints, included with this packet.

☑ Step 7.. Manage Your Security Settings

-Change the administrative password on your computer. Make the password hard to guess.
-Keep passwords to yourself.
-Remove un-necessary user accounts.
-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 frequently. Use a "usb" drive, zip disk or other device.
-Store backups in a safe place.

☑ Step 8.. Get Subscribed to Security Alerts

Get breaking computer security news automatically.
http://www.us-cert.gov/cas/signup.html

☑ Step 9.. Stay Informed. Be ready to act.

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.
http://www.microsoft.com/athome/security/online/default.mspx

Check out the NU security alert dashboard:
http://www.infoservices.neu.edu/get_help/symantec_norton_alerts.html

Watch the myNEU portal for announcements.
http://myneu.neu.edu

☑ Step 10.. Become "Security Streetwise"

Protect yourself by sharpening your information and computer security skills:

Protect your accounts and digital devices:
-Never share your passwords.
-Make your myNEU password and password reset challenge answer complex and hard-to-guess.
-Protect your laptop by using a security cable.
-Never leave cell phone, PDA, Blackberry or other digital devices unattended.

Protect your privacy and safety:
-Keep personal information to yourself. http://www.epic.org/privacy/consumer/
-Use discretion before choosing to share your picture or personal information.
-Make informed decisions around social networks (Facebook, mySpace, etc.)
-Don't give out 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.

Be a good 'net citizen:
-Got music or movies ? Use legal downloads only. Never share copyrighted material without permission.

-NEW FOR 2007: Read the updated Northeastern Appropriate Use Policy at http://www.infoservices.neu.edu/aup.html

-Plan to attend Security Awareness Training. Visit www.infoservices.neu.edu for schedules.

Office of Information Security and Identity Services

2007 Computer and Information Security Recommendations

Read and comply with the Appropriate Use Policy (AUP)
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.

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.

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.

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/keyloger detection software on every computer you own.
- Avoid performing highly 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.

File Sharing/Peer-to-Peer

- Comply with copyright law.
- Read and understand privacy policies before downloading 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 with everyone.
- 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.

2007 Computer and Information Security Recommendations

Read and comply with the Appropriate Use Policy (AUP)
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 sharing others' personal 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, as well as state and federal laws. Always get permission before capturing, transmitting or recording audio and/or video.

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 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 is a criminal offense, punishable by fines and imprisonment. Refer to the Appropriate Use Policy for more information.

2007 Computer and Information Security Recommendations
Additional Resources

Read and comply with the Appropriate Use Policy (AUP)
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.

Notice to Students and the University Community
Management of Copyright Infringement Complaints
4/4/07

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 twenty (20) 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

Considering Adding 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 service, use of unsanctioned devices can disrupt network service to classroom, research, residential and administrative venues. In addition, unsanctioned devices expose the University network and it's 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 networtk 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. In addition NUwave wireless service will be available by the start of fall classes in all administrative and classroom buildings. For more information about the NUwave expanded wireless project, please visit http://infoservices.neu.edu/wireless.

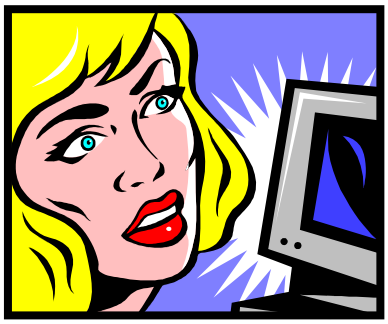
Members of the community who are considering network expansion are kindly asked to consider the service offerings listed above, as well as the Appropriate Use Policy, which may be read at http://infoservices.neu.edu/aup.html

For help with Appropriate Use Policy questions, please contact **itsecurity@neu.edu**. For general assistance, please contact help@neu.edu.

Information Security and Identity Services
IS Customer Service

Office of Information Security and Identity Services

Managing Your Electronic Reputation



Online speech has become a component of individual reputation, where even years later, inappropriate online speech is often discovered, resulting in negative consequences for the speaker.

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

When speaking online, consider…

- You own and are responsible for what you say.
- What you say online will likely be captured and stored forever.
- Others are likely to search for you online.
- What they see might affect their impression of you.
- What they see is likely to affect decisions made about you.

Tips for managing your electronic reputation…

- 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.
- Speak in ways that support the life goals to which you aspire.

Have Questions ? Need Help ?

If you need assistance with matters of electronic speech and your reputation, contact your advisor, supervisor, or itsecurity@neu.edu.