Office of Information & Technology Security

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Un-patched computers, those with missing or out-of-date antivirus software, those with missing, weak, or easily guessed administrative passwords, open file shares, guest accounts, spyware, or out-of-date operating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 other healthy computers; and disrupting both 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 & Technology Security offers this Computer and Information Security Guide. This year’s guide includes the following 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
• 2013 General Computer and Information Security Recommendations
• Managing Your Electronic Reputation

This guide is also available on the Information Technology Services SecureNU website: northeastern.edu/secureNU

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 ITS Service Desk at 617.373.4357 (xHELP) or our office directly at itsecurity@neu.edu.

Yours in security,

Mark T Nardone,
Directo, Information & Technology Security
## myChecklist for Computer and Information Security

### Do you have a new computer?
Before connecting a new computer to the internet for the first time, learn how to do it safely:

### Do you have antivirus software? Obtain, install and update FREE antivirus software.
Mac and Windows users can download FREE Symantec antivirus through myNEU
- **Students**: Log onto myNEU.neu.edu, select the Self-Service tab, and click the “Software Downloads” link. Download the appropriate software for your computer’s operating system.
- **Faculty/Staff**: Log onto myNEU.neu.edu, select the Services and Links tab, and click the “Software Downloads” link. Download the appropriate software for your computer’s operating system.

### Is your computer set up to get automatic software updates?
First, update your operating system and application software. Next, configure your computer to automatically download updates. To learn how to set automatic updates for Apple and Windows visit [northeastern.edu/secureNU/pages/protect](http://northeastern.edu/secureNU/pages/protect)

For other products, please consult the website for your supplier or manufacturer.

### Do you have spyware protection?
Protect your privacy by keeping spyware off your computer.
- **MalwareBytes**: [http://www.malwarebytes.org/](http://www.malwarebytes.org/)
- **SpyCop**: [http://www.spycop.com](http://www.spycop.com)
- **Lavasoft**: [http://www.lavasoft.com/](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.

### Have you completed the P2P file sharing and copyright checkup?
- 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 [www.campusdownloading.com](http://www.campusdownloading.com) and [northeastern.edu/secureNU/pages/copyright](http://northeastern.edu/secureNU/pages/copyright)
- Read the Notice to Students and the University Community on Management of Copyright Infringement Complaints, included with this guide or at: [northeastern.edu/secureNU/pages/copyright](http://northeastern.edu/secureNU/pages/copyright)
- You will be notified if you are involved in illegal downloading, and may face university sanctions as stated in the Northeastern University Acceptable Use Policy (AUP): [northeastern.edu/aup](http://northeastern.edu/aup)

### Have you managed your security settings and backups?
- 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 person’s password.
- Remove unnecessary user accounts from your computer.
- Remove guest accounts. Turn off file-sharing features.
- Turn off unnecessary services such as web, FTP, etc.
- Use a built-in or personal firewall.
- Backup critical data often.
  - Use a USB drive, external hard drive 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.
Have you subscribed to security alerts?
Follow the NU IT Security Twitter: @Securenu
Follow the NU IT Security Blog: northeastern.edu/securenu/blog

Stay vigilant, informed and 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. Visit northeastern.edu/securenu/pages/stayinformed for the latest updates.
Watch the myNEU portal for announcements: myneu.neu.edu

STUDENTS ONLY – are you ready to connect once on campus?
Before arrival, purchase a 25-foot Cat 5E or higher Ethernet cable. For those who may arrive without a cable, cables are available for purchase from the Northeastern Bookstore, and nearby retailers.
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.

Are you “streetwise” about your security?
Protect your accounts and digital devices:
• 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.
Read additional security tips at: northeastern.edu/securenu

Protect your privacy and online safety:
• 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. www.antiphishing.org/
• Guard identification, credit cards, passports and sensitive documents.
• Be careful what you throw away. Shred sensitive information promptly.
Read more privacy and safety tips at: northeastern.edu/securenu

Special Note:
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.
View phishing examples and learn how to protect yourself: northeastern.edu/securenu/pages/phishing
<table>
<thead>
<tr>
<th>Checklist for Protecting your myNEU Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your myNEU account is your passport to a world of information and electronic services. To help protect your account from unauthorized access, follow the steps below.</td>
</tr>
<tr>
<td><strong>Choose a strong password for your myNEU account.</strong></td>
</tr>
<tr>
<td>Choose a password that is strong and hard to guess. Make sure your password is at least eight characters long, with at least:</td>
</tr>
<tr>
<td>• one uppercase character</td>
</tr>
<tr>
<td>• one lowercase character</td>
</tr>
<tr>
<td>• one numeric character</td>
</tr>
<tr>
<td>• one special character</td>
</tr>
<tr>
<td>Example 1: Droopy$Jaw5 (note use of “$” character)</td>
</tr>
<tr>
<td>Example 2: REd$0x4MyLife</td>
</tr>
<tr>
<td><strong>Do not use these examples for your myNEU account.</strong></td>
</tr>
<tr>
<td><strong>Choose a difficult password reset challenge question and answer.</strong></td>
</tr>
<tr>
<td>Choose a difficult 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.</td>
</tr>
<tr>
<td>For example:</td>
</tr>
<tr>
<td>Challenge question: what is my secret shame?</td>
</tr>
<tr>
<td>Challenge answer: eating YELLOW flowers</td>
</tr>
<tr>
<td>Challenge question: What are the marks of the beast?</td>
</tr>
<tr>
<td>Challenge answer: PINK elephants with shoes</td>
</tr>
<tr>
<td><strong>Do not use these examples for your myNEU account.</strong></td>
</tr>
<tr>
<td>Never use any of the following for passwords or password reset challenge answers</td>
</tr>
<tr>
<td>• common words, dictionary words, phone numbers, sequences of numbers</td>
</tr>
<tr>
<td>• name of family member, favorite color, drink, song, celebrity, pet name, car brand, any information that is publically available: Consider how much information may be available via Facebook!</td>
</tr>
<tr>
<td><strong>NEVER share your myNEU password and/or password reset challenge question.</strong></td>
</tr>
<tr>
<td>Sharing your myNEU password and/or password reset challenge question compromises your account, can result in identity theft, and is a violation of the Appropriate Use Policy: northeastern.edu/aup</td>
</tr>
<tr>
<td><strong>Change your myNEU password and password reset challenge question and answer frequently.</strong></td>
</tr>
<tr>
<td>Consider changing your myNEU password and password reset challenge question and answer every 90 days or more frequently.</td>
</tr>
</tbody>
</table>
Security Requirements and Recommendations
This document describes the required and recommended security practices to be used with personally-owned routers and/or wireless access points connected to ResNet ports in the residence halls, which at the current time, may be connected in the private areas of all residence halls, except International Village. NUwave wireless networking service is currently available in International Village and the public common areas of residence halls.

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 northeastern.edu/aup

The university provides basic setup support for personal wireless access points and for potential conflicts between private devices but no troubleshooting of personal devices themselves. Where these devices conflict with ‘common area’ NUwave wireless service, ITS retains the right to modify or decommission ports serving any student-owned devices.

<table>
<thead>
<tr>
<th>Wireless Requirements and Recommendations (in order of set-up)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>STRONGLY RECOMMENDED</strong></td>
</tr>
<tr>
<td><strong>REQUIRED</strong></td>
</tr>
<tr>
<td><strong>REQUIRED</strong></td>
</tr>
<tr>
<td><strong>RECOMMENDED</strong></td>
</tr>
<tr>
<td><strong>REQUIRED</strong></td>
</tr>
<tr>
<td><strong>REQUIRED</strong></td>
</tr>
<tr>
<td><strong>REQUIRED</strong></td>
</tr>
<tr>
<td><strong>REQUIRED</strong></td>
</tr>
<tr>
<td><strong>STRONGLY RECOMMENDED</strong></td>
</tr>
</tbody>
</table>

continued on next page
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.

REQUIRED

1) 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”.
2) Domain name should be set to “neu.edu”.
3) MTU size should be “automatic”, or up to 1500 if automatic is not an option on your access point.
4) Set your wireless access point as a DHCP server, and to give out IP addresses in one of the following ranges:
   - 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
   Never set your device to give out IP addresses other than those shown above.
   5) If your router/wireless access point features a time zone setting, use the “Eastern” time zone.

REQUIRED

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.

REQUIRED

Do not hard-code DNS settings in your router or wireless access point. Use only DNS settings provided automatically by the University.

REQUIRED

Do not set your router/wireless access point to act as a bridge.

STRONGLY RECOMMENDED

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.

REQUIRED

Use AP-mode or Infrastructure setting on the wireless access point. Ad-hoc mode should NOT 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:

- www.belkin.com
- www.dlink.com
- www.netgear.com
- www.apple.com
- www.hp.com
- www.trendnet.com/?todo=home

The computing information and security guide can be found at northeastern.edu/secureNU/newstudent

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 Information Technology Services. For more information, please refer to the Appropriate Use Policy at northeastern.edu/aup.
Notice to Students and the University Community Management of Copyright Infringement Complaints
Amended 6/10/2009

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 (northeastern.edu/aup) 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 & Technology 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.
2013 General Computer and Information Security Recommendations
Read and comply with the Appropriate Use Policy (AUP) northeastern.edu/aup

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 unneeded 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?
  - how long will the information be kept and how will it be disposed of?

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 webcams 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.

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 any 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/confidential 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 unsecured (hotspot) networks. When on campus, consider using NUwave secure wireless service.

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, external hard drive 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 portable electronic devices**

• Secure all portable electronic 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 urls carefully. Make sure you have the correct site.
• Before supplying sensitive information to a website, 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 visit the ResNet Resource Center (students only) or call the ITS 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: [www.annualcreditreport.com](http://www.annualcreditreport.com).

**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/](http://www.loc.gov/copyright/)
US Copyright FAQ: [http://www.loc.gov/copyright/faq.html](http://www.loc.gov/copyright/faq.html)
Computer Security Resources
Microsoft: http://www.microsoft.com/security/
Apple: http://www.apple.com
Symantec: http://www.symantec.com/
CERT: http://www.cert.org/

Northeastern Information and Technology Security Resources
If you have questions about information security, please contact the Office of Information & Technology Security at itsecurity@neu.edu or online at northeastern.edu/securenu.
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.

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 or Need Help

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