Quarterly Security Reminder
Office of Information Security

As a member of the Northeastern Community, you are responsible for information security.

Security is a shared responsibility. We all have individual and institutional responsibilities to protect sensitive information. You are required to read and comply with university policies on the use of information and information systems. Do your part to help promote a safer and more secure computing environment. Observe and support secure practices in your academic or business unit.

Northeastern's Appropriate Use Policy (AUP) describes policies for use of all computers, networks and telecommunications facilities at the university. All members of the University community are required to read and comply with the AUP terms. Use of university computer/telecommunication networks and/or computers, implies agreement with the terms of the Appropriate Use Policy. Read More..
National Cyber Security Awareness Month
Security - A Shared Responsibility..

The month of October has been deemed National Cyber Security Awareness Month. Northeastern is taking the opportunity to help our community become more aware of cyber security threats, which can affect you in your work and daily life. Watch for posts from the SecureNU website and tweets from the Information Security Team. Also look for on campus events and remember that information security begins with you!

Fall Back - Sunday, November 6th!
Check your clocks as we return to Standard Time

Daylight Savings Time ends at 2 a.m. on November 6, 2016. Remember to set your clocks back one hour as we return to Standard Time. While most computer and electronic systems will automatically make the change, it is always a good idea to verify that it has occurred correctly to ensure proper functionality.

Hold Onto Your $$ and Your Files!
Beware of these trending cyber-crime tactics

Ransomware: The fastest growing cyber-crime over the last two years. The FBI reports that the revenue generated for criminals is expected to hit $1 billion this year.

How the scam works: Cybercriminals leverage traditional methods to infect your computer with their malware (phishing, infected websites or email attachments). The malware encrypts files on your hard-drive and any connected network shares or storage devices. Your computer will then display the notice: “Your files are encrypted, you have 10 days to send 200BC (bitcoins) to [Bad-guy's account]”

At this point your computer will do nothing more than boot up and display the ransom. Your files are inaccessible. The impact on an organization can be catastrophic. Many, including Hollywood Hospital have paid the ransom. Sometimes they get files back, sometimes they do not.
How to protect yourself: First and foremost, follow the best practices and develop awareness about phishing and malware. Second, utilize the university backup system which will allow you to recover from a ransomware event should you fall victim.

Protecting Northeastern and YOU
Ensuring that personal data is protected

Multifactor Authentication is a method of securing valuable information by requiring more than a password to gain access. Northeastern plans to implement it across our high value resources campus-wide - such as access to HRM and benefits data, protected student and financial data, VPN and more. This technology is very easy to use in conjunction with a mobile device and adds significant protection for users and the institution.

REMEMBER: Northeastern University WILL NEVER ASK FOR YOUR PASSWORD!
If you receive an email that claims to need your login and password - it should be deleted without replying. If you have given a password to another person, change that password immediately. You are responsible for all activity conducted under your user ID and password.

Protection of Sensitive Information
Compliance to NU policies and Federal law is critical

Sensitive information -including social security numbers, dates of birth, grades, non-public personal financial information, protected health information- are to be protected at all times from unauthorized disclosure. Use must be consistent with applicable university policies and applicable Federal laws, including:

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Financial Services Modernization Act (also known as Gramm-Leach-Bliley)
- CAN-SPAM Act of 2003
- Massachusetts Data Security Regulation MA201 CMR17.00

Personal information of members of the Northeastern community, including but not limited to students, faculty and staff, may not be posted or maintained on public networks or sites, unless fully compliant with applicable laws and regulations governing handling of personal info.
Copyright Law and Software Licensing
Compliance: legal use of software, copyrighted material

All members of the community are required to comply with copyright law and software licensing agreements. In addition, all software installed on university-owned devices must be legal copies, and remain properly licensed at all times.

University resources must not be used to offer, exchange or store copyrighted materials nor the indexes pointing to such materials, unless the use is in compliance with copyright law or other applicable regulation. All use of file-sharing technologies shall be in strict compliance with university policy and copyright law.

Our Responsibilities (That Means You!)
Important reminders about our legal requirements

1. **Sensitive Info** - Do not display or list in public venues such as bulletin boards, office doors, globally shared computer files, or publicly-accessible web sites.
2. **Privacy** - Observe privacy practices.
3. **Access** - Use appropriate safeguards to protect sensitive data and information-bearing devices from unauthorized access, alteration, theft or loss.
4. **Documents** - Ensure confidential/sensitive paperwork is properly discarded.
5. **Mobile Devices** - Must be appropriately protected from loss or theft.
6. **Hardware** - Computer disk drives and information storage devices must be properly processed to remove sensitive information prior to reallocation or disposal.

Disclosure or Loss of Sensitive Information
Consequences are serious for the user and university

The potential consequences of unauthorized disclosure or loss of sensitive information may include for the individual, loss of privacy, identity theft, financial loss, erosion of customer confidence, and for the University, damage to reputation, civil penalties, and regulatory sanctions.
By recognizing the value of protecting sensitive information, the university is better positioned to avoid these consequences, maintain customer trust, and enjoy a reputation more demonstrative of the university commitment to excellence and distinction.

If assistance is required, please contact us.

The Office of Information Security
OIS@NEU.EDU
617.373.4357 (xHELP)

...