Northeastern University

Office of Information Security

Spring 2017 Quarterly Information Security Reminder

Dear Members of the Northeastern Community,

This edition includes some quick recommendations for securing your personal information while on and off campus, along with reminders about your responsibilities around protecting sensitive university and student information.

Spring 2017 Information Security Tips:

Spring Forward

Daylight Savings Time begins at 2 a.m., Sunday March 12, 2017. Remember to set your clocks forward one hour. And 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.

Are you Truly Ready for Tax Season Scams?

Tax season is upon us, and government and law enforcement entities have reported an uptick in the number, and sophistication of tax fraud schemes targeting the public. Last year the IRS reported over $21 BILLION in fraudulent tax refund claims in 2016. One way to keep this from happening to you is to ensure that you protect your personal information, and to use only reputable and certified tax preparers. Your fees for tax preparation should **never** be tied to the amount of your refund. All tax preparers will also have a preparer tax identification number (PTIN), which can be checked at http://www.ptindirectory.com/. Also keep in mind that the IRS will **never contact you by telephone** if there are issues with your returns, or if they need information. They will **always send information by U.S. mail**, and only by email if you have requested and provided them with an address. Do not respond to any contact that is threatening or attempts alarm you (threatening audits etc). Always contact the IRS through their official website (www.irs.gov) or call for telephone assistance.

It is ALWAYS Phishing Season

Social engineering and Phishing scams are still the single greatest vector in data compromises and computer virus infections. This risk is heightened with the massive surge in Ransomware attacks across multiple industries. Healthcare, Financial, Higher Education and even Law Enforcement have been targeted, and have fallen victim. The computer virus will encrypt your files, data, even any online backups or network drives. Then offer you the chance to retrieve them, for a modest fee of $200-$5000. This can cause irrevocable harm to businesses if they have no available off-line back-ups. Recently a California Hospital had to transfer patients out of their facility, when all their systems and patient files where encrypted. Many of these incidents start with a simple Phishing email. Contact the Office of Information Security at OIS@northeastern.edu to find out how you can protect yourself and the institution.

Hold Your Password Close

Northeastern University WILL NEVER ASK FOR YOUR PASSWORD. Any email you receive claiming to need your login and password is spurious and should be deleted without replying. If you have given a Northeastern password to another person, change the relevant password immediately. Each of us at the university is held responsible for all activity conducted under our user ID and password.

Protection of Sensitive Information / Regulatory Compliance:

Social Security Numbers, dates of birth, grades, non-public personal financial information, protected health information, and other similar types of sensitive information are to be protected at all times from unauthorized disclosure and/or use, consistent with applicable University policies and/or applicable Federal laws, including the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Financial Services Modernization Act (also known as Gramm-Leach-Bliley), the CAN-SPAM Act of 2003, and 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 the user fully complies with applicable laws and regulations governing handling of personal information.

Compliance with Copyright Law and Software Licensing Agreements:
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 shall be the product of legal copies, and shall be properly licensed at all times. University resources shall 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.

Responsibilities under Regulation:
Our responsibilities under regulation includes, among other reasonable steps, that we refrain from displaying or listing sensitive information in public venues such as hallway bulletin boards, office doors, globally shared computer files, and publicly-accessible web sites, that we observe privacy practices, and that we use appropriate safeguards to protect sensitive information and information-bearing devices from unauthorized access, alteration, theft or loss. These responsibilities include taking appropriate steps to ensure confidential/sensitive paperwork is properly discarded, that mobile devices are appropriately protected from loss or theft, and that computer disk drives and information storage devices are properly processed to remove sensitive information prior to reallocation or disposal.

Consequences Arising from Unauthorized Disclosure or Loss of Sensitive Information:
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 sanction. By recognizing the value in protecting sensitive information, the University is better positioned to avoid these consequences, maintain customer trust, and enjoy a reputation more demonstrative of the University comment to excellence and distinction, and other goals to which the University aspires.

Requirement to Read and Comply with the Appropriate Use Policy (AUP):
The Appropriate Use Policy 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, which can be read at www.Northeastern.edu/aup. Use of University computer/telecommunication networks and/or computers, implies agreement with the terms of the Appropriate Use Policy.

Shared Responsibility
Security is a shared responsibility. Do your part to help promote a safer and more secure computing environment by observing and supporting secure practices in your academic or business unit. If assistance is required, please contact OIS@neu.edu

Thank you for your time and attention.

Warmly,

Mark T. Nardone,
Chief Information Security Officer