ISSUE: 7-10 YEAR: 2014

University Information Security Office Newsletter

Technological progress has merely provided us with more efficient means for going backwards.

-Aldous Huxley

Welcome

Thank you for taking the time to read our Information Security Awareness Newsletter. Our intent is to raise awareness to the common issues that put both university and personal information at risk and to give everyone helpful ways to lessen the risk and help you be safer on the Internet. The Information Security Team will be publishing this newsletter monthly and the topics will change every month so be sure to click the link in the Inside Loyola announcement window every month. We will also be listing our monthly in-person security events and we hope you will be able to find time to join in our discussion on safer computing.

Jim Pardonek
Information Security Officer

University Information Security Office

Email: DataSecurity@luc.edu
Telephone: (773) 508-7373
Location: GC Room230
Hours: M-F 8AM-4PM

Reducing the Amount of Spam You Receive

Created by Brett Weston

Spam has grown from a mere annoyance into something that can be quite dangerous. Cyber criminals are getting more sophisticated in their scams and phishing schemes, which are designed to steal personal data and financial information. They also exploit innumerable security flaws in web applications, PC operating systems, and software.
Spammers and virus creators are motivated by money and backed by organized crime on a global scale. They are also launching massive attacks on anti-spam organizations in an attempt to bring them down. Below are some frequently asked questions about spam and spammers with answers from experts.

How do spammers get my email address?

Spammers buy lists from brokers that continuously harvest email addresses from newsgroups, chat rooms, web sites, Internet directories, and more. Spammers also run dictionary attacks, throwing billions of combinations of words and numbers at an email database to find valid address combinations.

What are some common phishing scams?

People are being tricked by email phishing scams that masquerade as legitimate business communications from their bank, mortgage provider, credit card company, PayPal, or eBay. Spammers hijack these companies' domain names and set up fake web sites. Cheap Internet phone service has put a new twist on these scams. They're directing people to call a fake customer service phone number to give up their user ID and pin. Other popular spam-based Internet scams include foreign lotteries, investment schemes, chain letters, credit repair offers, advance-fee loan deals, check overpayment cons, and work-at-home ploys. Complaints can be filed through the econsumer.gov site.

How can I reduce spam?

To reduce spam, don't display your email address in public—newsgroups, chat rooms, web sites, or online service directories. You should understand privacy policies and forms, and use opt-out options. Try setting up two email addresses, one for real use and one for newsgroups and chats. Use an ISP that fights spam (see StopSpam.org for a list). An email filter and PC spam blocking software are absolutely critical.

About Us

The University Information Security Office (UISO) is a department within Information Technology Services (ITS) that is responsible for the confidentiality, integrity and availability of Loyola's computing assets. As part of protecting student, faculty, and staff information the UISO is responsible for training and awareness of students, faculty, and staff. If you have any questions or concerns, or you would like to have someone from the UISO present in class or for your department, please contact us at datasecurity@luc.edu

Personal Identifiable Information (PII)

Created by Yuan Liu

Confidential PII, like SSN, CCN or health insurance information should not be sent in regular email messages because of the risk of unauthorized access and disclosure. While in transit, emails can be intercepted and the contents disclosed to unauthorized persons. Also, if emailed to a wrong address, the information is irretrievable.
Even if the email reaches its intended destination without a breach, the recipient may retain the confidential PII in their email system, where it will be at risk for disclosure if their PC or email account is compromised.
Before sending confidential PII via email, it should be contained in an encrypted file. The password needed to decrypt the file should be sent separately, so that the information is protected even if one of the emails is intercepted or sent to the wrong address.
We perform the PII Compliance Program on campus for all Loyola machines. The Personal Information Security Compliance Review Protocol process covers all users of computers, electronic devices, and media capable of storing electronic data. The purpose of this protocol is to ensure that all divisions and departments of Loyola University Chicago are in, and remain in, compliance with the policies established for the security of Loyola University Chicago protected and sensitive data. This means that Loyola machines are scanned for PII, and any PII found on Loyola computers is securely deleted.

The purpose of this initiative is:
1. To protect sensitive information, i.e. Social Security and credit card numbers
2. To obtain safe harbor from data breach disclosure
3. To comply with regulatory data security requirements, including PCI DSS.

You can read the policy here:
http://www.luc.edu/its/aboutus/policies.shtml

Phishing: Email Links and Personal Information

Created by Joseph LaMagna-Reiter

More recent email phishing attempts try to raise a sense of alarm. They can come in the form of account lockout notifications, unauthorized account access notifications, or even password expiration notices. These phishing attempts will most likely include links directly in the email; however, the link may not be what it appears to be. The text "www.luc.edu" can be linked to any site on the Internet including a web site created by an attacker.

When seeing links in email messages, navigate to the organization's site manually by typing it into the address bar of your browser. This will help ensure that you are directed to an official web site and not a malicious look-alike created to obtain your sensitive information.

Other phishing emails that do not include links will ask you to provide information in an email reply. This information may be usernames, passwords, email addresses, phone numbers, or other personal information. This sort of information should never be sent through email because email is sent in plain text over the internet, and an attacker could intercept your email. Additionally, many reputable companies or organizations will never ask you for your password or other personal information.

If you are ever unsure if an email is a spam or phish, you can send it to helpdesk@luc.edu to help identify it.