ISSUE: 11-13 YEAR: 2014

University Information Security Office Newsletter

Any sufficiently advanced technology is indistinguishable from magic.

-Arthur C. Clarke

From the ISO's Desk

Most of the recent news articles involving technology are usually some report about the theft of information. Throughout the last year many of the businesses that we know well and shop at regularly such as target, Jewel, Home Depot and others have been infiltrated by hackers looking for a way to make a buck at your expense. You could blame the companies, and in these cases they are mostly at fault. But we have to realize that protecting our information and the information of others needs to be done by all of us in some way. Making sure that our computers are protected and that information is not kept in places where unwanted access is possible is all of our responsibility. The articles in this month's issue highlight the types of information that we have, where we can store it, and how we can use technology to protect it and to make sure that it cannot be acquired through nefarious means.

Jim Pardonek
Information Security Officer

University Information Security Office

Email: DataSecurity@luc.edu
Telephone: (773) 508-7373
Location: GC Room 230
Hours: M-F 8AM-5PM

What's Up With Anti-Virus?

Created by Jacob Schuldt

Antivirus software is essential on most computers to prevent malicious code from infecting a machine. If malicious code infects a device, the device may begin to slow down, restart randomly, start deleting data, reveal personal information to an outside source, or do other undesirable, and uncontrolled, actions. Because of the countless viruses out there, and for the need to keep Loyola's network secure, the ITS department has an antivirus policy in place for all computers that connect to the Loyola network to prevent viruses from infecting devices and spreading across the network.

The Policy

Depending on the operating system of your personal computer, the antivirus requirements vary. Users with a Windows or Mac machine are required to have an antivirus program running at all times. This program must be configured to automatically update the software and virus definitions daily. Linux users are not required to have an antivirus program running. Lastly, any device with an unlisted operating system is required to contact the Information Security team to see if the device must have an antivirus program, but regardless, the operating system must be supported with security updates and vendor support (Computer Security Standard policy).

Programs

There are numerous antivirus programs available on the Internet. AVG and BitDefender are among the highest ranking free antivirus programs, and provide real-time protection while surfing the web and downloading files. Malwarebytes on the other hand is among the best anti-malware solutions and is free, but it only provides the capability of removing viruses once they are already on the machine, unless you pay for the upgraded version.
Antivirus programs that are not free generally provide more customer support, and are suggested for devices with sensitive data. Norton 360, Kaspersky PURE, and Malwarebytes Premium are generally the highest rated, but sometimes costly, antivirus programs.
For Android users, Malwarebytes provides a task manager, scans your device, and shows which apps have access to information on your device, such as location or call records. Bluebox Security Scanner provides a system scan to check for any vulnerable or unpatched apps, untrusted apps, and for malicious data. AVG is also a highly rated mobile phone antivirus program. Many of the same antivirus solutions available for Android are also options for iPhone users, and with the increasing amount of viruses, it is suggested that all mobile users have their devices protected.

Summary

Loyola's ITS department suggests that every device has antivirus on it, not only for the sake of the network, but for the safety of every device. Infections can make a device unusable, but can be easily prevented. If you have any questions regarding antivirus solutions or about this policy, feel free to contact the Help Desk or Information Security team. Additional information on this policy can be found on the Loyola ITS website (luc.edu/its) under ITS Policies and Guidelines.

The Guide to Sensitive Information

Created by Yuan Liu

Overview

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.

Purpose

The purpose of this policy is to ensure that Loyola Protected or Loyola Sensitive data is not inappropriately stored on Loyola computers and electronic devices through systematic electronic examination; to obtain safe harbor from data breach disclosure; to comply with regulatory data security requirements, different laws and industry standards, including PCI DSS, FERPA, GLBA, HIPAA, and Illinois PIPA
Data Classification Policy:
All data produced by employees of Loyola University Chicago during the course of University business will be classified as one of these three types of data: Loyola Protected Data (LPro); Loyola Sensitive Data (LSen); Loyola Public Data (LPub)

Storing Loyola Protected Data Policy

- Social security numbers and other Loyola Protected Data must never be stored on individual workstations, laptops, email, phones, or smartphones/PDAs *(including in email on phones and mobile devices)*, even if they are encrypted
- When it is necessary to store social security numbers, they must be stored on a network drive that has limited access
- Only those with a strict business need, should have access to SSNs
- For files with large numbers of SSNs, it is additionally recommended that the files be encrypted.

Loyola PII Compliance Program:

We use Identity Finder software to search for and protect Social Security Numbers and Credit Card numbers on desktop and laptop computers.

We perform an Identity Finder scan twice a year, at least every six months. During each department scan, a remote scan for all machines in that department is scheduled. Each department decides when these scans occur. Every department has at least one primary Data Steward to helps ITS in the PII Compliance Program. After the scan, all users are responsible for remediation. No SSN or CCN are allowed to be stored on local machines. All files containing PII must be shredded, or moved to a network drive for security.

Encrypt All the Things!!!

Created by Brett Weston

In the last few years, the term “encryption” has become a word in nearly everyone’s vocabulary. Americans are now more afraid that their information will be wrongly disclosed than any other crime (http://www.theregister.co.uk/2014/10/22/americans_more_afraid_of_identity_theft_that_getting_killed_in_a_shooting/). Loyola’s Encryption Policy was drafted and is not enforced to limit the risk of lost data.

The policy states that any device that stores or accesses Loyola Protected data must be encrypted. As part of this policy, all Loyola issued laptops and desktops are encrypted by default. However, personal mobile devices must have encryption enabled, typically found in the devices settings menu. These types of encryption methods are considered encryption at rest.

In addition, certain data must also be encrypted in transit. When accessing Loyola Protected data through the web, the connection must be over https and not http. The “s” in https means that the server has been verified, trusted, and your connection is encrypted.
The good news is ITS takes care of most of the above requirements for you. Devices issued to you are already encrypted, and servers storing protected data use https by default. However, you should still be mindful of situations outside of work that could compromise personally identifiable information. For example, never type a password into a form on a web page that is not https. Hackers can easily grab your username a password and gain access to your accounts.