ISSUE: 8-15 YEAR: 2015

University Information Security Office Newsletter

When you know that you're capable of dealing with whatever comes, you have the only security the world has to offer.

— Harry Browne

From the ISO’s Desk

Welcome back everyone! We hope you’ve had an enjoyable and relaxing summer! A new academic year is always an exciting time for all of us as we see a return of our students and faculty for another year of teaching, learning, and engagement. In the Information Security Office we are excited to introduce you to some of the new and improved services and initiatives that we’ve been working on for you. First, our antiquated VPN has finally been replaced with Loyola Secure Access or LSA. LSA has a more streamlined look and feel, supports all popular operating systems and browsers and no longer requires an installed certificate on each computer that you have in order to use it. We are also excited to be offering a new series of awareness videos called Securing the Human. These will be made available for all faculty and staff with a new video each month on a different awareness topic. Look for those starting in September. For more information on LSA go to: http://www.luc.edu/uiso/resources/lsa.shtml

University Information Security Office

Email: DataSecurity@luc.edu
Telephone: (773) 508-7373
Location: GC Room 230

Physical Security

Created by Andrew Unger

Overview

While cyber-attacks occur often, we cannot forget about also securing our computers and devices physically as well. In addition, while physical attacks against data are less common, it is often simpler for criminals to physically steal information that is not secured. When physical attacks do happen however, they tend to have a far greater impact than the average cyber-attack.

Physical security is often one of the most challenging risks to an organization because there are many people coming to and leaving our facilities, including those who are not employees. To help protect against physical threats we need help from people within the organization with following.

Correctly disposing of confidential information

One of the easiest ways for a criminal to locate confidential information is to find it in an organization’s garbage. Often people do not think about the information that are disposing of. These items include documents, photographs, legal and accounting documents, and proprietary information. Assuming that the above materials are safe once they have been thrown away is a big misconception. Known as “dumpster diving”, during the multiple steps of the trash removal process a criminal can find and recover your confidential information. Known as “dumpster diving”. To protect yourself and your organization from this type of threat, ensure all sensitive information disposed of is either shredded or physically destroyed.

Doors and Access Ways

Another possible attack is a criminal pretending to be an employee and walking into our buildings and stealing what they find. If you open a door that requires badge access ensure that the door closes behind you. In addition, when entering a room that requires an access card be sure anyone else entering uses their access card as well. While our organization requires an ID card to gain access to most office areas, a common attack is for a criminal to follow behind you pretending to be another employee.

Have a clean desk

Unfortunately the security team is unable to catch all threats. At times we may have unethical contractors or employees in our building looking for unauthorized articles. To protect against these types of attacks, lock any sensitive information or valuable items when you leave your desk and do not leave passwords in an unsecured area. If you have any passwords written down, they must be secured. If you are leaving your computer make sure the screen is locked and password-protected. Once again, this ensures all authorized and unauthorized individuals cannot access your computer.

Your Laptop

Criminals do not always have to break into to buildings to steal information. Sometimes they can access to information via stolen laptops. If you must leave your laptop make sure it is secured. For example, always lock your laptop it in the trunk of your car if traveling. Never leave your laptop visible where criminals can easily see it and be persuaded to steal it.

What is PCI DSS?

Created by Cai Wang

PCI DSS stands for payment card industry data security standard. It is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes, including Visa, MasterCard, American Express, Discover and JCB. Others are not included in the scope of the PCI DSS. The main purpose of PCI-DSS is to protect the information used with a payment card.

PCI DSS contains six control objectives:

1)Build and maintain a secure network

2)Protect cardholder data

3)Maintain a vulnerability management program

4)Implement strong access control measures

5)Regularly monitor and test networks

6)Maintain an information security policy

The PCI DSS requirements apply to all entities involved in payment card processing, including: merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. Additionally, the PCI DSS affects all credit card acceptance channels, including retail, mail, telephone, fax and e-commerce. PCI DSS protect credit card information being from unprecedented assaults

The common processes and precautions for handling, processing, storing and transmitting credit card data established by the PCI DSS, help to combat the unprecedented assaults on personal and financial data which impact cardholders, retailers, banks, service providers and credit card companies.

For more information about PCI DSS, please visit: https://www.pcisecuritystandards.org/security_standards/

DMCA

Created by Yuan Liu

Copyright is a form of protection provided under United States law to owners of "original works of authorship." This includes literary, dramatic, musical, artistic and other creative works. Material that is not copyrighted is available for use by anyone without the author's consent. However if the work is copyrighted, the copyright holder can prevent others from copying, performing or otherwise using the work without their consent.

The Digital Millennium Copyright Act ("DMCA") of 1998 balances the interests of internet service providers and copyright owners when copyright infringement occurs in the digital environment. If the internet service provider meets certain statutory requirements the DMCA protects internet service providers from liability when users infringe upon copyrighted material.

To fall within the protection of the DMCA, an internet service provider must, among other things, take certain steps when it receives notice that infringed material resides on its network. The internet service provider must adopt and implement a policy that allows for termination in appropriate circumstances of users who are repeat infringers, while accommodating standard technical measures used by the copyright owners to identify and protect copyrighted works. The DMCA protects only the internet service provider, and not the users of its system who infringe copyrighted works.

At Loyola, we have policies and measures to prevent copyright violation. Every year in October we have cyber month, during which the Security Office will organize different kinds of security awareness activities, to spread information security awareness on campus. Also, we have a security awareness newsletter posted monthly on Inside Loyola, in addition to our blog, and posts on Facebook and Twitter. If you have a chance to read our newsletter, you will learn more about DMCA violations, and how to make sure you are not infringing upon copyrighted material.

If you receive a DMCA violation, our Security office has acknowledged a violation notice from a DMCA-Agent and has found you responsible for copyright infringement. Your internet connection will then be temporarily disabled until the following steps are completed. First you need to delete the copyrighted material, and uninstall the file-sharing program used. Second, you must complete a DMCA quiz using Sakai, and pass with 100% accuracy. After you have completed the above steps, you may send Loyola’s Information Security Office an email to DMCA-Agent@luc.edu and request your network access to be reinstated.