ISSUE: 1-3 YEAR: 2016

University Information Security Office Newsletter

"The only truly secure computer is one that is powered off, cast in a block of concrete and sealed in a lead lined room with armed guards. — Gene Spafford

Browsing Security

SANS Securing the Human

Your web browser is your primary tool for using the Internet. It is also the number one target for cyber attackers. By protecting your browser, you protect yourself against many of today's attacks.

The Internet has become a powerful tool for your daily activities. You use it to search for information, shop online, watch movies and manage your finances. In almost all of these cases, the primary tool you use is a web browser, such as Internet Explorer, Chrome or Firefox. Your browser is, in many ways, your gateway to the Internet.

Because so many people around the world use and depend on browsers for their daily Internet activities, your browser is a primary target for cyber attackers. These individuals have developed specialized hacking tools and built malicious websites designed to silently hack into your browser. Once hacked, attackers quickly gain total control of your computer and all of your information without you knowing. By protecting your browser and using it wisely, you can protect yourself against these threats and safely use the Internet for your daily activities.

Solution

You should always follow these steps to protect your browser and yourself.

Your Browser

A key step to protecting your browser is to always use its latest version. The vendor that developed your browser is constantly fixing new vulnerabilities and adding new security features to enhance its protection. By using the latest version, you ensure you have the latest security mechanisms in place. Enable automatic updating to ensure your browser is always current. This feature allows your browser to continually check for new patches. As soon as a new patch is released, your browser or operating system will download these patches and update the browser.

Avoid Plugins

Plugins, or add-ons, are additional programs you can install in your browser to give you more functionality. Common plugins include Adobe Flash, Java and Apple QuickTime. Every plugin you add becomes another window for attackers to break into your computer. In addition, it can be difficult to keep these plugins current; very few of them have auto-updating features. Install only authorized plugins you absolutely need, and always be sure you have the latest version installed. If you are no longer using a plugin, delete it from your browser.

Scan All Downloads

Scan any files you download from the Internet with updated anti-virus. When you download and install or run a new program, that program could be infected. It may appear to work just fine, but it can silently infect your computer. This is very common, especially with free files, such as free screensavers, video players or games. Be sure to scan anything you download with anti-virus before opening or running it.

Website Filtering and Protection

Browser website filtering (sometimes called Smart Screen Filtering, blacklisting or phishing protection) is a feature most browsers support. It helps protect you from visiting websites that are known to be malicious. You may not realize it, but there are security organizations that are constantly scanning the Internet and looking for any malicious websites. Whenever they find a malicious website, they add that site to their database. Most modern browsers have access to these databases. If you attempt to visit one of these websites, your browser will give you a warning. If you get one of these warnings on your browser, do not visit the website. Instead, simply close the browser tab or window. Keep in mind that this feature can only protect you against known malicious websites. It cannot protect or warn you about malicious websites no one knows about.

From the ISO's Desk

Our January Awareness topic is Browser Security. As applications become more web enabled, individuals and business perform much of their work and personal business using a web browser. Statistics show that on average, an employee spends over 21 hours a week using a web browser. According to the US Department of Homeland Security "There is an increasing threat from software attacks that take advantage of vulnerable web browsers." DHS has observed new software vulnerabilities being exploited and directed at web browsers through use of compromised or malicious websites. This problem is made worse by a number of factors, including: A tendency to click on links without considering the risks of one's actions, Web page addresses that are disguised to take you to an unexpected site, Computer systems that are bundled with additional software, increasing the number of vulnerabilities that may be attacked, browser security updates not applied, websites require that users enable certain features, or users do not know how to configure their web browsers securely. If you would like to know more about our awareness activities, please check out Inside Loyola or go to our web page: http://www.luc.edu/uiso

Jim Pardonek, Information Security Officer

Data Privacy Day
January 28, 2016

Data Privacy Day is an international holiday that occurs every January 28. The purpose of Data Privacy Day is to raise awareness and promote privacy and data protection best practices. It is currently 'celebrated' in the United States, Canada, and 27 European countries.

Data Privacy Day's educational initiative is focused on raising awareness among individuals, families, consumers and businesses about the importance of protecting the privacy of their personal information online, particularly in the context of social networking. In addition to its educational initiative, Data Privacy Day promotes events and activities that stimulate the development of technology tools that promote individual control over personally identifiable information; encourage compliance with privacy laws and regulations; and create dialogues among stakeholders interested in advancing data protection and privacy.

On January 26, 2009, the United States House of Representatives passed House Resolution HR 31 by a vote of 402–0, declaring January 28 National Data Privacy Day.

In response to the increasing levels of data breaches and the global importance of privacy and data security, the Online Trust Alliance (OTA) and dozens of global organizations embraced Data Privacy Day as Data Privacy & Protection Day, emphasizing the need to look at the long-term impact to consumers of data collection, use and protection practices.

For more information on Data Privacy and for some free tools and tip on maintaining a good privacy posture, the National Cyber Security Alliance and StaySafeOnline.org have provided a web site in support of Data Privacy Day. You can visit their site at https://www.staysafeonline.org/data-privacy-day/landing/

Stay Safe my Friends!

Avoid Bad Neighborhoods

In some ways, the Internet is a like a big city. It has everything you need, from banks and shopping centers to sporting events and movies. However, just like most big cities, the Internet has good neighborhoods and bad neighborhoods. Good neighborhoods are made up of well-known websites that are trusted. Bad neighborhoods are websites designed to attack or harm you or your computer. They do this by hacking your browser or distributing infected software, such as fake screensavers or infected games. Just like in a big city, one of the simplest ways to

stay safe is to avoid these bad neighborhoods. If you have never heard of the website, if the URL information looks incorrect or suspicious or if the website looks like it has dodgy information, then do not download any software or submit any information to it.

Loyola Aware

Our January topic is " Browser Security", which will be live on January 4th.

Please visit: http://www.luc.edu/uiso/awareness/loyola_aware.shtml for further information.

If you have any questions in regrading to Loyola Aware, please contact the data security team by email (datasecurity@luc.edu) or call x87373 (703-508-7373)

Contact Information

University Information Security Office

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