ISSUE: 10-9 YEAR: 2014

University Information Security Office Newsletter

All this modern technology just makes people try to do everything at once.

-Bill Watterson

From the ISO's Desk

October is National Cyber Security Awareness Month (NCSAM), conducted every October since 2004, this national public awareness campaign is intended to encourage everyone to protect their computers and our nation's critical cyber infrastructure. Cyber security requires vigilance 365 days per year. However, the Department of Homeland Security (DHS), the National Cyber Security Alliance (NCSA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC), the primary drivers of NCSAM, coordinate to shed a brighter light on what home users, schools, businesses and governments need to do in order to protect their computers, children, and data. As part of our program, The LUC Information Security Staff will be sending daily tweets and holding events on ways to encourage safer computing. If you would like to know more, please go to our web page https://www.luc.edu/uiso

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

Password Security

Created by Jacob Schuldt

We use passwords every day to access nearly every account on we have on the computer. For some people, this can mean memorizing (or storing) dozens of passwords. For others, this can mean having just a few similar passwords. In order to prevent your account from being compromised through password attacks and revealing all of your information to the attacker, it is suggested that you change your passwords frequently – every 30-180 days – and follow these helpful tips to have a strong and safely stored password.

Password Strength

Password security through complexity and protection is one of the easiest and fastest ways to ensure that your accounts are secure. Password complexity refers to creating a password that will not be easy to guess and having different passwords for multiple accounts. In order to have a "strong" password, many suggestions have been given to protect your accounts from hackers and malicious software. Depending on the account, passwords can, and should, contain lowercase letters, uppercase letters, numbers, and symbols. Some websites and applications will not allow the use of symbols or numbers, but it is best practice to use them when possible. In addition to having variation in characters, passwords should be at least 8 characters, but the longer the password, the better. Passwords shouldn't contain a complete word, your name, username, or the company or application's name in which you are creating the account.

If you are having trouble creating a password, there are numerous applications and websites that can help create a very complex password for you. An example is passwordsgenerator.net, which creates a password according to your requirements, and provides many other helpful tips to keep your passwords safe.

Password Storage

Some users like to store their password either in a plain text file, or on a piece of paper on their desk because memorizing many passwords can be difficult. For obvious reasons, these password storage techniques are unsafe, since they are easily accessible by others. In efforts to combat password stealing, applications like OnePassword, KeePass, and LastPass were created to manage passwords, making it where users do not have to actually remember their passwords. With these applications, an initial account is created with a password. After the initial created, you can change your settings to require multi-factor authentication to sign in, so you have to enter the password, and then choose another authenticator, such as a code that is texted to you and needed to sign in. Once the account is created, you can enter in your passwords to multiple websites and applications. Many users create a randomly generated password, enter it into the password manager application, then simply copy and paste it into the website they are trying to sign in to. The application stores the passwords and encrypts them, so that in the case your computer is compromised, the passwords will be extremely difficult, if not impossible, to obtain. From there, many of the password manager applications come with a browser add-on so your password will automatically fill-in when you go to a preconfigured site.

Memorizing lengthy and complex passwords can be a hassle, but for security reasons, these longer passwords can make every user less vulnerable to password and account hacks. Luckily, password management applications take the stress of remembering a password away, and allow users to have longer, varying passwords. Remember to always use these strong passwords for accounts, especially those with sensitive information, including billing information and social security numbers.

Browser Security

Created by Christopher Campbell

The web browser has become one of the most frequently used tools in today's computing environment. However, this makes them popular targets for web-based attacks, especially since they must interact so closely with active content in order to properly display complex web pages. Fortunately, there are a few simple precautions that can be taken as a user to improve the security of your browser(s) and make yourself a much harder target.

Firstly, it is important to look through the settings of each browser you use and make sure automatic updates are activated, and ensure you are comfortable with the level of information sites may store about you. It is also vital to verify that your connection to a website is properly secured (especially when conducting sensitive business such as online banking, shopping, or any other application where privacy is a concern). Websites implement HTTPS to accomplish this, but in order to protect your information it is important to make sure this is functioning in a secure fashion. In most major browsers, this can easily be accomplished by looking for a small lock icon in or around the address bar. Clicking this icon will inform you of whether or not the site's certificate can be trusted. If not, your connection is vulnerable and you may even be the victim of an attack in progress! Avoid the site until access is properly secured. Additionally, be wary of unknown applets attempting to run from a website (when in doubt, click no!)

There are many add-ons and services that can be used to further secure your browsing experience. Some useful security plug-ins available for most browsers include NoScript, HTTPS Everywhere, and Web of Trust. NoScript is an excellent addition that protects you by blocking active content such as JavaScript when you first visit a page. You may then choose to selectively enable any blocked functionality for this and all subsequent visits. Even if you choose to globally disable the entire script blocking feature, NoScript will still guard against many other common types of web-based attacks without any user action required. Here are some additional browser extensions to improve your security:

- HTTPS Everywhere – works with common sites in an attempt to deliver all content over a secure connection: https://www.eff.org/Https-everywhere
- Web of Trust – displays a small, colored icon to indicate the reputation of links, including whether the site may be unsafe to visit: https://www.mywot.com/
- LongURL.org – discover where shortened links (bit.ly, goo.gl, etc.) may actually redirect you: http://longurl.org/

Social Network Security

Created by Cai Wang

People use social networks to share their life with families and friends on a daily basis. Much personal information can be easily obtained through these websites, including your email address, birth date, and even your cellphone number.
Recently, some social media applications have added a function called "share your location". This "feature" not only shows where you are, but basically passes a message to anyone saying "I'm not at home".

You should avoid sharing information including travel plans, full address, birthdate, daily schedule and etc. It's great to share your experiences in "real time" but to protect your home and possessions, post your pictures when you get home.
Another way to secure your personal information is to change the privacy settings on your social media page to a proper level to control who can access your information. This is usually under settings.

Before you sign up at a website, you should read the privacy policies to make sure they do not share your information such as email address or user preferences with third-party businesses. These businesses will use that information to send you spam emails.

You should also be careful who you friend or add as a follower. They may not be who they say they are. Fake profiles can be easily created by anyone in the world. If you use chat, such as Facebook Messenger and any of your friends chat with you in an unusual way, you should double check with them to make sure they are not an imposter. Do not simply give them your personal information, because the person on the other side may not be your friend.

To protect you account against hacking you should always use strong and unique passwords and use different passwords for each account. Never click any suspicious links, these probably contain malware that will infect your computer or give someone access to your account.

Help Us Celebrate Cyber Security Awareness Month by Attending One of Our Awareness Events

Security and Donuts Sessions

- October 09, Thursday 10:00AM-11:30AM LSC Damen 214
- October 14, Thursday 10:00AM-11:30AM WTC Corboy302
- October 23, Thursday 2:00PM-3:30PM LSC Damen214