ISSUE: 4-30 YEAR: 2015

University Information Security Office Newsletter

Any sufficiently advanced technology is indistinguishable from magic.
-Arthur C. Clarke

From the ISO's Desk

Spring is in the air and with that new life is bursting out everywhere around us. As corny as that might sound for a security awareness newsletter, spring is also the time for ITS to roll out a few security improvements to a few of our important services.

In the next few weeks, we will all begin to take advantage of a new way to change our passwords which will not only make it easier for you to update your password, but you will be able to change it from virtually anywhere you have an internet connection. This service will help to eliminate the need for human intervention, decreasing the risk of fraud and impersonation and also eliminating the need to provide personal information to verify that you are who you are.
The second change will be coming soon to our VPN users. We will be retiring the old VPN and replacing it with a Loyola Secure Access application that eliminates the need to carry and install a certificate on every device that you want to use. For more information, check www.luc.edu/its

University Information Security Office

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

What is Adaptive Authentication?

Created by Chris Campbell

In the current climate of constant phishing campaigns and other (more advanced) threats, passwords are becoming less effective than ever. As a means of authentication, the password was never ideal. A password can only be as strong as it is complex, and the limitations of human memory are quickly being outpaced by raw computational power. Even with password complexity requirements becoming more stringent and popularly enforced, users tend to create the simplest password possible while still meeting the given requirements. Not only that, but many of us use the same password for as many systems as possible in an effort to reduce the burden associated with keeping track of so much information.

Two-factor authentication is simply adding a second way to verify your identity in addition to a password. Adaptive authentication is one solution that leverages user behavior and risk profiles to detect anomalous activity and decide whether to require a second level of authentication. Successful adaptive authentication mechanisms pull information from as many sources as possible when making a decision as to whether activity may be irregular. Actionable information may include a user's source IP address, location, operating system, web browser, and the time of day. Depending on what information may be accurately collected, tracked variables can be as granular as specific connection details or the amount of time it takes for the user to sign on.

Adaptive authentication is designed to improve the user experience by requiring two-factor authentication on the basis of risk. This also means that most systems can be fine-tuned to balance an organizations requirements with a predictable, hassle-free experience for the end-user. Many of us have seen options to "remember this computer", but be careful to never select this on a machine that someone else may have access to. Adaptive authentication can make life easier by allowing us to use connection characteristics as a second factor of authentication, but users of such systems should be mindful that the convenience of "remember this computer" must never be taken for granted.

Misconceptions about Information Security

Created by Yuan Liu

Information security is an increasingly important field. There are key concepts related to information security that many people understand, but also many common misconceptions. It's helpful to clear up such misconceptions, as they may mislead individuals who could make incorrect decisions or do the wrong things. Here are some common misconceptions:

"Password expiration and complexity reduces risk"
This is an example of wishful thinking. We can do more for password security. At Loyola, we require password to be changed every 180 days. All passwords for high security accounts will expire every 90 days. New passwords may not be the same as the last four passwords. Accounts will be locked out for thirty minutes after six failed login attempts. First time passwords will be set to a unique value. Passwords will be set to change immediately after first use. The IT department also suggests that employees to not use personal passwords for University systems.

"Buy this tool and it will solve all your problems"
This would be ideal, but is another form of wishful thinking. Organizations should adopt multiple plans based on risk analysis. There is no one tool that can solve all your problems. At Loyola, we have PeopleSoft Campus Solutions to manage and secure academic systems. Another example is Lawson, the tool we use for human resource and financial systems.

"The policy is in place, we are go to go"
As we all know, policy is important and necessary to standardize and restrict behaviors. However, security is not just writing things down. We need to take actions and follow best practices to eliminate risk. At Loyola, we establish strict responsibility and clear applicability. This means we need to follow the policy rather than just putting it aside.

"Encryption is the best way to keep your sensitive files safe"
Encryption is an excellent way to protect your sensitive data, but may not be enough on its own. We need to prevent data loss for situations where cryptography doesn't work. For example, we have a PII (Personally Identifiable Information) program at Loyola to scan all the PCs on campus to secure sensitive data like SSN or CCN. The fundamental way to prevent data-loss is not only to encrypt it, but also to save it in a secure place so that the risk will be reduced.

"It won't happen to me"
This is also wishful thinking. When people realize there is a problem, they need to do something to solve it. This may be time-consuming or expensive. However, assuming that something won't happen has nothing to do with solving problems. We need to be aware of security risks and take active measures to protect security information. We also need effective solutions when security problems do arise.

Mobile Phone Security Tips

Created by Jacob Schuldt

Mobile phones have grown to become the most common form of communication, holding large amounts of personal information and access to various accounts. It was once thought that mobile phones were not susceptible to viruses and hacks, but as time goes on, these attacks are becoming much more common. Because of this, as well as the increasing amount of information being stored on our cell phones, phone security is becoming much more important. Here are some helpful tips to protect your phone from viruses, data loss, and other malicious activities (such as those resulting from losing your phone):

Set a password, PIN, or pass-pattern to enter your phone.
This is similar to settings on a computer and is a simple step to prevent unwanted users from entering your phone and accessing data. Remember, the longer the password, the better.

Use one of the various phone finding applications.
These applications allow you to find your phone in the case of it being lost or stolen, by accessing GPS, the camera, ringer, and other phone features.

Install an anti-virus application.
Although it is debated whether anti-virus are needed on phones, attackers and their tools are becoming more sophisticated. An application such as Malwarebytes can protect your device, and show you what information on your phone apps have access to.

Use cellular connection (3G/4G)
When accessing any type of sensitive information, such as banking or accounts with personally identifiable information (PII), you can eliminate the security risk when accessing this information from a public place, or where there are Wi-Fi networks that are untrusted. Fraudulent Wi-Fi networks can be set-up in public spaces, and can literally steal your information out of thin air.

Check your privacy settings
When installing a new application, or when reviewing currently installed apps, check the privacy settings. Some applications access a lot of personal information when there might be no need. If the application is not necessary, consider uninstalling the app and finding another one that does not require so much information to be accessed.

Following these tips, along with basic computer security practices when using e-mail and web browsing significantly lowers the chances of having information stolen or your phone being infected. For additional tips on mobile security, check out various tech sites, such as Microsoft's website, Consumer Reports, and TechRadar.