ISSUE: 7-15 YEAR: 2015

University Information Security Office Newsletter

It used to be expensive to make things public and cheap to make them private. Now it's expensive to make things private and cheap to make them public.

— Clay Shirky

From the ISO's Desk

During the summer months, many of us take extra precautions to protect our skin from too much sun and to keep ourselves from being bitten by our regional bird of prey, the mosquito. So why not take a minute to make sure we are protecting our cyber life this summer. As our foes in cyberspace become more sophisticated we need to take the extra care of keeping our anti-virus up to date. Not only on our computers, but on our smartphones and tablets. As these smaller devices are being used in increasing numbers, criminals see this space as another opportunity to steal your personal information. We should also look for ways to configure our computers so that they information on them is harder to get if stolen. Lastly, just like we look for warning signs of severe weather, we should learn to look for warning signs in email messages to make sure we are not giving our personal information over to the criminals by sending emails that appear to be legitimate. Have a wonderful summer.

— Jim Pardonek

University Information Security Office

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

Who Needs Anti-Virus ?

Created by Fanqi Meng

Overview

Antivirus or anti-virus software (often abbreviated as AV), sometimes known as anti-malware software, is computer software used to prevent, detect and remove malicious software.

Using your computer without anti – virus software is like leaving your door wide open.

Antivirus software is one of the most important tools in protecting your computer and personal information from viruses and worms. When it comes to technology and security, computers are quite similar to houses. Most people would not leave their doors and windows wide open, exposing their residences to complete strangers. Yet, why are computers often left open and unsecured, virtually welcoming viruses to sneak in the front door or window?

As a Loyola University Chicago student or faculty or staff member, acquiring and using antivirus software to secure your computer is as easy as locking a door, all at no cost to you. ITS provides recommended antivirus software for both university-owned and personal systems. While ITS does recommend specific antivirus software packages, other antivirus programs are also acceptable. Read more about antivirus here: http://luc.edu/uiso/resources/antivirus.shtml

Common Signs of being infected by a virus

- Your computer seems to be displaying an inability to start (boot up) or taking longer than normal to start up
- Your system shuts down spontaneously and frequently, even if you don't use it
- Your hard disk fills up and you can't find the files that use up all the disk space
- Your virus scanner crashes and cannot be started again
- Your Internet connection slows to a crawl even while you are not doing anything significant
- Your computer is exhibiting unpredictable program behavior

Update your Antivirus Regularly

Remember, your virus protection is only as effective as its last update. New viruses appear all the time (industry experts estimate that there are currently more than 50,000 viruses in existence and approximately 200 discovered each month). If your antivirus software isn't current, the latest viruses or worms can sneak in. Thus, updating antivirus scanner definitions is a crucial part of keeping your computer safe from viruses and worms. This process will keep your scanner up-to-date, so it will be able to detect the most recent virus or worm. Antivirus automatically checks for antivirus engine updates when virus definitions are updated. It's recommended you update your software at least once a month.

Policy:

Use of antivirus software - All computers using the Loyola network may be required to use antivirus software depending on their operating system. If a computer is required to use antivirus software, that software must be configured to automatically install updates to both the antivirus software and the virus definitions. Failure to use appropriately configured antivirus software may result in loss of access to the Loyola network. Read more about antivirus policy here: http://luc.edu/its/itspoliciesguidelines/antivirus_policy_.shtml

Hardening Your Computer

Created by Chris Campbell

While hardening a computer may be a foreign concept to the vast majority of users, many of us take actions that fall under this category without even realizing it. One of the easiest (and most essential) best practices to follow is always choosing to automatically download and apply updates to your operating system, as well as any programs that support automatic updates. You should also have an anti-virus program running to protect your computer at all times.

Full-disk encryption is often overlooked, but is packaged with most modern operating systems and has become quite easy to implement (BitLocker on Windows and FileVault on Mac). Such measures may seem like overkill, but it is a trivial matter for an attacker with physical access and no knowledge of your password to read all of your information from an unencrypted device.

Passwords are quickly becoming outdated as a form of authentication, but most workstations leave users with no readily-available alternative. As a best practice for hardening your devices, we recommend using passwords of no less than twelve characters that draw from as many character sets as possible (such as special characters/punctuation, numbers, and upper and lowercase letters). Many users avoid creating strong passwords because they are so difficult to memorize. Others keep plain text records of all their passwords, which must be avoided at all costs. Consider using a password manager to store strong passwords and keep all of your account information safely encrypted. Many of these programs are even able to enter your login information for you! Read more about password managers here: http://luc.edu/uiso/resources/passwordmanagers.shtml

Social Engineering

Created by Andrew Unger

What is social engineering? Social engineering is a type of psychological attack where an attacker misleads you into doing something they want you to do. While the idea of scamming or conning someone is not new, cyber attackers target millions of people on the internet using this technique.

Some common indicators of a social engineering attack include:

1. Someone creating a tremendous sense of urgency. If you feel like you are under pressure to make a very quick decision, be suspicious.
2. Someone asking for information they should not have access to or should already know.
3. Something is too good to be true. A common example is you are notified you won the lottery, even though you never even entered it.

Fortunately, there are precautions you can take to help prevent exposing yourself to social engineering attacks.

1. Never share you passwords: No organization will ever contact you and ask for your password. If someone does ask you for your password, it is most likely an attack.
2. Don't share too much: The more an attacker knows about you, the easier it is for them to find and mislead you into doing what they want. The less you share publicly on social media sites, product reviews, and public forums and mail list all reduce the risk of you being attacked.

3. Verify contacts: At time you may be called by your bank, credit card company, mobile service provider, or other organization for legitimate reasons. If you have any doubt as to whether a request for information is legitimate, ask the person for their name and extension number. Though it may seem like a hassle, protecting your identity and personal information is worth the additional step.