ISSUE: 3-2 YEAR: 2016

University Information Security Office Newsletter

Treat your password like your toothbrush.. Don't let anybody else use it, and get a new one every six months.

-Clifford Stoll

Passwords

SANS Securing the Human

Once someone knows your password, they can steal your identity or access all of your personal information. Let's learn what makes a good password and how to use them securely. There are two key points to good passwords:

- First, you want passwords that are hard to guess. This means do not use simple passwords such as 123456, your pet's name or your birth date.
- Second, use passwords that are easy to remember. If you keep forgetting your passwords, they are not very helpful.

The problem is cyber attackers have developed sophisticated programs that can guess, or brute force, your passwords, and they are constantly getting better at it. This means they can break into your accounts if your passwords are weak. To protect yourself, you want your password to be as long as possible. The longer your password is, the stronger it is. In fact, instead of using just a single word as your password, use multiple words. This is called a passphrase. For example, your passphrase could be something simple like:

Where Is My Coffee?

To make your passphrase even more secure, consider doing the following:

- Use a number in your passphrase.
- Have at least one lowercase and one uppercase letter in your passphrase.
- Use a symbol in your passphrase.

For example, you can replace the letter 'o' with the number zero or the letter 'e' with the number three. In addition, you are using symbols when you use common punctuation such as spaces, a question mark or an exclamation point. As a result, you can have a strong password that is very difficult for cyber criminals to compromise, yet is simple to remember and easy to type. In addition to strong passwords, you must protect how you use them:

- Be sure to use different passwords for different accounts. For example, never use the passwords for your work or bank accounts for your personal accounts, such as Facebook, YouTube or Twitter. This way, if one of your passwords is hacked, the other accounts are still safe. Never share your password with anyone else, including fellow coworkers. Remember, your password is a secret; it is no longer secure if anyone else knows it.
- Do not use public computers, such as those at hotels or libraries, to log into a work or bank account. Since anyone can use these computers, they may be infected with malicious code that captures all of your keystrokes. Only log into your work or bank accounts on trusted computers or mobile devices you control.
- If you accidently share your password with someone else, or believe your password may have been compromised or stolen, be sure to change it immediately.
- Be careful of websites that require you to answer personal questions. These questions are used if you forget your password and need to reset it. The problem is the answers to these questions can often be found on the Internet or your Facebook page. Make sure that you use only information that is not publicly known if you answer personal questions.
- Many online accounts offer something called two-factor authentication, or two-step verification. This is where you need more than just your password to log in, such as codes sent to your smartphone. When possible, always use these stronger methods for authentication.
- Finally, if you are no longer using an account, be sure to disable or delete it.

From the ISO's Desk

Our March Awareness topic is Password Security. Passwords are the keys to your kingdom. You must use them wisely. In this newsletter, we discuss how to create strong passwords that cyber attackers cannot easily guess and cover how to use them securely .This newsletter is full of tips and tricks to help you create and remember complex passwords. The video in Loyola Aware, will tell you how to create secure passwords as well as show you how hackers can get your information.

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

Safe Computing to you all!

The 25 Most Popular Passwords of 2015

Created by Yuan Liu

Good passwords are a balance between security and convenience. If a password is too complex you tend to forget it. Too easy and your accounts can be compromised. Let's take a look at the most common passwords of 2015 and think about how to be even more secure in 2016.

Here is the list of 2015 worst passwords from Splash Data: (Changes from 2014)

1. 123456 (Unchanged)
2. password (Unchanged)
3. 12345678 (4)
4. qwerty (5)
5. 12345 (3)
6. 123456789 (Unchanged)
7. football (10)
8. 1234 (7)
9. 1234567 (11)
10. baseball (8)
11. welcome (New)
12. 1234567890 (New)
13. abc123 (14)
14. 111111 (15)
15. 1qaz2wsx (New)
16. dragon (9)
17. master (19)
18. monkey (12)
19. letmein (13)
20. login (New)
21. princess (New)
22. qwertyuiop (New)
23. solo (New)
24. passw0rd (New)
25. starwars (New)

Security professionals recommend using strong passwords with a combination of upper-case characters, lower-case characters, numbers, and symbols.

More tips to help you set up passwords wisely:

1. Use passwords with twelve characters or more and mixed types of characters. Avoid common information like your name, date of birth, or phone number.
2. Don't share your password with others or write them on post-it notes.
3. Don't use the same password for all your systems.
4. Use a password manager to protect passwords.
5. Change passwords frequently.

Password Managers

One of the key points we covered in this newsletter was using a different, unique password for each of your accounts. This way, if one account is compromised, your other accounts are still secure. However, you may have so many accounts you cannot remember all their passwords. If that is the case, consider using a password manager. This is a special program you run on your computer that securely stores all of your passwords for you. The only passwords you need to remember are the ones to your computer and your password manager program. Some password managers even integrate with your browser, logging into websites for you. Check with your supervisor, the help desk or the information security team to see if a password manager is an option you can use.

Loyola Aware

Our March awareness topic is “ Password Security”, which will be live on March 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
Some Material © SANS Institute 2015