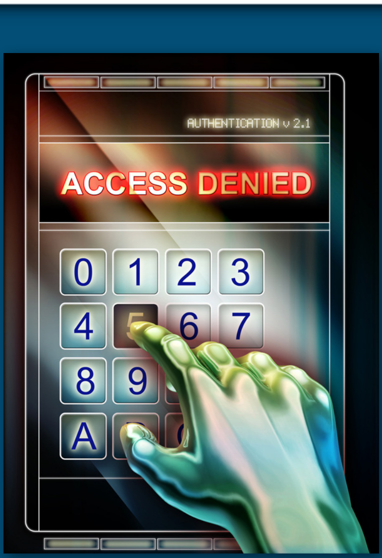
CYBER SECURITY NEWSLETTER

PASSWORDS

Passwords are the keys to the kingdom. 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.



Passwords

Passwords are the keys to your kingdom; you must use them wisely. In this newsletter we discuss how to create strong passwords that bad guys cannot easily guess and how to use them securely.

The problem is cyber criminals have developed sophisticated programs that can guess (or brute force) your passwords, and they are constantly getting better at it. This means that they can break into your accounts if your passwords are not strong enough. 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:

time for chocolate

To make your passphrase even more secure, do the following:

- Use a number in your passphrase.
- Have at least one lower case and one upper case letter in your passphrase.
- Use a symbol in your passphrase.

This newsletter is published by St. Luke's IT Security.

For more information or to report an IT Security incident, please contact the St. Luke's Cyber Security Incident Response Team (CSIRT) at csirt@slhs.org

Let’s take our passphrase and make it even more secure by replacing some of the letters with numbers and symbols, as we just discussed. First, replace the first letter with a capital letter. Next, we can replace letters with numbers or symbols. For example, you can replace the letter ‘a’ with the ‘@’ symbol or replace the letter ‘o’ with the number zero. In addition, we can add symbols using common punctuation such as spaces, a question mark or an exclamation point. As a result, we now have a strong password that is very difficult for cyber criminals to compromise, yet is simple to remember and easy to type:

Time for ch0c0l@te!

Using Passwords Securely

In addition to creating strong passwords you must also use them securely. A strong password is of little use if the bad guys can easily steal it from you.

- Never share your password with anyone else, including fellow employees. Remember, your password is a secret; if anyone else knows your password it is no longer secure.
- 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 even your Facebook page. Make sure that if you answer personal questions you use only information that is not publicly known.
- 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.

Different Passwords for Different Accounts

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.

If you have too many passwords to remember, 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 the password manager program. Check with your supervisor, the help desk or the information security team to see if a password manager is an option you can use.