Cyber Security Awareness

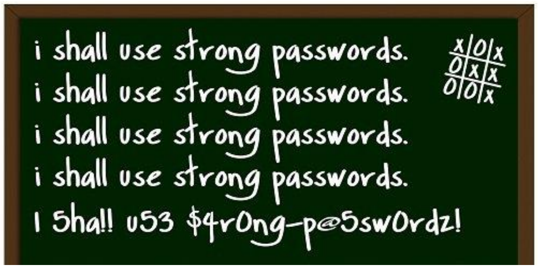
SLC CYBER Security: timely information, you need to know …

You may be thinking you have a **strong password** and you're probably right! Most credible websites have stringent password policies to ensure the safety of their users and their user's private information. Most people can remember around five or six passwords at a time. We tend to reuse these passwords between different services often taking on numbers or characters at the end, or in the middle. However, in today's technological world new ways of password exposure are created daily - from key board copiers to viruses. Brute force hacking devices can test millions of combinations based off of your profile information and dictionary words and each of these devices cause challenges in protecting your personal information. Technology is constantly evolving and IT departments everywhere try their best to keep your information safe – but, holes open up with every update. These holes if found can cause exposure effecting an entire database and millions of accounts.

Here at SLC we want to keep you safe so check out our Top 10 do's and don'ts for your password protection.

CYBER Security: password protection tips

1. **Try using a Passphrase!** A Passphrase is a series of characters that are separated by spaces. These phrases can be random and don't need to be grammatically correct. Using a Passphrase will increase the complexity of the password by increasing the number of variables. Here are a couple examples of Passphrases to get you started:
   "SLC_IS_THE_COOL"
   "APPL3_D1SHW4SH3R_TR33"
   "PrOuD_2_B_SLC"
2. **Creativity is key!** Be creative and avoid dictionary words as hackers see


i shall use strong passwords.
i shall use strong passwords.
i shall use strong passwords.
i shall use strong passwords.
I Sha!! u53 $4r0ng-p@5sw0rdz!
X O X
O X X
O O X

them as low hanging fruit. Using words outside of the dictionary as well as abbreviations such as “grt” (short for great). This creativity will take the target off you and decrease the chance of you falling prey to a brute force attack.

3. **Change your Password!** Passwords should be changed every 30 days, changing your password will extend the amount of time it takes for a hacker to get access to your account by forcing them to re-attempt all previous guesses. By changing your password every thirty days you also make passwords and personal information that has been breached safe again, causing the old information to be obsolete. Change up the characters, using uppercase and lowercase, numbers and special characters. This will increase the number of variables making your password more unique and keeping you safe from malicious attempts on your personal information.
4. **Use dual authentication when possible!** Dual authentication is when you use a secondary device to unlock you account. There are plenty of third-party sites such as “Lastpass” that are developed to manage and protect your passwords. These sites act as a search engine plug-in and allow the user to randomly generate passwords and set dual authentication criteria that are then stored in your browser.

CYBER Security: remember – do not …

1. **Don’t repeat characters** (222, iii)
2. **Don’t Share your password!** This may seem like a pretty straight forward concept but you would be amazed by how many people fall prey to this simple mistake. Imagine giving a copy of your house key to a friend, yes you may trust them but what happens if they lose it or leave it somewhere that can be stolen? This would expose your house to potential break-ins! Treat your password as you would your house key and don’t let your computer be the next victim of a “Break and Enter”.
3. **Don’t use the same password for multiple sites**. Using the same password for multiple sites is like having several copies of a master key to all your personal belongings. By diversifying your password bank, you decrease exposure when a password is breached or corrupted. One tactic hacker’s use is targeting sites with less credibility to try and find passwords. They can then use these passwords and test them against personal information and passwords on multiple accounts such as Facebook, Instagram or Linked-in.

4. **Don’t use personal information in selecting passwords.** This information can be manipulated and hackers can try and guess your password such as adding generic symbols, numbers and words! Try to make your passwords irrelevant and random - increasing the number of potential password combinations.

5. **Don’t leave your device unattended and unlocked!** By walking away from your unlocked screen(s), is like walking away with your car still running. Leaving your device unattended can leave you prey to tampering. Tools such as “keystroke copying devices” can be downloaded or plugged into your device and someone could begin tracking your every move. Get in the habit of logging off when you leave your screen --- *every time!*

Now that you’re an expert in password protection… SHOUT OUT TO US! Let us know your top five password protection tips by tweeting us or mentioning us on FB!

For more topics on e-security click here.

Got a great idea for next months’ **SLC CYBER Security –** timely information, you need to know? Share it! Let us know here or tweet us using #SLCE-security.