Security Awareness

San Diego State University

Leadership Starts Here

February 08, 2016

Passwords are sometimes the single key to accessing our computer accounts. With knowledge of our password, a hacker can read our email, impersonate us on Facebook, LinkedIn or Twitter, and make fraudulent purchases with our credit card on Amazon or PayPal.

To make it harder for hackers to crack passwords, they should be at least ten characters long and contain three of the following four character sets: uppercase letter (A-Z), lowercase letter (a-z), number (0-9) and symbol (!@#$%^&*-+?).

One good approach to creating secure passwords is to take a phrase of four or five random words, like "correct horse battery staple", and then modify it to meet the password complexity requirements:

correctHorsebattery$taple

The resulting ***password phrase*** is 25 characters long and uses three character sets. It would take a hacker over **135,554,903,739,926,000,000 days** to brute force this password, and it is easy to remember and easy to type on a keyboard.

With the power of a computer sold at Costco or BestBuy, it would take over 2000 days to crack every complex 10-character password. SDSU users can be comfortable changing their passwords every 180 days or six months without concern that their password will be cracked. Alternatively, it takes less than a day to crack every 8-character password with current computers.

Avoid using personal names, birthdates, places and dictionary words to create a password, such as: Maryanne10, birthdayJan2, work@Oggies

Once you have created a secure password, it is important that you **do not re-use this password**! Studies indicate that 92% of people re-use their passwords. If your email, Twitter, Facebook and LinkedIn password are all the same, a hacker only needs to hack ***one*** of these websites to have access to ***all*** of your accounts.

Jeff Luhnow, current General Manager of the Houston Astros, reused a password he had with the Cardinals when he went to work for the Astros. The Cardinals were able to use his old Cardinal password to login and gain access to important player information in the Astros database.

Luckily, there is free or inexpensive password management software available to help us create and retrieve passwords. LastPass is one software solution that creates, saves and automatically fills in passwords we enter into our browser. You could have a 99-character password for an account and never have to remember the password or type it in!

When selecting a password management software, like LastPass, be sure it offers the best encryption and hashing algorithms to date and that it encrypts all passwords stored in the software. You need only remember one ***master password*** to unlock LastPass and have it fill in your username and password for other accounts. Make sure to use a very strong ***master password*** (12 characters or more).

PC Magazine recently released a list of the best password management software for 2015:
http://www.pcmag.com/article2/0,2817,2407168,00.asp

Internet accounts (such as Facebook, Google, Twitter, Amazon) that can be accessed from anywhere in the world, are currently subject to over 3000 attacks per second. We should use Two-Factor Authentication to protect our accounts from these attacks. Two-Factor means a "factor" in addition to using a username and password.

A common two-factor is sending a text message with a passcode to the user's cell phone during login. It works like this: a user types in their username and password for an account, a passcode is then sent to their phone, the user receives the passcode and then completes their login by typing in the passcode.

Image Credit: hubspot.net

Two-Factor login makes it harder for a hacker to access an account, as the hacker must know or guess the username/password and must also have the passcode from the user's phone (something in the user's possession). Activate Two-Factor login on every account that offers it!

Never store a list of passwords in a file saved on your computer, mobile device or phone.

Another way to manage passwords is to write them down. You can purchase an "Internet and Password Logbook" from Peter Pauper Press for less than $10 at your local bookstore, including the SDSU bookstore. Coincidentally it comes in black or red!

Here's a link to a simple booklet you can also print and share for free:
http://security.sdsu.edu/iso/pdfs/passbook.pdf

Be sure to store your password booklet in a secure location, like a locked drawer or cabinet.