President's Corner: July, 2015
Password Security
By Eric Moore

At the July 2015 general meeting of CUGG, I will give a presentation on the topic of password security. Understanding how to secure your financial, email, and other accounts from criminals is always a timely topic. This article is written to complement the presentation for those who are unable to attend. I cover many of the basics that all users should be aware of, but these are not intended to be exhaustive. An Internet search for "creating strong passwords" will lead you to various additional sources of information with recommendations for you to consider in creating secure passwords.

Personal Information

The first cardinal rule of password security is not to use personally identifiable information in creating a password. Using "social engineering," hackers can easily guess such passwords if they know enough about you and the people you know. A crafty hacker can find ways to tease out details about you directly from information you provide about yourself on a personal website, in email messages, and on social media sites. They may also be able to gain such information from people you know as well as public records, newspapers, and news broadcasts. As a rule no password of yours should contain any of the following:

- Your first, middle, or last name
- Nicknames
- Names of your relatives, friends, or pets
- The name of your employer
- Your occupation
- Significant dates such as birth dates and anniversaries
- Street addresses
- Phone numbers
- Hobbies, sports, or interests
- Favorite books, TV shows, movies, or celebrities

Avoid Weak Passwords

Hackers know about various "weak" passwords and will use by trial and error to try to crack into your the accounts. The following is not a complete list. You may learn more about the most commonly used weak passwords by searching the Internet for "worst passwords." Among the common types that you should avoid are:

- Dictionary words (spelled forwards or backwards)
- Foreign words
- The word "password" or "drowssap" ("password" spelled backwards)
- Alphabetic sequences such as "abcdefgh"

- Numeric sequences such as “12345678”
- Combinations letter and number sequences, such as abcd1234
- Names of common sports such as “baseball,” “football,” and “golf”
- Names of celebrities
- Names of well-known fictional characters such as “batman”
- Dictionary words (see the first bullet point in this list) with common character substitutions such as "@" for "a", "3" for "E", and “1” for lower case “L”
- Password suggestions you read about in published words

An important note to make about the last bullet point is that hackers do collect long lists of commonly used weak passwords. They will also include suggested passwords found in online articles (including this one), as well as books and magazines. Such examples are to be considered illustrations and nothing more.

Aim for Complexity

In addition to not using information about yourself or weak passwords, you should aim for complexity (sometimes referred by the technical term of “entropy”). This guards against “brute-force” hacks, where a program is used to iteratively work through a list of possible passwords (one character at a time) to crack those that do not fall under the previous two categories. An example is a program that tests all possible eight-character lower-case alphabetic passwords such as “aaaaaaaa,” “aaaaaaab,” “aaaaaaac,” etc. The following are the minimum recommendations to aim for when creating a password:

- The longer the better—twelve character are better than eight; sixteen are better than twelve
- Use a mix of upper case, lower case, numbers, punctuation, and other symbols
- Popular symbol substitutions are fine, as long as they are incorporated in long, complex passwords (see previous section of this article)
- Use for your own idiosyncratic symbol substitutions, such as "8" for "h"
- Introduce extra characters, such as punctuation symbols to obfuscate dictionary words in a phrase (see next section of this article)

Tips for Easy Memorization

When creating a long, complex password, there are many possibilities to consider. The following are just a few:

- Meaningful or whimsical phrases only you would know, such as “Cl@mBake$AreBest!” (17 characters)
- A before & after phrase, such as “Shuffl3OffToBuffaloB!lls” (24 characters)
- Abbreviations, such as “Mik3$bday12,Dec” for “Mike's birthday is the 12th of December”

If you need to write down a password or save it to a USB drive, keep it locked away when not needed. If you use a program such as RoboForm or LastPass, be certain to use a strong password for the master

password, as well as strong passwords for your individual accounts.

Other Recommendations

A few last recommendations to consider are:

- If you suspect a password has been hacked, change it as soon as possible
- Use a unique password for every account
- If possible, do not use your name or a publicly known email address for the login name; make up a strong login name
- Use absurd or fantastic answers for security questions, such as "Nasturtium" for your mother's maiden name or “Tom Selleck” for the name of your maid of honor
- Take advantage of two-step authentication when offered, such as providing an answer to a security question, or requiring you to enter a one-time code that is emailed or texted to you upon logging into a site
- If a web site limits your choice of characters, say only allowing you to use numbers and letters, be certain to make your password as long as possible
- Beware of phishing—don't click on links in emails—as you could be fooled into providing your login information to a fake website
- Beware of misspelling the address of a website, as misspellings could also take you to fake websites
- Never give away your password to anyone, not even someone who is (or claims to be) your relative or friend, financial institution, ISP, or other service provider
- Test the strength of a password at a site such as Gibson Research, How Secure Is My Password, and The Password Meter.