CONSUMER ADVISORY

September 2014 By Attorney General Tom Miller

How to Hinder Hackers? Protect Your Password!

Tips to better secure your computer and online accounts

Someone walks into a bank and says he'd like to withdraw all the money from your account. The teller says, "What's the password?" The guy doesn't know, but he guesses. "Um, it's 123456." The teller hands him the money and he leaves.

While that scenario may seem absurd, in many cases cyber criminals, with little effort, can access bank accounts, credit card accounts, financial and personal information with little effort when they hack into computers or online accounts. And, according to a report by security application provider SplashData, the most common password people used in 2013 was "123456." In second place: "password."

Your password can be the key to the lock that either stops someone from opening the gateway to your personal information, or it allows them right in. And, when using the same password for many accounts and a hacker learns that password, you've just handed someone the master key.

Passwords

Strong passwords, and passwords that are unique to each account, provide better protection from hackers and malicious software.

- Create a password that is unique to each account.
- Passwords should contain at least eight characters (the longer the password, the more secure). They should contain upper case letters, lower case letters, numbers, and non-alphabet symbols. For example, if you owned a cat named Tiger, "Tiger1" would be a weak password. "*McTh9L@H!" would be a much stronger password (short for "My cat Tiger has nine lives at home").
- Don't use plain words you'd find in the dictionary, common names or names of family members, pet names, or favorite things like sports teams or hobbies.
- Make sure that when you change passwords, the new ones are completely different from the old ones.
- Don't write down your passwords and store them at your computer or stick them to your monitor. Store them in a safe place.
- Use a secure password manager. Password managers allow you to create and store highly secure passwords, and you only need to remember one password.

Phishing

Phishing occurs when a fraudulent email, website or phone call, convinces a user to divulge personal information. For example, a user receives an email "alert" that they need to confirm account information. The user clicks on a link and enters the personal information on a website that looks legitimate, but is not.

Don't click on any links included in an unsolicited email that claims it's urgent and you must confirm or provide personal financial or account information. (Anytime you submit personal information on a website, make sure it's a secure website with an address that begins with **https://**. The "s" means it's secure.) Don't email personal information unless it's encrypted. If you have any question about the legitimacy of an email, find contact information on a previous statement or invoice, or a known website through a known search engine, and call to confirm.

Use Updated Security Software

Updated security software is one of your best defenses against cyber-attacks, including computer viruses and malware, and phishing scams. Use security software that automatically updates itself. Several companies offer subscription-based security suites, and there are programs available for free that will help protect you against online threats including viruses, malware and spyware.