Have You Been Pwned?

Secrets to effective password protection

Now that I have your attention, let's discuss some topics related to the safety of internet information and cybersecurity. The term "pwn" means to compromise or take control of another computer or application. The website www.haveibeenpwned.com hosts a collection of data derived from the numerous breaches of websites such as LinkedIn, Target and Yahoo. Those breaches usually involve a theft of user names, emails, passwords and sometimes additional information. If you visit that website and enter your personal information into the blanks, the site will tell you whether that information has ever been stolen from a website you may have used or registered on. If your info has ever been obtained in a breach, you can bet it's for sale for pennies on the dark internet.

We all have a tendency to reuse the same password, and you can immediately conclude that the hacked information included your login information that someone can now use to attempt a login to other sites at which you used the same credentials. Analysts are now debating "password fatigue." That refers to human behavior that results when we are told to revise frequently our passwords and to make them more complex. An ordinary reaction is to vary one letter or another or add another letter to respond to the cautionary or mandatory prompt. Hackers know that would be an ordinary human response and will exploit it.

The secret to an effective password is probably not so much its complexity as its length. Using dictionary passwords is no solution. Hackers can crack those within minutes, even seconds. Steve Gibson's website contains substantial information about cybersecurity and password perfection. Test the strength of your favorite passwords by visiting www.grc.com/haystack.htm. If you add a few additional characters to your regular passwords, you can observe the rapid escalation of their strength.

The federal government's National Institute of Standards and Technology (NIST) regularly publishes studies and papers on issues of computer security. It is presently involved in a lively discussion of the use of passphrases rather than passwords. A passphrase is simply a series of dictionary words that is easily remembered. You wouldn't want to use a particular known quotation, but you can easily concoct a phrase that has no relation to reality. For instance, "whenIgrowupIwanttobeanastronaut." Enter that passphrase into Gibson's Haystack and observe the estimate that even a massive attack might take several hundred thousand trillion centuries to break it. Obviously the passphrase should not reflect components readily available to visitors to your Facebook page or your LinkedIn profile. However, it's easy to construct an easily remembered but thoroughly fictitious passphrase.

> "If your info has ever been obtained in a breach, you can bet it's for sale for pennies on the dark internet."

When developing a security strategy, consider revising your answers to security questions. You might be surprised by how much information about you is already available on the internet. You may not have posted it, but your friends or family members may have. Some good advice is to create answers that are not only false but absurd. For instance, I was born in Kiev, my mother's maiden name was Hubert Humphrey, or my high school was P.S. 92101. And certainly consider two-factor authentication that requires not only login credentials but the entry of a security code sent to your mobile device.

There is a highly recommended solution to optimal password management: the utilization of a "password manager" such as LastPass or OnePass. After establishing an account, using it is simple. You merely log into the password manager and then launch any website you might want to visit or log onto. You have to create a master password and remember it, but after that you can utilize incredibly complex passwords that the manager will generate for you and remember in its vault.

We all regularly use mobile devices for personal and client purposes. Those devices may automatically log onto unsecured public Wi-Fi networks. The only true way to protect the confidentiality of your personal or client information is to use a virtual private network (VPN). Some are free such as TunnelBear, and some are more robust and require an annual or lifetime subscription. All valid VPNs will protect the confidentiality of your banking or client information when utilizing the public Wi-Fi networks typically found at Starbucks, airports and hotels.

None of these are perfect solutions, but a combination will go a long way toward protecting our personal information and the confidential information of our clients. Trust me, without assistance, we cannot outsmart the criminals and hackers.

Bill Kammer (wkammer@swsslaw.com) is a partner with Solomon Ward Seidenwurm & Smith, LLP.