ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Password Management and TFA

Technology, Privacy, and eCommerce

We've recently heard about security breaches impacting Yahoo, Google, Apple, and other companies. Many such breaches disclose login information, including usernames and passwords. For corporate counsel, avoiding these and similar situations is important, not only because their personal security may be jeopardized, but also because they have an obligation to keep their clients' confidential information safe.

I have touched upon security issues before, but I want to provide more detailed advice on password management and the use of Two Factor Authentication (TFA).

As the breaches mentioned above indicate, passwords can be compromised at no fault of the user. If an ISP, cloud service, or another provider gets hacked, your login information could be among the casualties. In addition, some hackers may use "brute force attacks" to access individual user accounts by trial and error, manipulating computers to generate enormous numbers of random character combinations. As a result, until we implement more secure access methods, you should assume that some of your login information will periodically be stolen.

Hackers know that most people are unskilled or lazy — utilizing the same or similar login information for all of their accounts. That's why stealing the key to a "linen closet" may also give them the keys to the "master bedroom."

Hackers also know that many people rarely change their passwords, even after they learn about a breach that may affect them. In fact, some hackers will wait months or even years after a breach before using the login information they've obtained, to lull users into a false sense of security.

This has several implications. First, you should always use unique login information for any important account. I know that passwords in general are a pain — to come up with, to remember, and to input. However, you should have very different, and very strong, passwords for any sites involving you or your clients' confidential data.

You should also change these more critical passwords regularly. I know several US-based lawyers who change every important password whenever daylight savings time occurs. I recommend changing your passwords at least once or twice a year, and always immediately after one of your critical sites has reportedly been hacked.

Third, use complex passwords with at least 10 to 12 characters that contain a random combination of letters, numbers, and special characters. A decade ago, it may have been okay to use your dog's name followed by its birthday, but modern brute force attack algorithms prioritize the combinations many people use because they are easier to remember.

To make this more straightforward, you should invest in a good password manager. These will (1) keep your passwords secure through strong encryption; (2) generate long, complex passwords; (3) automatically and appropriately fill in your login and user information; (4) handle TFA (see below); and (5) allow you to do an audit of your passwords to see which are too simple or too old.

TFA is a method of confirming a user's claimed identity by requiring a combination of two different unique identifiers (i.e., requiring a PIN in addition to an access card). In most cases today, that second "factor" is simply a special code sent via text to a user's mobile phone whenever a login attempt is made through a device not previously authorized. In response, a hacker would not only have to have the user's name and password, but also their mobile phone. My guess is that pretty soon, TFA will become so commonplace that lawyers who don't use it will be considered negligent.

A final word about security questions, which are another form of TFA. The answers to many common security questions (e.g., what high school did you attend, what is the name of your favorite pet, etc.) are now available on Facebook or through Google searches. Pick random answers to those questions and store them in your password manager.

From a cyber perspective, we live in a dangerous world. While nothing except internet abstinence can guarantee your security, there are some relatively simple things you can do to greatly improve your chances. Please do them.

And as always, feel free to contact me directly if you have any questions.

Greg Stern

Former Global Integration Counsel

Chubb, Independent Consultant