What's Old is New Again: Passwords and Multi-Factor Authentication

by Sharon D. Nelson, Esq. and John W. Simek

Introduction

It has been years since we talked about passwords in this column. While passwords seem a bit old school, they are still what most people, including lawyers, use to gain access to protected networks and data. As Verizon's *2018 Data Breach Investigations Report* noted, "Eighty-one percent of hacking-related breaches leveraged stolen and/or weak passwords." Clearly, passwords are not serving law firm security well. Recently, we have seen multi-factor authentication (MFA) adopted more widely, but at a tortoise pace.

Based on the questions we get from audiences at CLES, there is now a fairly burning interest in upping security in law firms – and that's a very good thing. Let's start at the beginning with concepts that are sure to be new to some readers.

Fair warning: This is a good time to get a cup of strong coffee.

Multi-Factor Authentication

Multi-Factor authentication simply means a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. While it's been around for a long time, it was ignored by most small businesses as it simply added another element of complexity and possible cost.

As we note constantly, users pick convenience over security every time. But as data breaches became commonplace and the compendium of known breached passwords became enormous, it was clear that we needed a stronger way to protect our data. If you visit the "Pwned Passwords" website of Microsoft Regional Director and Most Valuable Professional awardee for Developer Security, Troy Hunt, as of August 28, 2018, there are 517,238,891 real world passwords previously exposed in data breaches. And yes, the bad guys can get to similar compendiums of real world passwords and hurl them against targeted people and companies in an attempt to get to their data.

Troy's database was introduced in August 2017 after the National Institute of Standards and Technology (NIST) released guidelines recommending that user passwords be checked against those revealed by known data breaches. This means that the "good guys" can now download the "Pwned Passwords" list and integrate it into their systems. They can now literally block the use of those compromised passwords, which is a very prudent move to make. While that's a terrific new step to be taken, most small law firms have not taken it – yet. Time to consider taking that step – and the next one would be to move to multi-factor authentication.

Simplifying Multifactor Authentication

Here's how we explain MFA to audiences. First, there is two-factor authentication, which is one form of multifactor authentication. Technically, many two-factor authentication systems are actually two-step authentication systems, but we won't quibble over the little stuff. Small law firms are indeed beginning to use two-factor authentication, especially to get access to data in the cloud – perhaps client data or perhaps the firm's CPA, payroll or banking data.

Two-factor authentication is often referred to in short as 2FA. All of us, at this point, use 2FA somewhere in our lives. One common usage is when you enter your ID/password and you are sent a code via text message or via email. You then enter the code and your login is complete. This methodology is often used when we wish to change a password – and since lawyers notoriously forget passwords and need to reset them, we're guessing most of you have been exposed to this scenario many times!

A common form of multi-factor authentication is something the user knows (a password), something the user has (a token) and something the user is (biometrics). This is known as defense in depth, adding layer upon layer of security.

Let's give you a few examples of multi-factor authentication just to make things simpler:

1. You swipe a card and enter a passcode.
2. You swipe a card and scan your finger or you use a retina scanner for biometric verification.
3. You download a Virtual Private Network client with a digital certificate and log into the VPN before you can get into the network.
4. You attach a USB hardware token to a laptop that generates a one-time passcode which you use to log into a VPN client.

There are many variations on the theme, but you get the idea.

Why Do Lawyers Resist Multi-Factor Authentication?

Lawyers dislike learning new technology – at least most of our lawyer clients do. And they fear it will cost them time. Actually, MFA doesn't have to be hard. For instance, suppose we want to log into our bank account. With our bank, we can identify our laptops and smartphones as "trusted devices." Therefore, so long as it is our device that logs into our account with the proper ID/password, nothing further is necessary. However, if we log in from an unknown device, additional verification will be required, whether it is in the form of security questions, a one-time code sent to our phone, or some other form of authentication.

The truth is, we can't even get our law firm clients to compose good passwords. What prayer do we have of getting them to accept MFA? We are actually apt to use the term 2FA because it scares them less than MFA (somehow they all seem to think this means three or more authentication factors rather than two or more). Constant prodding, and providing them with security statistics, has helped many law firms agree that 2FA is a minimum security requirement these days – and that is victory indeed in the cybersecurity world.

Preaching about Passwords (But the Gospel Has Changed)

We're not even going to talk about the old rules of coming up with passwords. The rules changed in 2017 when NIST issued its new *Digital Identity Guidelines*. The new guidelines were in large part based on an August 2016 Carnegie Mellon study which shows that, when it comes to passwords, length beats complexity. So those passwords you can't remember because they are all random characters meaning nothing? Trash them.

What you need are passphrases that you can remember. NIST recommends that passwords be 14-64 characters long – and we are here to tell you that lawyers are not going to enter 64 character passwords. Therefore, use a passphrase of 14 characters or more that you can remember and improve its complexity with a special character or two.

An example (and a blast from the past): In the old TV series *Batman* (RIP Adam West), Robin was fond of saying "Holy (insert a word) Batman" – he actually said "Holly Switcheroo Batman!" in one episode. Since we know that many systems don't allow for spaces in a password, we came up with "HolyswitcherooBatman!" as a good example of a strong password that you can remember.

And why is it important that you remember? Because a 2017 Pew Research Center study showed that 65% of Americans rely mainly on memorizing passwords. 49% write at least some of them down (sigh, obviously not a good practice – and yes, since we do undercover forensics examinations, we know where you all place your password sticky notes). 24% keep a list of their passwords on one of their digital devices (encrypted, one would hope, but we doubt it). Only 3% primarily rely on password management software to keep track of their passwords.

Worse yet, we reuse our passwords. The average user has 40 sites requiring a passwords, but only 5 passwords. We are our own undoing. As we said before, we sacrifice security for convenience.

Certainly, our best advice is to use password management software. But we are realists and know that many lawyers will choose not to do that. So at least make your passwords strong under the new NIST standards – and do not reuse or share them. Never, ever reuse a password for your law firm network anywhere else – that is an engraved invitation into the law firm network if that password is breached on another site.

Final Words

- Do have passphrases as passwords and make them at least 14 characters long with a special character or two
- Do not reuse passwords
- Do use multi-factor authentication wherever it is available
- Do not share passwords with others

One final benefit of the new NIST guidelines – we don't need to change our passwords as frequently as was once thought. As long as the passwords are checked against a database of known compromised passwords and meet minimum criteria, they really don't need changing on a regular basis. Huzzah for not having to go through this nuisance every 30-60-90 days. This could save you a fortune in sticky notes!!!

The authors are the President and Vice President of Sensei Enterprises, Inc., a cybersecurity, information technology and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com