Passwords May be Extinct Sooner Than You Think

by Sharon D. Nelson, Esq., John W. Simek, and Michael C. Maschke

Lawyers Hate Passwords

Lawyers have hated passwords since passwords first made their appearance. They resisted having them until their employer (or cyberinsurance company) compelled them. Then they constructed simple, too short passwords – 123456 and the like – easy to guess or crack. They used the names of their pets, their children, their favorite sports teams, etc. They set themselves up for failure at every point.

They left post-it notes on their monitors, under keyboards and in their desk drawers. They reused their passwords all over the internet. They shared their passwords with colleagues at their law firms. Even those who agreed, after much gnashing of teeth, to use a password manager, hated them – and they still reused and shared passwords.

The misery of data breaches is also a compelling argument to get rid of passwords. According to Verizon's 2022 Data Breach Investigations Report, 61% of all breaches were traced to compromised credentials. Combine that statistic with IBM's estimate that the average cost of a successful phishing attack was about $4.9 million in 2022 and bad news for your firm is just over the horizon.

Along Came AI to Make Cracking Passwords Easier

At this point, AI can crack the majority of passwords in under a minute. Seven letter passwords can be cracked in under six minutes despite having numbers, upper and lowercase letters, and symbols. If you are still using passwords in your law firm, you should have passwords with at least 15 characters and make mandatory the use of lower and upper-case letters, numbers and symbols.

Security fatigue is real – and, in the era of mandated two-factor authentication, worsening. But wait – there is a growing movement to ditch passwords forever.

Going Passwordless

We aren't going passwordless overnight, but it is on the horizon and lawyers should be embracing it. Quite a stir occurred in May 2023 when Google began allowing you to log into Google websites using passkeys.

It has been a long time coming, but Apple, Microsoft, Google and others have been working toward going passwordless using passkeys instead of passwords. Passkeys typically use biometrics – fingerprints or facial recognition being the most common.

There was already passkey support by Google for its Android phone and Chrome browser, but Google websites have been added. Not convinced? No problem. In a very smart move, Google made its passkeys work but retained your ability to use other login methods so you can take a test drive and reassure yourself that this new technology is great – which it is.

Ultimately, you will see passwords disappear as more systems support passkeys. Not all at once, but when enough folks have seen how easy it is to use passkeys, and understand the monumental increase in security, the days of passwords will be numbered.

Law Firms are Warming to Passwordless

Law firms have begun to feel comfortable with the cryptographic standards that underlie passkeys. Law firms are bedeviled by data breaches, notably those pesky phishing emails/texts that try to get you to share your credentials or other confidential information.

Firms are especially delighted that some password managers (like Dashlane) can store passkeys – Dashlane even allows you to log in with a passkey instead of a password- Huzzah! Other password managers are following suit.

Another boon is that passkeys are pretty easy to understand. Your phone or your laptop creates a private and unique cryptographic key which is tied to the device. In the case of Google, your account will issue a "digital challenge" that the passkey can sign, unlocking access. Then you only need a fingerprint scan or screen-lock PIN to make sure it is you that's logging in. A point to note is that the passkey stays on the device and is not transmitted as part of the authentication process. In other words, it is not sent to Google.

Let's try another way of thinking about passkeys. You sign into your device just as you always did, using a PIN or biometrics (facial or fingerprint recognition). You set your accounts to trust your computer or phone. This is what makes it so safe. A cybercriminal would have to physically possess your device AND have a way to sign into it.

What if you lose your phone? Good question. Your passkey can be stored securely in the cloud with your phone's other data, which (no doubt you've guessed it) can be restored to a new phone.

Bad guys are outwitted and the good guys have a simpler means of secure access. Now that's a win-win for the lawyer and law firm.

Final Words:

There's a reason why you can go to Amazon and buy a tee shirt that says "I f***ing hate passwords."

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* *snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.* *jsimek@senseient.com*

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.* *mmaschke@senseient.com*