Common Sense Passwords Coming to Law Firms Soon

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

How Happy is Your Law Firm with the Current Password Requirements?

The usual answer is “we’re not happy, not at all happy”

Anyone who understands passwords has bemoaned the current state of law firm passwords which make no sense and cause more harm than good. The National Institute of Standards and Technology (NIST) is preparing to change that. Who would believe that a federal agency got it right?

Amazingly, NIST has come out with a well thought out set of changes, released in August 2024, which is very likely to be adopted with little modification sometime after the deadline for responding to Public comment on its second draft (via email dig-comments@nist.gov) which is open until 11:59 pm Eastern Time on October 7, 2024.

Can You Make the Commonsense New Rules Effective Now?

Sure you can. As a Managed Service Provider (MSP), which provides cybersecurity for many law firms, we distributed the late September NIST proposed rules to our cybersecurity staff. They breathed a sigh of relief that we are contemplating adopting some of the rules soon, after we’ve had a chance to sit down around a conference table and evaluate each new rule and its suitability for law firms and other clients.

We were heartened when cybersecurity specialist Bruce Schneier, famous in our world, reviewed the proposed rules and gave them a rousing “Hooray!”

Bruce may have been as surprised as we were when he titled his post “NIST Recommends Some Common-Sense Password Rules.”

You can almost hear his oft-repeated criticism of the old rules when his first sentence says “NIST’s second draft of its “SP 800-63-4“—its digital identify guidelines—finally contains some really good rules about passwords.”

So, What are the New Rules?

NIST will no longer recommend using a mixture of character types in passwords or regularly changing passwords. Do we hear lawyers shouting “Hurray”? We sure do.

NIST sets forth technical requirements as well as recommended best practices for password management and authentication. The latest guidelines instruct credential service providers (CSP) to stop requiring users to set passwords that use specific types of characters or mandating periodic password changes (commonly every 60 or 90 days). Also, CSPs are instructed to cease using knowledge-based authentication or security questions when selecting passwords.

When NIST first introduced its password recommendations (NIST 800-63B) in 2017, it recommended complexity: passwords made of a mix of uppercase and lowercase letters, numbers, and special characters. However, complex passwords aren't always strong (i.e., the famous "Password123!"). And complexity led to users making their passwords predictable and easy to guess, writing them down in easy-to-find places, or reusing them across accounts. We can't recount the huge number of those mistakes that we encounter regularly with new clients. The NIST focus is on longer passwords which are harder to crack with brute-force attacks and are easier for users to remember without being predictable.

NIST is now recommending password resets only when there's a credential breach. Making people change passwords frequently means they tend to choose weaker passwords. When passwords are sufficiently long and random, and there's no evidence of a breach, making users change passwords could potentially lead to weaker security.

Previous versions used the words "should not" while this draft says "shall not," which means the rule has moved from a suggestion to an actual requirement. Yay!

What Lawyers Should Do Sooner Rather Than Later

Be open to changing the way you protect your data. The advice from NIST is very sound and changes made after the October input are likely to be minor. Be wary of MSPs that want to keep things just as they are. 'Just as they are' will not properly protect you.

Our guess is that the cyberinsurance folks will start requiring compliance with the new NIST guidelines, likely in 2025. Get ahead of the curve. Be safer sooner!

Final Thought

One more quote from cybersecurity specialist Bruce Schneier "Complexity is the worst enemy of security, and our systems are getting more complex all the time."

Sharon D. Nelson *is an 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 Chief Executive Officer at Sensei Enterprises, Inc. Mr. Maschke is an EnCase Certified Examiner (EnCE), a Certified Computer Examiner (CCE #744), an AccessData Certified Examiner (ACE), a Certified Ethical Hacker (CEH), and a Certified Information Systems Security Professional (CISSP). He is a frequent speaker on IT, cybersecurity and digital forensics and he has co-authored 14 books published by the American Bar Association. He can be reached at* *mmaschke@senseient.com*.