ASK KK

BY MARCUS BLUESTEIN AND NINA LUKINA

Marcus Bluestein is the Chief Technology Officer at Kraft Kennedy. He leads all of Kraft Kennedy's technical practice groups, drawing on more than twenty years' experience of designing and implementing information systems at law firms as well as on his current research in enterprise technology. He specializes in helping law firms develop, implement, and test business continuity and disaster recovery plans. **Nina Lukina** is a Marketing Associate in the New York office of Kraft Kennedy. She researches and writes about emerging topics in technology. A former consultant at Kraft Kennedy, she's worked on many IT strategy and information security projects for law firms.

Password Management for Law Firms

To KK:

My firm has an annoying but duly cautious password policy that means I'm juggling new passwords every 90 days, on top of all the ones I need for research sites. I know emailing lists and sticking Post-Its to my desk isn't safe, but I'm hesitant to trust a password vault tool. What if it gets hacked? How are attorneys with client-sensitive data dealing with password management these days?

Med Mal Attorney

Med Mal:

Dealing with a profusion of passwords is indeed a challenge. You are not alone in your frustration.

Password managers like LastPass, RoboForm, and 1Password are great tools for web-based passwords, such as the ones you use for Westlaw and Lexis, as well as your personal online accounts. They won't help you log into your firm's network, though.

The best solution to simplify network login is Windows Hello, which uses facial and fingerprint recognition technology. Hello is a feature of Windows 10. While it is, admittedly, still rare for the Hello camera to be available, the fingerprint scanner is available on most computers now. You can also purchase it separately in a keyboard. Aside from Hello, there are few options that are both secure and convenient. You are correct that the Post-It is not a good idea.

Web password managers are an effective remedy for a deluge of passwords. Your concern that these tools themselves may get hacked, however, is reasonable. A hacker who gets into your password vault will have all your passwords. To mitigate the risk, use a popular manager that's been tried by many users before you, such as one of the platforms we name above.

Further, make sure that the password you use for the vault itself is extremely secure, as in 20 characters or longer. I recommend using a passphrase – a sequence of words that, while long for a password, is not hard to remember. Security researchers now believe that passphrases are more secure than shorter, complex passwords that include numbers, symbols, and upper-case letters.

That said, password managers can make your life easier and actually heighten your security online. Crucially, they offer the option of randomly generating long, complicated passwords for your accounts. Use these. Your account will be harder to hack and you won't have to remember and type your credentials upon every login. ■