What Kind of Fool Am I (That Doesn't Use MFA)?

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

Those of you of a certain age will remember the song "What Kind of Fool Am I?" That song was about love, but for Pete's sake, why is it that some lawyers keep insisting that they won't use MFA (multi-factor authentication)?

Thanks to our good friend Ben Schorr (who works at Microsoft) for sending us an August 7 Microsoft update on why multi-factor authentication is so critical. It is short, sweet and should be read by anyone who has resisted multi-factor authentication (and there's a lot of you!).

From the post:

"*When you sign into your online accounts - a process we call "authentication" - you're proving to the service that you are who you say you are. Traditionally that's been done with a username and a password. Unfortunately that's not a very good way to do it. Usernames are often easy to discover; sometimes they're just your email address. Since passwords can be hard to remember, people tend to pick simple ones, or use the same password at many different sites.*

That's why almost all online services - banks, social media, shopping and yes, Microsoft 365 too - have added a way for your accounts to be more secure. You may hear it called "Two-Step Verification" or "Multifactor Authentication" but the good ones all operate off the same principle. When you sign into the account for the first time on a new device or application (like a web browser) you need more than just the username and password. You need a second thing - what we call a second "factor" - to prove who you are."

Probably the most important point is that you do not need to use the second factor every time. You can make your phone and laptop "trusted devices." If the bad guys know your ID and password, but try to access your account from another device, they will need that second factor. Statistics show that using MFA stops over 99.9% of all account takeover attacks. It doesn't get much more persuasive than that.

When will you HAVE to use the second factor? When you get a new device or change the password for your account. But that's not very often. Sometimes, you

may be required to enter the second factor when you are accessing particularly sensitive data – medical sites and financial institutions often require two-factor authentication at every logon for your own protection. But for the most part, it won't be nearly the inconvenience that most people think it will be.

If you are really interested in security, consider the different kinds of two-factor authentication. SMS texts are infinitely better than not using 2FA, but there are more secure methods that you might consider.

SMS text messages are the least secure of the MFA implementations, primarily because it is vulnerable to SIM-jacking. That's where someone obtains a SIM card with your phone number and hijacks your phone number to another phone. Those SMS text messages then get sent to the hijacked phone.

A more secure MFA method is to use an authentication app such as Authy, Duo, Google Authenticator, Microsoft Authenticator, etc. The app generates a unique six-digit code every 30 seconds. When prompted for the MFA code, you type in the code that is displayed in the authenticator app. This type of MFA is susceptible to man-in-the-middle (MITM) attacks where the code can be intercepted as you type it in.

An even more secure MFA method is to receive a push notification to your authentication app. When you logon, the system sends a push notification to your registered phone. All you do is tap the notification to allow access. This means there is no code to enter or intercept.

Finally, the most secure of the MFA methods is a physical security key. YubiKey is a very popular security key as is the Titan Security Key from Google.

Recently, we have seen more account takeovers than ever. Read the Microsoft post carefully – it will answer most common MFA questions. And then begin to use MFA for all your online accounts. It's almost always FREE (your favorite price, right?). Very effective too. Just do it.

Sharon D. Nelson, Esq. 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 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 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.