Security Fatigue and its Impact on Law Firm Security

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

People are inherently lazy. After all, why do something today that you can put off until tomorrow? Users hate to do anything that would slow down their access to their computer or data. That means they would much rather just sit at a keyboard and start to surf the Internet instead of entering logon credentials and then entering a second factor. How many times have you been tired of the constant password changes only to resort to using one you know you'll remember and have previously used? Didn't feel like creating a new account so passed on that online purchase? You are not alone.

A recent study from the National Institute of Technology (NIST) found that the majority of typical computer users experience security fatigue, which leads to risky computing behavior at work and in their personal lives. Security fatigue is defined as a reluctance or weariness to deal with computer security. So what does this mean for law firms? A balanced approach is the way to go. If you make things too difficult for the users, they will find ways around the security measures.

Noted security guru and cryptographer Bruce Schneier says "Stop trying to fix the user." As Bruce said in a recent blog post, "The problem isn't the users: it's that we've designed our computer systems' security so badly that we demand the user do all of these counterintuitive things. Why can't users choose easy-to-remember passwords? Why can't they click on links in emails with wild abandon? Why can't they plug a USB stick into a computer without facing a myriad of viruses? Why are we trying to fix the user instead of solving the underlying security problem?"

We need to be smarter in how to design secure environments for law firm users. Forget about the security warnings. Do you really think anyone reads the pop-up dialog box that warns that the certificate is expired or not verifiable? The user doesn't really care. They would much rather see a "get rid of me" button so they can get to the website. Passwords aren't much better, especially for sites that are rarely visited. The user will elect to save the password in the browser (never a good idea and a huge security risk) or constantly use the "I forgot my password" link, which means they are falling back on the security of their e-mail system since that's where the reset link will go. User's aren't going to pay attention to links either, whether valid or from phishing attacks. Users know that a link gets you where you want to go so we'll never fully teach them to be suspicious of links.

We need to stop trying to protect the user from themselves. In order to combat security fatigue, we need to make the environment more secure no matter what the user does. Virtual environments and sandboxing will keep the applications running in a "walled" off area that is separated from the user's system so you don't have to worry about embedded malware. Automatic updates will help too, since the user won't have to remember to manually apply updates.

The NIST study provided evidence for three ways to help reduce security fatigue.

1. Limit the number of security decisions a user needs to make
2. Make it simple for a user to choose the right security action

3. Design for consistent decision making whenever possible

We will never be able to provide a 100% secure environment, but we can get a heck of a lot closer by reducing security fatigue and removing the user from the decision making process as often as possible.

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