THE CASE FOR TWO-FACTOR AUTHENTICATION

Cyberattacks and data breaches are becoming increasingly common and pose significant risks to law firms. Storing sensitive and confidential information such as financial and banking information, client identification, and client documents and medical records, makes law firms very attractive targets for cybercriminals.

The consequences of a cyberattack or data breach for a law firm can be serious, not only in terms of financial costs and loss of productivity, but they can also affect a firm's reputation, client trust, and can result in claims against the firm and lawyer.

The good news is that 2 Factor Authentication ("2FA") is an effective way to help keep confidential data secure and avoid cyberattacks, and it is often something that we have available to us at no additional cost.

2FA is a security feature that requires two different means of identification when logging into an account. Most law firms operate using an email account (such as Microsoft Outlook or Gmail), practice management software, and bank accounts.

Traditionally, the first step when signing into an account (whether it is an email, bank or other network account), is to enter a username and password. The password is a "single factor authentication". Today, passwords alone do not offer enough protection against cybercriminals. 2FA adds an extra layer of protection.

After you enter your password, you will be prompted to enter a temporary code which is either emailed to you or sent to you by text message on your cell phone, or through an authenticator app that you download onto your cell phone. The code is usually valid for a short period of time. To gain access to your account, you need to enter the code on the log in page. The code is a "second factor authentication".

With 2FA enabled on your accounts, a cybercriminal would need to (1) know your password, and (2) access your cell phone to obtain the code that is needed to log into your account. The second step makes it more difficult for a successful cyberattack.

You may not realize it, but you likely have access to 2FA through your current email and bank accounts - all you need to do is enable the 2FA feature.

For example, 2FA can be activated through email security settings. You can set up 2FA on bank accounts through your online account or by contacting your bank. Many practice management software systems also offer 2FA. If you are unsure whether your practice management software includes the 2FA feature or how to enable it, check with the software provider's customer support.

It's important to assess your current accounts and software applications and identify where 2FA can be set up. Where available, implement 2FA, and ensure that employees know how to use it and why it is important.

One of the simplest and most effective ways law firms can secure and protect confidential information and data is by enabling 2FA on their accounts and software. Doing so will help you avoid cyberattacks and will contribute to the smooth operation and success of your law practice. ■

Leanne Fasciano is Communications Counsel at LAWPRO