Vol. 24 No. 20 The Journal of the Allegheny County Bar Association October 7, 2022

LAWYERS JOURNAL

LAW PRACTICE MANAGEMENT

The importance of using multi-factor authentication tools

By Alicia A. Slade

"An ounce of prevention is worth a pound of cure" originated in 1736 by Benjamin Franklin to educate the citizens of Philadelphia about fire prevention and awareness. The phrase was used to convince the citizens of the city that it is better to prevent fire than fighting a fire and rebuilding afterwards.

Benjamin Franklin's phrase is applicable today to explain how important it is to use multi-factor authentication (MFA) tools to prevent a ransomware attack or cybercriminals from gaining access to your emails and your client's data. Prevention and being proactive to thwart off a cyberattack will save you time, money, and your reputation.

Two-factor authentication (2FA), also referred to as multi-factor authentication (MFA) or dual-factor authentication is taking an extra step during the account login process. The extra step verifies your identity via a cell phone app, a text message, or an email to the owner of the account. Many people feel that this extra step is too difficult because they need to enter a secure code or approve the login via an app on their smartphone. Just think, this is no different than taking the extra step to lock your office door or residence before leaving. You hold the key to reenter the premises.

Cybersecurity professionals agree that having a strong password is important but using multi-factor authentication (MFA) is 99% more effective at stopping cybercrimes. The extra step prevents an IT disaster and keeps your client's data safe.

Email compromise schemes are prevalent. The contents found within emails and attachments are valuable to cybercriminals. Over the past several years, firms have moved their email from on-premises Exchange Servers to either Microsoft 365 Exchange Online Hosted Email or some other hosted email service, such as Gmail. The migration of email to a hosted environment moves the emails from servers within your office to the Microsoft Cloud or some other provider. With this, a cybercriminal doesn't need to breach the office network, servers, or computer. The cybercriminal can breach an individual's cloud account instead.

When a cloud account is breached, the individual is oblivious that a cybercriminal has gained access to their email or data in the cloud. The only way to know if a cybercriminal is trying to access your account is by using multi-factor authentication. When the cybercriminal breaches the login ID and password of a hosted email account, prior to permitting access to the account, a verification request is sent to the owner of the account with a code or an Approve/Don't Approve alert notification. When the individual receives the alert and knows that they themselves are not accessing the account, they can stop the cyberattack.

Unfortunately, too many people think if their firm is small or if they don't have important data, a cybercriminal would not try to get access. They could not be more wrong. The size of the firm does not prevent an attack and many types of data are valuable to a cybercriminal to exploit.

While writing this article, one of my technicians received a call from a client. An attorney at a fifteen-person firm realized that their email had been compromised. Bank information had been changed and emailed to an attorney at a different firm. The attorney realized the compromise when the other attorney sent a response email that stated they "got it." The compromised attorney saw the response and knew that they had not sent the email and called the other attorney immediately. After some investigation, it was determined that the cybercriminal had been in the attorney's email account for over a week. The cybercriminal observed incoming and outgoing emails and the responses, waiting for banking information to be exchanged. Although implementing multi-factor authentication had been recommended many times to the firm, the attorney had refused implementing it because they did not want to take the occasional verification extra step. The extra verification step is only needed when an email account is accessed from an unfamiliar IP address, geographical location, or device.

A few months ago, I received a call from the director of a four-person non-profit organization who was referred to me. The director proceeded to explain that the non-profit organization used an Instagram account with over 4,000 followers. The director explained how it had taken several years to cultivate these social media followers. Posting to Instagram was the method the organization used to communicate with donors and general followers of the organization. A cybercriminal had gained access to the non-profit's Instagram account and was holding the account for ransom. The director was rightfully upset and realized the consequences of the ransom attack. This attack happened easily because the organization was not using multi-factor authentication to protect the Instagram account.

It is important to use multi-factor authentication not just for your email and remote access but for social media accounts and your website (LinkedIn, Facebook, Instagram, Twitter, etc.). Additionally, any online portals you use to access financial investments, banking, payroll, and insurance, should be setup to use multi-factor authentication. The option to setup two-factor or multi-factor authentication is typically found within the account security or privacy settings of the portal.

Email is a goldmine for cybercriminals. The data stored in OneDrive, SharePoint, Google Drive, Dropbox, or wherever in the cloud is too. A cybercriminal does not need to breach your computer network or your computer to get to your emails and documents since they can more easily breach your cloud account. The only way to know that a cybercriminal is trying to gain access to your online account is by using multi-factor authentication so you will be notified of the peculiar access request and can stop it.

Taking precautions and being proactive, can and will save you money. If your plan is to sit back and think that it won't happen to you or why would the cybercriminal want anything you have, it is just a matter of time before it happens to you, or your data is held for ransom.

An ounce of prevention is worth a pound of cure (Benjamin Franklin, 1736) could not be truer when it comes to using multi-factor authentication. I want to sound the alarm and make you aware of the importance of taking the extra step within your accounts. Use multi-factor authentication to prevent a cybersecurity attack! ■

Alicia A. Slade, MS, MBA, is the President of Plummer Slade, Inc., a computer networking, Managed Services Provider (MSP), and Managed Security Service Provider (MSSP) located in downtown Pittsburgh. Plummer Slade provides IT Managed services and solutions to hundreds of law firms in Pittsburgh and the surrounding area. Plummer Slade is exclusively endorsed for IT Solutions by the Allegheny County Bar Association. She can be reached at 412-261-5600 or aslade@plummerslade.com.