Think Multi Factor Authentication is a Silver Bullet for Cyber Security? Not Necessarily ...

Risk management topics:

Cyber Security | Practice Management

Candice Perriman
Risk Education Manager

Many law practices are told to take comfort once Multi Factor Authentication (MFA) is switched on. It feels like a strong line of defence to a cyber attack however as Lead Cyber Analyst Luke Fardell from Tokio Marine Kiln insurance cautions, MFA is not a silver bullet and in some cases can be used against you.

Picture this...

A solicitor briefing counsel in a litigation matter receives an email that appears to come from chambers:

> Your documents exceed file size limits. Please upload them securely using the updated SharePoint link.

The solicitor clicks the link, which opens a Microsoft login page that matches the usual page. They log in, approve the MFA request, but nothing happens. They repeat the process and successfully access SharePoint on the second attempt, but no new documents appear.

What is likely to have occurred is an 'MFA bypass attack', which is now a common type of cyber attack. The attacker has captured the authentication token (a temporary token that proves you have completed the MFA step e.g. entering a code from an authenticator app) and is able to access your confidential litigation documents, pleadings and client strategy.

As Luke explains, attackers can sit in the middle of the login process using a convincing replica page, the solicitor or staff member enters their details, completes MFA, and the attacker captures the authentication "cookie" (a small file that is stored in your browser that proves you have successfully logged in) that shows MFA has already been obtained. From there, the attacker can access the law practice's system without needing the password.

Think Multi Factor Authentication is a Silver Bullet for Cyber Security? Not Necessarily ...

Luke points out that the "bounce back" that occurs after login is part of the distraction. This prompts the solicitor to enter their details again and is meant to look like a harmless glitch. There are no visible signs that anything is incorrect; the email reads well, the login page looks legitimate, and MFA still triggers.

The consequences for the law practice can be serious, with potential breaches of confidentiality and privacy obligations, as well as possible loss of client legal privilege. It can also lead to significant financial losses resulting from data theft, payment misdirection and even ransomware deployment.

Despite the sophistication of these attacks, Luke explains that there are a few signs that law practices can look out for:

Receiving an email requesting you to **log in via a link or attachment**

Being asked to **log in again** via a link when you are **already signed in**

A successful MFA **prompt followed by a pause, glitch or redirect** back to the login page

Any **urgent request** that cannot wait, especially late in the day or at the end of the working week

Think Multi Factor Authentication is a Silver Bullet for Cyber Security? Not Necessarily ...

The takeaway

From a risk management perspective, controls should focus on behaviour, not just technology:

Instil link discipline:

Staff should avoid logging in via links that have been emailed or messaged and instead use trusted bookmarks or go to the page directly. This includes accessing any portals, apps, and SharePoint sites

Act quickly:

If a login is redirected, 'bounces back' or behaves unusually, report it and lock down the account for review. Ensure there is a clear pathway for reporting so that appropriate and quick action can be taken

Be suspicious:

Treat any unexpected re-authentication request as suspicious

Strengthen payment controls:

Independently verify any change to bank details offline using a known and verified contact method.

Educate:

Increase awareness and train staff to scrutinise emails, links and attachments. Do not rely solely on detecting poor spelling, obvious errors or spam filters. These emails are now highly convincing.

Think Multi Factor Authentication is a Silver Bullet for Cyber Security? Not Necessarily …

MFA remains extremely important, but it does not eliminate all cyber risk. As Luke cautions, it can be actively leveraged by attackers if solicitors are not alert to how these attacks work. For law practices it is important that all staff understand the risk, recognise the warning signs, and know exactly what to do when something doesn't feel right.

TOKIO MARINE KILN

Tokio Marine Kiln are the underwriters of the Lawcover Cyber Risk Insurance Policy. This policy is available for all insured law practices, at no cost. See details of the cover at ***lawcover.com.au/insurance/cyber-risk-insurance/***

Luke Fardell ***(luke.fardell@tokiomarinekiln.com)*** *is Tokio Marine Kiln's lead cyber analyst supporting cyber underwriting. With a background in UK intelligence, he has worked for the UK's Ministry of Defence and National Cyber Security Centre, investigating nation state cyber attacks. Luke has investigated over a hundred ransomware incidents affecting both the public and private sector conducting forensics examinations on all types of systems and infrastructure. Luke is also involved in building and maintaining TMK's Cyber Threat Intelligence platform.*

For specific and practical guidance on safeguarding client funds, see ***Cybersecurity expectations for NSW Trust Account Management*** by Sharon Blake, Chief Trust Account Investigator at the Law Society of NSW. Published in Ethics and Standards Quarterly, the article explores steps law practices can take to strengthen controls and reduce exposure to cyber-enabled trust account risks. It is a timely companion piece for any practice reviewing its cyber resilience and trust account processes.