Protecting against business email compromise attacks: guidance for barristers and chambers

Due to the nature of their work dealing with sensitive information, barristers and chambers can be a lucrative target for cybercriminals. In recent months there has been an increase in business email compromise (BEC) attacks on the legal sector. This briefing is to warn against these emerging threats and highlight the importance of protecting against the risk of a BEC attack.

Cybercriminals are becoming increasingly sophisticated in these types of attacks, using new techniques which are circumventing traditional forms of multi-factor authentication (MFA). Since COVID-19 and subsequent hybrid working policies, the increased usage of Microsoft Teams has opened a pool of opportunity for cybercriminals attempting to carry out a BEC attack.

This poses a challenge for targeted organisations to prevent, identify and stop these types of attacks and therefore, in this briefing, we explore essential steps and strategies to safeguard barristers from BEC attacks.

Understanding BEC attacks

A BEC attack is a form of cybercrime where fraudsters impersonate a trusted entity to manipulate the recipient into taking actions harmful to their organisation. In the context of barristers, BEC attackers may pretend to be clients, colleagues, or other trusted third parties to deceive a barrister into sharing sensitive information or making fraudulent financial transactions. Unlike standard phishing emails that are sent out to millions of people, BEC attacks are crafted to appeal to specific individuals and can be difficult to detect.

The legal sector has seen hackers increasingly stealing session cookies to bypass MFA requirement to access an account, using advanced phishing techniques known as Adversary-in-the-Middle (‘AitM’) that rely on the use of maliciously intercepting and relaying traffic in the middle of a legitimate login process. The widespread availability in the criminal underground of easy-to-use tools to facilitate these techniques, such as a phishing kit known as “EvilProxy”, has lowered the barrier to entry and the expertise required to use these methods.

Don’t fall victim: how to protect against BEC attacks

Cybercriminals can gain access to a barrister’s account by obtaining their credentials through phishing campaigns or purchased on the dark web. Due to the increased sophistication of the cybercriminals conducting these attacks, barristers should look to implement several measures to reduce the risk of a BEC attack, such as:

1. Use strong authentication methods *and importantly, consider further strengthening these*

One of the primary ways to protect against BEC attacks is to employ robust authentication methods. Barristers can make their account harder to compromise by turning on MFA which requires a code, pin, or fingerprint to log in, as well as a password.

40 St James’s Place
London
SW1A 1NS

contactus@tlorisk.com
020 7183 4925

tlorisk.com

Whilst this is not a silver bullet, it can deter the less sophisticated threat actors from successfully authenticating. However, to prevent AitM phishing attacks, some MFA implementations are better than others: so, if possible, use a FIDO2-certified authenticator. Examples of this are ‘Windows Hello for Business’ or alternatively a ‘physical’ Yubi hardware key.

Combine best practice MFA with conditional access policies to require authenticating devices to be trusted or compliant and come from trusted locations.

Avoid using application-based MFA authentication with push notifications where possible, as these may be subject to notification fatigue attacks.

Where possible, avoid using MFA solutions based on SMS or one-time password via authenticator applications as these are vulnerable to multiple methods of interception

2. Educate and train members and staff

Barristers often work in collaboration with others. It is therefore essential to educate and train all team members on how to spot phishing emails and look out for red flags such as a domain and email address mismatch. Simulated phishing tests that match the current levels of sophistication can also help team members recognise and report suspicious activity.

3. Implement email authentication protocols

Email authentication protocols such as DMARC (Domain-based Message Authentication) verify the authenticity of emails and prevent unauthorised individuals from sending messages on behalf of the organisation’s domain. Therefore, implementing these protocols can help barristers secure their email communications and reduce the risk of email spoofing and impersonation.

4. Establish a secure communication policy

Chambers should develop a clear and secure communication policy. This can include guidelines on how sensitive information should be shared, especially personal or financial details. Encouraging clients and colleagues to verify the authenticity of requests for financial transactions through other means such as a phone call, can add an extra layer of protection.

5. Think twice about what you share online

Cybercriminals can also use information about you that are on your work and private websites such as social media accounts to make phishing emails more convincing. It is therefore important to review your social media privacy settings and think about what you want to post across your social and professional profiles.

40 St James’s Place
London
SW1A 1NS

contactus@tlorisk.com
020 7183 4925

tlorisk.com

The consequences of a BEC attack

Being victim of a BEC attack has several significant consequences for barristers and chambers, including:

- Reputational damage and loss of trust with instructing solicitors and lay clients
- Direct potential losses and/or third-party liability for funds lost by clients when monies are fraudulently diverted
- Heightened regulatory scrutiny

Furthermore, once an account has been compromised, cybercriminals have also been seen to access the users' LinkedIn account to obtain a list of email addresses for future phishing attempts, putting other people at risk.

We are here to help

Protecting against BEC attacks involves a combination of technical measures, employee training, and strong security. By staying vigilant and implementing protective measures, barristers can significantly reduce the risk of falling victim to these malicious attacks, safeguarding their reputation and sensitive client information.

As a specialist Professional Risks insurance broker, TLO Risk Services (TLO) can help you navigate the insurance market, ensuring your organisation has the most appropriate cover in place. Get in touch with our expert team for more information about protecting your members and chambers against BEC attacks and broader cyber risks:

+44 (0) 20 7183 4925
contactus@tlorisk.com