The Law Society

The Law Society’s Risk and Compliance Service
Top Tips Series

Email scams

Email is a very effective method of communication, but as the technology behind most emails does not use encryption or authentication, the contents of every message can be exposed. For law firms who exchange sensitive or confidential information daily, this poses a significant security risk.

Read on for our top five practical tips to effectively safeguard your firm.

Pearl Moses, Head of Risk and Compliance, The Law Society

1 Use best practice

- Take your time and respond to emails in a considered manner – fraudsters often use urgent requests to panic recipients into thinking they must respond quickly.
- Do not redirect or forward emails from a secure office email account to external or personal email accounts such as Hotmail or Gmail.
- Never put confidential information in the body of an email or in an attachment unless it is encrypted. The encryption password should then be communicated via an alternate channel such as texting or, preferably, ringing the recipient.

2 Be aware

- Treat emails requesting sensitive information – such as bank details – with utmost caution. Always verify suspicious requests using previously known or independently researched contact information, and not contact information provided in the request.
- Beware of emails and requests that use idiomatic phrases or sound as if they are translated – grammatical or spelling errors in emails are red flags.
- Check the **SRA’s scam alert pages** regularly – these list bogus emails being sent to firms.

3 Train all staff to stay alert

- Encourage staff to pay attention to detail – check all incoming and outgoing email addresses to protect against ‘spoofing’ (forgery of an email header that appears to have originated from someone/somewhere other than the source).
- Inform staff not to open unusual emails until they are cleared by your IT department.
- Provide specific training on spotting ‘phishing’ through simulations or real-life examples to help staff to identify such emails.

4 Protect against phishing

- Protect against undetected phishing emails and malware by only using supported software and devices, and ensuring all software is up-to-date.
- Having a security monitoring capability can help to detect and respond to incidents quickly. Consider either monitoring tools built into your off-the-shelf services such as cloud email security panels, an in-house team, or outsourcing to a managed security monitoring service.
- For more comprehensive support on phishing, visit the **NCSC’s support pages**.

5 Ensure you have watertight policies and procedures

- Ensure your email security policy is actively communicated to all staff and regularly reviewed.
- Consider highlighting in your client care letter that email is not a secure method of transmitting sensitive data – the client should be alert to email scams as well.
- Have a password policy – the **NCSC** advocates using three random words, which are easy to remember but hard for or non-authorised users to guess.
- Implement a simple crisis-management process, identifying who will take specific action in the event of a successful scam.

For additional support on cybersecurity and compliance-related issues facing law firms, visit: **www.lawsociety.org.uk/riskandcompliance**

To receive a weekly digest of cybersecurity news update, sign up to the Law Society’s weekly cybersecurity news digest **here**