Security detail

A culture of security can help protect your law firm from hostile third parties, says Gary Shaw at Accesspoint

As we all now know, assuring a high level of security within your firm has become increasingly difficult, especially as the world continues to move in a more digitally motivated and agile direction.

Law firms remain top targets for cyberattacks, as they hold sensitive client information and handle significant funds – making the financial rewards for such attacks ever more appealing. Judging from the last 18 months, we can all vouch for the fact that remote working is here to stay, so now is the time for you to revisit the ways your firm maintains a high level of security and rigour.

Security defence starts within a law firm's team. A recent survey found that 56% of senior IT technicians think their employees have picked up bad cybersecurity habits, with nearly 39% admitting that their cybersecurity practices at home are more relaxed than those practiced in the office, due to less surveillance and a high level of correspondence. Just imagine the amount of damage that could occur if a successful attack is made on even one transaction between a client and firm. Not only will sensitive data become exposed but the level of trust that any current or future clients have in the firm will instantly diminish. Keeping your team aware of the most common threats that your practice can face – such as phishing scams, data breaches and other common tactics – will make a huge difference. Don't assume everyone knows or understands!

Several tell-tale signs could alert a member of the team to a scam, such as email and website spoofing, malicious links and attachments, urgent subjects, calls-to-action, and more. Keep your team clued in on current methods and consider partnering up with a reputable legal-IT specialist to provide phishing awareness training. This could ensure your team knows how to protect your firm from unauthorised third parties.

Additionally, always encourage your team to act fast and inform someone immediately if they think there has been a breach of data. On average, it can take up to 279 days to identify a breach. Perhaps think of ways to create a safe and approachable workplace environment, especially with home working. It could save you a world of trouble.

It is important to note that although cyber-criminals are not always tech-savvy geniuses, they are becoming more organised and moving from scattered attacks to more calculated hits.

Learn more about fending off cyberattacks on the LPM website. LPM

ACCESSPOINT GROUP
Our group of companies offers specialised services, products, support, and consultancy in legal IT
Contact Gary on:
020 3189 2645
theaccesspoint.co.uk
@theaccesspoint

Accesspoint
Group Holdings

CHECK OUT OUR CHANNEL PARTNERS
p8

GO TO LPMMAG.CO.UK