CHURCHERS
SOLICITORS

LIFE IN LAW

THE CYBER CHALLENGES AND THREATS FACED BY LAW FIRMS

CHURCHERS SOLICITORS

Why are law firms targeted?

- Holding significant level of client funds
- Sensitive client data and information
- Nature of transactional business dealing with businesses and public

CHURCHERS SOLICITORS

Incidences of attacks

- The top 100 law firms have experienced attacks rising from 45% in 2018-19 to 73% in 2022
- 55% of those victims of attacks were via a virus or other malware
- The move to increased remote working and reduced level of face-to-face meetings has fuelled a rise in data breaches

CHURCHERS SOLICITORS

Types of attack

Phishing.

- Obtaining sensitive data or access to client funds by impersonating a trustworthy source
- Perpetrated via a number of means – not just electronic communication
- Untrained and unsuspecting staff are the most at risk.
- The most common threat recognised.
- More targeted version called ‘spear-phishing’

CHURCHERS SOLICITORS

Fake/Cloned emails

- Fake emails not usually sophisticated
- Cloned emails more difficult to spot as from a genuine email address
- ‘CEO’ fraud – whereby senior management request funds transfer or task undertaken. Most often from fake email addresses.
- ‘Friday fraud’ – usually the most busy day for property completions, hence busy accounts teams. Common attempts to advise of changed bank account details

CHURCHERS SOLICITORS

Zero Day attacks

- Exploiting a vulnerability in a software application before this is identified and fixed

Ransomware

- Malware preventing the user from accessing files or data. Commonly installed via a rogue link

CHURCHERS SOLICITORS

Countering the threat

- Email filtering and anti virus
- Disabling USB ports
- Encrypting laptops
- Firewalls
- Strong passwords and two factor authorisation
- Equipment supplied to those WFH
- Mobile Device Management
- No saving of data on local device
- Training and awareness!