News release

Cybercrime warning for law firms during lockdown

23 April 2020

Law firms and their employees have been urged to be extra vigilant during the coronavirus lockdown amid increased reports of cyber attacks against businesses whose staff are working remotely.

Cybercriminals are trying to take advantage of lower levels of security brought about by increased remote working, IT challenges, and the different mindset people may have when working from home. We have received specific reports about law firms being targeted. In one such example criminals attempted to create a standing order for £4,000 a month from a firm's client account.

With huge numbers of law firm employees working from home, possibly for the first time, we have published information at the start of the month advising firms on key cybersecurity issues. Law firms and solicitors handle sensitive information and large amounts of money, so are an attractive target for criminals.

Paul Philip, SRA Chief Executive, said: "Cybercrime is a priority risk for the legal sector and it's not going away during the Covid-19 pandemic.

"Criminals are always looking to take advantage and they know that security arrangements are likely to have changed as people move to homeworking. Several agencies have reported a spike in cyberattacks and we are beginning to get reports from firms that have been targeted.

"We have published information for law firms on the risks during lockdown, and I urge everyone to be particularly vigilant at this time."

Our coronavirus cyber security information includes targeted advice from the NCSC and has a useful checklist for firms to reassure themselves about eliminating risks. The advice is part of wider support for the profession during the coronavirus lockdown that includes answers to common questions around Accounts Rules, completing proper due diligence and renewing indemnity insurance.

The NCSC has this week launched a Cyber Aware campaign [https://www.ncsc.gov.uk/cyberaware] to help keep workers and the public safe.

NCSC's takedown services have already removed more than 2,000 online scams related to coronavirus in the last month, including:

- 471 fake online shops selling fraudulent coronavirus-related items
- 555 malware distribution sites set up to cause significant damage to any visitors
- 200 phishing sites seeking personal information such as passwords or credit card details
- 832 advance-fee frauds where a large sum of money is promised in return for a set-up payment

You can also read Action Fraud’s warning for small businesses based on coronavirus confusion.