News

Learning the lessons from Cybercrime incidents

03 February 2022

Solicitor firms hold large amounts of money and confidential information, which makes them an attractive target for cybercriminals.

There are many ways that scammers try to trick firms and clients into sharing access to files and systems. Even the most experienced practices can fall victim, as we have seen in recent months.

Conveyancing company Simplify was hacked last year and its systems were frozen, causing disruption for clients trying to purchase property. Simplify's regulator, the Council for Licensed Conveyancers, has written a blog [https://www.clc-uk.org/the-role-of-the-regulator/] about this, setting out the consequences of a successful attack.

The Law Society of Ireland meanwhile this year told of an incident [https://www.lawsociety.ie/News/News/Stories/cyber-security-alert/?filters=&location=&category=&area=#.Yd2D2GDP1PY] it had been made aware of. This attack began by the solicitor clicking on a link in an unexpected email that was received from a fraudster.

The hacker was able to stalk the inbox and create rules to automatically divert emails from particular clients. The hacker also created a new email address that was very similar to the solicitor's own email address. This allowed them to contact the client directly.

The fraudster was able to identify from previous emails that a number of transactions were about to occur and told the clients to transfer money to their bank account, which the clients did.

Keep yourself safe by looking at our cybercrime pages [https://www.sra.org.uk/solicitors/resources/cybercrime/] which has tips and case studies that you might find useful.