



CASE STUDY – PHISHING SCAM



Fraudster gains access following phishing scam

The scam began in April 2018 when one of our insurers policyholder's employees received an email purporting to be from Microsoft. The email explained that the employee's email account had been suspended, but stated that if they could verify their account details on an attached link, Microsoft would be able to revoke the suspension. The employee clicked on the link which took them to what appeared to be a legitimate-looking webpage with a section for entering their Outlook username and password. Thinking that this was genuinely an email from Microsoft, the employee duly entered their credentials and carried on with their work.

However, unbeknownst to the employee, they had actually provided their log-in details to a fraudster. The law firm had not enabled multi-factor authentication on their employees' email accounts and so the fraudster was able to access this particular staff member's account remotely. This allowed the fraudster to monitor communication to and from the employee and gather information about upcoming transactions, including the identity of the buyers and sellers and their respective real estate agents, the amount of funds to be disbursed and the dates of closing. Having selected a suitably lucrative transaction to target, the fraudster bided their time and waited until the closing day.

Contact us – engage@neuro8.com



Prior to having their email account breached, the firm had been working on a property transaction and was holding the buyer's final payment funds in escrow in readiness for them to be transferred over to the seller on the date of closing. It had

been agreed in advance that the final payment would be made by check and sent via mail to the seller. However, on the actual date of closing, the fraudster used the information they had gathered from the breached email account to hoodwink both our policyholder and the seller's real estate agent.

The fraudster's first step was to impersonate the law firm. They set up an email address that looked very similar to the actual attorney's but they added an additional letter to the address line. So instead of saying @xyzlegal.com, it became @xyzlegall.com. Using this fraudulent email address, they then sent an email to the seller's real estate agent, stating that, as previously agreed, the final payment had been made by check and had been posted by mail that day. As this was in accordance with the plan, this didn't raise any alarm bells with the real estate agent.

The second step involved the fraudster impersonating the seller's real estate agent. Once again, the fraudster set up an email address that looked very similar to the actual real estate agent's email address but added another letter to the address line.

Posing as the seller's real estate agent, the fraudster sent an email to the attorney explaining that they had just spoken with the seller and that there was a change of plan: the seller now wanted the money to be sent by wire rather than check, and attached wire instructions to enable the transfer. To add an air of authenticity, the fraudster also copied the real estate agent's genuine email signature on to the bottom of the email and imitated the real estate agent's writing style, such as the use of the phrase "Best regards" when signing off an email. Assuming that they were genuinely in contact with the seller's real estate agent and because wire transfers are a popular payment method for property closings, the attorney duly transferred over £243,672 to the fraudster's account.

A few days later, the seller explained to their real estate agent that they had still not received their check for the final payment. The real estate agent relayed this to the attorney, and it was only at this point that the attorney realised that something was amiss and that the funds had gone elsewhere. The incident was reported to law enforcement and the bank that the funds had been wired to. But because wire transfers do not put a hold on funds and the recipient can withdraw the funds immediately, it meant that all of the funds transferred had already been siphoned off to offshore accounts and attempts to retrieve the funds were unsuccessful. This unhappy state of affairs meant that there were no funds available to finalise the property transaction, leaving both the buyer and the seller unhappy and the attorney feeling embarrassed for having fallen for such a scam. Thankfully, however, the law firm had purchased cybercrime cover on their cyber policy with CFC and the loss was covered in full, meaning that the property purchase still went ahead successfully

Contact us – engage@neuro8.com