CASE STUDY

Conveyancing Firm Clients Targeted for Funds Transfer Fraud

COMPANY
UK Conveyancing Firm

EMPLOYEES
2-10 employees

KEY COVERAGE
Breach Response

Phishing often leads to funds transfer fraud and the earlier we catch it, the more likely we can help to recover any stolen funds.

A staff member of a conveyancing firm fell victim to social engineering through a phishing email they received from a client and as a result, a threat actor gained access to their Microsoft Office 365 account and changed settings. The threat actor set up a number of auto-deletion and auto-forwarding rules in the email account. At the same time, they also set up a spoof email address, impersonating the firm. The firm became aware of the incident when a client claimed to have paid an invoice but the firm had not received the funds.

Legal and forensic experts from Coalition Incident Response[1] were engaged quickly to assist the conveyancing firm with the investigation. It was discovered that the threat actor had communicated with 17 clients in total.

All 17 clients were contacted promptly. In total, only two fell victim to the impersonation fraud from the threat actor. The policyholder also had legal obligations to notify the ICO and Council for Licensed Conveyancers. Legal experts assisted with this.

The investigation found that the threat actor was observing communications in the mailbox and intercepting client communications at the appropriate time using the spoof email address to trick clients into thinking that the policyholder's bank details had changed. Any replies that might alert the account owner to the deception were auto-deleted by the rule that had been set up by the threat actor.

Coalition Claims quickly engaged legal and forensic assistance. We worked with the experts and the conveyancing firm to investigate quickly, and helped their clients recover their money from the respective banks.

Lessons Learned: Phishing is often just the beginning

Even if a firm has the capability to investigate a phishing attack internally, it's always worth notifying Coalition Claims immediately. Phishing often leads to funds transfer fraud and the earlier we catch it, the more likely we can help to recover any stolen funds.

1. Breach response included the engagement of an incident response firm; the insured selected Coalition's affiliate, Coalition Incident Response via firm panel.

The claim scenarios described here are intended to show the types of situations that may result in claims. These scenarios should not be compared to any other claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law

The descriptions contained in this communication are for preliminary informational purposes only. Coalition is a trading name of Coalition Risk Solutions Ltd. which is an appointed representative of Davies MGA Services Limited, a company authorised and regulated by the Financial Conduct Authority (FCA), registration number 597301, to carry on insurance distribution activities. You may check this on the FCA register by visiting the FCA website www.fca.org.uk. Coalition Risk Solutions Ltd. is registered in England and Wales: company number 13036309. Registered office: 34-36 Lime Street, London, United Kingdom, EC3M 7AT. Copyright ©2023. All rights reserved. Coalition and the Coalition logo are trademarks of Coalition, Inc.