COALITION CYBER CASE STUDY

Racing against the clock to recover $1.3M from a phishing attack

In late January 2020, attackers compromised the email account of a nonprofit's Finance Director. Four months passed as the attackers searched the policyholder's mailboxes for terms related to finance, banking account information, payment, and funds requests. Next, the attackers set up rules to move a series of legitimate emails from the policyholder's inbox to their junk folder.

The attacker spoofed the nonprofit's legitimate domain, set up email rules to divert replies, and sent compromised attachments. They sent an email to six people facilitating two very large fund transfers of roughly $620,000 each — totaling nearly $1.3 million. The subject line was 'Change banking service,' citing COVID-19 as the reason.

Shortly after the payments were made, employees received emails requesting gift cards. Additionally, the policyholder did not receive the proper confirmation of funds received. The policyholder quickly realized an event had occurred and reached out to the Coalition Incident Response (CIR). CIR sprung into action, changed the passwords of the compromised account, and forced a global password reset.

Coalition's Claims team coordinated with law enforcement to file a report and stop the funds from being transferred. CIR also put in a takedown request to remove the fraudulent domain, preventing the policyholder from receiving additional fraudulent emails from that domain. Due to our swift response, we managed to claw back all of the money except $500.

Coalition brings together active monitoring, incident response, and comprehensive insurance to solve cyber risk.

INDUSTRY

Early childhood education

EMPLOYEES

1-25

COMPANY

- Funds transfer fraud
- Breach response

RESOLUTION

Shortly after the payments were made, employees received emails requesting gift cards. Additionally, the policyholder did not receive the proper confirmation of funds received that they were familiar with. They knew something was wrong.