CASE STUDY

Cyber Claims Triggered by Phishing Attacks

Phishing attacks are often the gateway for threat actors to commit lucrative cyber crimes. Coalition Claims data shows that in 2022, 76% of our claims began with a phishing attack — which underscores that any organization of any size can be phished.

Let's look at three examples of recent claims that began with a phishing attack before the threat actors pivoted to monetize their crimes. We'll explore how organizations of varying industries were compromised, then recommend four easy steps businesses can take to respond to these attacks.

The case of the 'trusted' charity vendor

A fund management company received two wire transfer requests from a charity vendor with whom they regularly work — one for $2.5M and another for $1M. However, the charity's email had been compromised, and the instructions for the wire transfer were fraudulent. The policyholder unknowingly routed $3.5M in payments to the threat actor's bank account. Thankfully, the insured notified Coalition promptly, allowing us to go beyond simply paying out the claim to work with law enforcement to claw back $2.5M of the stolen funds. The sublimit on their Funds Transfer Fraud (FTF) coverage[1] paid $250,000 to the policyholder.

The case of the stolen W-2 forms

The HR department of a utility company was contacted by their Chief Financial Officer (CFO) to share employee W-2 tax forms. When the CFO began filing his taxes, he was notified they'd already been filed. A threat actor had compromised the CFO's email via phishing and impersonated him to get the employee documents. The threat actor was able to file other people's taxes to cash out on the returns. While the policy covered notification costs, forensics, and attorneys fees, it did not cover individual employees' stolen tax returns. The impacted employees had to work directly with the IRS to receive the tax return amounts owed to them.

The case of seven fraudulent transactions

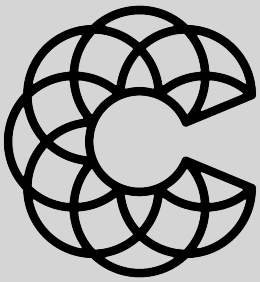
A loan provider fell victim to a phishing email, leading to business email compromise (BEC). The BEC resulted in their accountants sending seven fraudulent transactions totaling approximately $3M. When the policyholder attempted to implement multi-factor authentication (MFA), they discovered a threat actor had already done it. Unfortunately, because the last fraudulent transaction occurred two months before the reported claim, Coalition could not recover any of the stolen funds. Ultimately, the policyholder's coverage kicked in and their losses were partially covered, but they still experienced significant losses.

How every business can help prevent phishing attacks

In each of these cases, MFA could have helped reduce the likelihood of a claim — whether implemented on email, bank accounts, or other possible access points. Additionally, policyholders that are able to notify Coalition soon after experiencing an incident can often reduce the cost and impact of a claim. Here are four simple steps to keep in mind to help prevent phishing attacks:

1. Turn on MFA for all accounts. MFA provides an additional layer of protection that would prevent **95% of the claims Coalition sees**.
2. Exercise caution when clicking links or responding to urgent requests. Threat actors want victims to overlook cybersecurity best practices and make hasty decisions in the hopes that their requests go unquestioned.
3. Trust, but verify, all wire instructions. If it appears the payment instructions have been altered, always confirm by calling the individual. Call the requestor using a known good phone number — not a number included in the email — to confirm they sent a link or attachment.
4. Use an email security product, such as **Armorblox** or **Material Security**. These tools help flag and quarantine suspicious emails so they're less likely to land in your inbox in the first place.

Get more familiar with how to spot phishing emails that could slip through the cracks by reviewing our phishing checklist.



Coalition®

COALITIONINC.COM

COALITION INSURANCE SOLUTIONS, INC.

44 MONTGOMERY STREET, SUITE 4210, SAN FRANCISCO, CA 94104

HELP@COALITIONINC.COM