CEO Fraud: Are You Next?

Here's how your worst day starts. You call your newest finance director to check how they're settling in. The conversation is positive until they mention, "I transferred the two million like you asked."

With a sinking feeling, you realize you may be the victim of CEO fraud.

Also known as Business Email Compromise, CEO fraud is rising at an alarming rate. By spoofing emails and impersonating executives or suppliers, these criminals trick people into sharing data or making a large wire transfer. According to the FBI, US victims have lost a total of $960 million to these criminals over the last 3 years – and there's been a 1,300 percent increase in reported incidents since January. CEO Fraud is expected to be even more costly than Ransomware.

Those numbers should give any leader pause. And so should this one: only 4 percent of funds are ever retrieved. Usually the fraud isn't detected in time for recoupment, with most transfers successfully reaching criminal hands in China and Hong Kong.

Companies both large and small are targeted, and both fall for the scams. Aerospace company FACC lost around $54 million to CEO fraud in January 2016; SS&C Technologies Holdings, a financial services software firm, was fleeced for $5.9 million; hard drive manufacturer Seagate inadvertently shared the personal information of 10,000 existing and former employees that was used to file fraudulent tax returns.

Anatomy of Fraud

Most CEO fraud begins with that ever-popular criminal standby: the phishing email. A typical scam might use the right email address and correct logo to pose as a trusted bank, supplier, IRS official or C-suite leader. Often the criminals will mine details from LinkedIn, Facebook and other sites to demonstrated detailed knowledge of the company workings. Sometimes they even access the network months beforehand, observing habits and protocols to more accurately impersonate the right executive or authority. By appearing as plausible as possible, these emails often convince even savvy employees to transfer a large sum of money or share sensitive data.

"But no one falls for phishing emails anymore," you might be thinking. The Verizon Data Breach Investigations Report says differently: 23 percent of recipients open phishing messages and 11 percent click on attachments, according to their findings.

The targets range from HR and IT teams to C-level leaders and anyone with finance approval. The actual techniques vary. Sometimes an email will mimic a long-standing wire-transfer relationship with a supplier, but ask for the funds to be sent to a different account. Or they might hack an employee's email account to invoice company suppliers, with payments transferred to bogus accounts. Accountants and HR staff might be asked to send employee information or W-2 forms to a new email address.

Because the requests seem legitimate and justified, the fraud is rarely discovered soon enough to be stopped. And it's not just the money stolen that impacts the company. Several lawsuits have been filed on behalf of employees angry that their workplace did not protect their data with stronger security.

Stopping Scams with Education

While there is always a chance of an employee or leader falling for a convincing email, certain preventive steps can go a long way toward deflecting these attempts.

Step 1. Think about your high-risk users: senior leaders, HR staff or financial personnel. Anyone who has the power to share money or data falls into this category. Check how much information is available about them online, especially job duties and contacts from other teams and companies. Then evaluate how easy it would be to impersonate them by email.

Step 2. Implement security controls, like email filtering, two-factor authentication, access and identity controls, and permission levels. Adopt whitelists or blacklists for external traffic. These won't completely block phishing emails, but they'll eliminate quite a few.

Step 3. Create policies and procedures that can catch hasty mistakes. A strict wire transfer policy requiring multiple authorizations, time delays and identity verification can all go a long way toward preventing disaster and loss. Register as many domains as you can that are just slightly different from the actual company domain. Implement domain spoof protection and create detection system rules that flag any e-mails using extensions similar to company e-mail.

Step 4. Train your staff to look for red flags. While most phishing emails are well-architected, small tells are usually present, such as grammatical errors and odd wording. Often the company name will be altered slightly. Another warning sign: the request for an expedited turnaround. Criminals want your staff to act quickly, before they can realize something is wrong. If an email repeatedly mentions an "urgent wire transfer" or an "urgent invoice payment" and includes "new account information" or other "new" accounts and changes, it's a sign of a scam.

If you do discover a fraudulent transfer of funds or data, act quickly. Your first move: contacting your bank. Provide as many details as possible to see if they can stop or even recall the transfer. After that you'll want to contact law enforcement, starting with the FBI office. Sometimes they can work with the U.S. Department of Treasury Financial Crimes Enforcement Network to return or freeze your funds. You should also contact your insurance company to see if your policy covers this kind of attack.

Finally, your IT team will need to look inward and do damage control. That means closing off the attack vendor, recovering hacked email accounts, and eradicating malware. Don't hesitate to bring in outside security specialists; they likely have experience in these kinds of attacks and can suggest new techniques for strengthening your security controls.

Given its lucrative nature, CEO Fraud isn't going away any time soon. Criminals will continue to phish for your data and financial assets as long as technology exists. But by educating your workforce and leadership, you can boost your security and avoid becoming the catch of the day.