FBI ALERT: Business Email Compromise Causes $1.2 Billion Damage

The FBI came out with hard numbers showing how big this new Business Email Compromise (BEC) cyber-crime wave really is. It's also known as "CEO Fraud" and has cost organizations a whopping 1.2 billion dollars over the last year.

New Wave of Cybercrime: Case Study from CyberheistNews.

A reader recently shared an email that was sent to their comptroller, which by all accounts was a near-perfect social engineering attempt. However, awareness training, combined with full executive support to question any suspect request, prevented what could’ve been a massive financial hit to the organization. The email, which was addressed to the comptroller from an account that (at a glance) belongs to the CEO, is itself similar to prior communications she had gotten from him.

The email mirrors the organization's Outlook template, uses the CEO's image, even the clip and tone of the message itself looks normal. There are spelling errors, and formatting issues, but again these are expected in quick communications and rather common during day-to-day operations. The message sent to the comptroller, complete with errors, is as follows:

In regards to an Acquisition that we are currently working on, Attorney Richard Spink will be getting in contact with you. If you can please devote your full attention and comply with any requests that he makes. We will need to proceed with several payments in regards to this operation. He will further explain to you how to execute the wire instructions following the regulations in place.

Over the last few months, we have been working on it under the supervision of the SEC. It is crucial for the company that this operation is executed swiftly and efficiently.

You have my full approval to proceed with any payments that he may request on my behalf. You need to keep this matter extremely confidential as you are the only one currently aware of the situation.

You will need to maintain absolute discretion and work exclusively with Richard.

Any question you may have must be addressed directly to him.

We will be going public with the acquisition next week and the rest of the company will be made aware. I will personally meet with you and Richard a couple of days prior and expect to be fully updated on your progress.

Thank you for treating this with your utmost attention.

Best regards.

This is where the entire Phishing / SE attempt failed.
It almost worked. The comptroller was set to comply with instructions, but there was something off about the email; a little thing really – but it stood out. It was signed using the CEO’s full name. The CEO never uses his real name, always the shortened version of it – i.e. Dick instead of Richard.

Awareness training is a constant within the reader’s organization. No matter what, employees are encouraged to report anything and everything if they have even the slightest bit of doubt.

As such, anyone within the organization is allowed to ignore an executive's request and report it to the security team for verification. In this case, because the organization has ties to a number of critical markets and industries, a scam such as this could be disastrous.

Because the name was different, the comptroller felt the request should be verified and flagged. It was the right call. For the record, this wasn’t a training email. It was a real attack, and it was nearly successful. The only thing that prevented it was awareness and encouragement.

The attack presented here happened within the last 30-days. It’s possible other firms working in and around the financial industry have gotten similar messages, so the reader felt that sounding the alarm and sharing this incident with the public was worthwhile."