Risk Insights

Provided by:
Brady, Chapman, Holland & Associates

The Fake President Fraud

The "fake president fraud" is a type of scam in which a criminal posing as a company executive convinces an employee to voluntarily transfer a large sum of money directly to the criminal's account. It may be hard to imagine that any of your employees would authorize a wire transfer to an unknown account, but law enforcement officials have seen a marked rise in the occurrence of this scam over the past several years.

What's especially dangerous about this particular type of fraud is that many companies — even those with both crime and cyber policies — might **not** be covered unless they have a social engineering fraud endorsement on their crime policy. Read on to better understand how the scam works and what you and your employees can do to mitigate the risks.

UNDERSTANDING SOCIAL ENGINEERING

The scam's success relies on criminals using something called "social engineering." Social engineering refers to tactics that exploit common psychological weaknesses and preconceived notions about authority and social relationships to make people engage in certain behaviors. Often, that means exploiting patterns of behavior that are automatic and subconscious, so that victims might not even realize what they've done until after the fact.

Because social engineering relies on exploiting your employees' assumptions and subconscious thought patterns, it can be hard to recognize unless someone points it out. That's why the best way to defend your organization is to learn how a scam works and educate your employees about it.

HOW DOES THE FAKE PRESIDENT FRAUD WORK?

The fake president fraud may vary in some of its details, but it always contains four major elements. Learning how to recognize them is the first step in combating the threat.

1. The "president" makes contact. Someone posing as a high-level executive in the company — often the president, CEO or CFO — will reach out to the target employee. This contact often occurs via email, either from a domain that is deceptively similar to the company's actual domain, or via a "personal account."

2. The "president" asks for a wire transfer. The "president" asks the employee to wire a large sum of money to a foreign bank account. The employee might be told that the money is for a host of seemingly legitimate purposes (recent acquisitions, paying off debts, paying vendors, etc.).

3. The "president" pressures compliance. At this point, many employees may question the unusual request or the break in typical company protocol. That's when the "president" deploys psychological pressure on the employee to accept the scenario as genuine and comply with the request. Those pressures can rely on a number of different factors, including the following:

a. Authority: The criminal will emphasize his or her rank to convince the employee. This offers the criminal many options, such as using that authority to intimidate the employee or preying upon the employee's desires to impress a superior.

b. Time pressure: Criminals will often claim that the transfer is an urgent matter, forcing the employee to ignore typical protocol and eliminate the chance that he or she might disclose the transfer to another party or verify the information before making the transfer.

c. Secrecy: Often deployed in conjunction with time pressure, the "president" may emphasize that this deal must remain secret for strategic or legal reasons. Having the employee "in" on the secret can make him or her feel special and thereby increase the chance that the transfer will go through.

4. The employee makes the transfer. The employee contacts the bank, and the bank then makes the transfer. Even if it is unusual, the bank will transfer the funds to the account if the employee making the request is authorized to do so.

Risk Insights

Provided by:
Brady, Chapman, Holland & Associates

WHY THIS SCAM IS NOT COVERED BY A CYBER POLICY

This scam bears similarities to certain cyber scams, like spear phishing. Insofar as both kinds of scams involve sending emails targeted to specific employees, the tactics are similar. However, there are some crucial differences.

Spear phishing targets an employee in order to convince him or her to open an email or click a link, which downloads malicious code onto the employee's computer and allows the criminal to access the company's network. With phishing scams, the crime is an **unauthorized data breach**, and, as such, the exposure would be addressed by a cyber policy.

By contrast, in the fake president fraud, the employee willingly authorizes a wire transfer to the criminal's bank account. Even though the crime was initiated via email, the fundamental criminal act is **fraud**, not data breach, and **will not** be covered by a cyber policy.

The FBI reports that the average business email scam costs a company between $25,000 and $75,000 —totaling nearly a billion dollars in losses each year.

MITIGATING RISKS

There are a number of things companies can do to reduce the risk of falling victim to such a scam. These include the following.

- Educate Employees. It's essential that all employees — especially those who are authorized to make wire transfers — are aware of the scam and how it works. Ultimately, this scam works by preying on a number of psychological blind spots, including ignorance. Combat that by making your employees aware of the risk and diligent about company procedure.
- Demand Adherence to Protocols. Your company should have protocols for authorizing the transfer of funds. Reinforce the importance of adhering to these protocols.
- Verify Identities. This can be especially important if employees have infrequent contact with C-suite executives or if requests are frequently made remotely. Establish guidelines for independent means of verification if requests fall outside of established protocols or if timelines must be accelerated.

MAKE SURE YOU'RE COVERED

Insurance solutions for the fake president fraud are available, but they often come in the form of a specific endorsement on a crime policy. For more information on coverage solutions to the fake president fraud, contact your partner at Brady, Chapman, Holland & Associates today.

bch | BRADY, CHAPMAN, HOLLAND & ASSOCIATES
When it Matters.