The Monthly Security Awareness Newsletter for Everyone

OUCH!

IN THIS ISSUE...

- What Is CEO Fraud?
- Protecting Yourself

CEO Fraud

What Is CEO Fraud?

Cyber criminals are sneaky—they are constantly coming up with new ways to get what they want. One of their most effective methods is to target people like you. While cyber attackers have learned that unaware people are the weakest link in any organization, they have forgotten that knowledgeable people like OUCH! readers can be an organization's best defense.

Guest Editor

Angela Pappas is a director of information security training and awareness at Thomson Reuters. In her role, Angela is responsible for the ambassador program, eLearning, and educating employees about topics that pose a significant risk.

Cyber criminals have developed a new attack called CEO Fraud, also known as Business Email Compromise (BEC). In these attacks, a cyber criminal pretends to be a CEO or other senior executive from your organization. The criminals send an email to staff members like yourself that try to trick you into doing something you should not do. These types of attacks are extremely effective because the cyber criminals do their research. They search your organization's website for information, such as where it is located, who your executives are, and other organizations you work with. The cyber criminals then learn everything they can about your coworkers on sites like LinkedIn, Facebook, or Twitter. Once they know your organization's structure, they begin to research and target specific employees. They pick their targets based on their specific goals. If the cyber criminals are looking for money, they may target staff in the accounts payable department. If they are looking for tax information, they may target human resources. If they want access to database servers, they could target someone in IT.

Once they determine what they want and whom they will target, they begin crafting their attack. Most often, they use spear phishing. Phishing is when an attacker sends an email to millions of people with the goal of tricking them into doing something, for example, opening an infected attachment or visiting a malicious website. Spear phishing is similar to phishing; however, instead of sending a generic email to millions of people, they send a custom email targeting a very

CEO Fraud

small, select number of people. These spear phishing emails are extremely realistic looking and hard to detect. They often appear to come from someone you know or work with, such as a fellow employee or perhaps even your boss. The emails may use the same jargon your coworkers use; they may use your organization's logo or even the official signature of an executive. These emails often create a tremendous sense of urgency, demanding you take immediate action and not tell anyone. The cyber criminal's goal is to rush you into making a mistake. Here are three common scenarios:

CEO Fraud is a powerful attack that can bypass most of our security defenses. Ultimately, you are our best defense.

- Wire Transfer: A cyber criminal is after money. This means they research and learn who works in accounts payable or the team that handles your organization's finances. The criminals then craft and send an email pretending to be the targets' boss; the email tells them there is an emergency and money has to be transferred right away to a certain account.

- Tax Fraud: Cyber criminals want to steal information about your coworkers so they can impersonate employees for tax fraud. They research your organization and determine who handles employee information, for example, someone in human resources. From there, the cyber criminals send fake emails pretending to be a senior executive or someone from legal, demanding certain documents be provided immediately.

- Attorney Impersonation: Not all CEO Fraud attacks involve just email; other methods like the telephone can be used. In this scenario, criminals start by emailing you pretending to be a senior leader, advising you that an attorney will call about an urgent matter. The criminal then calls you pretending to be the attorney. The criminal creates a tremendous sense of urgency as they talk about time-sensitive, confidential matters. This sense of urgency tricks you into acting right away.

CEO Fraud

Protecting Yourself

So what can you do to protect yourself and your organization? Common sense is your best defense. If you receive a message from your boss or a colleague and it does not sound or feel right, it may be an attack. Clues can include a tremendous sense of urgency, a signature that does not seem right, a certain tone you would never expect, or the name used in the email being different from what the person actually calls you. The attacker may even use an email address or phone number you have never seen before, or an email address that is similar to your coworker's or boss's email. When in doubt, call the person at a trusted phone number or meet them in person (don't reply via email) and confirm if they sent the email. Never bypass security policies or procedures. Your organization may have policies that define proper procedures for authorizing the transfer of funds or the release of confidential information. Requests that attempt to bypass those policies, regardless of their apparent source, should be considered suspicious and be verified before any action is taken. If you receive such a request and are not sure what to do, contact your supervisor, the help desk, or information security team right away.

Tip of the Day

Every day we post a new tip on how to make the most of your time online and how to stay safe. Get your daily security tips at https://www.sans.org/u/iS7.

Resources

Social Engineering:	https://securingthehuman.sans.org/ouch/2014#november2014
Phishing:	https://securingthehuman.sans.org//ouch/2015#december2015
What Is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Two-Step Verification:	https://securingthehuman.sans.org/ouch/2015#september2015
Tip of the Day:	https://www.sans.org/tip-of-the-day

License