Whaling Attacks Present a Larger Challenge for Businesses and Their Owners

May 20, 2016

Technology has made the speed of business lightning quick. iPhones, Androids and mobile devices have decreased response times and increased expectations of responsiveness to communications. File sharing services, the Cloud and other developments have made our lives much easier. Similarly, criminals have become even quicker to develop schemes. Sophisticated Phishing schemes are being executed to acquire sensitive information such as usernames, passwords, credit card details, and sometimes, money. Phishing attacks are designed for criminal purposes, often disguising thieves as trustworthy, powerful individuals authorizing action through electronic communication.

Phishing schemes have become increasingly clever and complicated. A new trend called Whaling Attacks has started to hit businesses and their executives. The tactics used have taken the art of Phishing to a new level. Whaling Attacks are where sophisticated criminals send spoof e-mails that appear to be from an executive within a company. This attack is usually sent to another executive, usually one with decision making power and access to sensitive information. One example had an e-mail seemingly appear from a CEO, informing the CFO to transfer funds for a confidential business deal to a designated account. This scheme allowed the thieves to falsely authorize a transaction and obtain access to company funds.

According to *SC Magazine*, a new security advisory report found that more than 50% of the organizations surveyed showed an increase in Whaling Attacks within the past year. The overwhelming majority of attacks (72%) were disguised as e-mails from key executives who had authorization to conduct significant transactions.

In order to carry out this level of fraud, significant research is conducted, including the utilization of public intelligence to build the company profile. Domains with similar appearance and structure are created to mask the attack. The fraudsters then use that domain name, carefully craft an e-mail, and create something as genuine as possible.

In order to minimize the risk of these attacks, many executives are more closely monitoring their e-mails and double checking domain names and other characteristics from the e-mail.

Additionally, any financial transactions or wire transfers should be utilizing a second form of authorization, like two-factor authentication. A second form of authorization could include something as simple as voice verification or a randomly generated key code.

These attacks will continue to evolve as criminals improve their strategies, heightening the importance of information security and fraud awareness.