January 23, 2020

Keeping Your Money Safe: Corporate Account Takeover

Denise Owens, CFE, SVP, Fraud Department Manager

Businesses and individuals lose billions of dollars every year due to fraud. While PlainsCapital Bank has a seasoned fraud prevention team in place to protect our customers, we understand that the best protection is education. To that end, our Fraud Prevention Series, "Keeping Your Money Safe," highlights the latest fraud scams with helpful tips on how you can avoid them.

In the current landscape of technology-driven commerce, cybersecurity becomes even more important and not just for your personal benefit, but for your business too. Did you know that according to Barracuda's Spear Phishing: Top Threats and Trends Vol. 2 report released in 2019, one in seven organizations studied fell victim to a phishing attack that led to a corporate account takeover?

How Does the Scam Work?

A corporate account takeover is a form of business identity theft where cyber criminals gain control of a business' bank account by stealing employee passwords and other valid credentials. The attackers can then initiate fraudulent wire and ACH transactions to accounts they control.

According to Barracuda's report, 63 percent of phishing attacks used generic messages, such as those discussing an account error or shared document. The attackers then requested access to the account via login credentials.

How to Prevent Corporate Account Takeover

Keep in mind that legitimate organizations and institutions (e.g., your bank, the IRS) will never ask for passwords or confidential information over the phone or through email. Here are several tactics you can employ to recognize and thwart corporate account takeover attempts:

1. Educate your employees. Education is paramount to avoiding these kinds of attacks. By providing security awareness training, either from an internal department or outside consultant, you can teach your employees how to be suspicious of requests for confidential information. This also includes teaching them the art of password protection, i.e., how to create strong passwords, not using the same password for multiple accounts, and not storing a list of passwords on their computer.

It's also important to stress that threats don't just occur at the office. For example, an employee who takes their laptop home and accidentally downloads malware can put the entire business at risk when they return to work and log back in to the network. One simple mistake can lead to a corporate account takeover, so it is essential to educate every employee.

2. Use multi-factor authentication. Multi-factor authentication (MFA) requires the user to present two or more pieces (factors) of evidence to prove who they are (authentication). For example, when employees dealing with sensitive information first log in to a network, MFA will provide an additional layer of security by asking to send a verification code to the user’s email or mobile device. The user must then receive and enter the code before gaining access to the network.

3. Update antivirus software frequently. This is another easy-to-follow security practice for your business that simply requires attentiveness. Unfortunately, the reality is that new viruses and malware are created and deployed on a consistent basis, which means you must be just as consistent in making sure your employees’ computers, servers, and networks are always up-to-date with the latest protection software.

Keeping Your Money Safe

While these practices can greatly reduce the risk of falling victim to a corporate account takeover, there is no end to the attempts perpetrated by cyber criminals. Therefore, it is imperative to stay vigilant and consistently educate your employees about this type of attack. PlainsCapital Bank’s Fraud Department provides educational resources for businesses and customers to help detect and prevent fraud on their accounts. For more information about our fraud prevention efforts, visit our fraud resources page.