Corporate Account Takeover/Business Email Compromise – Things Every Business Owner or Manager Should Know

Keith Hughes, Vice Chairman and CEO

Corporate Account Takeover

Corporate Account Takeover occurs when cyber thieves gain unauthorized access to a business account, often through the theft of online credentials or by hijacking an online session, and initiate transactions, change contact information, and gather information on the account's history to commit other crimes.

Businesses of all types and sizes are attractive targets for cyber criminals as they traditionally carry higher balances than personal accounts. Small to medium sized businesses, however, are often the most at risk as they likely do not have as much to spend on security and often believe that due to their size they are less likely to be targeted. In fact, the opposite has been found to be true – criminals are looking for businesses with lower security and bigger balances.

Employees often serve as entry points into a company's networks by unknowingly providing their access credentials through phishing sites or by downloading malware onto the system after clicking on malicious links or opening infected attachments. Employees and businesses of all sizes are targeted through phishing and other social engineering attacks in order to download and spread malware that will allow unauthorized access to financial accounts and other sensitive information.

Business Email Compromise

Fraudsters also target senior executives in Business Email Compromise scams in order to gain access to the executive's legitimate email account, impersonate them, and direct employees to conduct wire transfers or payment transactions on their behalf.

The key to reducing the risk from this type of scam is to understand the criminals' techniques and deploy effective payment risk mitigation processes such as multiple levels of approvals before wire transfers are approved. Losses associated with these frauds can be substantial and devastating to the business.

The First recommends businesses implement controls to detect, prevent and respond to these types of frauds and to conduct frequent employee training to raise awareness of the potential of this happening.

This article adapted from information provided by the American Bankers Association.