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 retail accounts. Employees often serve as entry points into the 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.

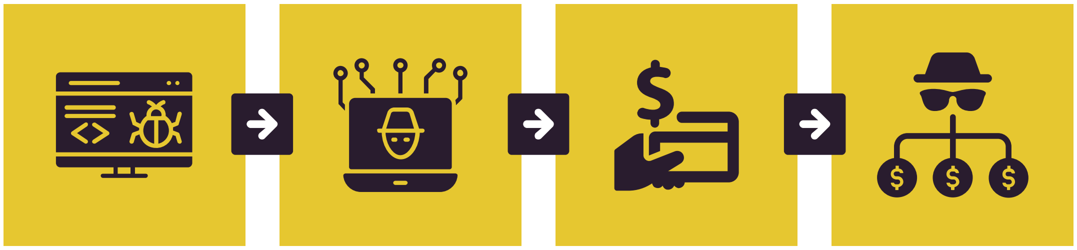
Employees and businesses of all sizes are targeted through phishing and other social engineering attacks in order to download and spread malware that will allow unauthorized access to financial accounts and other sensitive information. Fraudsters also target senior executives in Business Email Compromise 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.

Business Email Compromise

A current scam targeting corporate clients is Business Email Compromise in which a legitimate business email account is compromised through social engineering or computer intrusion techniques to impersonate an executive and conduct the unauthorized transfers of funds. The key to reducing the risk from BEC is to understand the criminals' techniques and deploy effective payment risk mitigation processes. (See the News and Resources section below for more information.)

Losses associated with these frauds can be substantial and devastating to the business. As banks have implemented controls to detect, prevent and respond to these frauds, businesses must do the same. Banks play a significant role in this partnership by educating their corporate clients on the evolving risks, providing them with tips to identify these threats, and ensuring the customers take advantage of security controls offered by the bank to protect them.

As with all defenses of Cybercrime, your best protection is an early prevention strategy and proper training for your employees. The most common methods of BEC rely on misleading tactics and the deception of the message receiver. Most incidents of Business Email Compromise can be evaded by using your email with good judgment and logic of what is being requested/asked by the sender of the message. Some frequent questions you should ask yourself if you ever have doubt on the authenticity of the message:



Cybercriminal compromises employee email

Compromised account is used to send notifications to customers

Payments are transferred to cybercriminal's account

Cybercriminal receives money

- Is the email coming from a trusted sender's proper email address? (the company's approved and trusted email server?
- Would this person ask me for this personal information in a real-time conversation?
- Does the email ask for specific details regarding personal information? (Social Security number, bank routing information, etc.)

We recommend having a regular schedule where your business is constantly re-evaluating their Cybersecurity strategy and approach to preventing Business Email Compromise.

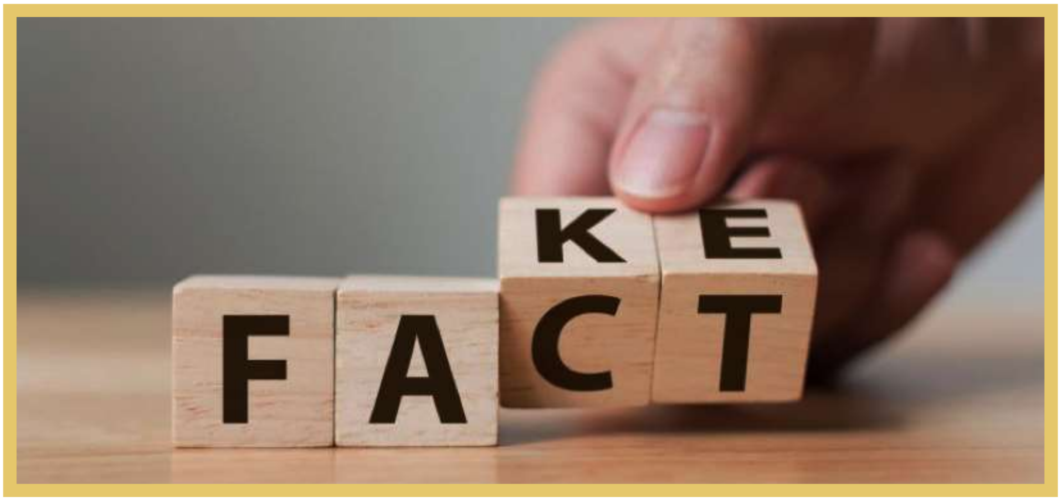
- Verify that all security, scan and anti-virus software is updated and working properly on an ongoing basis.
- Establish a dedicated computer for online banking with no e-mail installed, and no internet surfing allowed by employees.

Managing Access To Online Banking:

- Restricted Access by Employees. No Shared Passwords or Credentials. Set Specific Access Privileges for Every Employee.
- Company Policy on Internet Usage and Privacy.
- Employee Training on Corporate Account Takeover, Annual Training at a Minimum.

Monitoring Accounts:

- Set Up Email Alerts
- Daily Account Reconciliation
- Positive Pay



If you have any additional questions, please contact us at: (844) 626-0262