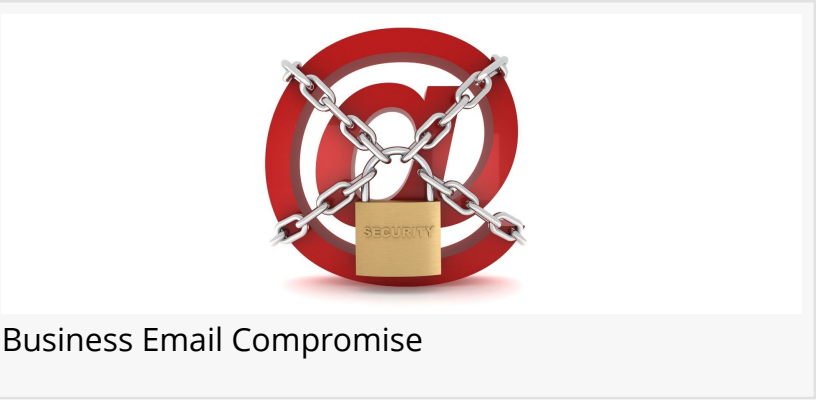
Business Email Compromise: How to Guard Against Cyber-Scams

One out of every three cybersecurity breaches involves a corporate email being compromised due to a phishing attempt.



Business Email Compromise

LONG BEACH, CA, UNITED STATES, September 7, 2021 /EINPresswire.com/ -- According to Verizon's 2019 Data Breach Investigations Report, one out of every three cybersecurity breaches involves a corporate email being compromised due to a phishing attempt. The statistics are alarming and make it essential for businesses to emphasize cybersecurity to protect their business and assets. Read on to learn about Business Email Compromise (BEC) and how it may affect you.

Understanding Business Email Compromise

Business Email Compromise is an online scam that targets organizations that execute wire transfers and have international suppliers. Executive or high-level employee email accounts related to finance wire transfer payments are compromised using phishing assaults to make fraudulent transfers, resulting in hundreds of thousands of dollars in losses.

A phishing attack occurs when a fraudster poses as a trustworthy institution and contacts you via email or other social media platforms in order to obtain your personal information, login credentials, credit card number, or bank account information. This social engineering scheme has evolved into a lethal weapon known as Business Email Compromise or Email Account Compromise (EAC).

Types of BEC Scams

Subject lines in several business email compromise examples include words and phrases like request, payment, transfer, and urgent. The FBI has identified five types of BEC scams:

CEO Fraud: Attackers impersonate the company's CEO or any other executive and send an email

to finance personnel requesting transactions to an account they control.

Bogus Invoice Scheme: Companies with international suppliers are frequently attacked with this strategy, in which attackers pose as suppliers and seek fund transfers to a fraudulent account.

Account Compromise: A hacker gains access to an executive or employee's email account and uses it to send invoice payments to vendors mentioned in their email contacts. The funds are subsequently transferred to bogus bank accounts.

Data Theft: In this attack, HR and bookkeeping employees are targeted to get personally identifiable information (PII) or tax returns of employees and executives. This information could be exploited in future assaults.

Attorney Impersonation: Attackers impersonate a lawyer or a law firm member who is reportedly in charge of sensitive and confidential information and makes a request for unauthorized payments. Such fake requests are usually made via email or phone at the end of the business day.

Unlike traditional phishing or spam emails, BEC communications rarely contain clickable links or files to download. Traditional solutions cannot detect these scams because they do not contain any dangerous links or attachments.

However, employee education and awareness can aid businesses in detecting this form of fraud. Furthermore, an investment in cybersecurity services can help mitigate risk and its effects.

How BEC Works?

Fraudsters employ a variety of tactics to send these emails as part of their impersonation, including one or more of the following:

Domain Spoofing: An attacker will impersonate a colleague or a trustworthy vendor's display name and sender address in an email to make it appear as if it originated from a colleague or a trusted vendor. This technique is known as domain spoofing.

Compromised Accounts: An attacker could hack an account or gain access to an employee's username and password in any other way to send a compromising email.

Lookalike Domains: To confuse the receiver, the attacker sends emails from domains that seem similar to the actual domain name, such as "abc@amazon.com" may be duped as "abc@amaz0n.com." Another technique is to use a combination of two or more letters in place of a single letter to confuse the receiver, such as duping "abc@company.com" as "abc@cornpany.com".

Formulating a BEC Response Plan

In the event of a BEC attack, it is crucial to assess the scale of the attack to minimize the damage. The BEC reaction plan must begin with a simultaneous study of concurrent procedures, including legal, financial, business continuity, and forensics.

A combination of automated procedures, artificial intelligence (AI) tools and expert analysis should be used to determine the source of the attack, examine the logs, collect information, and examine personal and protected files and data for security flaws.

It is also essential to have a contingency plan in place. Here are some elements to consider when formulating a plan to tackle any unwanted situation.

Intimation: Planning ahead and informing team members of their duties is important. It is vital to know who will oversee key tasks, including containment, recovery, and reporting to the appropriate authorities.

Timing: When an attack occurs, timing is everything. You will need a timeframe to trigger various steps, such as informing all stakeholders, top management, federal agencies, and employees, among others.

Action Plan: Take action by isolating the compromised email or account. It can include changing passwords, alerting employees or relevant teams, creating a backup account, and other measures.

Timeframe: It entails the estimated time it will take to recuperate or return to normal.

Protect Your Business against BEC and other Cyberattacks with Windes

With business email compromise scams on the rise, Windes can help you assess risks, manage cyber security issues, and respond to attacks.

The key to dealing with a Business Email Compromise is to act quickly to optimize recovery time. The Windes cybersecurity team can assist you in formalizing a rapid and successful reaction plan. This is a critical parameter when reporting a BEC incident to the IRS or FBI.

In the event of a scam, we will also provide experienced guidance to help you develop an immediate, short-term, and mid-term reaction strategy. Our professionals will not only provide legally appropriate documentation but will also assist you in implementing damage mitigation strategies.

Our experts can also help you choose security and infrastructure-strengthening tools and resolve disputes with law enforcement and insurance companies. Connect with us today to learn

more about our services or get a free cyber health check.

Connect With Windes
Windes
+1 844-494-6337
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
