Clearedin

Preventing BEC Phishing Attacks

Table of Contents

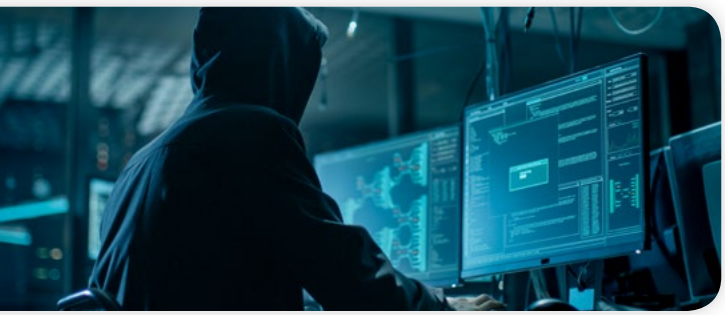
Pay no attention to the man behind the curtain.

While this famous line from The Wizard of Oz predates phishing by about 55 years, it could very well be used to describe this act of online deception. Today, hackers operate behind their own curtain, pretending to be someone else in what is known as a Business Email Compromise (BEC) attack. A BEC, sometimes called Email Account Compromise (EAC) is a sophisticated type of phishing scam that looks like it's coming from a trusted business contact (either internal or external). The attack leverages the innate trust in that relationship to trigger activities such as wire transfers, credential theft, or getting sensitive financial data or other PII (Personally Identifiable Information).

136%

increase in BEC attacks between December 2016 and May 2018.

According to the FBI, between October 2013 and May 2018, BEC was responsible for 41,058 fraud complaints from U.S. victims, totaling more than $2.9 billion in exposed dollar loss. Even more alarming, BEC attacks show no signs of slowing down; the FBI reports that there has been a 136% increase in BEC attacks between December 2016 and May 2018. In addition, 83% of organizations say that they experienced a phishing attack just last year—that's up from 76% the previous year.



Common BEC Attacks & Tactics

BEC attacks continue to evolve and become more sophisticated; when people catch on to one type of BEC, hackers move on to another technique. Here are some of the most common BEC attacks today and how they are carried out by criminals.

Business Executive Impersonation

Hackers will spoof or compromise the email accounts of top business executives, often members of the C-suite. They'll then email lower-level employees with an urgent request for a wire transfer to a fraudulent account (sometimes in the form of gift cards).

Data and W-2 Theft

Using a compromised high-level executive's email account, criminals request personal information from lower-level employees that have access to it, and who are unlikely to question their "authority."

Real Estate Transaction Interception

During the course of a real estate transaction, hackers impersonate someone involved in the transaction, such as a realtor, title company, or law firm, and request that the buyer wire funds into a fraudulent account.

Invoice Scam

This method of BEC is as simple as it sounds; criminals send phony invoices, usually from a vendor a company does business with, and requests immediate payment to a fraudulent account.

Supply Chain Transaction Interception

During a pending business deal, transaction, or invoice payment, hackers will impersonate someone involved and request a redirection of funds into a fraudulent account.

Legal Transaction Interception

Criminals learn about trust accounts or litigation and impersonate a law firm's principal or client. They then request the firm to transfer money into a fraudulent account.

Account Takeover

BEC goes from bad to worse in the form of an Account Takeover (ATO). Many of the attack methods in the section above are successful because they employ ATO tactics. Rather than simply spoofing an email account—which some savvy recipients may be able to spot—ATO is when the hacker is able to actually access someone's real account and email others inside or outside of the organization from this trusted, legitimate address. Attackers have numerous methods for gaining access to credentials, such as installing malware, password cracking, buying credentials on the dark web, and even plain old "shoulder surfing," in which they hover behind the user and watch them type in their password.

Examples of Real-World BEC Attacks

While discussing the various types of BEC attacks is useful and builds awareness of the threats, it helps to see some real-world examples to better understand exactly how the attacks go down.

FACC

Austrian aerospace parts manufacturer FACC was duped out of $61 million in a business executive impersonation scam. The hacker posed as the company CEO and phished an entry-level accounting employee, convincing him to transfer the funds into a fraudulent account for a fictitious project. This case is notable for another reason: the company is actually suing the CEO and CFO to recoup losses, stating that the two leaders failed to adequately protect the company from BEC attacks.

Google and Facebook

Between 2013 and 2015, lone cybercriminal Evaldas Rimasauskas executed an invoice scam, posing as Taiwan-based Quanta Computer—a company that Google and Facebook both work with—and sent fake invoices to employees involved in conducting transactions requesting payment to fraudulent accounts in Cypress and Latvia. Invoices appeared to be be signed by top executives of the company, further legitimizing them. It worked, and Rimasauskas conned the two tech giants out of more than $100 million before being caught. It goes to show you that if employees at multi-billion dollar tech companies can be duped, it can happen to anyone.

O'Neill Bragg & Staffin

BEC attacks don't just happen to the big guys, and in this legal transaction interception scam they targeted Pennsylvania-based law firm O'Neill Bragg & Staffin. Hackers accessed the principal's email account and requested that a member of the firm transfer more than a half-million dollars from their Interest on Lawyer Trust Account to the Bank of China, "on behalf of a client." The ruse worked, and the money was transferred. The firm took Bank of America to court, claiming they were responsible for the damage for not protecting them, but the case was dismissed and O'Neill Bragg & Staffin is now permanently closed.

How to Identify BEC Phishing Attacks

Why do BEC attacks continue to proliferate? Because they're hard to identify (and nearly impossible if they're an ATO). However, there are a few tactics for spotting phishing emails.

Check the sender's address (not just their name)

Spoofed email accounts will have a very similar address to the legitimate account so they aren't easily spotted. However, a keen eye will notice that:

- Jim@Company-ABDC inverted a letter to appear as Jim@Company-ABCD
- Jim@Company_ABCD used an underscore to appear as Jim@ABCD-Company
- Jirn@Company-ABCD used an "r" and an "n" to look like the "m" in "Jim"

Scrutinize the subject line

Many BEC subject lines are similar in nature. Here are some to watch out for (and variations of these, as well):

- Payment - Important
- Payment Notice
- Process Payment
- Quick Request
- Fund Payment Reminder
- Wire Transfer Request
- Bank Transfer Enquiry
- Confirmation of Receipt

Beware of urgency

Hackers want to get their victims to act fast, so they'll often say that the need is immediate or urgent. This makes the recipient feel that there's no time to confirm the request with a phone call or a response email (plus, a response email is likely to go right back to the hacker, who will confirm the request).

Look for typos

Although hackers have improved their spelling and grammatical errors considerably over the years, which used to be a telltale sign, it's still something to take notice of.

How to Avoid BEC Phishing Attacks

Avoiding BEC phishing attacks requires putting thought into the actions taken following receipt of anything suspicious. Here are some good avoidance techniques that you can use.

Contact the sender via email

If you choose to adopt this process, the recipient of any requests shouldn't just hit "reply," as it will simply go back to the spoofer. Instead, recipients need to write a new mail asking if the request was legitimate. Of course, in the event of an ATO, this method can fail as, again, the response will go to the attacker.

Contact the sender via phone

This may be awkward, especially for lower level employees reaching out to someone in the C-suite, but it's much safer than emailing due to the possibility of an ATO. And think about it: would you rather the company lose hundreds of thousands or even millions of dollars, or the CEO lose a minute out of their day?

Navigate by typing the URL instead of clicking to get to websites

If employees receive any suspicious links asking for payment, they should always go directly to the site rather than log in from a link. For example, if an invoice comes in from a vendor, go to that vendor's website and view the company account to see if payment is really due.

Watch social media posts

BEC criminals do their homework, and they may watch what someone is posting on social media sites for weeks or even months before they make their move. For example, if someone posts about an upcoming vacation, hackers will pose as that person claiming urgency because "they're about to get on a long flight".

Set restrictions on transactions

How many people need to be able to authorize transactions over a certain amount? Limit or eliminate transaction abilities among most employees, and consider having only one or two employees who are extremely well-versed in BEC phishing be allowed to authorize costly transactions.

How to Recover from a BEC Attack

"We can't expect users to remain vigilant all the time…" says Kate R of the National Cyber Security Center. "Being aware of the threat from phishes whilst at your desk is hard enough. But phishing can happen anywhere and anytime, and people respond to emails on their phones and tablets, and outside core hours. Clicks happen."

If you've been the victim of a BEC attack, here are seven steps you can take.

1

Alert the FBI

This is especially critical to aid in financial recovery if the attack involved the transfer of funds. You can file a complaint with their Internet Crime Complaint Center at www.IC3.gov.

2

Scan devices

Run tests on the victim's devices to check for malware. BEC phishing doesn't always involve malware, but it's frequently how attackers compromise credentials and monitor your network for higher value fraud opportunities. If malware is discovered, you should quarantine and analyze the device and then re-image it to a clean state.

3

Check for spread

There's a good chance the victim may have inadvertently compromised someone else's device, so check their sent email folder and the server to determine who they've emailed and potentially compromised. Because hackers are savvy enough to delete items from the Sent folder, also scan emails received from the compromised account during the window of exposure.

4

Stop the spread

Quarantine all others who the victim may have compromised.

5

Analyze the threat

There may be little forensic evidence left behind, but IT experts may be able to find something that can help determine where the attack originated and how it was executed in order to prevent future attacks.

6

Educate employees

Implement cybersecurity awareness training programs now to help prevent another attack. These should be ongoing to keep BEC phishing top-of-mind and make sure employees at every level attend.

7

Develop security solutions

If not already in place, it's important to implement email and security solutions to reduce the likelihood of a future attack. This may include the creation and roll-out of computer use policies, adoption of multi-factor authentication (MFA), email password protocols, and other security measures.

Types of Anti-Phishing Solutions

Despite your best efforts, you may not be able to prevent a BEC attack on your own. After all, the average email user receives 67 spam emails per month, many of which are phishing attempts. Even if there's just 10 employees, that's 670 opportunities for hackers to be successful every month. Here are some of the ways to protect yourself.

Email provider protection

Google and Microsoft have recently boosted their anti-phishing solutions, so many companies rely on them for protection. However, G-Suite and Office 365 are far from foolproof. For example, Microsoft's Advanced Threat Protection (ATP) only applies to incoming mail, and both providers largely ignore file sharing, messaging, and other outlets for malicious phishing attacks.

Security gateways

Anti-phishing companies such as Mimecast or Proofpoint require emails to be routed through their servers. That means only incoming email is checked, leaving outgoing emails and employee-to-employee emails unscanned. This puts organizations and those they work with in danger as a hacker may employ an ATO strategy and the phishing email will appear as a legitimate.

Natural Language Processing (NLP)

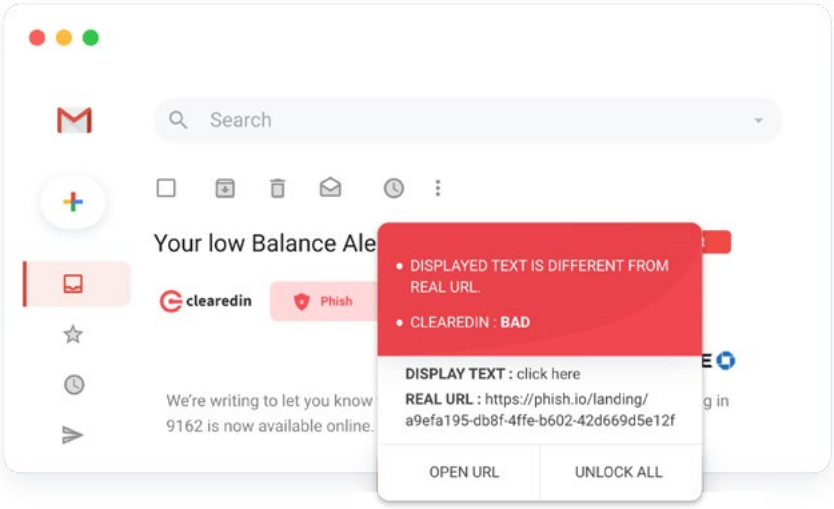
This anti-phishing strategy creates profiles based on the way people communicate. For example, some people use particular phrases often, or may have a sophisticated vocabulary; others always use emoticons and texting abbreviations. NLP quarantines any email that deviates from the profile, considering it an attack. One challenge with this approach is that people communicate differently based on who they're writing to; an email to an executive may look very different than an email to a colleague.

Training

Offered by anti-phishing software companies such as KnowBe4, Cofense, and Wombat, training programs involve ongoing e-learning courses and videos, and essentially rely on education to build a "human firewall"; but despite the best training, humans make mistakes and on its own this isn't a solid protection plan.

Simulations

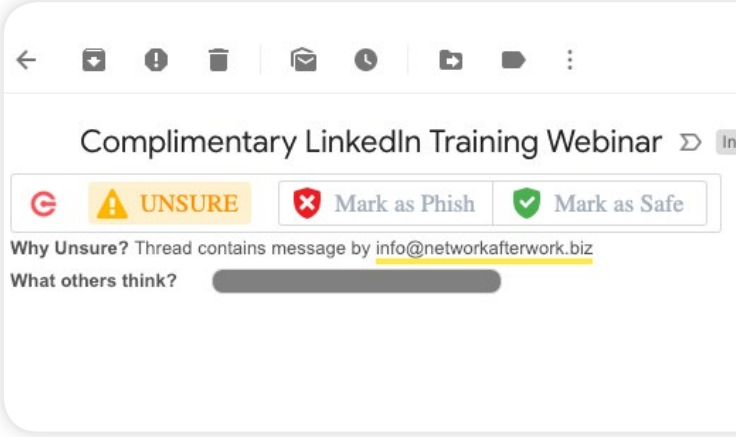
Known as "phishing your own employees," this more sophisticated means of anti-phishing training involves sending simulations of phishing emails to employees to see if they'll take the bait. If they do, the IT team will be notified and the employee may be reprimanded or even terminated if they are a repeat offender.



Active Defense

The most comprehensive anti-phishing solution, which detects both BEC and ATO attacks, is an active defense system such as Clearedin. Clearedin is a Cloud Communications Security platform that analyzes company communications over multiple platforms—as well as messaging channels such as Slack—and uses machine learning to develop a Trust Graph–a living digital model of an organization's communications patterns.

As new messages come in, ClearedIn validates them against this Trust Graph based on the normal flow and frequency of past communications. It also checks embedded links and analyzes email addresses for spoofing attempts. When phishing scams are detected, an active defense system will flag the email as phish, and recipients will be informed as to why the email was flagged (displayed text is different from the URL, sender belongs to an unsecure domain, email address is questionable, etc.) Until they've marked the email as safe, they cannot forward it or reply to it.



SCHEDULE A DEMO

Learn more about Clearedin anti-phishing software for Business Email Compromise and Account Takeover

REQUEST A DEMO