



Criminal Business Email Compromise: Are You Prepared?

Aggressive Cybercriminals Are Sophisticated; Security,
IT and Finance Teams Must Be Too



EMAIL US AT
info@vendorinfo.com

www.vendorinfo.com



Criminal Business Email Compromise: Are You Prepared?

Aggressive Cybercriminals Are Sophisticated; Security,
IT and Finance Teams Must Be Too

Table of Contents

Table of Contents.....	2
Introduction	3
The Most Financially Costly of Internet Crimes.....	3
What Is BEC?.....	4
BEC Techniques	6
The Defense	7
Guidelines for the Organization:.....	8
Conclusion	8





Introduction

People receive more than 120 emails at work per day on average. That's a lot of emails. So, we categorize and strategize our email activity. But when we see an email from the boss, we tend to open it. And cybercriminals count on that normal behavior to carry out business email compromise (BEC) schemes.

BEC has been on the rise over the last five years, attacking businesses, nonprofits and government. Among the prime targets are executive officers and individuals responsible for making payments or accessing sensitive information.

BEC emails are a confidence game. They appear to be from a known source making a legitimate request. The apparent source might be the company CEO, a business partner or a reliable vendor. An unsuspecting recipient is disposed to comply with the request, only to discover the deception later.

Technologically, email is among the oldest tools on the internet. But, as practical as it is, it was never designed to be particularly private or secure. Along with the technology, another dimension of the BEC problem is people. People are susceptible to being fooled.

These days, the email threat is no longer likely to be from an earnest if syntactically challenged Nigerian Prince needing your help to get millions of dollars out of his country. Instead, it's likely an instruction from your CEO to wire money to an account or from your vendor instructing you to change their bank account information.

The Most Financially Costly of Internet Crimes

BEC is costly and growing. The FBI calls BEC the most financially costly of online crimes. The FBI put the known cost of BEC in 2020 at \$1.8 billion. That is just what organizations have reported to the FBI's Internet Crime Complaint Center (IC3). And despite the alarming threat posed by ransomware attacks, FBI figures show that the cost of BEC dwarfs that of ransomware attacks.¹

Research and advisory firm Gartner reported that in 2019 BEC increased 100 percent. The threat is

¹ The FBI acknowledges gaps in the costs attributed to ransomware, but the current estimate of BEC cost is 64 times that of the calculated ransomware costs. See [the FBI Internet Crime Report 2020](#).



Case 1 – NONPROFIT VICTIM

In 2018, an authorized wire transfer originator for a nonprofit business initiated a \$28,000 transfer from its bank to another bank. The nonprofit's bank received and verified all appropriate documentation and conducted out-of-band authentication per bank policy to an authorized person other than the wire transfer originator to verify the request's legitimacy.

The nonprofit executive director had approved the wire request based on an email he believed was from his colleague, who also was an authorized account signer. Later in the afternoon, however, the executive director contacted the bank to report that the wire transfer request was fraudulent and that he shouldn't have approved it. They had discovered an imposter had sent the email requesting the wire transfer. While reviewing the emails after the incident, the executive director noticed several grammatical errors that might have served as a warning sign.



considerable. And the criminals are agile. For example, they quickly exploited the urgency and chaos of 2020 as the pandemic drove the shift to remote work, often on personal computer equipment. Gartner reported an increase in reports of coronavirus-related business email compromise (BEC) and phishing scams, as well as credential theft attacks. But even apart from the pandemic, BEC has been on the rise.

What Is BEC?

Gartner describes BEC as a dangerous combination of low-tech tools and high-quality skills. BEC criminals are sophisticated and patient. They take time to research and gather information on their targets before emailing them. The BEC scam targets businesses, nonprofits and government—that is, organizations rather than individuals. In particular, it targets those

responsible for wire and other payments. Email account compromise (EAC) is a similar threat to individuals but on a smaller scale. BEC is much more lucrative.

A BEC attack looks like an email from a known source making a legitimate request. It may appear to be from a regular vendor requesting you to update their mailing address or banking information. Or it might appear to be from your CEO, instructing you to make an urgent wire payment or to purchase a batch of gift cards for rewards and send all the numbers to the CEO. That “action” email comes after some preliminary work by the fraudster that could be months in the making.

In many cases, BEC involves email hijacking and credential theft through spoofing or spear-phishing, through which the criminals take control of critical email accounts, such as the CEO’s. Or they may hack the company’s attorney or a key vendor. One variation is a hack at a vendor’s



Case 2 – BUSINESS VICTIM

The president of a company received a phishing email from a criminal that harvested his credentials. The criminal then sent an email to a contact in the president’s address book, including an email to the company’s bank, for a wire transfer request for \$148,500.00 to a receiver with which the business had no prior payment history or documented business relationship.

A bank representative replied that the bank needed a completed wire transfer request form and sent a blank form via secure email. However, the criminal could not open the secure email and asked the bank representative to fax wire instructions. The criminal then instructed the bank to send the \$148,500.00 to an account at another bank. When the bank performed an “out-of-band authentication” – a phone call back to the client’s phone number on the bank’s records, the fraud attempt was uncovered and stopped – the business lost no funds, thanks to internal bank controls.

Upon reviewing the situation, the company’s IT department discovered that the domain name of the fraudulent email used was misspelled by only one character, closely simulating the company’s domain name.



to set up BEC attacks against the vendor's large customers. They can do this while remaining "invisible" to the account owner by adjusting email settings.

Not all BEC involves hacking into emails. Sometimes a BEC attack is simply a spoofed email—an email that appears to be from a familiar or legitimate source but masks the actual sender. Spoofs work because of effective deception, called "social engineering." Sometimes, in one out of many attempts, a payables manager or staffer is fooled into acting because the email looks legitimate, and the request seems ordinary.

But the more sophisticated BECs hack into email accounts, resulting in access to email threads and presenting two issues. The first is that sensitive information included in emails (including attachments) is compromised. Hackers can capture tax identification numbers, birthdates and other information used in identity theft, and they can capture financial details, including bank account numbers. These threads contain considerable intelligence.

The second issue is access to "intelligence" regarding the organization's relationship, interactions and transactions with vendors and customers. Reviewing historical emails and monitoring ongoing traffic, the



Case 3 – NONPROFIT VICTIM #2

A nonprofit organization paid out \$650,000, which equates to 26 percent of its annual revenue, in what the organization thought was legitimate project payments. When the executive director spoke to the contractor, she expected confirmation that things were underway. But the contractor had not received any of the payments made—only an email from the nonprofit the previous month stating that it had to delay payment.

The three payments had gone elsewhere. The bookkeeper, a third-party serving the nonprofit, was the initial victim of business email compromise (BEC). Once the hackers had gotten into the bookkeeper's email system, they infiltrated existing email chains. Then they gathered the information needed to imitate the parties and redirect payments.

They intercepted an email from the contracting company with an invoice to the executive director. The criminals sent the "payment delay" email to the contracting company posing as the executive director. Then they resent the legitimate invoice to the director, but this time altering wire-transfer instructions for the payment. In the next few weeks, they emailed two more phony invoices modeled on the legitimate one.

Based on these three payable invoices from the contractor, the executive director made three wire transfers totaling \$650,000. All appeared normal. According to the director, there was not any poor grammar, strange language, or unusual expressions. Everything was as expected. It was not until her conversation directly with the contract group that she realized there was a problem.



criminal learns the nature of relationships, tone of communication and timing of transactional events.

Consequently, they know just when to email a particular kind of request, for example, a payment address change. Criminals know just how to address their “contact.” The perpetrators know when to send a spoofed invoice—they might even resend an actual captured vendor invoice following a “bank change” notice. Once the perpetrator gets inside an email account, the tremendous amount of information allows them to produce persuasive email messages.

BEC Techniques

Masking

Masking is a simple technique that inserts a legitimate name or email address in the display setting, so an email appears to be from a known source. But if you hover over the “from” name or email address, you can uncover the actual email address. The same thing is possible with URLs. When an email presents a link—often just a graphic, which may be an official logo or another site graphic of the legitimate organization—if you pause and hover over it without clicking, the actual URL should appear at the bottom of your screen. The actual URL shown will be unrecognizable.

Whether emails or URLs, everyone should check them carefully before clicking. A complicating factor is that a legitimate URL may be hard to decipher due to email tracking codes because the link goes through the legitimate sender’s email marketing program, which tells the legitimate sender that you clicked the link. When in doubt, don’t click the link; open a browser and key in the correct URL.

Spoofing

Another technique is spoofing. The scammer’s email or URL has slight variations from a legitimate organization’s email or URL that go undetected. For

example, an email might be from johnnagel@company.com rather than johnnagle@company.com. Or a website like www.hackemgrp.com might be spoofed as www.hackerngrp.com. Depending on the font, an “r” next to an “n” might look very much like an “m.”

Masking and spoofing are techniques that perpetrators might initially use to obtain secure information. Or a spoof email might constitute the primary line of attack. For example, the criminal might spoof your bank, citing a security breach or positing some other premise and direct you to log on—via the link in the email—to sort it out. If the recipient does so, they’ve just given away their username and password to the bank account. A spoof might urge the recipient to click a link or download a “requested” document. The result of a click is the download and installation of malicious software.

Email Compromise

Sophisticated schemes hack into email systems and operate from within them. The hacker can adjust settings to make themselves undetectable. So, how do they break in? Getting into many email accounts is not difficult for professionals. To begin with, the user ID is simple. Most are simply the email address itself, and companies typically have a straightforward email name protocol, such as first-initial-last-name@company-name.com. So, the ID is easily guessed for a particular person, whether the CFO or the vendor master file or ACH specialist.

Next, the hacker needs the password. Because of some people’s low tolerance for frustration or laziness, their passwords are easy to discover. Every year a password “hall of shame” is published on the internet. Year after year, many people still use such passwords as “12345678,” “password,” or “11111111.” Other simple passwords incorporate the current year with a first name, or a favorite sports team, ditto a favorite curse word. Or the person spells their name or company name, substituting look-alike numerals for letters—the hackers are way ahead of them.



Such passwords offer no protection. Never mind that people post passwords on sticky notes on a computer screen or openly share them, which can leak out. Another common problem is using the same password across several applications and sites, rendering each of those applications and sites vulnerable.

Phishing Variations

Phishing is requesting or demanding information under pretense via email. Variations on phishing include vishing, smishing and pharming. They involve unsolicited email, text messages or telephone calls

purportedly from a legitimate organization requesting login credentials. One ex-scammer says to get passwords, he sometimes just called someone in the company and asked. Do not underestimate the social engineering skills of criminals. They can be persuasive.

The Defense

Organizations must recognize the risks. And they must devise and carry out training. Training should include C-suite executives, who may be smart but are also prime targets. The record of incidents shows they are



Case 4 – CITY VICTIM

Scammers posing as a construction company doing business with the city of Ocala, FL, got a city employee to change information that eventually resulted in a \$742,376.73 payment to a fraudulent bank account. According to reports, a city accounting specialist received an email purportedly from an accountant at a construction company working for the city. The email included a city form requesting they change the contractor's banking information. The document provided a bank routing and account number and a copy of a voided check from the account.

A month later, the construction company submitted a legitimate invoice related to the construction of a new terminal at the Ocala International Airport, part of a \$6.1 million project.

The city paid the invoice, but the payment went to the fraudulent bank account. A few days later, city personnel discovered the fraud after the contractor said it had not received the payment.

The representative from the construction company, whose name was attached to the phony email, had not sent the email. Furthermore, upon closer examination, the email address showed a slight difference from the legitimate email address—it included an extra "s" at the end.

The Ocala director of finance told investigators it was unclear how the scammers gained access to the vendor numbers and other information necessary to perpetrate the scheme.



susceptible. Employees should be alert to schemes. In training, include preventative strategies and reactive steps to take in case the company becomes a victim.

Practical guidelines for individuals include:

- ✔ Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members and your birthday, you can give a scammer all the information they need to guess your password and answer your security questions.
- ✔ Don't click on anything in an unsolicited email or text message asking you to update or verify account information. Instead, look up the company's phone number in your records, don't use the one a potential scammer is providing. Then, call the company directly to ask if the request is legitimate.
- ✔ Carefully examine the email address, URL and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust.
 - Ensure the URL in emails is associated with the business that appears to have sent it.
 - Be alert to hyperlinks that may contain misspellings of the actual domain name.
 - Hover over links to see the actual email address or URL.
- ✔ Be careful what you download, never open an email attachment from someone you don't know, and be wary of email attachments forwarded to you.
- ✔ Do not supply login credentials or personally identifiable information (PII) in response to any emails.
- ✔ Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it.
- ✔ Verify payment and purchase requests in person if possible or call the person to make sure it

is legitimate. Verify any change in an account number or payment procedures independently with the person making the request.

- ✔ Be especially wary if the requestor is pressing you to act quickly.

Guidelines for the Organization:

- ✔ Use and require secondary channels or two-factor authentication to verify requests for changes in account information.
- ✔ Monitor financial accounts frequently for irregularities, such as missing deposits.
- ✔ Keep all software patches on and all systems updated.
- ✔ Ensure the settings on employees' computers are enabled to allow a view of full email extensions.
- ✔ Avoid using email to send or receive sensitive information; do not leave sensitive information sitting on email servers.

Conclusion

To protect against BEC, cultivate awareness. Develop and conduct fraud prevention training. Create an alert culture that reaches everyone, from the CEO to new hires. Refresh the training periodically. Do not underestimate the criminals. Some may give themselves away with poor grammar, but many others and their schemes are sophisticated.

Do not use email to transmit, request or receive sensitive information such as vendor information forms, W-9 or W-8 forms or banking forms. Doing so puts that information at risk. Instead, collect sensitive information via a secure portal.

Protect your organization, your vendors and customers from BEC.



Financial Operations Networks
2100 RiverEdge Parkway, Suite 1010
Atlanta, GA 30328
P: (678) 894-4600

