proofpoint.

E-BOOK

The Business Email Compromise (BEC) Handbook

A Six-Step Plan for Stopping Payment Redirection, Supplier Invoicing Fraud and Gift Card Scams

Today's Costliest Cybersecurity Threat—With No Simple Solution

Someone emails the finance department of a parts supplier owned by one of the world's largest automakers asking for a $37 million wire payment. Though large by most standards, the transfer is a normal business transaction for the global company. But this time, the request didn't come from a vendor, business partner or executive. It came from an attacker pretending to be someone else—one of the largest-ever documented examples of business email compromise (BEC).[1]

The 2020 Internet Crime Report from the FBI's Internet Crime Complaint Center (IC3) says that last year's "internet crime spree" included about $1.8 billion in losses for the victims of email fraud schemes.

In Arizona, a businessman sends an email to his colleague to let her know the company will be doing business with a new vendor, RS Enterprise. The businessman is too busy traveling and can't set up the $157,000 payment that's been promised to the vendor. So, helpfully, he provides all the details his colleague needs to send the money. More than 350 people in Arizona received emails with similar instructions—messages that appeared to come from a vendor or another familiar business associate. And the senders? They were cyber criminals who collected more than $30 million, according to the Federal Bureau of Investigation (FBI).[2]

A man sends a plaintive email, telling the recipient he's self-isolating because he has COVID-19 symptoms. He's distressed because in his haste to quarantine, he forgot to bring his mobile phone and other essential items with him. So, he asks the recipient if they would please purchase $250 worth of iTunes or Walmart gift cards. He also asks them to take a picture of the cards

1 Nicole Lindsey (*CPO Magazine*). "Toyota Subsidiary Loses $37 Million Due to BEC" September 2019.

2 Susan Campbell (*azfamily.com*). "Arizona workers lost $30 million to work email scams, FBI says." April 2021.

and their codes, so that he can use them to buy the necessary daily essentials while he's in isolation.[3]

A costly trend

These stories are all recent examples of BEC fraud attacks. And they are only three out of many thousands carried out since the beginning of 2020, targeting users and businesses in the U.S. In fact, 2020 was an especially productive year for cyber criminals, who took full advantage of the pandemic-related disruption and people's heightened dependence on technology during the crisis.

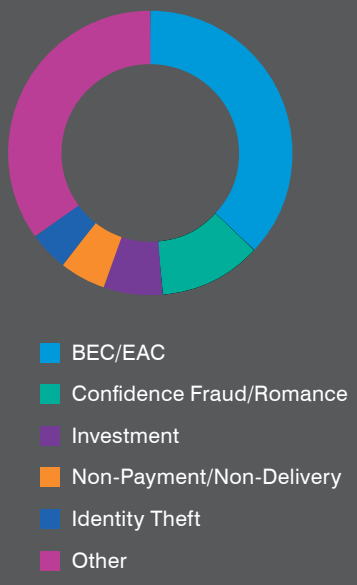
Standing out among all that nefarious activity are BEC attacks, which have proved to be the costliest for victims. The 2020 Internet Crime Report from the FBI's Internet Crime Complaint Center (IC3) says that last year's "internet crime spree" included about $1.8 billion in losses for the victims of email fraud schemes.[4] That represents close to half (44%) of all the business and consumer losses due to cyber crime reported last year, according to the report.

The $1.8 billion figure is also 64 times greater than the financial losses attributed to the wave of ransomware campaigns cyber criminals carried out in 2020.[5] The amount of financial loss is even more impressive when you consider that only 19,369 of the record 791,790 complaints the IC3 received from cyber-crime victims in 2020 related to email fraud scams. That's just 2.4% of all complaints.

The good news: with the right insight, approach and action, these threats can be managed. This e-book explains how BEC attacks work, what forms they take and how you can avoid being the next headline-grabbing example.

Reported BEC Losses

Share of Total Reported Cyber Crime Losses



Source: FBI

3 "Lance Whitney (*TechRepublic*). "Scammers exploit coronavirus for Business Email Compromise campaigns." April 2020.

4 FBI. "2020 Internet Crime Report." March 2021.

5 Sara Pan (*Proofpoint*). "FBI Internet Crime Report Shows that Email Fraud Represents the Largest Financial Losses in 2020." March 24.

Table of Contents

Why are BEC fraud attacks so successful?

The short answer: These attacks are hard to detect and highly persuasive.

BEC relies heavily on social engineering techniques to deceive victims and abuse their trust. That means messages don't usually include malware or malicious URLs that standard cybersecurity protections—including legacy tools, point products and native cloud platform defenses—can block or catch and analyze.

Also, BEC attacks tend to be highly targeted. Bad actors may send only a few messages to select users in an attack. The low volume of messages helps the attacker stay under the radar of many security tools.

Strategies for deception: impersonation techniques

Cyber criminals also use different techniques for setting up and executing BEC attacks. Identity deception tactics are core to BEC, for example, because the attacker needs the recipient to believe that the email instructions are legitimate.

Fraudsters often research organizations to identify their targets—a process that involves determining, usually through public resources like LinkedIn, which people in an organization have access to critical data, systems and resources—and who they work with and trust. Next, they will likely employ one or more of the following strategies to initiate their BEC fraud attack. (Most BEC attacks, in fact, use multiple impostor tactics.)

Display-name spoofing

Attackers will use the name of company executives, attorneys, business partners, suppliers, or any other person or entity a user might trust in the "From" field of an email message. That field is typically the easiest email identifier for fraudsters to manipulate. Most BEC attacks use display-name spoofing alongside other spoofing methods, like domain spoofing (see below).

Domain spoofing

This phishing scam involves attackers hijacking a company's brand in their effort to steal money or data through a BEC attack. They will use an exact match of a company's trusted domain(s) to send their fraudulent emails. Cyber criminals may go so far as to create a fake website at a spoofed web address, mimicking an organization's branding to convince users they're interacting with a legitimate entity.

Lookalike domains

Another impersonation technique attackers use is registering a domain that looks confusingly similar to the target company's trusted domain. For example, a malicious actor aiming to dupe users who work at or do business with "greatcompany.com" might register a domain like "great-company.com" or "greattcompany.com" and then send fraudulent emails using that lookalike domain. The fake domain is so close to the true domain that few users notice the difference—until it's too late.

Account compromise and takeover

Call it the ultimate impersonation technique. When attackers compromise the account of a trusted sender, they have access to that person's email history, contacts and calendar. In other words, they have all the information and access they need to impersonate the person who owns that account. In a sense, they aren't just pretending to be the user—for all practical purposes, they *are* the user.

Invasion of the body snatchers: how accounts are compromised

Credential phishing

This strategy for compromise has existed for decades and is designed to lure users into divulging confidential account credentials. For example, a targeted user might receive an email that looks like it came from their company's IT department—perhaps even showing "Help Desk" in the "From" field—asking them to click a link to validate their login information for a business application.

Brute-force password attacks

This is another approach to taking over a user's account that's been around for a long time. Essentially, malicious actors keep trying to guess a user's login info until they manage to "muscle" their way into an account. It's aggressive, but also often effective and quick because many people still use easy-to-crack username and password combinations. So, it remains a go-to method for many attackers.

Cloud app OAuth tokens

An open authentication (OAuth) app integrates with a cloud service and may be provided by a vendor other than the cloud service provider. These apps add business features and user-interface enhancements to cloud services such as Microsoft 365 and Google Workspace. Most OAuth apps request permission to access and manage user information and data and sign into other cloud apps on the user's behalf.

Given the broad permissions they can have, OAuth apps are a growing attack surface and vector. Malicious actors will use third-party add-ons and social engineering schemes to trick users into granting access to their company's cloud apps via token-based authentication. And once an OAuth token is authorized, access continues until it's manually revoked.

Malware

Some attackers rely on malware to get the information they need to access and take over a user's account. Common malware types used in account takeover include:

- Keyloggers, which capture a user's typing, including login credentials
- Information stealers or "info stealers," which, as their name suggests, steal data like contact information and browser passwords

The dollar loss associated with payroll diversion soared 815% between January 1, 2018, and June 30, 2019.[6]

—FBI

Three Types of BEC Attacks

Once an attacker has all the information in place to launch a BEC attack, they'll typically carry out one of the following three types of attacks:

Payroll diversion or payment redirection

With this attack method, cyber criminals are literally asking, "Send me the money."

In a **payroll diversion** scheme, the attacker, by either impersonating employees or using their compromised accounts to "be" them, aims to redirect legitimate payroll payments from employees' bank accounts to their account.

And in a **payment redirect** scam, the cyber criminal may pose as an external sender, such as a supplier, asking the company's representatives to deposit an invoice payment to a different bank account than usual (that is, the attacker's account).

6 FBI. "Business Email Compromise: The $26 Billion Scam." September 2019.

Payroll diversion and payroll redirect attacks may be straightforward in their purpose, but they aren't so simple for malicious actors to carry out. For one, they require a fair amount of intelligence gathering from the outset. The attack must correctly identify someone in a company's human resources (HR) or payroll department—information that can be gathered from publicly available resources such as LinkedIn, the company's website and commercial databases.

And there's another tricky step for fraudsters. Payroll diversion and payment redirect attempts must also demonstrate credible familiarity with an organization's payroll or invoice payment process, so that they appear legitimate and won't raise a target's suspicion.

How payroll diversion and payment redirection attacks work

1. Attacker contacts HR or payroll

An attacker impersonating an employee contacts the organization's HR or payroll department via email, asking to update their direct deposit information. (The new routing and account numbers belong to the attacker, not the employee being impersonated.)

2. HR or payroll changes account

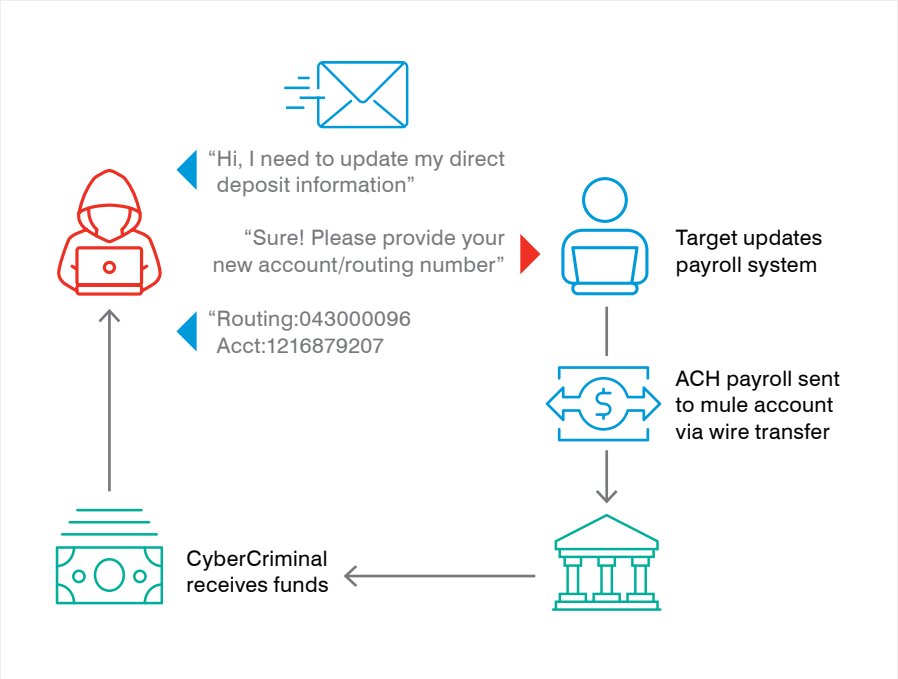
The HR or payroll department, believing the request is legitimate, changes the account information.

3. Paycheck is sent

The employee's next paycheck is sent to the attacker's account.

4. Attacker withdraws money

The attacker withdraws the money and closes the account before the employee notices they haven't received their paycheck.



Gift card scams

Say you received an email from your boss, asking you to purchase a few gift cards from a popular retailer. She tells you that she plans to give these gift cards to team members as rewards for working so hard on a recent project. And since you're all working remotely, she asks if you'd please send the gift card codes as well, just to make it easy for people to use them.

Would you question that request, or fulfill it without thinking twice? If you'd do the latter, you definitely wouldn't be alone—and sadly, you'd be scammed.

According to the Federal Trade Commission (FTC), since 2018, consumers have reported spending nearly $245 million on gift cards that they used to pay cyber criminals for a wide variety of scams.[7] And the Better Business Bureau (BBB) reports that more than one-third (35%) of business impostor scams, which include BEC attacks, involve fraudsters asking victims for gift cards.[8]

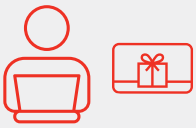
But why do attackers want victims to send them gift cards? Because it's a quick and easy payoff. No complicated wire transfer instructions involved—avoiding victims' natural suspicions and organizations' usual fiscal controls.

Plus, gift cards are an ideal tool for money laundering. Fraudsters can use them to buy and resell merchandise or just sell the codes at a discount online. And once the gift cards are redeemed, the money can't be recouped.

How gift card payment attacks work

1. Cybercriminal impersonates employee/friend/CEO

An attacker impersonates a trusted figure in the organization, such as a CEO, and sends an email to a target, such as an executive assistant, requesting the purchase of gift cards. The attacker may imply that the gift cards are giveaways to employees, customers o r vendors. They also instruct the victim to send card numbers and any redemption codes needed to use the cards.



2. Target user acquires giftcard and sends relevant card information

The victim fulfills the request.

3. CyberCriminal receives funds

The attacker cashes out the cards or redeems them for merchandise, which is then resold. Or they may sell the codes directly on the black market

7 FTC. "FTC Data Show Gift Cards Remain Scammers' Favorite Payment Method." December 2010.

8 Better Business Bureau. "BBB Investigation on gift card payment scams: Why do scammers love gift cards?" March 2021.

Over a seven-day study period in early 2021, 98% of organizations were targeted by attacks impersonating or compromising a supplier.

Supplier invoicing fraud

Supplier invoicing fraud is, as it sounds, an attack where a bad actor poses as a vendor, supplier or other business partner to get a company to pay a fake invoice. The fraudster's tactics typically include spoofing the legitimate supplier's email or taking over the email account of one of the supplier's employees.

The supplier invoicing scheme is a rising star among BEC attack types, with a growing number of attackers using the supply chain and partner ecosystem as a threat vector to launch indirect attacks toward target organizations. Consider the following:

- Over a seven-day study period in early 2021, 98% of organizations were targeted by attacks impersonating or compromising a supplier[9]
- Impersonated and compromised suppliers account for one in four phishing emails[10]

Attackers impersonate office supply retailers, web design agencies, marketing firms, cleaning services, caterers, pest control services—you name it. And they can often get away with their impersonation game for a long time because many companies, especially larger organizations, lack visibility into their supply chain. They don't know how many vendors they have, and which ones might pose a risk.

The potential for big payouts

Supplier invoicing fraud often accounts for the largest financial losses among BEC attacks due to the sizeable business-to-business (B2B) payments that can be involved.[11] These scams are highly effective because they "piggyback" on routine business processes, often using the legitimate business email accounts of the vendors or other business partners the victim trusts. Compromised but otherwise legitimate accounts pass undetected through many security controls.

Some extra-bold and crafty attackers even pose as vendors that don't even exist—and still find success. For example, one fraudster and some co-conspirators bilked more than $100 million from Google and Facebook from 2013 to 2015 through a complex supplier invoicing fraud scam. They set up a fake company in Latvia using the name of a real Taiwan-based company that the technology companies did business with. Google and Facebook got lucky in the end, though: the criminals were caught, and the companies reportedly were able to recoup all or most of the money.[12]

9 Sara Pan (*Proofpoint*). "98% of Organizations Received Email Threats from Suppliers: What You Should Know." February 2021.

10 Ibid.

11 Sara Pan (*Proofpoint*). "FBI Internet Crime Report Shows that Email Fraud Represents the Largest Financial Losses in 2020." March 2021.

12 Vanessa Roma (*NPR*). "Man Pleads Guilty to Phishing Scheme That Fleeced Facebook, Google of $100 Million." March 2019.

From: Chris@supplier (compromised supplier account)
To: Jason (target)

External Message
Thanks Connie~

Dear Jason,

Hope you are well.
The following invoices are due or will be due in Apr. And now we haven't received the payment from you side.
Could you please help to arrange the payment in Apr? Thank you.

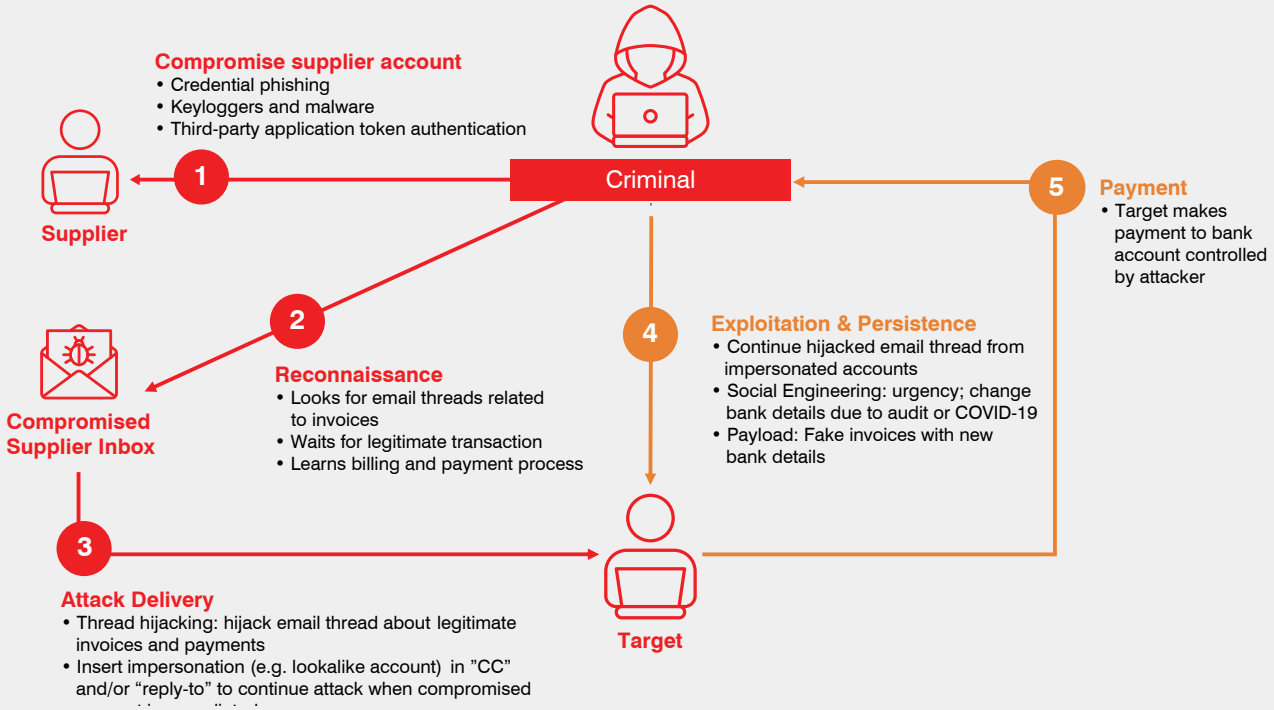
Total amount: USD 2,791,867.92

Class	Number	Amount(USD)	Days Late	Transaction Date	Due Date
Invoice		179,976.49	43	12-26-2019	03-10-2020
Invoice		15,328.07	34	01-04-2020	03-19-2020
Invoice		36,128.50	31	01-07-2020	03-22-2020
Invoice		29,744.80	31	01-07-2020	03-22-2020
Invoice		62,243.65	29	01-09-2020	03-24-2020
Invoice		9,306.72	28	01-10-2020	03-25-2020
Invoice		8,846.00	28	01-10-2020	03-25-2020
Invoice		1,873.20	28	01-10-2020	03-25-2020
Invoice		3,439.44	27	01-11-2020	03-26-2020
Invoice		54,257.82	27	01-11-2020	03-26-2020
Invoice		1,267.58	24	01-14-2020	03-29-2020
Invoice		11,290.40	22	01-16-2020	03-31-2020

Example of an email sent as part of a supplier invoice fraud attempt.

Attackers attempting supplier invoicing fraud might use both impersonation and compromised accounts to steal users' credentials, distribute malware, and, of course, send counterfeit invoices. So while attackers are looking to get paid from these scams, they'll also lay the groundwork for other attacks if they have the time and opportunity.

How supplier invoicing fraud works



1. Malicious actor takes over email account

Supplier invoicing fraud typically starts with a malicious actor taking over the email account of an employee at a trusted supplier or creating a confusingly similar lookalike account.

2. Attacker scans for invoice-related emails

The attacker then scans the contact list in the compromised supplier account and searches the user's inbox for invoice-related emails.

3. Attacker piggybacks on a legitimate transaction

With information about the target organization's billing and payment processes in hand, the attacker waits for the opportunity to piggyback on a legitimate transaction.

4. Attacker replies in an existing email thread

At this point, the attacker typically switches to a domain lookalike account and replies in an existing email thread to maintain access to the legitimate conversation—even if the targeted organization regains control of the account.

5. Attacker sends counterfeit invoice

When the supplier sends an invoice to the targeted organization, the attacker intervenes and sends a counterfeit invoice instead. That invoice includes payment details leading to an account controlled by the attacker and possibly, a request for the target organization to change the existing payment details they have on file.

6. Organization sends payment to the attacker's account

The targeted organization pays the invoice, and the payment is sent to the attacker's account. By the time the real supplier realizes it hasn't received payment, the attacker has withdrawn the funds and closed the account.

Six Steps to Protect Your Organization from BEC Attacks

Cyber criminals use multiple tactics and combinations of impersonation and account compromise in email fraud attacks. And every attack is different. One critical factor common to every BEC attack, though, is a need to abuse people's trust to be successful.

No single line of defense will be effective at helping to prevent these complex, sophisticated and stealthy attacks. Instead, a multilayered, fully integrated and people-centric approach is required.

Here's a breakdown of six key strategies involved in building that kind of defense:

1. Get visibility into your users' BEC risks

A people-centric approach begins with people, of course. Each person is unique. And so is their value to cyber attackers and thus, the risk they may present to an organization. An infinite combination of three factors—vulnerability, attacks and privilege—comprise a user's overall risk profile.

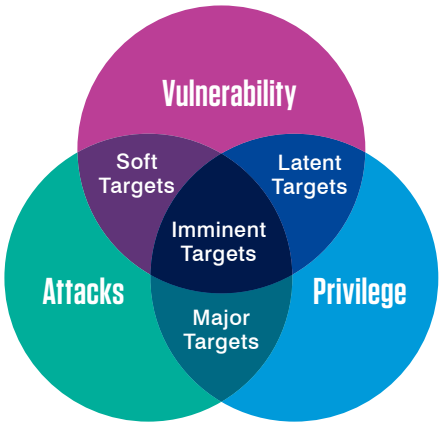
You can determine the risk profile for users in your organization by evaluating:

- **Their digital habits and weak spots (vulnerability).** Consider questions such as: What is a user's role? What are they authorized to do? How do they work? What do they click? How do they access company assets? What kinds of apps and data do they have access to?
- **The types of threats they might face (attacks).** Is the user likely to face a highly targeted attack, like BEC, and therefore in need of more advanced protection and security awareness training? Or would they encounter more garden-variety, commodity-type cyber threats that standard defenses and basic cybersecurity training could help to contain?
- **Their level of access (privilege).** Privilege measures all the potentially valuable things a user has access to, such as data, financial authority and key relationships. Where someone sits in the organizational chart—for example, in the finance department or in the C-suite—is another factor for scoring privilege. But it isn't the only factor, and often not the most important one.

Elevated risk levels in any of these three categories is cause for concern and, in most cases, additional layers of security. When two or more are elevated, it's a signal of a more urgent security issue.

Here are four categories of users that highlight how combinations of vulnerability, attacks and privilege affect your overall risk:

- **Latent targets**: These are high-privilege users who are also more vulnerable to phishing lures.
- **Soft targets**: These users are highly attacked and vulnerable to threats.



ASSESSING USER RISK

Just as people are unique, so is their value to cyber attachers – and risk to employers.

They have distinct **vulnerabilities**, digital habits, and weak spots. They're **attacked** in diverse ways and with varying intensity. And they have different levels of access **privileges** to data, systems and resources.

These intertwined factors determine a user's overall risk.

- **Major targets**: These high-privilege, highly targeted users face a constant barrage of attacks that could cause serious damage to the organization if successful.
- **Imminent targets**: This fourth category contains users who should be treated by the organization as an urgent security priority. They have high levels of all three risk factors: vulnerability, attacks and privilege. In other words, they're susceptible to the tools and tactics of threat actors. They're in attackers' sights. And have access to data, systems and other resources that would cause lasting harm in a successful compromise.

2. Increase supplier-level visibility

Understand who your suppliers are, what domains they're using to send email to your users, who your users typically interact with at those businesses.

Identifying the people in your organization who are more vulnerable, attacked and privileged is a critical step toward preventing BEC attacks. But the supply chain and partner ecosystem are an important threat vector for cyber criminals to launch indirect attacks against targets. That's why you must ensure that you have good visibility into your company's supply chain and understand the risks that some third parties may pose.

Understand who your suppliers are, what domains they're using to send email to your users, who your users typically interact with at those businesses. Also, know who your supplier's suppliers are, to the extent possible. Take the time to create a catalog of vendors that's as detailed as necessary so you can gain visibility into supplier risk.

To make this process easier, look for a solution that can help you automatically:

- Identify who your suppliers are and the domains they're using to send email to your users
- Find lookalikes of supplier domains
- See threats from supplier domains, including impostor, malware, phishing and spam
- Validate suppliers' DMARC records and block attacks that attempt to spoof supplier domains

3. Detect and block BEC threats before they enter

This third recommendation might seem like obvious advice, but keep in mind that not all cyber defenses are effective at detecting and blocking impersonation tactics.

BEC attacks aren't like other cyber threats. That's why stopping them requires advanced solutions and strategies for dynamically analyzing and staying vigilant for potential threats. Static rules-matching detection isn't enough to identify and stop BEC attacks—they just can't keep up with evolving techniques and tactics.

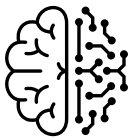
Where to look for signs of BEC

- Message header data
- Sender's IP address
- Sender/recipient relationship
- Sender reputation
- Sentiment, tone and language

Supplier invoice fraud—which usually involves a legitime-but-compromised supplier account—can be even tricker. Your defense must be able to block even the most sophisticated supplier fraud attacks. Look for a solution that dynamically analyzes messages for numerous tactics associated with supplier invoicing fraud.

Supplier invoicing fraud tactics

- Reply-to pivots
- Use of malicious IP addresses
- Use of impersonated supplier domains
- Words or phrases commonly used in supplier fraud attacks



Machine learning tools can adapt to the latest BEC threats without requiring the constant manual tuning that legacy tools need to keep up.

Machine learning

Machine learning tools can adapt to the latest BEC threats without requiring the constant manual tuning that legacy tools need to keep up. The most effective machine learning can react quickly to changes in attackers' tactics, stopping the bad while delivering the good.

But make no mistake: machine learning, in a vacuum, is no magic bullet. ML models are only as effective as the breadth and depth of the data set they're trained on and the human threat expertise that helps fine-tune them. ML models trained with bad or incomplete data and no threat context generate high false positives. That's more work for security and messaging teams and a poor user experience.

4. Make your users more resilient

BEC attacks rely on social engineering, not technical exploits. And they only work when users fall for them. That's why well-trained users are your organization's last—and strongest—line of defense.

All employees should be aware of impostor threats. However, because these attacks are highly targeted toward specific individuals, focus your security awareness training on employees in departments like accounting and finance, HR and procurement, so they're aware of and on the lookout for common deception tactics. Also, make a point to:

- Provide those in high-profile roles in the company, such as the CEO and CFO, with appropriate training.
- Include any other employees who pose a higher risk because they are more vulnerable, attacked or privileged.
- Consider offering security awareness training to third-party contractors and freelancers with access to corporate systems, too. These workers are often a common part of the modern employment landscape—especially in today's even more distributed and remote work environment. But they're often overlooked from a security perspective.
- Address the risk of supplier-invoicing fraud with users most likely to encounter this type of BEC attack.

Security awareness training and other education about BEC fraud attacks shouldn't just be one-time or infrequent exercises, as these threats, like most cyber threats, are constant—and always evolving.

Enlisting help from a third-party resource with expertise in security awareness training can help ensure you deliver the right training to the right people; for example, conducting phishing simulations informed by real-world BEC attacks to train users on the threats they're most likely to face.

Another tip for combating BEC attacks is to encourage users to report suspicious emails—and make it easy for them to do it. Security teams also need to be responsive when a user flags a message—and make a quick determination of whether the email is a threat or not. If they don't get quick (or any) feedback, users may be less inclined to report suspicious messages in the future, and they could become careless about opening or replying to risky emails.

By automating key aspects of email analysis and response, security teams can better prioritize their work and respond to threats and user-reported email more quickly.

5. Automate incident, response and remediation

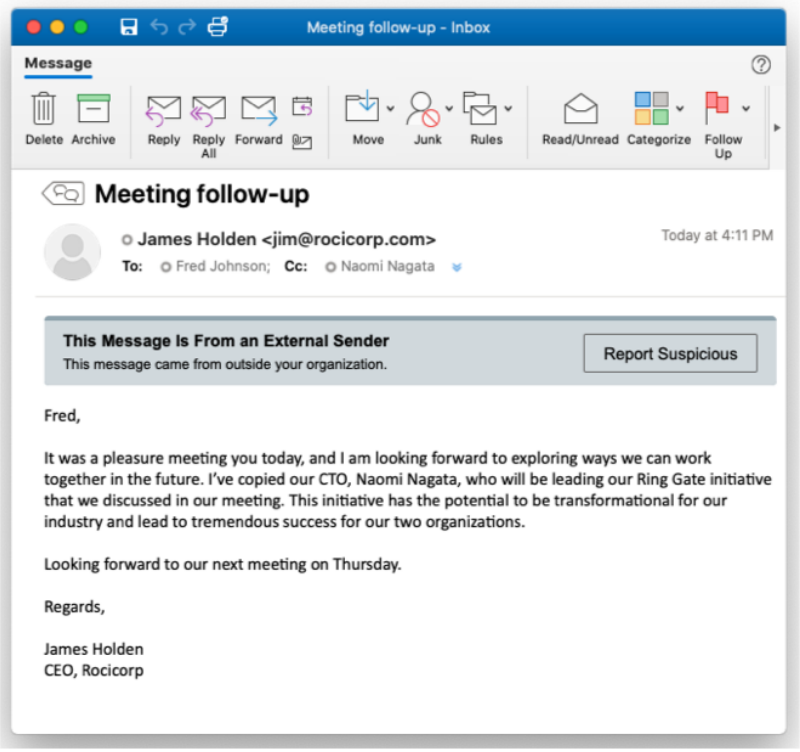
Most organizations struggle with IT security staffing shortfalls. Security teams are overwhelmed by the need to manage so many security vendors and products that usually don't talk to each other. As a result, quickly finding, investigating and cleaning up BEC threats across the organization is difficult. And the longer it takes, the longer the organization is exposed.

By automating key aspects of email analysis and response, security teams can better prioritize their work and respond to threats and user-reported email more quickly. Security teams should also let worried users know they can help them access information in an email marked as suspicious, if needed, while a message is being analyzed.

Tagging external emails automatically to inform recipients of the origin of the email can also prompt users to take a closer look at a message to ensure it's a legitimate message—and not from an impostor.

If a message is found to be malicious, it and any other copies (including those that were forwarded) can be automatically quarantined. No need to manually manage or investigate each incident, saving time and effort for your team.

To complete the cycle, users will receive a customized email letting them know the message was malicious. This reinforces behavior and encourages them to report similar messages in the future.



Consider a solution that protects your brand and organization's reputation by preventing fraudulent emails from being sent using your trusted domains.

6. Protect against attacks targeting your customers—and brand

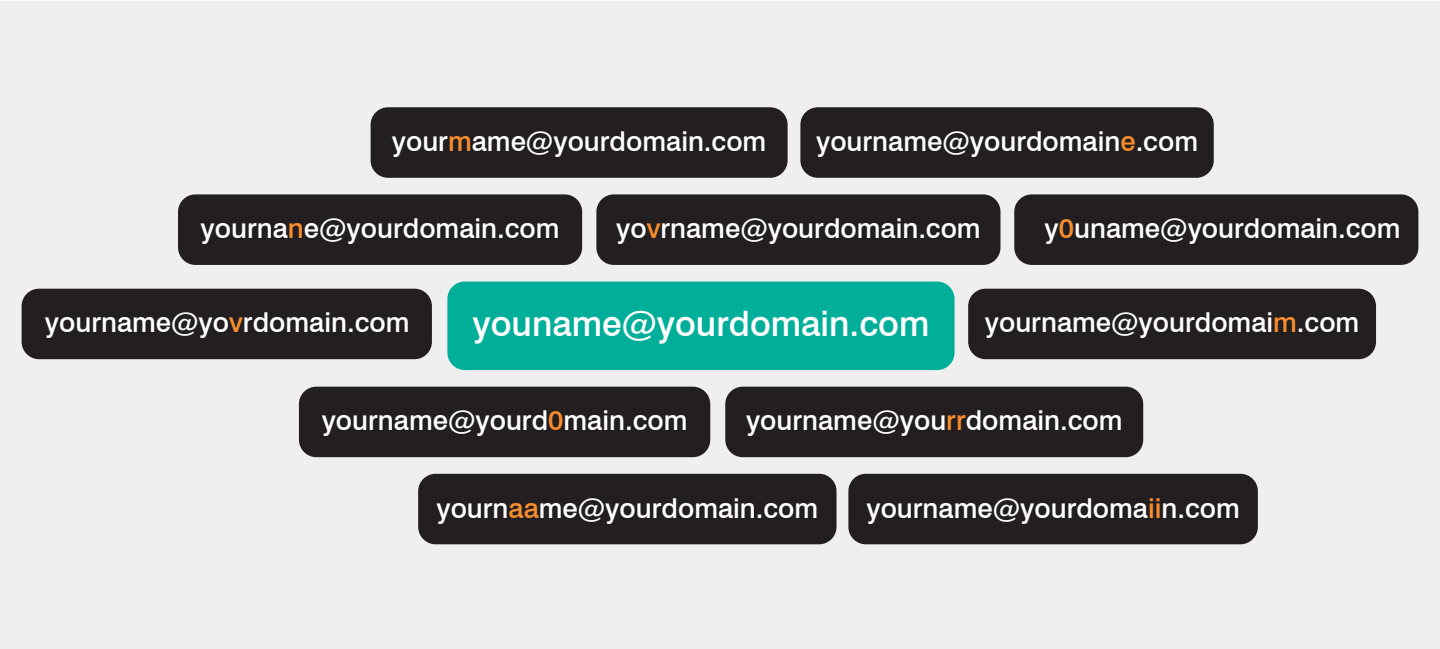
In the case of brand spoofing, attackers will turn you against your customers and business partners by using your company's name and brand to steal money from them.

Brand spoofing may not cause direct financial loss to your organization. But it can damage your organization's reputation, erode customer trust and cause lasting harm to your business

Consider a solution that protects your brand and organization's reputation by preventing fraudulent emails from being sent using your trusted domains. It should verify all emails delivered to and sent from your organization through industry-standard DMARC (Domain-based Message Authentication, Reporting and Conformance) controls.

The solution should also reveal all the emails being sent using your domain, including trusted third-party senders.

Even if you've locked down your domain, lookalike domains can be a problem. Malicious lookalikes can lead customers to fall for BEC emails that appear to be from your organization. Look for newly registered domains posing as your brand in email attacks or by phishing websites—before they move from parked to a live, weaponized state. The same goes for attackers are impersonating your brand across other digital channels, such as web domains, social media and rogue darknets.



Conclusion: The Power of a Unified, People-Centric Defense

To build a multi-layered, fully integrated, people-centric approach to protecting your organization from the risk of BEC fraud attacks means letting go of a "silo mentality" toward security. Even if you have point products to address every avenue of attack, these elements need to work tightly together, with each element of defense reinforcing the other.

When you have a unified or integrated email security solution, you can streamline your security operations and make better use of your IT resources. You can reduce costs and manual work. And most important, you can become much more effective at protecting your organization against the ever evolving BEC threat landscape.

Learn more about Proofpoint solutions for protecting your organization from BEC attacks at:

proofpoint.com/us/solutions/bec-and-eac-protection.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0503-004-01-01 06/21