proofpoint.

E-BOOK

Unmasking BEC and EAC

The Complete Guide to Stopping Business Email Compromise, Email Account Compromise and Today's Biggest Impostor Threats

proofpoint.com

INTRODUCTION

If your users receive an email they think is from their manager, chances are they'll open it. And they'll probably do what the email asks them to, especially if it's part of their regular job. The same goes for emails that appear to be from business partners, vendors and customers.

"Transfer money to this account." "Send the payment here." "Attach employee files." Most of the time, these are all a normal part of doing business.

But unfortunately, a growing number of requests like these are fraudulent. They're not from the person they appear to be. Instead, they're from an impostor using a lookalike email address—or in some cases, the impersonated sender's own email account. These email-based financial scams are part of an increasingly common cyber attack known as business email compromise (BEC) and its close relative, email account compromise (EAC).

According to the FBI, BEC and EAC attacks have cost businesses upwards of $26 billion worldwide since 2016 in exposed (actual and potential) losses.[1] The average attack nets the attacker nearly $130,000.[2]

>$26B

Attacks have cost businesses upwards of $26 billion worldwide since 2016 in exposed (actual and potential) losses.[1]

$130,000

The average attack nets the attacker nearly $130,000.[2]

[1] FBI. "Business Email Compromise: The $26 Billion Scam." September 2019.
[2] Darla Mercado (CNBC). "New online financial scam costs victims $130K per attack." February 2018.

Whether they result in fraudulent wire transfers, misdirected payments, diverted payrolls, supply-chain fraud or exposed personal data, BEC and EAC attacks are growing. Gartner predicts that BEC attacks will double each year, totalling $5 billion in actual losses by 2023.[3] These attacks subvert human trust and imperfect financial controls—not technical vulnerabilities—to defraud victims out of thousands, sometimes millions, of dollars. And they're hard to stop, especially with conventional email defences aimed at stopping unsafe attachments and URLs.

EAC, also known as email account takeover, is often associated with BEC because compromised email accounts are used in a growing number of BEC-style scams. (EAC is also the basis of other kinds of cyber attacks). The FBI started to track them together in 2017. EAC is accelerating in an era of cloud-based infrastructure. A recent Proofpoint Threat Research study reveals that 40% of organisations using the cloud had at least one compromised account.[4]

The good news: these threats can be managed. With the right technology, tighter fiscal controls and a people-centric approach to stopping them, you can unmask BEC and EAC attacks before they reach your users.

This guide explains how BEC and EAC attacks work, why they're so effective and concrete steps you can take to keep your users safe.

$5B

Gartner predicts will double each year, totalling $5B in actual losses by 2023.[3]

40%

40% of organisations using the cloud had at least one compromise.[4]

[3] Gartner Research. "Protecting Against Business Email Compromise Phishing." March 2020.
[4] Proofpoint. "Cloud Attacks Prove Effective Across Industries in the First Half of 2019." September 2019..

BEC AND EAC EXPLAINED

ABC-TV describes the stars of its hit show "Shark Tank" as "tough, self-made, multi-millionaire and billionaire tycoons." But that doesn't mean they can't be duped.

Barbara Corcoran, one of the judges on the show who decides whether to invest in the dreams of various entrepreneurs, was robbed of close to $400,000 by a BEC scam in February 2020.

Corcoran, who made her millions as a real estate broker, said her bookkeeper transferred money as instructed in an email to someone posing as an assistant, ostensibly to pay for a real estate renovation. After the money was sent, Corcoran found that the email address was not actually that of her assistant; it was one letter off from the real address. "There was no reason to be suspicious, as I invest in a lot of real estate," Corcoran told *People* magazine.[5]

Although Corcoran is one of BEC's highest-profile victims, the attack followed a playbook that has become all too routine.

BEC: the art of impersonation

In BEC scams, the attacker pretends to be someone the victim trusts. It usually starts with an email address disguised to look like it belongs to the trusted person—typically a boss, co-worker, supply-chain vendor or business partner. Here are a few of the techniques attackers use to disguise themselves as a trusted sender:

- **Domain spoofing.** The attacker forges the sender address (the "MAIL FROM" or "return-path" field in an email) using a trusted domain. The recipient sees the forged address rather than the sender's actual domain.
- **Lookalike domains.** To get around domain-spoofing measures, attackers often register a domain that resembles the one they're trying to impersonate. The domain might use the numeral "0" instead of the letter "O," for example (y0urcompany.com).
- **Display-name spoofing.** Email senders can easily set their display name to anything they want. Many mobile email clients show only the display name by default, especially on mobile devices, making this a simple but effective technique. Most BEC attacks use display-name spoofing alongside other spoofing methods.

Using that phoney identity, the attacker tricks the victim into transferring money, changing payment account details or some other act of financial fraud.

Other techniques to get users to open and act on requests in emails include: using branded elements (such as the company's display name, logo and overall look-and-feel) and urgent language, clickbait subject lines and content marked "confidential."

Because of their targeted nature, use of social engineering and lack of malicious payload, detecting and stopping these complex and evasive attacks is difficult and time-consuming.

[5] Robyn Merrett (People). "Shark Tank's Barbara Corcoran Gets Back $388K Stolen in Phishing Scam: 'I'm Thrilled!' March 2020.

EAC: invasion of the email snatchers

EAC is closely related to BEC, but it uses identity deception with a twist. In some ways, EAC is even harder to detect and stop than BEC.

In BEC, the attacker tries to impersonate a trusted person's email account. In EAC, the attacker takes over that trusted email account. The email account doesn't just seem legitimate—it's the real thing. EAC leaves two victims: the person whose account is compromised and the email recipient who falls for any requests from that account.

Having control over a trusted account gives the attacker a trove of information to make the impersonation that much more effective—contacts, calendar appointments, old emails and more.

Consider a cyber attack Proofpoint threat researchers encountered last year.

Attackers had breached a G Suite email account and were seeking out more victims. They didn't need to look far. Like most of us, the compromised user had unfinished emails sitting in the draft folder. The attackers found a draft that looked nearly complete, attached malware to it, and hit "send."[6]

The hijacked message was timely and relevant. It came from a legitimate email address—someone the recipient knew, actively engaged with and was probably expecting to hear from. And it was written in the unwitting sender's own voice and tone, not the awkward prose that might give a less advanced attack away.

It's no wonder these attacks are so effective.

Here's how attackers usually compromise legitimate accounts:

Brute-force attacks. The attacker, usually through an automated script, tries a username/password combination across many accounts until one works.

Breach replay attack. It's a bad practice, but many people use the same password for multiple accounts. If one of those passwords is leaked in an unrelated data breach, any other account with the same username (often an email address) and password is at risk.

Phishing. Old-fashioned credential phishing remains an effect way to get a victim's password. Without controls such as multifactor authentication (MFA), lost credentials can lead to compromised accounts.

Malware attacks. Keyloggers, stealers and other forms of malware can expose user credentials, giving attackers control of victims' accounts.

Once they have control of an account, EAC attackers can launch a variety of attacks, such as:

- **Internal phishing:** Emails sent from employee to employee within the same organisation using a compromised corporate account
- **Supply-chain phishing:** Most organisations do business over email. An attacker who gains control over a legitimate account can assume your employee's identity to defraud customers and business partners.
- **BEC-style attacks:** Think of EAC as the ultimate impersonation tactic. In EAC, attackers hijack an email account to essentially become the person it belongs to. EAC bypasses many email authentication controls.
- **Data exfiltration:** Gaining access to someone's mailbox, attackers can access not just email, but also calendar events, contacts and sensitive data in file shares.

[6] Ryan Kalember (writing for Infosecurity). "Year in Review: Social Engineering Attacks." December 2019.

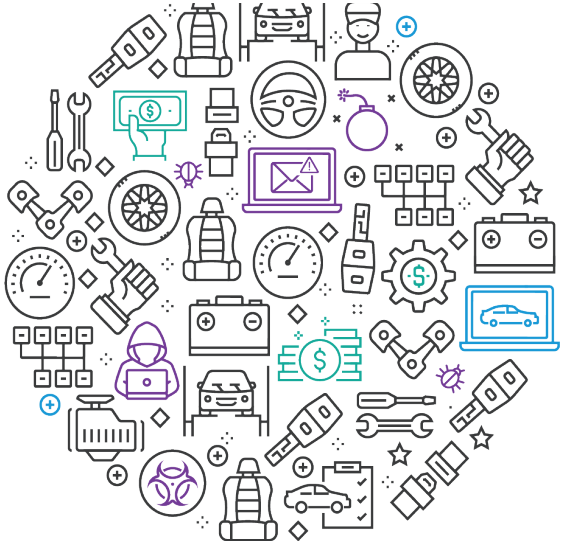
Life is full of compromises: recent BEC attacks

BEC attacks come in many forms, with a wide range of targets, tactics and goals. Here are a few examples that demonstrate BEC's broad scope:

- In December 2019, someone posing as an executive at New York nonprofit VillageCare Rehabilitation and Nursing Center tricked an employee into sending patient medical records. These records contained the first and last names, dates of birth and medical insurance information for 674 patients.[7]
- One of the biggest BEC victims—and payouts—in recent months was Toyota Boshoku. The Toyota subsidiary, which supplies seats and other interior components, was swindled out of $37 million in August 2019. Someone posing as a business partner sent emails to people in the company's finance and accounting department, requesting payment into the attacker's account.[8]
- Providence, R.I.-based Brown University warned users in January 2019 that scammers were emailing staffers in the payroll department with bogus requests to change employees' direct-deposit details. The emails convey a sense of urgency ("how soon can that be done?" one reads), a common BEC tactic. Other techniques to get users to open and act on requests in emails include: using branded elements (such as the company's display name, logo and overall look-and-feel) and urgent language, clickbait subject lines and content marked "confidential.[9]

$37 Million

stolen in largest reported BEC attack



[7] Sarah Coble (Infosecurity). "Fake Exec Tricks New York City Medical Center into Sharing Patient Info." January 2020.
[8] Nicole Lindsey (CPO Magazine). "Toyota Subsidiary Loses $37 Million Due to BEC." September 2019.
[9] Brown University. "Request to change direct deposit information." January 2019.

BEC and EAC: so much alike, so different to defend against

BEC and EAC are growing problems that target organisations of all sizes and across every industry worldwide—in all 50 states and in 177 countries. They share a similar playbook and are often linked (the FBI tracks them together). But they have key differences that are important to understand when building out a defence strategy.

How BEC and EAC are similar

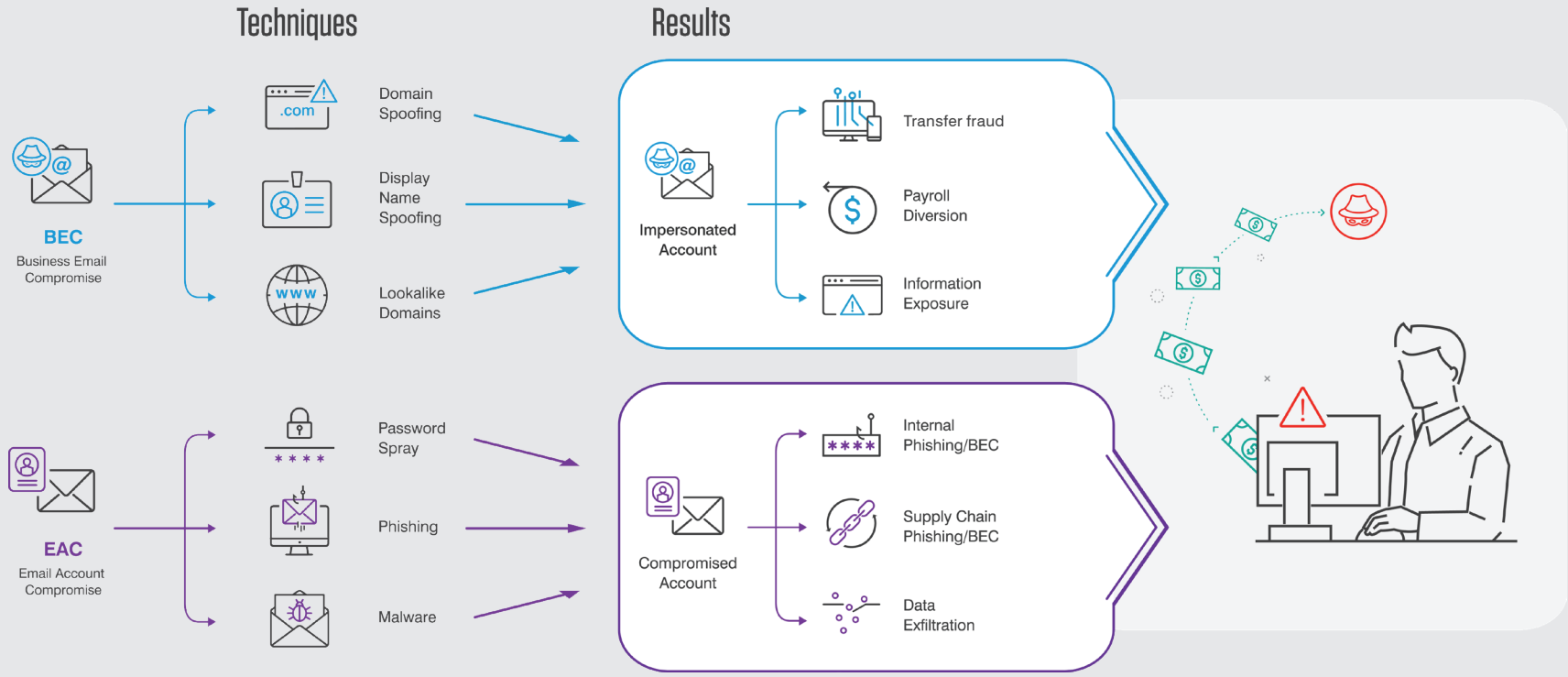
Both BEC and EAC:

- Target people and rely on them to carry out desired actions
- Rely on social engineering rather than technical vulnerabilities
- Are designed to solicit wire transfers or payments of funds or sharing sensitive data
- Are narrowly targeted, making them more difficult to detect

How they are different

Here's how BEC and EAC attacks diverge—and why they can't be stopped in the same way:

- BEC attacks use email that looks like the account of someone the recipient knows and trusts.
- EAC attacks use a trusted person's actual account.



BEC: a global phenomenon

Japanese media giant Nikkei isn't the stereotypical victim of financial fraud.

It's one of Japan's biggest media conglomerates, the owner of London's the Financial Times and its namesake stock index on the Tokyo Stock Exchange.

That sheer size and financial heft made it an especially lucrative target of scammers. In September 2019, an employee of its U.S. subsidiary, Nikkei America, transferred $29 million based on instructions from an email that appeared to be from an executive at the parent company.

Unfortunately, the email was from someone merely posing as the executive. (Some reports suggested that the attacker may have actually taken over the executive's account,[10] which would make it an EAC attack; the media company and authorities have provided few details publicly.)

WHY NO SINGLE APPROACH CAN SOLVE BEC AND EAC

BEC and EAC attacks are inherently focused on people, rather than technical vulnerabilities. That shift renders traditional infrastructure-focused defences useless against them. Unlike large-scale attack campaigns, BEC and EAC attacks are specific and highly targeted. So they go unnoticed by security tools that look for network traffic patterns and other detection techniques.

Because BEC and EAC rely primarily on social engineering and human psychology, there are no malware attachments or malicious URLs to be analysed. In fact, malicious emails sent from compromised accounts usually pass authentication and even content-analysis checks.

BEC/EAC is a multifaceted problem

BEC and EAC are complex, using multiple techniques. There are several reasons why point products working independently from one another cannot do the job.

Advanced BEC and EAC attacks are often blended

Bad actors use many techniques that span multiple technologies and channels. Today's threats often combine email and cloud vectors, including apps and services such as Amazon Web Services, Box, Google G Suite, Microsoft 365 (Office 365), Slack and others.

By getting corporate users to respond to a single malicious email, attackers can infiltrate a cloud account. This can then lead to phishing or email fraud both internally and across supply chains.

Even if you have a solution for one or some of BEC/EAC techniques, you're still exposed to others

Attackers are constantly shifting tactics and always evolving. Your solutions probably aren't covering all the possible ways attackers can use to impersonate people your users trust. That leaves you exposed to other advanced deception techniques you may not even be aware of.

If you're solving for techniques in a siloed manner, your security tools might miss important signals from other channels

For example, financial requests from the CFO that might appear routine in isolation can take on new significance if you know that person is being targeted with account takeover attempts such as credential phishing.

[10] Lindsey O'Donnell (ThreatPost). "BEC Scam Costs Media Giant Nikkei $29 Million." November 2019.

A PEOPLE-CENTRIC APPROACH

By taking a holistic approach to BEC and EAC attacks, you can keep your people and your organisation safe from these insidious and difficult-to-detect threats

Preempting BEC: first steps

There are some things you can do to prevent the potential damage that can be done by BEC and EAC attacks. These recommendations may seem obvious at first, but they can go a long way toward safeguarding your organisation.

> "An effective compliance culture supports employees with the protocol they need to follow up with confidence. Without the internal isolation BEC criminals depend on, their attacks are more likely to fail.[11]"

Change your financial processes

Start by tightening the reins on who can process and authorise wire transfers. Minimise the number of people involved and make sure authorised employees stick to process and learn to recognise suspicious requests for wire transfers.

Another step in the right direction is to use multiple verification steps for wire transfers. For example, if a transfer exceeds a certain amount, you might want to require authorisation by someone higher up in the chain of command. And because BEC and EAC attacks use email, you can use other means of verification such as an old-fashioned phone call.

For example, some attacks ask the targeted employee to change account information. Again, you can confirm with a phone call. Just make sure the phone number is legitimate and not spoofed.

Deloitte suggests that changes to the workplace culture, such as instilling the importance of following corporate protocol, can also head off BEC attacks. In a recent article, the global professional services network offers this piece of advice.

An effective compliance culture supports employees with the protocol they need to follow up with confidence. Without the internal isolation BEC criminals depend on, their attacks are more likely to fail.[11]

Deploy multifactor authentication

Another useful tool to prevent some account takeovers is multifactor authentication (MFA), which asks users to provide two or more ways to identify themselves. Just about everyone is familiar with logging into a bank account first with a password and followed by entering a numerical code that is sent to their mobile phone.

MFA provides an extra layer of security against account takeovers. But it doesn't do anything for BEC attacks. And even in EAC attacks, it isn't bulletproof.

[11] Deloitte. "Five ways to mitigate the risks of email compromise attacks." 2019.

Deploy an Email Security Solution Purpose-Built to Fight BEC and EAC

BEC and EAC are complex issues, and there is no single approach that can protect against every kind of impostor attack. A security tool may stop one or two tactics but still leave you exposed to a multitude of others.

That's why you need a solution that addresses every angle of these sophisticated and complex threats. Look for an integrated, holistic solution. Your BEC/EAC defence must address all attacker tactics. It must provide visibility into malicious activities and user behaviour. And, for the most effective BEC/EAC defence, it should automate detection and threat response.

Helping security leaders meet the challenge head on

- A truly purpose-built solution will help CISOs, CIOs and other security leaders achieve the following:
- Minimise the risk of BEC and EAC by protecting against a wide range of attacker tactics and techniques.
- Gain visibility into who receives impostor email and into who sends these emails using your company's domain. That includes both trusted third-party senders and compromised accounts.
- Strengthen overall security by blocking impostor email and fraudulent use of domains by accurately detecting compromised cloud accounts.
- Understand and clearly communicate the risks to the board of directors. That starts with identifying and describing the human attack surface. You should know who your Very Attacked People™ are, who is being attacked with credential phishing and impostor emails, and who is vulnerable to credential theft.
- Reduce costs and improve operational effectiveness by consolidating security vendors and products.

Make your security team more effective and efficient

A solution built expressly to stem the tide of BEC and EAC threats will enable your security team to:

- Cut through the noise. The team should be able to prioritise incidents and investigate potential threats by accurately blocking impostor emails, detecting suspicious cloud account logins and activity, and stopping attempts to steal account credentials.
- Train users how to recognise, reject and report BEC and EAC attempts.
- Prevent fraudulent use of your organisation's legitimate domains.
- Provide actionable insights into who is being attacked with impostor emails and credential phishing. Based on that insight, provide risk-based security controls to those users, such as isolating access to unknown websites and targeted security awareness training.
- Reduce manual work, save time and accelerate threat response. Automate detection, investigation and remediation.

Attackers will never stop looking for ways to exploit your users and prey on human nature and business processes. But with an effective BEC/EAC solution, you can greatly reduce the chances of impostors reaching your users—and your users from falling for tricks that cause lasting damage.

PUTTING THE PIECES TOGETHER

Here are the components of an effective BEC/EAC defence.

Gateway

- Block attacks that use display name spoofing, spoofed domains and lookalike domains
- Analyse message headers to identify anomalies
- Analyse all email content with machine learning
- Enforce email authentication policy

Authentication

- Create global email authentication policy (DMARC) and enforce it on an Internet-wide basis
- Block all attempts to send unauthorised emails from your trusted domains
- Report on lookalike domain registrations

Cloud Application

- Identify suspicious cloud account activity and compromised accounts
- Detect brute-force attacks
- Build policies to prioritise alerts

Web Access

- Isolate access to unknown websites
- Provide read-only access until security analysis is complete
- Control content entering your organisation through personal webmail accounts

Visibility

- Identify VAPs
- Provide user-centric visibility into account attacks
- See which users are being attacked with impostor and phishing attacks

Automated Remediation

- Identify and remove suspicious emails that have entered the organisation
- Remove unwanted email from internal accounts that are compromised
- Force password resets and disable accounts that are compromised
- Use an account authentication solution to re-authenticate sessions
- Investigate account compromise incidents
- Automate abuse mailbox process

Education

- Assess user vulnerability to BEC and EAC threats
- Train users on how to identify threats and credential theft
- Simulate real-world BEC and phishing attacks

Take a free assessment and learn more about how Proofpoint can help you build an integrated, holistic, people-centric defence at
https://www.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 company that protects organisations' 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 organisations 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.

XXXX-XXX-XX-XX 7/20