AREA 1

FAKE EXECUTIVE EMAILS, REAL FINANCIAL LOSSES

What to Know About Business Email Compromise

THE GAME: THEFT BY IMPERSONATION

THE STAKES: HIGH AND RISING

Criminal ingenuity intersects with clever social engineering to create the frustratingly successful swindle of Business Email Compromise or BEC, also called CEO Fraud or Imposter Attacks.

According to the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN), U.S. businesses have been hit with nearly $9 billion in attempted BEC theft since 2016. This figure exceeds even the FBI's previous calculations of $1.3 billion per year. Gartner analysts were alarmed enough to make BEC a Top 10 Security Priority in 2019.

BEC is a specific type of phishing email that operates without links and without attachments (two of the standard markers that perimeter defenses look for). However, instead of taking over a computer or stealing data, BEC hackers impersonate an executive (a known CEO, CFO or other CxO), and persuade the recipient (an employee) to perform some action – like wiring money or attaching information to an email.

LESS IS MORE LOSS

BEC is a highly effective social engineering attack – as well as a phishing attack.

Deceptively simple, BEC emails lack links, files, malware, and enclosures. They arrive from seemingly valid accounts, sliding past Secure Email Gateways (SEGs) and even Office 365 and Gmail's heavily arrayed security suites. The arrival of a BEC phish can trigger worse financial harm than the most sophisticated cyber invasion.

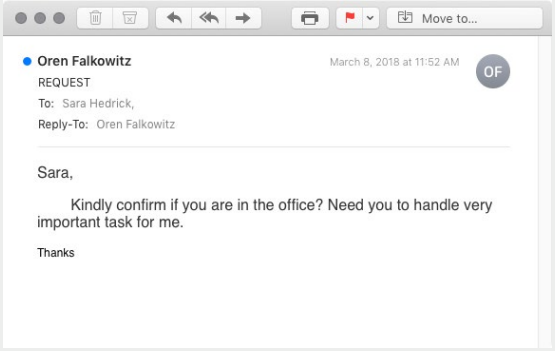
What makes BEC so effective has more to do with human nature than with Boolean logic. The very traits that make us social beings – willingness to trust, desire to help, and respect for authority – can be weaponized by BEC and turned into a tool for thieves.

BANKRUPTING OUTDATED DETECTION METHODS

With BEC's treacherous cousin, Email Account Compromise (EAC), hackers manipulate a company officer's legitimate email account to send employees or business partners phony invoices or contracts and request wire transfers into their own (criminal) accounts.

However, BEC is even simpler: hackers don't trouble to attack the actual email but merely spoof a business officer's identity. This is enough to convince a trusting, uninformed, or distracted employee to transfer money at the criminal's direction.

In this actual BEC example, a cyber actor impersonates Area 1's CEO, Oren Falkowitz, to contact a real Area 1 employee:



Area 1's detection algorithm blocked it before the employee even saw it.

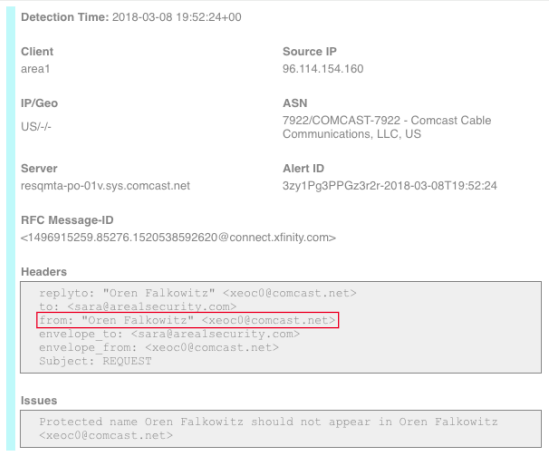
Consequences, starting with dismay and embarrassment, soon flood in, often eclipsing the monetary loss itself. A publicly disclosed attack can trigger an audit, damage the brand, and shatter trust in the company's integrity and security. Share prices may fall; agreements, acquisitions and mergers may be in jeopardy.

DISABLING DMARC AND OTHER DEFENSES

Like other types of phishing attacks, BEC emails handily evade legacy perimeter defenses that only offer protection from known, active campaigns, and focus on reaction (rather than blocking them in advance) and heavy payloads.

Security defenses that rely on email authentication – SPF, DKIM, and DMARC – are ineffective against skilled spoofing. Statistics prove that they fall short, landing and lurking in executive and employee inboxes, and awaiting the click to trigger massive loss.

An Imposter email sent from a valid service provider (e.g., Comcast, Gmail, Yahoo) will bypass authentication and DMARC:



There are a number of ways fake email and phishing attacks get past email authentication and DMARC. For example, hackers can establish spoofed accounts with free email services such as Gmail or Yahoo, with a name similar to a trusted party. Because many free email service providers implement DMARC, SPF, and DKIM, these spoofed accounts will pass email authentication checks and can land in end-user inboxes and cause harm.

Another hacker trick is to create look-alike domains. With look-alike domains, hackers establish a domain with a name similar to a trusted organization's domain or a trusted partner's domain. The hacker can set up the domain with SPF, DKIM and DMARC configured so that emails sent from the hacker's domain will pass authentication checks and land in end users inboxes undetected, fooling recipients into believing that the email is from a trusted source. Hackers often launch and shut down these domains quickly, before reputation databases mark them as malicious.

Finally, although DMARC standards have been available for several years, adoption is still limited. Industry leaders estimate that only 5% of domains and only 30% of email traffic have DMARC policies implemented. Therefore, using DMARC to validate senders and detect fake email phish isn't 100% reliable, and leaves a significant security gap if you're relying on email authentication exclusively to protect you from fake email.

No matter how efficient spam filters are at screening the swarms of frivolous, unwanted, and misleading nuisances that we think of as spam, the filters are architecturally and conceptually impotent against phishing. Built to catch high volume, repetitive emails, spam filters cannot sense phish, which are low volume, unique, and can't be detected by signature and reputation-based defenses.

> *Q: Does DMARC block all types of phishing attacks?*
>
> ***A:** No. DMARC is only designed to protect against direct domain spoofing. If the owners/operators of **example.com** use DMARC to protect that domain, it would have no effect on **otherdomain.com** or **example.net** (notice the ".net" vs. ".com").*
>
> *While impersonating a given domain is a common method used for phishing and other malicious activities, there are other attack vectors that DMARC does not address. For example, DMARC does not address cousin domain attacks (i.e. sending from a domain that looks like the target being abused – e.g. **exampl3.com** vs. **example.com**), or display name abuse (i.e. modifying the "From" field to look as if it comes from the target being abused).*
>
> Source: DMARC.org FAQ

Security Awareness Training of employees, while popular and required for certain industries, can also actually backfire by causing overconfidence and trust of the "clean" phishing emails. Further, phish still need only one impulsive or reflexive click to advance the attack.

BEC hackers are patient, persistent, and trained for that one moment of opportunity that can deliver a rich payoff. For example, one Area 1 client reported receiving more than 30 phish a week landing in an inbox, poised for a user to give them an opening to pounce.

It is no wonder corporate boards are deeply concerned about stopping this stalking, since board members are often targets.

EXPLOITING THE SOCIAL CONTRACT

BEC doesn't need to enlist sophisticated technology because it is based on the ancient, universal and powerful tactic of impersonation – an adversary posing as an ally.

Another major advantage that makes BEC an audacious enemy is that it parasitizes and exploits the behaviors and values most of us learn from childhood, as well as the workplace professionalism we apply on the job:

Respect for authority

Employees view their CEO as the emblem of the company. They feel honored and even inspired when entrusted with a task involving some important company function – such as transferring funds or complying with a contractual obligation. That feeling works to outweigh the skepticism and natural caution an employee might feel when approaching a major transaction. This can put the decision-making process at the mercy of manipulation by a criminal.

One of the family

Reassurance is key to BEC. The ability to communicate with the imposter encourages an employee to lower their guard. A clever, well-prepped thief can reinforce their authenticity by showing employee-like familiarity with company functions, acronyms, and protocols. Cyber actors might spend months doing research on a company's Facebook and LinkedIn profiles, subscribing to the target's company newsletters, or studying press interviews and earnings calls, to gain granular knowledge of the executive's writing style, habits and schedule. They assume the work culture, including informal behaviors and nicknames that people use with colleagues. In other words - they try to look like one of the family.

Squeaky-clean and credible-sounding

As employees have trained not to click on links or open attachments, BEC hackers have also wised up. So a BEC phish carries no baggage; no treacherous links, sites – or attachments to trigger suspicion. But a phish is anything but innocent; in fact it represents a massive threat. Even well-trained employees can be deceived by their own misplaced sense of trust at such a clean email.

Urgency as the strategy

BEC also warps the social contract by insisting that the transfer is urgent. It must be done quickly or the company will lose an opportunity or miss a deadline. This 'need for speed' works to the advantage of the criminal, of course. An employee hurries through the steps of a transaction and may miss clues to its fraudulent nature or hesitate to raise a doubt for fear of displeasing the CEO.

THE KEY TO DEFEATING BEC: UNDERSTANDING SOURCE AND SENTIMENT

Phishing is the cold heart of the BEC strategy. Without phish, BEC could not exist.

Because C-level executives and their employees are so vulnerable to BEC, and because the stakes are so high, it's vital that they be covered by an anti-phishing service – for safety, for peace-of-mind, and for productivity slowed by the distraction of suspecting every email. It shouldn't be the burden of employees to correctly flag every suspicious BEC phish that happens to get past their company's SEG and perimeter defenses.

BEC PHISH TYPES: HOW TO SEE THROUGH THEIR CAMOUFLAGE

Just like their namesakes in nature, BEC phish come in many species, but their attacks are evolving for predation in real time. This snapshot of BEC types gives you a checklist of what can lurk in your mailbox. Don't hook one!

- **Domain Spoof Attack:** lets cybercriminals generate emails that appear to originate within your company or a partner domain. People assume it is authentic and transact with that sender. Scammers also use a spoofed organization's real domain in the "From" address, but a different domain in the "Reply-To" address.
- **Display Name Spoof Attack:** uses your CEO or other executive's exposed email address to send email as that officer. Attackers can then lure recipients into whatever activity they choose, such as transferring funds.
  - **Smartphone users:** Email apps show only the sender's display name. When you see an email from your boss, check its actual email origin too.
- **Domain Proximity Attack:** cyber actors change a couple of letters, switches upper or lower case, or alter some other minor detail in the domain address, hoping it'll go unnoticed.
- **Attributes Spoof:** corrupts or obfuscates body or email headers and might display a copycat logo, logotype, brand name, or other identifier to get over and masquerade as a legitimate identity to the target.
- **Encoded Message Attack:** substitutes certain characters in the message to avoid SEGs. For example, fraudsters might swap certain ascii characters like 'a', 'c', 'e', 'y' with equivalent Cyrillic characters.
- **Long Scenario Deception:** a bold new trend is to send a long, personalized message sharing legal implications of a sensitive business requirement - even referencing bona fide legal firms. Attackers request fund transfers to a specific account using similar bank titles but with different banks, or even the same bank in a different geography.

Gartner strongly recommends that security leaders adopt BEC anti-phishing as a top priority security project, and employ technology that can inspect message context by looking at the trustability and authenticity of the sender.

Phishing, especially BEC and executive impersonation attacks, remains not only a major financial threat, but a cruel hoax that threatens the integrity, morale, and viability of an organization. Whether the company is as large as Google, which recently lost $100 million to BEC, or as close as the startup sharing your building, the principle is the same. Stopping attackers who undermine the implicit trust among employees is one of the most important challenges facing CISOs and security teams today.

To learn more about how Area 1 helps organizations protect their executives against BEC and against other advanced phishing attacks, visit www.area1security.com/overview.

GARTNER CALLS OUT AREA 1 SECURITY as a "state of the art" anti-phishing technical control that stops BEC and phishing. At Area 1, we use a combination of techniques that look at the source and the sentiment of an email to detect BEC. Sophisticated matching models check that messages appearing to be from an executive actually originate from known sending domains and – in combination with language analysis of email subject and content to understand the sentiment – Area 1 can effectively detect BEC email that traditional defenses miss, and therefore prevent delivery of imposter email to employee inboxes.

AREA 1

About Area 1 Security

Area 1 Security delivers the industry's most comprehensive anti-phishing solution. Area 1 Horizon™ stops phishing campaigns during the earliest stages of an attack cycle, before a phishing attack on an organization can occur. Phishing is the root cause of 95 percent of security breaches, according to Gartner.

Area 1 Security works with some of the most sophisticated organizations in the world, including Fortune 500 banks, insurance companies, and healthcare providers to preempt and stop targeted phishing attacks at the outset, improve their cybersecurity posture and change outcomes.

Learn more at www.area1security.com, join the conversation at @area1security or follow the blog for the latest industry news and insights on how to deal with phishing.

▸ Learn More INFO@AREA1SECURITY.COM