Abnormal

H1 2023
EMAIL THREAT REPORT

“Read” Alert: Data Shows 28% of BEC Attacks Opened by Employees

Executive Summary

Since business email compromise attacks first started in the mid-2010s, they've created challenges for organizations worldwide. These text-based emails often bypass traditional security tools, and attackers have found increasingly savvy ways to take advantage.

With $43 billion in exposed losses over five years, this financially-devastating cybercrime must be taken seriously. Why? Because these attacks are increasing in volume at a significant rate and perhaps even worse—your employees aren't reporting them.

Employees Are Your Greatest Asset—and Your Biggest Cybersecurity Liability

When it comes to email attacks, the odds are stacked against your workforce. While employees must be right 100% of the time, threat actors need to be right only once—and they know this.

Between July-December 2022, the median open rate for text-based business email compromise (BEC) attacks was nearly 28%. And of the malicious emails that were read, an average of 15% were replied to. Additionally, if your organization relies on employee reporting for visibility into attack frequency, we have bad news: on average, only 2.1% of all known attacks are reported.

Business Email Compromise (BEC) Maintains Consistent Growth

Making matters worse, the threats targeting organizations are increasing, meaning that employees have **more** emails to watch for—and more sophisticated ones at that.

Just as organizations utilize business intelligence to more effectively target customers, modern threat actors conduct extensive research to determine how best to execute BEC attacks. By leveraging information on LinkedIn, SEC disclosures, and even the target organization's website, cybercriminals can create convincing emails that are more likely to trick employees, and at increasing volumes. Over the past two halves, BEC attacks grew by more than 81%, and over the past two years, BEC attack volume increased by 175%.

2.1%

Percentage of attacks reported to the security team by employees.

78%

Percentage of text-based BEC attacks read and replied to by entry-level sales associates.

81%

Increase in the number of BEC attacks between H1 and H2 2022.

147%

Increase in BEC attacks targeting SMB organizations over last two halves.

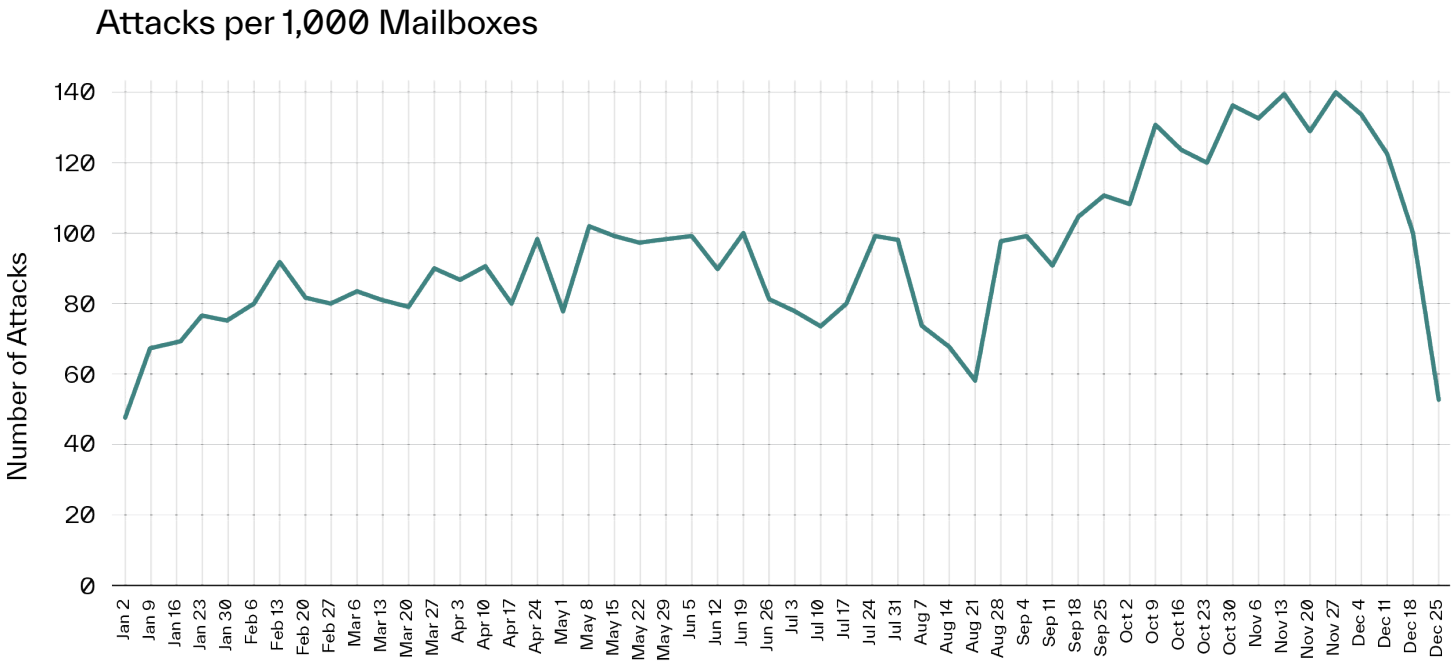
Table of Contents

Attackers Continue to Exploit Inherent Vulnerability of Email

When email was first introduced, the focus was simply on facilitating communication, with security as an afterthought. Tools put in place since have been ineffective at stopping new types of attacks, and as a result, email remains one of the easiest ways to infiltrate organizations. So long as we’re stuck playing catch-up, threat actors will continue to utilize email as an attack vector.

Attack Volume Rises by More Than 20%

Over the past year, overall attack volume increased by 22%, from an average of 85.13 attacks per 1,000 mailboxes during January-June to an average of 104.04 during July-December.

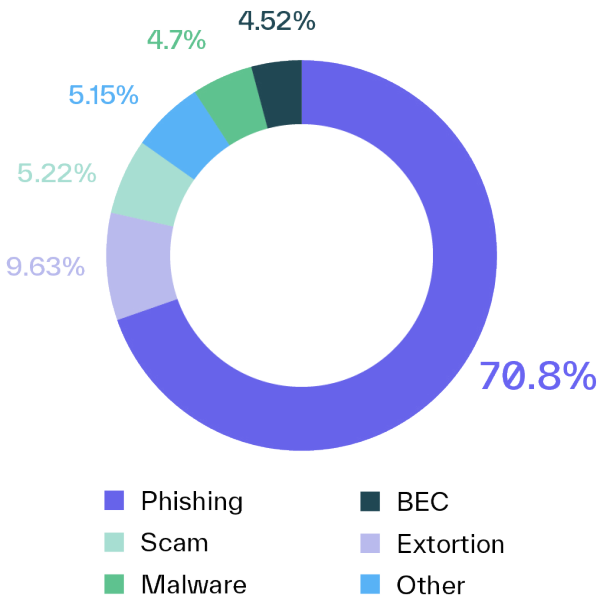


After a relatively static summer period, attack volume began dramatically rising during the third week of August, with the number of attacks growing by nearly 40% between the weeks of August 14 and August 21. Starting in early September, attack volume was consistently above 100 attacks per 1,000 mailboxes and hovered around an average of 120 until the week before Christmas. Based on the data, it would seem cybercriminals quickly transitioned from back-to-school attacks to holiday-themed campaigns with little downtime.

Still, similar to what we've seen in prior years, attackers did appear to take their own holiday break, as attack volume dropped significantly in the last two weeks of 2022. This is most likely due to two things: threat actors understand the majority of their potential targets won't be online during this period (which decreases their chances of success) and/or they want to pause to enjoy the holiday with their families as well.

As has been the trend since 2019, phishing continues to be the most common email attack type, accounting for 70% of all advanced attacks in the second half of 2022. But one interesting thing to note is the marked increase in extortion.

Percentage of Advanced Attacks by Type



During the first half of 2022, extortion accounted for 7.01% of all advanced attacks. However, **between the first and second halves of the year, extortion attacks increased significantly, and from July-December 2022 they comprised almost 10% of email attacks.**

One possible explanation is that cybercriminals are taking advantage of a volatile job market. While the unemployment rate has somewhat stabilized after record highs in 2020, macroeconomic conditions have led to large-scale layoffs over the past year. This would make employees highly motivated to acquiesce to attackers' demands if they believed it would prevent their employers from becoming aware of any accusations (whether valid or baseless) that could put their job in jeopardy.

Likewise, the loss of consumer or employee trust can be catastrophic for organizations of all sizes. Data from PwC shows that both consumers and employees consider protecting data and cybersecurity the top foundational element of trust in a business. In another PwC survey, 71% of employees reported they would leave their employer if it lost their trust, and 71% of consumers said it's unlikely they would buy from a company that lost their trust.

Naturally, business leaders would feel compelled to pay hefty sums to avoid the exposure of compromising information—circumstances that threat actors may be all too happy to exploit.

Employees Should Never Be Your Last (or First) Line of Defense

Your employees are your greatest asset. They also pose the greatest risk to your organization’s security. And when it comes to email attacks, the odds are stacked against them. Attackers are increasingly taking advantage of social engineering tactics with fear and urgency to encourage employees to open their emails, respond, and complete the request—whether that is buying gift cards, paying an invoice, or changing banking account details for a vendor.

Employee Reporting Rates are Troublingly Low

If your organization relies on employee reporting to understand the full extent of attack frequency, we have bad news: on average, **only 2.1% of all known attacks are reported.**

Between July and December 2022, the average weekly number of attacks per 1,000 mailboxes was 104. That means in a mid-market enterprise with 1,500-2,000 employees, ***every workday*** there are 30-40 attacks not being reported to the security team. For organizations over that threshold, the number can be much, much larger.

On top of frighteningly low reporting rates for attacks, the majority of messages reported to security teams aren't even malicious. On average, 84% of employee reports to phishing mailboxes are either safe emails or graymail.

Why Aren't Employees Reporting Malicious Emails?

The Bystander Effect

Though most often applied in emergency situations, the bystander effect also pertains to any environment in which multiple individuals are facing the same issue. This phenomenon can be summed up in five words: "Someone else will handle it." Essentially, employees assume that they aren't the only target of an attack and therefore, they don't need to report the email because surely a coworker already has.

What should be emphasized is that even if a threat actor targets multiple employees in an organization, the sooner a malicious email is reported, the sooner all related messages can be remediated.

No Harm, No Foul

Some employees may believe that as long as they don't engage with the attacker, they have fulfilled their obligation to the organization. But security professionals know that opting to just delete the email without reporting it can be almost as damaging since it eliminates the opportunity for the security team to warn other employees about the attack.

Employees need to understand that a message that they immediately recognize as a phishing attack or attempted invoice fraud may not raise any red flags for a colleague. And if they don't report it, the threat actor can move on to their next target.

Fear of Being Wrong

The data shows that most reported emails are not actually malicious attacks. Knowing this, some employees may feel that they are not equipped to tell the difference between a safe email and an attack, and rather than submitting a report ***just in case***, they decide not to—either out of fear of embarrassment or because they simply don't want to create needless work for the security team.

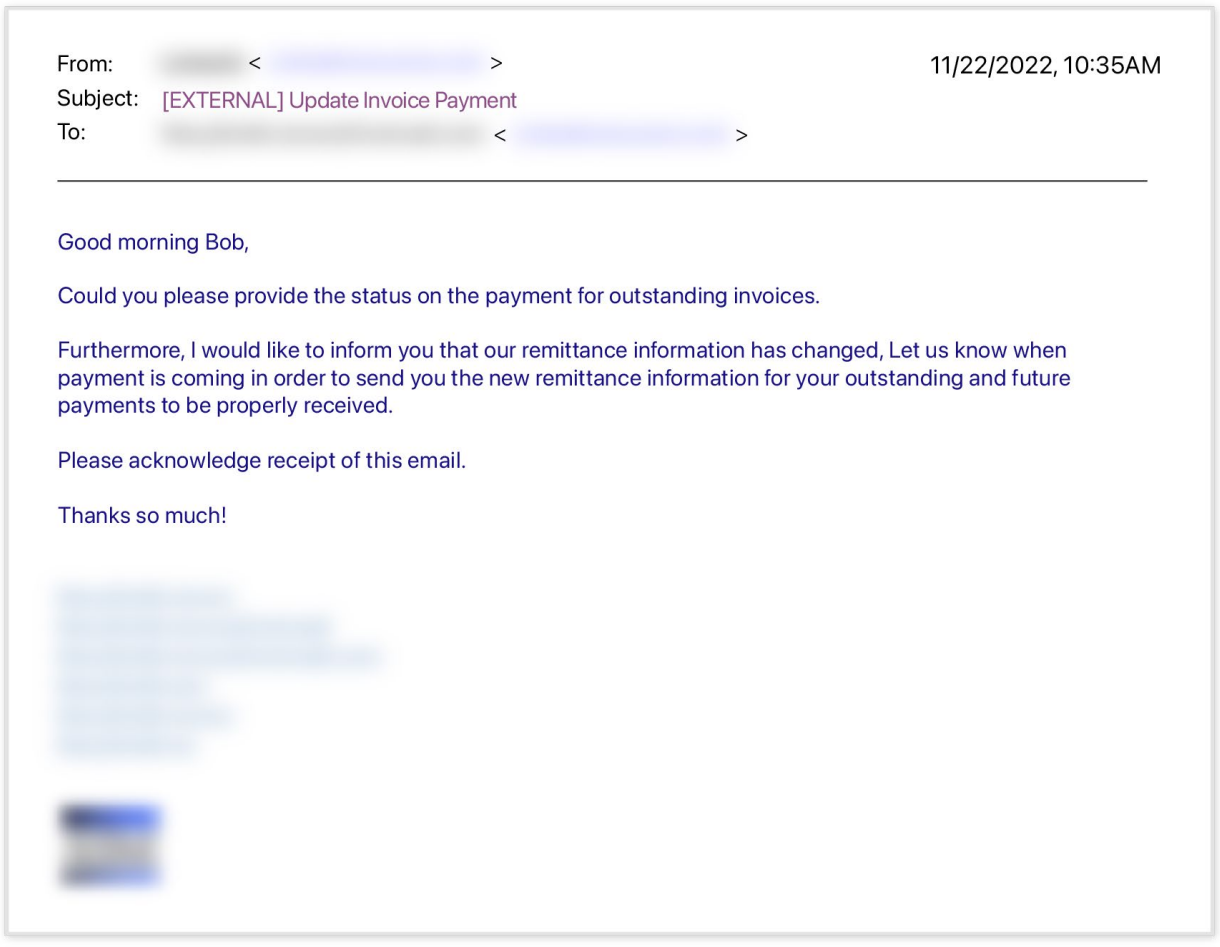
When the consequences of a successful attack can be so costly, creating an environment where employees err on the side of "better safe than sorry" can be crucial.

Real-World Example of an Employee Engaging with a BEC Attack

Note: This attack was observed during a risk assessment in which Abnormal was operating in read-only mode, which is why the attack was not proactively blocked.

Many professionals are operating under the assumption that today's email attacks are just as poorly-worded or obviously malicious as those from ten years ago. But modern threat actors have optimized their strategies and are launching attacks that not only bypass legacy security tools, but also trigger no alarm bells for the average employee.

In the text-based BEC attack below, the threat actor impersonated the office manager of a small safety management business and emailed the facilities manager of a food distribution company. The attacker first requested the status of payments for outstanding invoices and then informed the recipient that the company's remittance information had recently changed.



From: [redacted] < [redacted] > 11/22/2022, 10:35AM
Subject: [EXTERNAL] Update Invoice Payment
To: [redacted] < [redacted] >

Good morning Bob,

Could you please provide the status on the payment for outstanding invoices.

Furthermore, I would like to inform you that our remittance information has changed, Let us know when payment is coming in order to send you the new remittance information for your outstanding and future payments to be properly received.

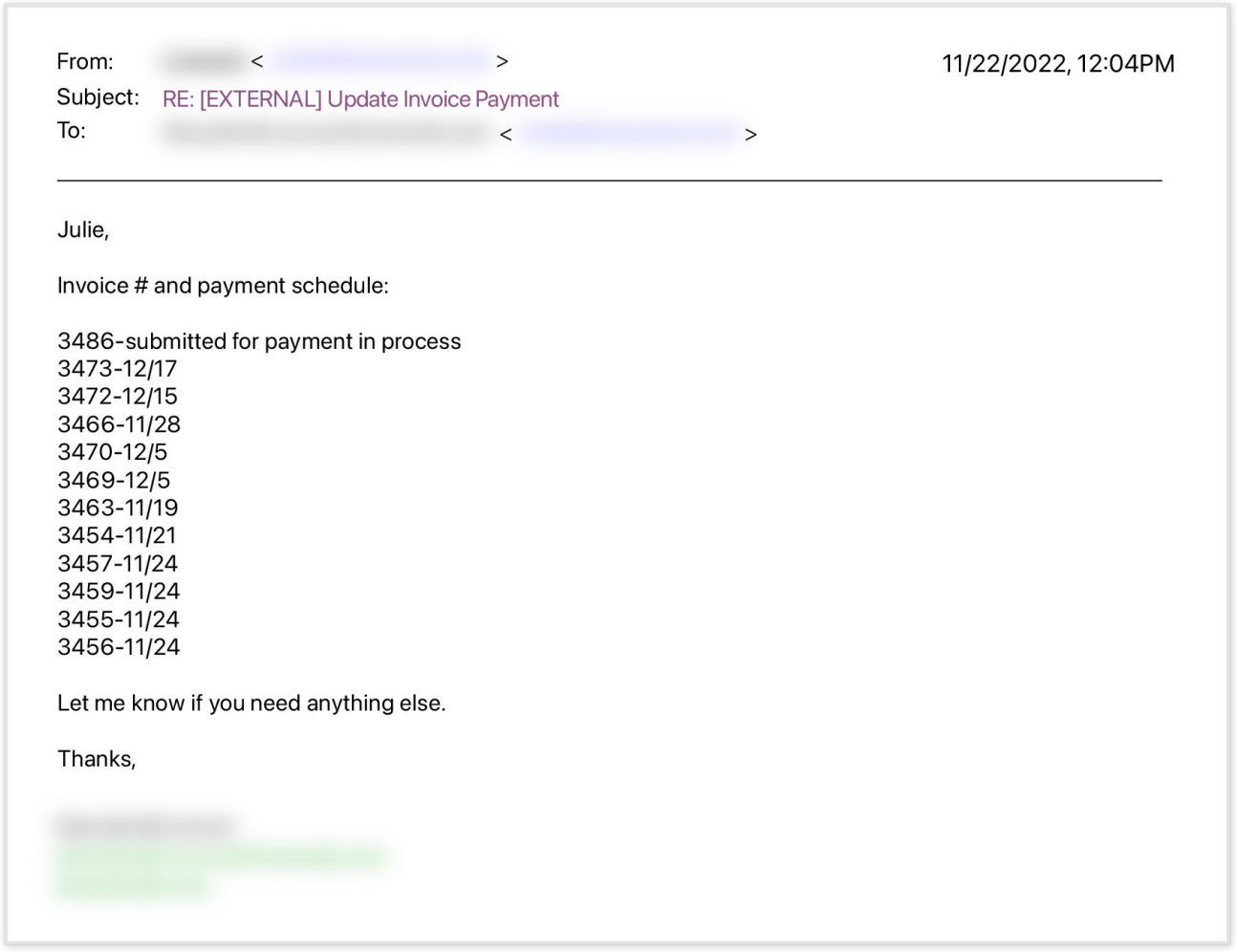
Please acknowledge receipt of this email.

Thanks so much!

[redacted]

To give the appearance of legitimacy, the attacker created a lookalike email address on a domain with a tiny misspelling that could easily be overlooked. For privacy purposes, all identifying information has been censored, but a comparable example would be if the real domain was ***initialus.com*** and the threat actor's email address was hosted on ***intialus.com.***

As you can see, there are no misspellings, no malicious links or attachments, and only minor grammar and punctuation issues. The attacker also used the office manager's real email signature with the company's contact information and logo. Simply put, to most employees, the email would raise zero red flags, which is likely why the target provided the requested information shortly after receiving the message.



From: [redacted] < [redacted] > 11/22/2022, 12:04PM
Subject: RE: [EXTERNAL] Update Invoice Payment
To: [redacted] < [redacted] >

Julie,

Invoice # and payment schedule:

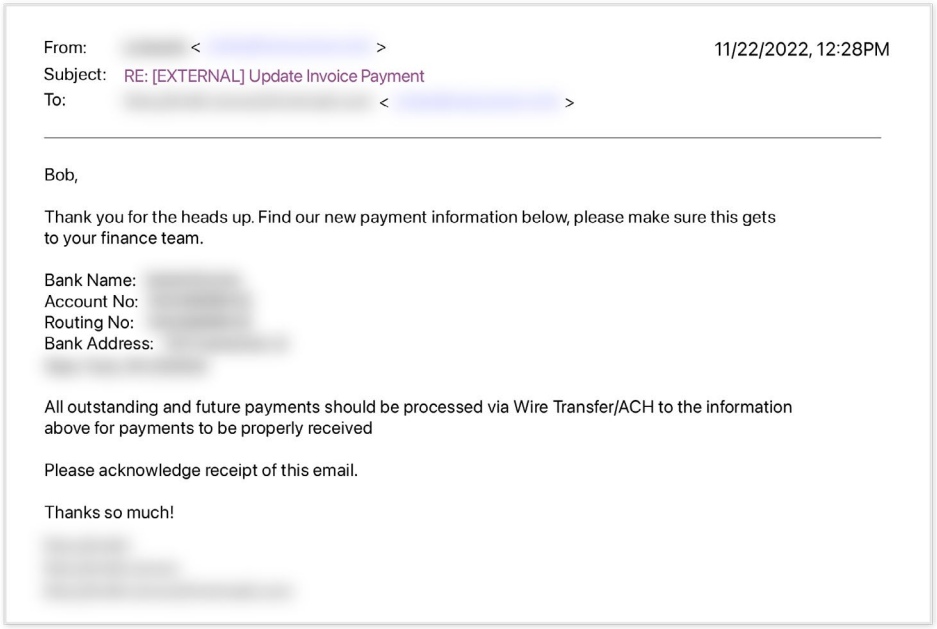
3486-submitted for payment in process
3473-12/17
3472-12/15
3466-11/28
3470-12/5
3469-12/5
3463-11/19
3454-11/21
3457-11/24
3459-11/24
3455-11/24
3456-11/24

Let me know if you need anything else.

Thanks,

[redacted]

The attacker then quickly replied with the "new" bank information, asked that all future payments be sent to that account, and requested that the target confirm receipt of the email.



From: [redacted] < [redacted] > 11/22/2022, 12:28PM
Subject: RE: [EXTERNAL] Update Invoice Payment
To: [redacted] < [redacted] >

Bob,

Thank you for the heads up. Find our new payment information below, please make sure this gets to your finance team.

Bank Name: [redacted]
Account No: [redacted]
Routing No: [redacted]
Bank Address: [redacted]

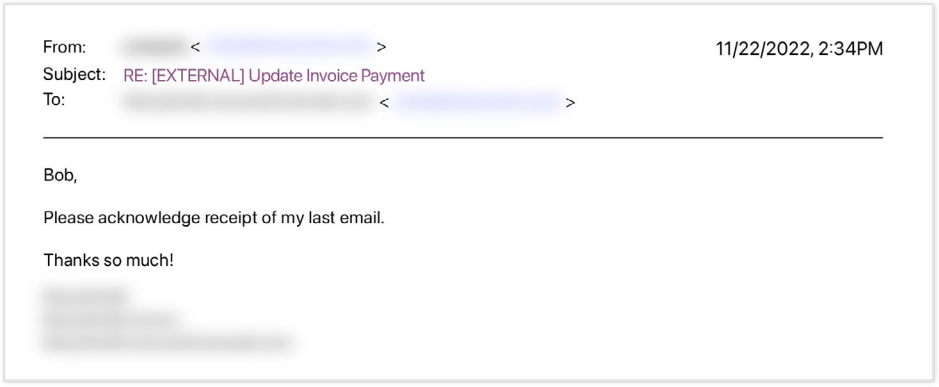
All outstanding and future payments should be processed via Wire Transfer/ACH to the information above for payments to be properly received

Please acknowledge receipt of this email.

Thanks so much!

[redacted]

Understanding that the real office manager could email at any time and torpedo the attempted fund diversion, the threat actor turned up the pressure and sent two follow-up messages in short succession.



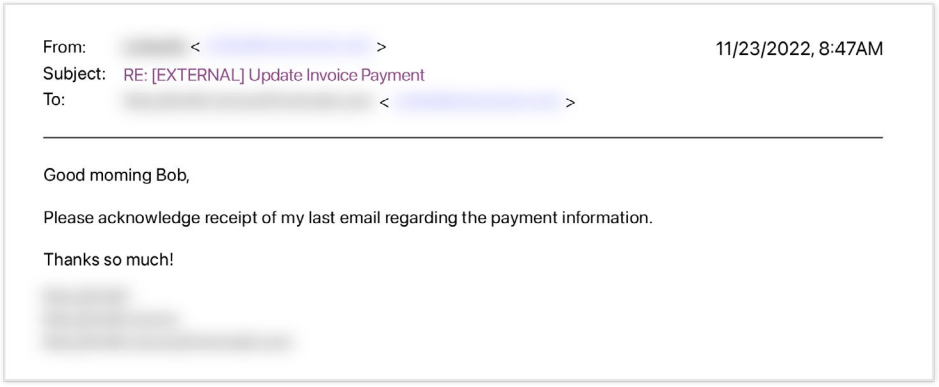
From: [redacted] < [redacted] > 11/22/2022, 2:34PM
Subject: RE: [EXTERNAL] Update Invoice Payment
To: [redacted] < [redacted] >

Bob,

Please acknowledge receipt of my last email.

Thanks so much!

[redacted]



From: [redacted] < [redacted] > 11/23/2022, 8:47AM
Subject: RE: [EXTERNAL] Update Invoice Payment
To: [redacted] < [redacted] >

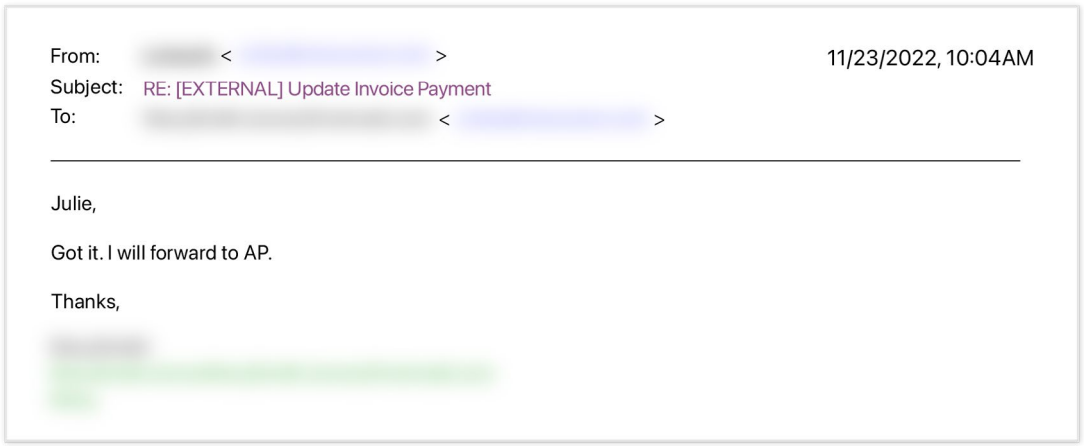
Good moming Bob,

Please acknowledge receipt of my last email regarding the payment information.

Thanks so much!

[redacted]

The technique was successful, and the facilities manager confirmed the new account and routing information would be forwarded to the company’s accounts payable department. At this point, Abnormal stepped in to prevent the attack from moving forward, despite being in passive-only mode.


From: [redacted] < [redacted] > 11/23/2022, 10:04AM
Subject: RE: [EXTERNAL] Update Invoice Payment
To: [redacted] < [redacted] >

Julie,

Got it. I will forward to AP.

Thanks,

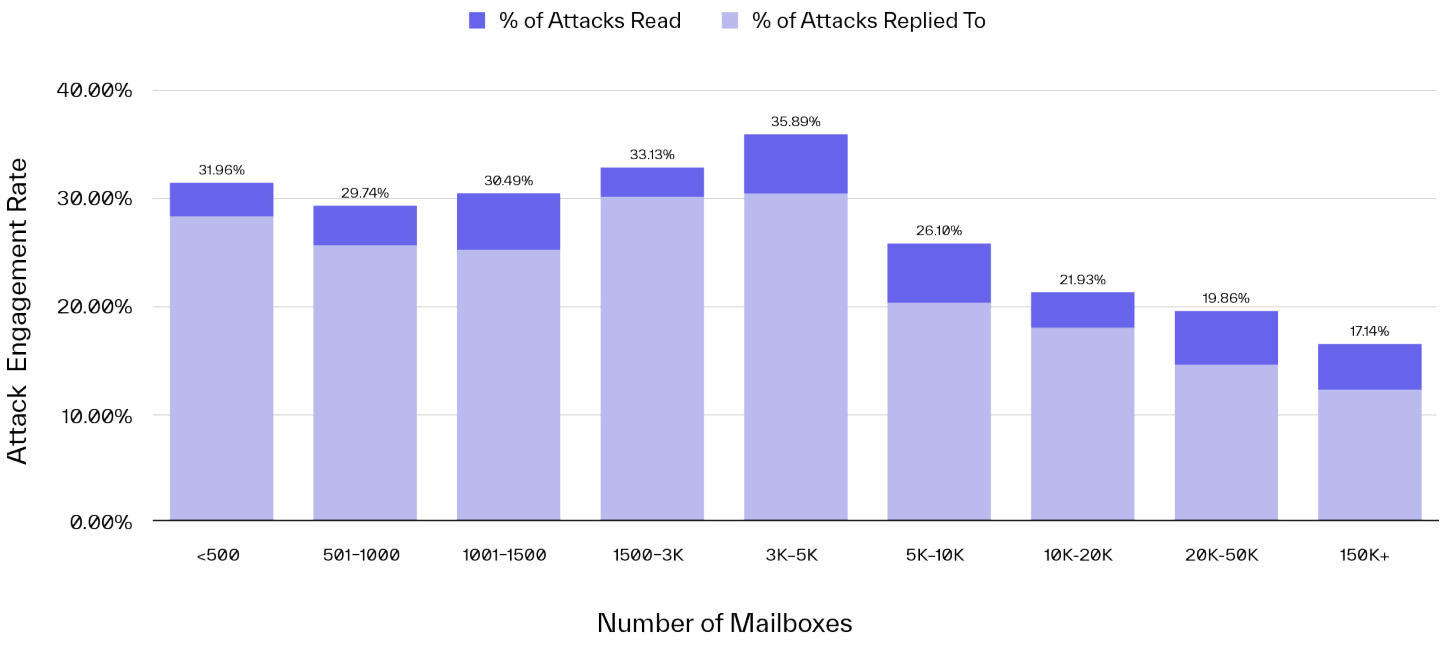
[redacted]

This attack is a prime example of how convincing modern email attacks can be and how cybercriminals can expertly leverage social engineering to trick employees. It emphasizes just how crucial it is to minimize opportunities for your workforce to engage with malicious emails.

Attackers Successfully Engage Employees at Organizations of All Sizes—Often More Than Once

Not only are employees neglecting to report attacks they encounter, but they are also engaging with malicious emails at an alarming rate.

Attack Engagement Rate by Organization Size



Between July and December 2022, we monitored the email environments for hundreds of organizations of various sizes in multiple industries. These companies had implemented Abnormal Inbound Email Security in passive, read-only mode, which means the Abnormal platform was integrated with the organization's mail client but not actively blocking attacks.

During this period, the median open rate for text-based business email compromise attacks, impersonating internal executives and external third parties, was nearly 28%, with an overall average read rate of 20%. Even more concerning was that, of the malicious emails that were read, an average of 15% were replied to.

Further, while only 0.28% of recipients engaged with more than one attack, **over one-third of replies were initiated by employees who had previously engaged with an earlier attack.** While it is impossible to know why this is, there are a few reasons why an employee might become a "repeat responder".

Perhaps they didn't receive sufficient training after the first incident. Employers should not assume that once an employee has experienced the negative consequences of falling victim to an attack, no additional coaching is needed to avoid repeating the error. In fact, as threat actors change their tactics, security awareness training is more important than ever before.

Another explanation could be that these employees are targeted by a greater volume of attacks—particularly if they work in finance. Even with adequate follow-up training, if an employee is bombarded with malicious emails at an above-average rate, the chances of them mistaking an attack for a valid email also increase.

> And finally, there's the possibility that after falling victim to an attack once, an employee may adopt the attitude that "lightning never strikes the same place twice." In other words, rather than becoming more vigilant, they erroneously believe they won't be targeted again.

15%

Average reply rate for text-based BEC attacks.

36%

Percentage of replies to malicious emails initiated by employees who had engaged with an earlier attack.

Employees at All Levels of an Organization Engage with Attacks

Another interesting trend we examined was the apparent correlation between an employee's role in an organization and the likelihood of them reading and/or replying to malicious emails.

Category	Example Job Titles	% of Attacks Read	% of Attacks Read & Replied To
Account Management	Account Manager, Account Director	5.42%	18.75%
Accountant	Accountant, Senior Accountant	21.61%	11.76%
Accounting/Accounts Payable	Accounts Payable Manager, Accounting Analyst	36.25%	8.62%
Accounting Management	Accounting Manager, Controller	22.74%	8.97%
Administrative	Administrative Assistant, Executive Assistant	21.76%	12.77%
Business Development	Account Executive, Sale Development Representative	29.37%	37.84%
Education	Teacher, Assistant Professor	20.95%	10.59%
Entry Level Sales	Sales Associate, Sales Specialist	4.43%	77.78%
Entry- to Mid-Level Human Resources	HR Generalist, HR Coordinator	25.79%	18.29%
Executive/C-Suite	CFO, Vice President	13.63%	18.49%
Finance Management	Finance Manager, Finance Director	18.18%	0.00%
HR Management	Human Resources Manager, Director of Human Resources	30.98%	14.63%
IT Management	IT Manager, Infomation Systems Manager	21.15%	0.00%
Office Administration	Office Administrator, Office Manager	17.65%	6.67%
Payroll	Payroll Manager, Payroll Specialist	20.82%	13.93%
Project Engineering	Project Engineer	16.96%	47.37%
Project Management	Project Manager, Senior Project Manager	13.62%	24.53%
Sales Management	Sales Manager, Regional Sales Manager	21.77%	29.63%
School Administrator	Principal, Assistant Principal	28.17%	0.00%
Student	Student, Graduate Assistant	13.36%	21.74%

Employees in roles across human resources and accounts payable had some of the highest open rates, ranging from 26–31% for the former and 22–36% for the latter. However, the rate at which they replied to malicious emails was not nearly as high as employees in other positions. This may indicate that these professionals are growing increasingly aware of their popularity as attack targets and becoming more adept at recognizing when an email is suspicious.

On the other hand, employees in mid-level, sales-specific positions, most notably Sales Managers and Account Executives, had some of the highest open and reply rates, ranging from 22-38%. Interestingly, although employees in entry-level sales roles like Sales Associates and Sales Specialists had below-average open rates, **they replied to threat actors a whopping 78% of the time** when they opened the email.

It's not surprising to see that employees in sales-oriented roles are more likely to read and respond to malicious emails.

These positions rely heavily on email correspondence, are usually among the most public-facing in an organization, and often involve interacting with a variety of different departments and vendors—not to mention customers. Additionally, the roles are traditionally commission-based, which means employees are financially motivated to be helpful, respond to inquiries quickly, and resolve issues promptly.

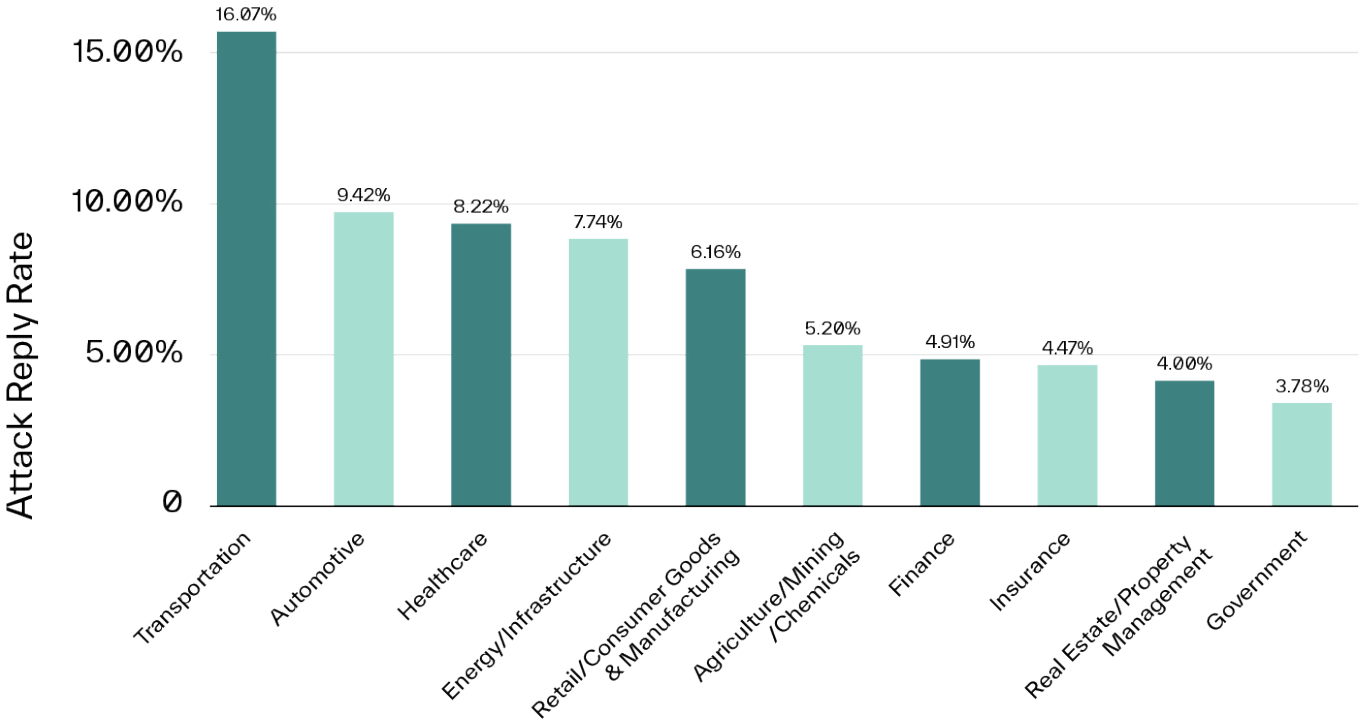
> That said, while these results aren't unexpected, they are certainly concerning. What the figures underscore is how important it is to provide proactive and ongoing security awareness training to employees in these positions since, by the nature of their roles themselves or the personalities of those who fill them, they are at a greater risk of responding to these email attacks.

Transportation, Automotive, and Healthcare Employees Most Likely to Reply

While professional services providers, educational institutions, and religious organizations received the highest volume of attacks during the last half of 2022, employees at these businesses were not the most likely to read and reply to malicious emails.

Our data showed that it was actually employees at transportation providers, automotive enterprises, and healthcare organizations who were most likely to reply to attacks.

Industries with Highest Attack Reply Rates



Historically, transportation providers have been focused more on physical security than cybersecurity. In fact, it's only within the past five years that CEOs have begun reporting cybersecurity as a top priority—and usually only after experiencing a major security incident.

Abnormal™

Additionally, there is generally an increased sense of urgency with respect to maintaining operations in the transportation industry. Resolving an issue quickly (whether that's providing information or settling an outstanding balance) can mean the difference between business as usual and a catastrophic disruption in services.

While professionals in any industry are fighting an uphill battle against email attacks, employees at automotive enterprises are at a particular disadvantage. The names, positions, and contact information for employees at all levels (including executives) as well as the organizational hierarchy for auto groups are usually easily accessible—often on the company's website. These are all details cybercriminals can easily leverage to make convincing socially-engineered attacks.

In addition, automotive groups rely on complex supply chains and vast vendor ecosystems, which means attackers have ample third parties to impersonate and vulnerabilities to exploit.

And finally. employees at healthcare organizations are also at a greater risk of falling victim to socially-engineered attacks, albeit for different reasons. The healthcare industry tends to attract individuals who have a stronger desire to help others—a characteristic that cybercriminals will gladly use to their advantage.

Further, there is a high rate of turnover in larger healthcare organizations and hospital systems, so employees are less likely to know their colleagues personally, making impersonation easier.

Business Email Compromise Shows No Signs of Slowing

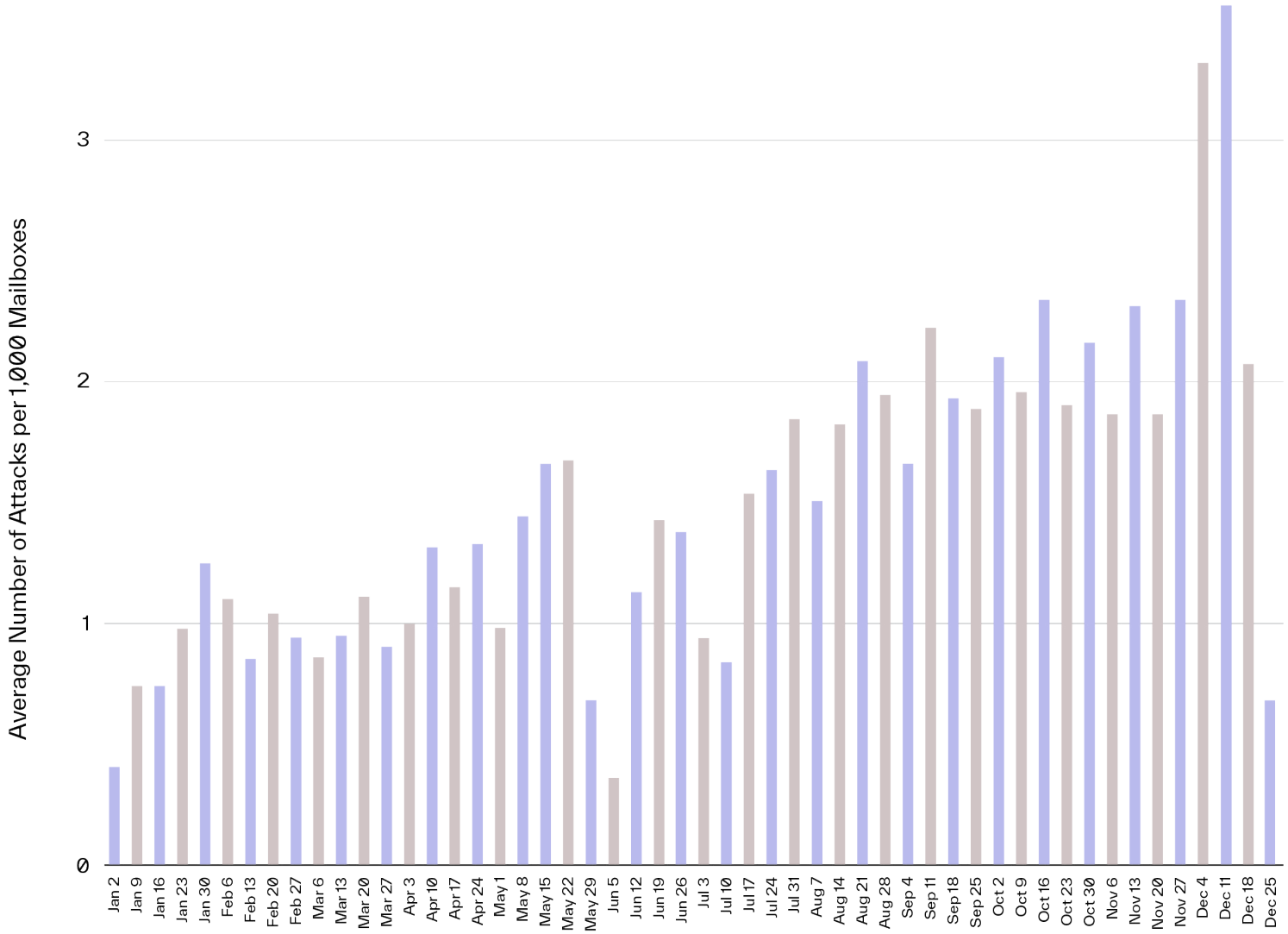
Most companies pride themselves on their ability to effectively target customers by conducting extensive research on their audience. This is exactly what modern threat actors do. Rather than launching high-volume, low-value attacks like the spam campaigns of the past, cybercriminals now create convincing and targeted text-based emails that bypass traditional security solutions.

Making matters worse, these business email compromise attacks are becoming more sophisticated as threat actors leverage information on LinkedIn, SEC disclosures, and even the target organization’s website to create emails that are more likely to trick employees.

Significant Growth in Business Email Compromise Attacks Continues

BEC attacks grew by more than 81% between the first and second halves of 2022, from 1.07 attacks per 1,000 mailboxes to 1.94—a similar percentage increase to what we recorded in 2021.

Median Weekly BEC Attacks per 1,000 Mailboxes



Abnormal™

Interestingly, there was a considerable spike in volume at the beginning of December. The average number of attacks per 1,000 mailboxes in the first two weeks of December was 64% higher than the overall weekly average in October and November.

As mentioned earlier, we consistently see a significant decline in attack volume during the last few weeks of the year. With this in mind, the most likely explanation for the sharp increase is cybercriminals attempting to acquire as many funds as possible prior to the holidays. Then, as expected, BEC attack volume plummeted starting the week before Christmas before picking back up in January.

In previous reports, we've called out the number of weeks in which there was at least one attack per 1,000 mailboxes. As BEC attack volume has steadily grown, we're now seeing multiple weeks in which there were at least two attacks per 1,000 mailboxes. In the second half of 2022, we observed 10 weeks where this was the case.

> While this may not appear to be a large number, it's important to remember that due to their nature, BEC attacks result in the most financial damage. The fact that these numbers have nearly doubled in only six months is indicative of attackers' continued success and their search for additional ways to trick employees into providing them with money and access.

Smaller Organizations See Nearly 150% Increase in BEC Attacks

Similar to what we observed in our analysis of January-June 2022, organizations with fewer than 1,000 mailboxes experienced the greatest increase in BEC attacks during the second half of the year—from an average of 1.75 per 1,000 mailboxes to 4.33.

Number of BEC Attacks per 1,000 Mailboxes by Organization Size

Clearly, the risk of business email compromise isn't limited to large multinational enterprises as even smaller organizations are vulnerable to these attacks. And while breaches in huge enterprises create the headlines, the data shows that threat actors are still very attracted to small organizations. In fact, smaller businesses are potentially ***more*** susceptible, as budget restrictions may prevent them from allocating adequate resources to cybersecurity tools and training.

Additionally, while larger organizations experience fewer BEC attacks per 1,000 mailboxes, this doesn't mean their risk is lower. Business email compromise is highly targeted, with threat actors focusing primarily on the employees who either manage the company's finances or control access to sensitive data. As a result, the number of BEC attacks doesn't necessarily increase as the size of the organization grows.

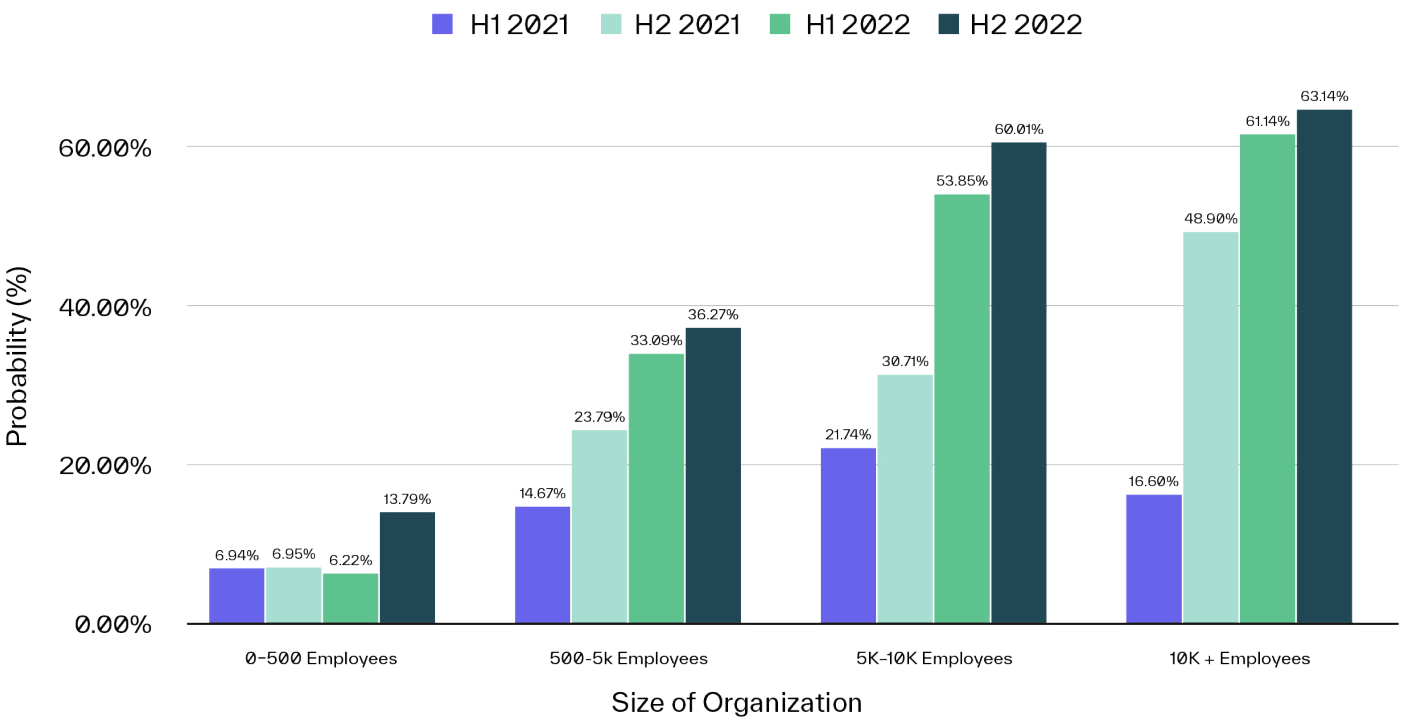
Supply Chain Compromise Persists as Popular Attack Strategy

When cybercriminals take over vendor email accounts, they can send fraudulent invoices and requests to update payment account information to any customer of that vendor. What makes this form of BEC, often referred to as supply chain compromise or vendor email compromise, especially insidious is that because attackers have access to previous correspondence, they can hijack ongoing conversations or mimic vendor communications exactly.

Larger Organizations Have Highest Probability of Supply Chain Compromise Attack

While even the smallest businesses likely work with at least a few vendors, larger companies have supplier numbers in the hundreds or thousands. And when every partner represents another entity that can be impersonated or compromised, it's not surprising that the likelihood of an organization being targeted by sophisticated supply chain compromise attacks rises as company size increases.

Probability of Receiving a Supply Chain Compromise Attack by Organization Size



At nearly 14%, the probability of an organization with fewer than 500 employees experiencing a supply chain compromise attack certainly isn't so low that smaller businesses should dismiss the threat entirely. Security leaders should still take steps to educate and protect employees as even a single successful supply chain compromise attack can have devastating consequences—particularly in smaller organizations. In fact, the largest supply chain compromise attack stopped by Abnormal included a fake invoice for over $2.1 million.

That being said, the risk for larger enterprises with a workforce of over 5,000 is considerably higher—averaging above 60% over the last half of 2022.

Abnormal™

While the likelihood of any organization being targeted by a supply chain compromise attack has risen over time, we saw a notable increase in the second half of 2022. For an organization with 5,000-10,000 employees, the probability of experiencing an attack grew by 26%, from 53% to 67%, between Q3 and Q4. Similarly, for an organization with more than 10,000 employees, the likelihood jumped by 22%, from 57% to 70%.

Because threat actors know that companies are closing out their books at the end of the year, they tend to ramp up their attacks at the start of Q4. This is likely due to the fact that not only do organizations tend to be busier and thus more distracted, but there is also typically an increase in legitimate financial requests during this time period.

> As macroeconomic conditions worsen and acquiring funds through legitimate means becomes progressively more difficult, we can anticipate continued growth in these sophisticated, vendor-focused attacks.

70%

Probability of an enterprise with more than 10,000 employees receiving a supply chain compromise attack in Q4 2022.

Hospitality, Construction, and Retail Organizations Most Targeted by Vendor Fraud

Along with larger organizations, there are certain industries that cybercriminals appeared to target more often for supply chain compromise in the second half of 2022: hospitality, construction/engineering, and retail/consumer goods and manufacturing.

Industry	Likelihood of Being Targeted (July–December 2022)
Hospitality	92.0%
Construction/Engineering	91.9%
Retail/Consumer Goods & Manufacturing	91.5%
Agriculture/Mining/Chemicals	90.9%
Healthcare	88.7%
Automotive	87.5%
Professional Services	86.7%
Transportation	86.4%
Energy/Infrastructure	82.8%
Food Processing & Distribution	80.0%

Attackers know that hotels, resorts, and other hospitality businesses have troves of personally identifiable information (PII) on guests. Plus, breaching one property in a centralized network often grants access to the entire chain. Additionally, like employees in the healthcare industry, hospitality personnel are generally more willing to go to great lengths to be helpful.

Hospitality organizations also have massive vendor ecosystems composed of furniture and fixture providers, HVAC maintenance specialists, property maintenance companies, cleaning services, and more—all of which can be impersonated or compromised.

Construction was not far behind, as modern construction projects require the use of multiple digital systems spread across numerous job sites and offices, all of which result in a large attack surface. Coordinating major projects necessitates a constant flow of confidential and proprietary information (including financial data) between a broad network of vendors, contractors, and subcontractors, which creates ample opportunities for attackers to hijack conversations.

Moreover, the construction industry as a whole has avoided heavy regulation with respect to data security and privacy laws—making them especially vulnerable to cyberattacks.

And even before the COVID-19 pandemic, major retailers and consumer goods companies relied on enormous email ecosystems of employees and vendors. But starting in 2020, these organizations had to rapidly expand their supply chains and partner networks to avoid stockouts and disruptions to operations. Many also had to hastily augment their ecommerce capabilities or even build ecommerce environments from scratch.

Establishing these new relationships and making these investments were arguably necessary to support business continuity, but they also created new entry points for cybercriminals to take advantage of.

> Unfortunately, no matter which industry your organization is part of, supply chain attacks are targeting you. It’s only a matter of time before threat actors figure out who they need to impersonate, and how to do it, in order to be successful in these vendor-focused attacks.

Protecting Your Organization From Email Threats

As long as companies use email, cybercriminals will launch email attacks. And as attackers continue to upgrade and enhance their strategies, it will become increasingly difficult for your employees to differentiate these threats from legitimate emails.

While security awareness training will help reduce the risk of employees engaging with a threat actor, it's even better to minimize the number of attacks they receive in the first place. Any time an employee has to assess whether an email is malicious is an opportunity for them to make a mistake—and for an attacker to capitalize.

And the data shows that employees are notoriously bad at making that distinction. Thus, the most effective way to prevent your workforce from falling victim to an attack is to invest in an email security solution that ensures attacks are never delivered in the first place.

Because advanced email attacks like business email compromise and supply chain compromise exploit trusted email accounts and relationships, organizations need email security that can detect even small shifts in activity and content. The most effective email security platforms baseline known-good behavior across employees and vendors, and then detect and remediate malicious emails in milliseconds to prevent end-user engagement.

Traditional email security solutions lack the capabilities needed to block these advanced inbound email attacks. And as we've seen over the past few years, these threats will only continue to grow both in frequency and complexity. Implementing modern email security technology that pairs advanced behavioral science with risk-adaptive detection is the only surefire way to defend your organization against advanced threats and keep your employees from making a catastrophic decision.

Abnormal

Abnormal Security provides the leading behavioral AI-based security platform that leverages machine learning to stop sophisticated inbound email attacks and dangerous email platform attacks that evade traditional solutions. The anomaly detection engine leverages identity and context to analyze the risk of every cloud email event, preventing inbound email attacks, detecting compromised accounts, and remediating emails in milliseconds—all while providing visibility into configuration drifts across your environment.

You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly. More information is available at abnormalsecurity.com.

Interested in Stopping Modern Email Attacks?

Request a Demo:

abnormalsecurity.com →

Follow Us on Twitter:

@AbnormalSec

 v_1.0 / February_2023