

Abnormal



EMAIL THREAT REPORT / H1 2022

Fraudsters Use Email in Phone Fraud Scams, Targeting **89%** of Organizations

Executive Summary

Modern threats continue to increase in volume and severity, as cybercriminals turn from low-value attacks to more sophisticated, high-value strategies that rely on social engineering to trick recipients into sending money or leaking sensitive information. And because these threats contain few indicators of compromise, they evade secure email gateways and other traditional systems, landing in employee inboxes where they can cause significant damage.

New Malware Tactic Involves Phone Fraud

Starting in the spring of 2021, Abnormal noticed an increase in scams that encouraged recipients to do something fairly unexpected—pick up their phone and call the scammers. Once they do so, they are asked to download a file that contains BazarLoaders malware, from which cybercriminals can deploy ransomware. This relatively new tactic increased dramatically throughout the last half of the year, with nearly a third of all organizations receiving at least one attack in the third quarter, and over half in the fourth quarter. Probability of receiving an attack peaked in early December, with an 89% chance of attack for each organization.

Executives Impersonated Less... But Attacked More

While the number business email compromise attacks per 1,000 mailboxes nearly doubled this half, impersonation tactics have changed. While we've traditionally seen attacks impersonating VIPs, there was a 32.7% decrease in attacks impersonating executives from the first to last quarter of 2021. In contrast, the number of attacks received by these same executives increased by nearly 24% over the same period.

84%

increase in the number of business email compromise attacks in H2 2021.

72%

probability of receiving a phone fraud attack each week for large enterprises.

67%


chance of receiving a supply chain compromise attack this half.

23.9%

increase in executive targeting between the first and last quarters of the year.

Table of Contents

Email Attacks Increase in Volume as Cybercriminals Change Tactics	4
Phony Phone Fraud Starts with Email	7
Supply Chain Compromise Risk Remains Steady	12
Business Email Compromise Increases as Cybercriminals Turn to High-Value Attacks	15
Expect an Increase in Modern Attacks	22
About Abnormal	23



Email Attacks Increase in Volume as Cybercriminals Change Tactics

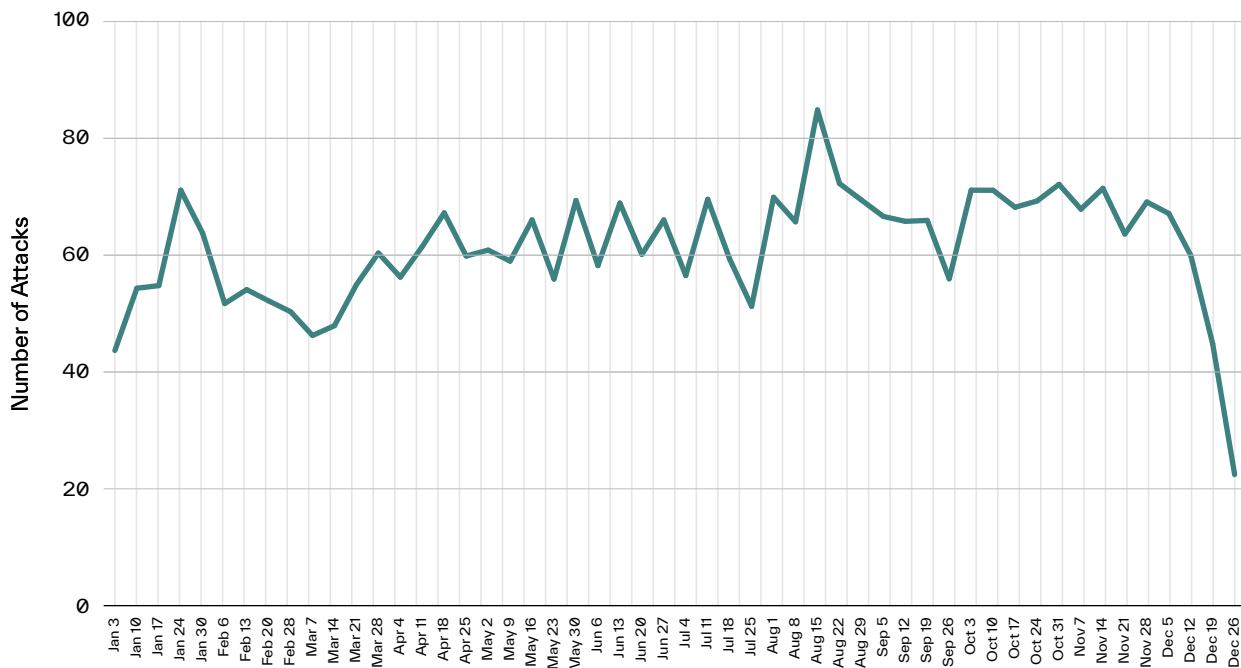
As email security becomes more prevalent for organizations worldwide, we may expect the number of email attacks to drop, as cybercriminals look for new ways to penetrate organizations and complete their scams. Data from the last year shows that this is simply not the case.

Attack Volume Increases by 10%

Over the course of the last half of 2021, overall attack volume increased by 10.33%, from an average of 58.26 attacks per 1,000 mailboxes to an average of 64.28. While no singular attack type stands out as the culprit here, it's clear that threat actors are continuing their schemes, focusing on tricking end users into providing credentials and sending money to their bank accounts.

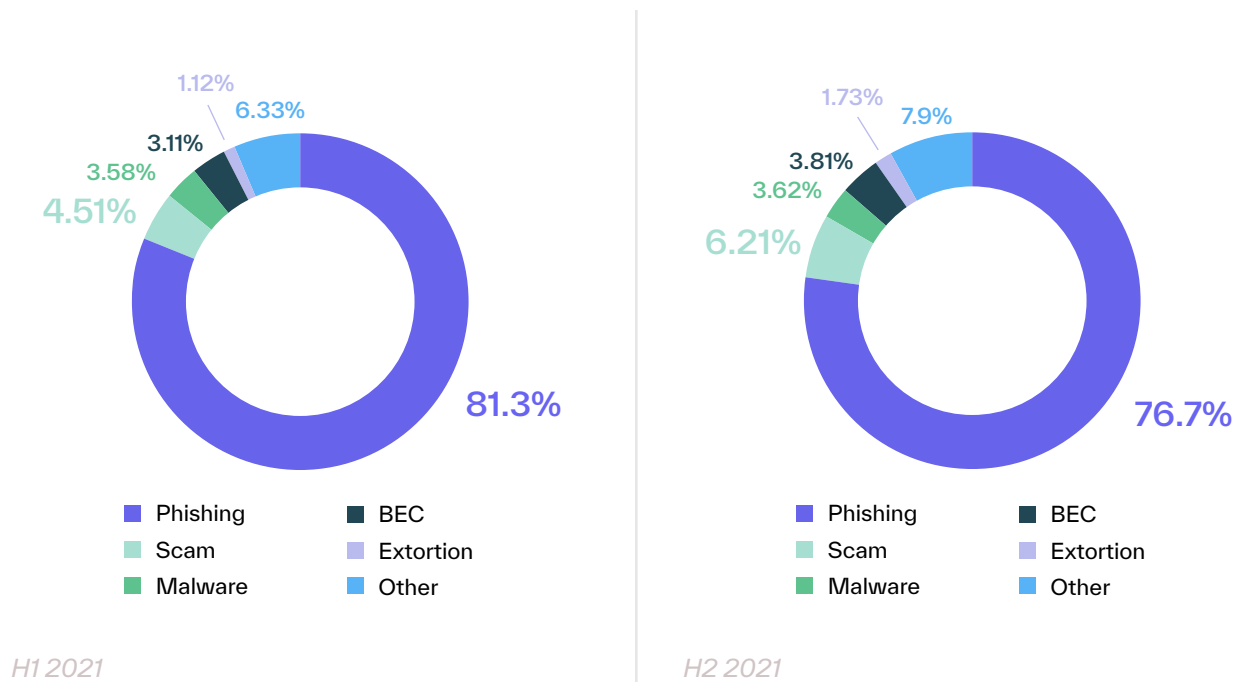
One interesting callout is that while the holidays tend to be a slow period as employees take time off to spend it with their families, the same can be said for these threat actors. The average weekly attack volume dropped significantly in the last two weeks of the year, from an average of 59.97 per 1,000 mailboxes in the second week of December, to only 22.44 attacks the week between Christmas and New Year's Day.

Attacks per 1,000 Mailboxes



When looking at attack type, the percentage of attacks focused on credential phishing dropped a bit, while scams and business email compromise rose. This could be attributed to the fact that cybercriminals are seeing more success with text-based attacks that bypass traditional security tools, so they're moving away from attacks that include a link—a common attribute in credential phishing attacks.

Percentage of Advanced Attacks by Type



We also saw an increase in scams this half, as threat actors turned to new tactics, heavily relying on phone calls to steal money from their victims.

22.6%
 increase in business email compromise as percentage of all attacks.

Phony Phone Fraud Starts with Email

Starting in the spring of 2021, Abnormal noticed an increase in scams that encouraged recipients to do something fairly unexpected—pick up their phone and call the scammers. These emails use a variety of scare tactics, often involving a pending charge, to prompt their targets to call the phone number provided within the email.

Subject: Subscription renewal charge...
Sender: Geek Squad <jenniferalex877y@gmail.com>
Recipient: Esquada, Alma <alma.esquada@ [REDACTED]>
Nov 12th 06:36 AM PST

Hello subscriber,

Your subscription for Geek Squad protection has been successfully renewed and updated. The debited amount will be reflected within the next 24 to 48 hrs on your account statement,

PRODUCT INFORMATION:

Invoice No: W-97635464

Product Name: Geek Squad SECURITY

Order Date: November-12-2021

Expiration Date: 1 Year from the date of purchase

Price: 299.99 USD

Payment Method: Auto-Renewal

If you wish to cancel this subscription then please feel free to contact our billing department as soon as possible. you can reach us on **+1 (818) 921 7115**

Once they do so, they are directed to a website to download some type of file that then installs a form of malware, typically BazarLoader, on their computer. This initial installation allows attackers to then install additional malware that can be used for ransomware attacks.

An Emerging (and Growing) Trend

Vishing, or voice phishing, has become an increasingly popular tactic in recent years, but these phone fraud attacks are different in that they start with a phishing email. They then direct users to call them, versus directly calling the target as part of the vishing scam. These phone fraud attacks are likely geared toward consumers, but it is clear that threat actors were willing to scam organizations as well—and may even prefer them. In cases uncovered by Abnormal, impersonated brands included PayPal, Microsoft, Amazon, Norton AntiVirus, and Best Buy, all of which could be used for both personal and business transactions.

These phone scams were first detected [in the first part of the year](#), but started increasing in the third quarter and picked up significantly in December—right before the holidays, perhaps when the scammers knew that people would be more concerned about money being unexpectedly deducted from their bank accounts.

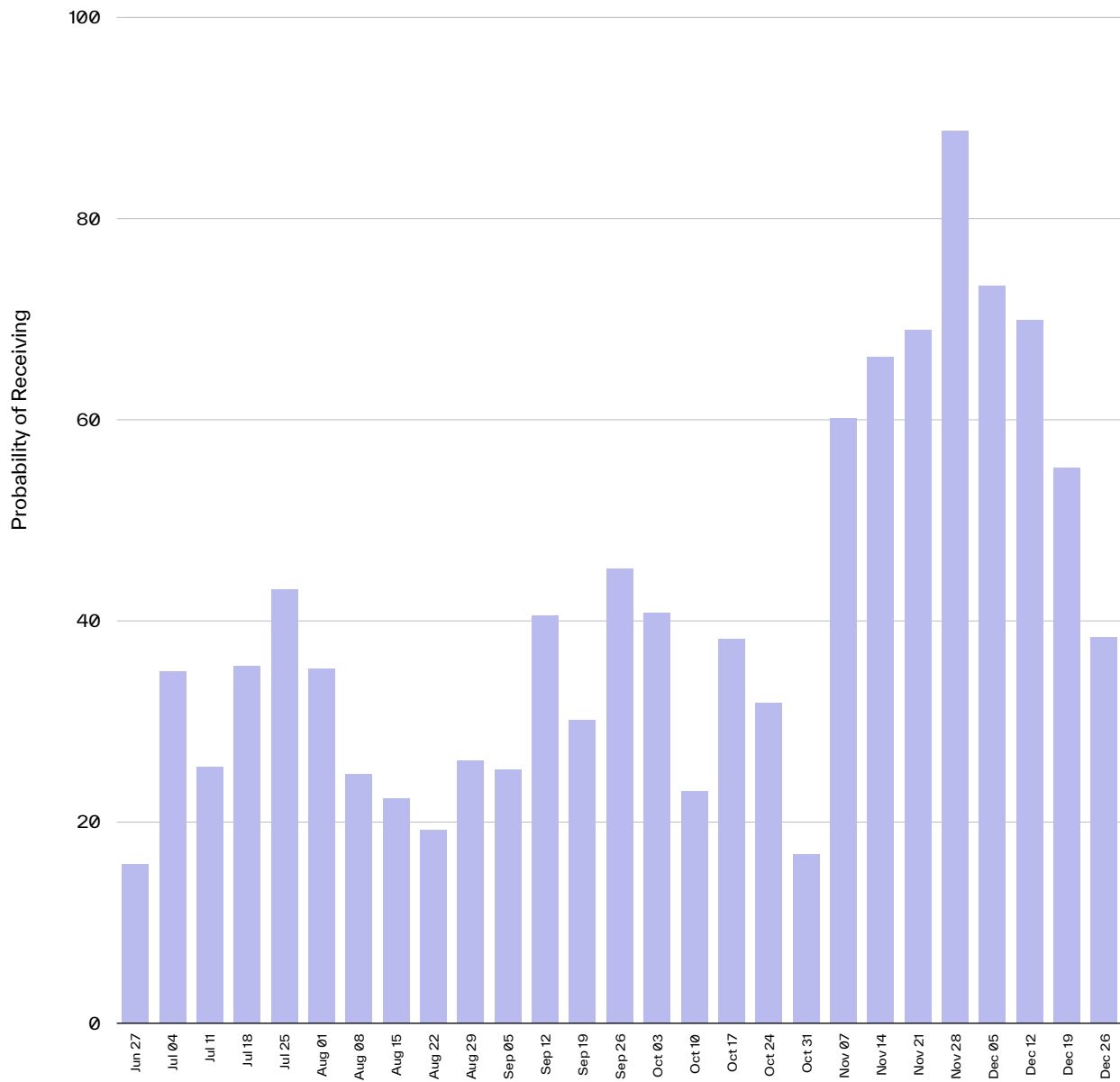
The likelihood of receiving these attacks increased dramatically throughout the last half of the year, with 31.4% of organizations receiving at least one attack in the third quarter, and over half in the fourth quarter. But that number jumped even more in December, with organizations reaching a 59.2% likelihood of attack in the last month of the year. The highest week saw a 89% chance of attack, before dropping back to average levels closer to the holidays.



59.2%

chance of receiving a phone fraud attack in December.

Weekly Probability of Receiving Phone Fraud Attacks

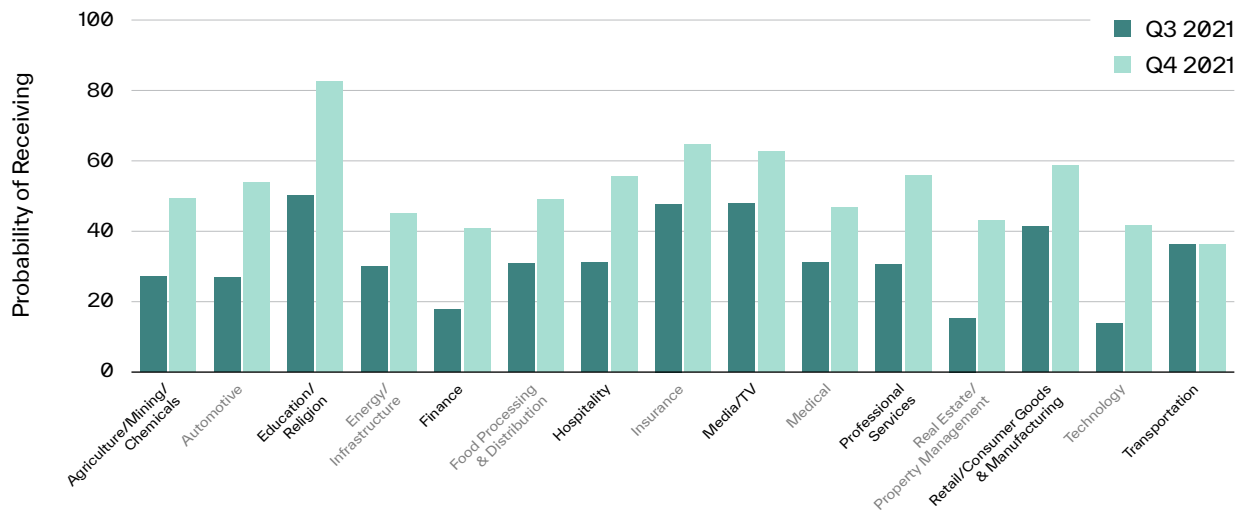


Education and Religious Organizations at Highest Risk for Phone Fraud Attacks

While all industries are targeted by these phone fraud attacks, there was one that had a significantly higher chance of receiving an attack: education and religion. Perhaps because this industry is comprised largely of nonprofits who may not have the budget for email security tools, organizations within the industry had a 82% probability of receiving an attack like this in the last three months of the year.

This was followed by the insurance and media industries, both with over a 60% probability of attack each week in the fourth quarter. Shortly following were retail and consumer goods, professional services, and hospitality with more than a 50% probability of receipt.

Weekly Probability of Receiving Phone Fraud Attacks by Industry



That said, all industries were impacted both by the initial round of attacks in July through September, and especially by the additional attacks in the last quarter of the year. The largest increase in probability was felt by the technology industry, which experienced a 203% increase in probability of receipt over the course of the quarter.

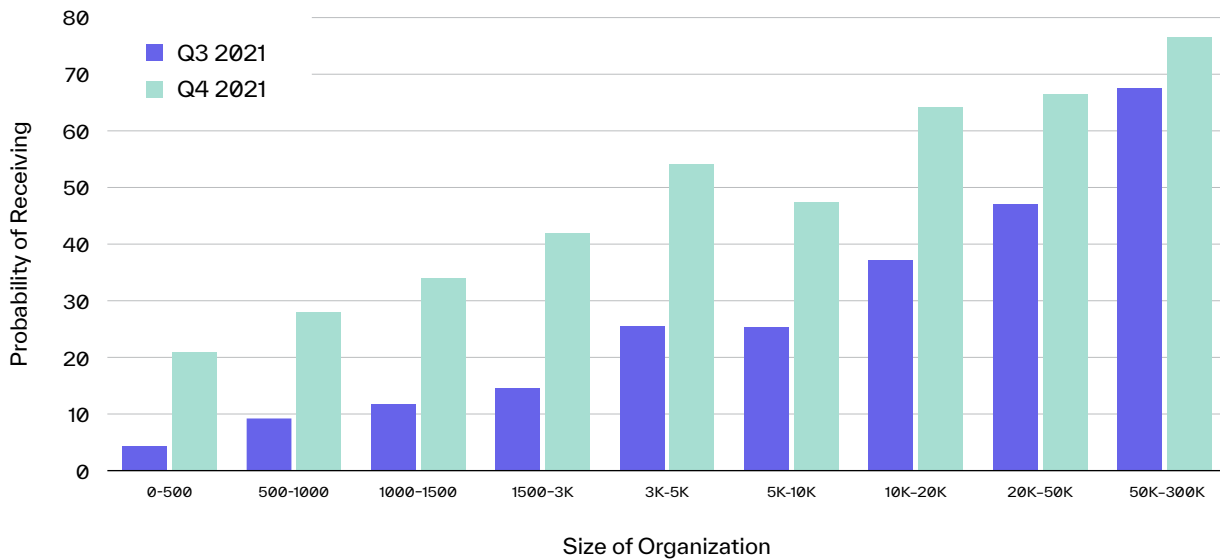
64%

increase in probability of receiving a phone call attack for education and religious organizations.

Largest Organizations at Largest Risk for Phone Fraud

Perhaps unsurprisingly, those organizations with the most employees had the largest probability of receiving an attack. Small businesses under 500 employees were fortunate to experience only an average 12% probability of attack throughout the half, but large organizations comprised of more than 50,000 employees received an attack nearly three weeks out of each month.

Weekly Probability of Receiving Phone Fraud Attacks by Organization Size



While business email compromise attacks mainly target executives or those in the finance department, these phone fraud attacks could be relevant to almost anyone. As such, it makes sense that the chance of receiving an attack simply grows alongside the number of people within the organization.

No matter the size, one thing is for sure—threat actors saw success with phone fraud attacks in 2021 and doubled down on this attack type in the last quarter of the year. It remains to be seen if this trend will continue into 2022, particularly as end users become more aware of the tactic.

72%
 probability of receiving a phone fraud attack each week for organizations with 50,000+ employees.

Supply Chain Compromise Risk Remains Steady

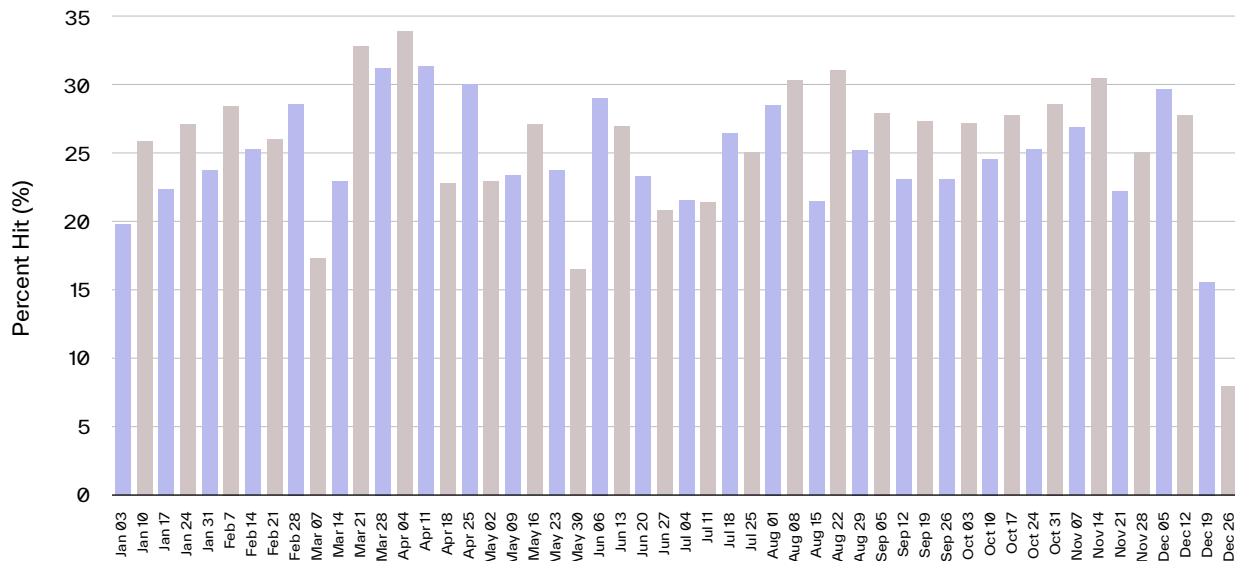
Known also as vendor email compromise, supply chain compromise is a relatively new cyber threat in which cybercriminals successfully phish for vendor email credentials, access the email accounts, and then use those compromised accounts to send attacks on partners—often related to an unpaid invoice or a billing account update.

Because the threat actor can use the compromised account to access past and ongoing conversations and then use that knowledge to trick recipients, this attack type is extremely dangerous to those who receive one of these emails.

Threat Remains Constant Across 2021

Since Abnormal has tracked supply chain compromise, the risk has continuously increased, at least until the last half of 2021 where it remained steady for the first time. That is not to say that the threat should be taken lightly, as more than a quarter of all Abnormal customers were the target of at least one of these threats each week.

Percentage of Abnormal Customers Targeted with a Supply Chain Compromise Attack Each Week



This means that nearly two-thirds of all customers are likely to receive at least one attack over the course of the half. And with the average attack size remaining at \$183,000, this is not a threat to be taken lightly.

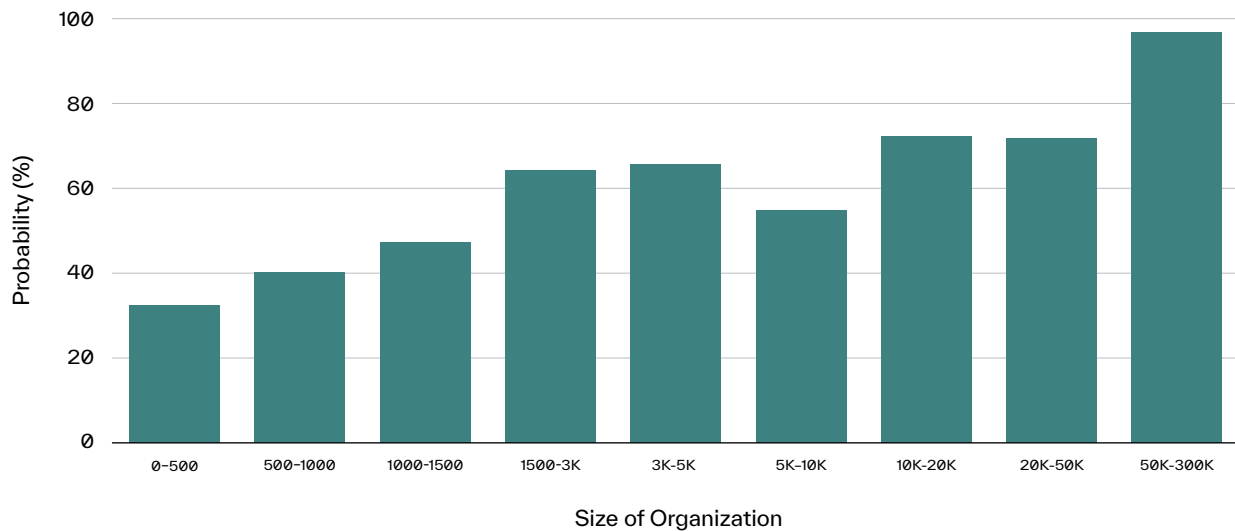
67%

chance of receiving a supply chain compromise attack in H2 2021.

Large Organizations Still at Largest Risk

Similar to what we've seen with phone fraud attacks, those organizations with more employees are simply at the largest risk of receiving an attack. While this is likely a result of there being more employees to target, particularly within the finance department, some of this can also be attributed to the fact that larger organizations often have more vendors who can become compromised. When it comes to the numbers game, cybercriminals often win.

Probability of Receiving a Supply Chain Compromise Attack by Organization Size



Those organizations with 50,000 or more employees receive an attack from their supply chain nearly every single week, and even those with more than 1,500 employees are likely to receive one nearly two weeks out of every three. It's only when looking at small businesses that there is a small amount of relief, with threat actors hitting those with employee counts below 500 only one week in every three.

Regardless of the reason, the issue is clear—all organizations must secure their email from vendor fraud, particularly because these attacks are nearly impossible to recognize by the human eye.

96.7%

probability of receiving a supply chain compromise attack each week for organizations with 50,000+ employees.



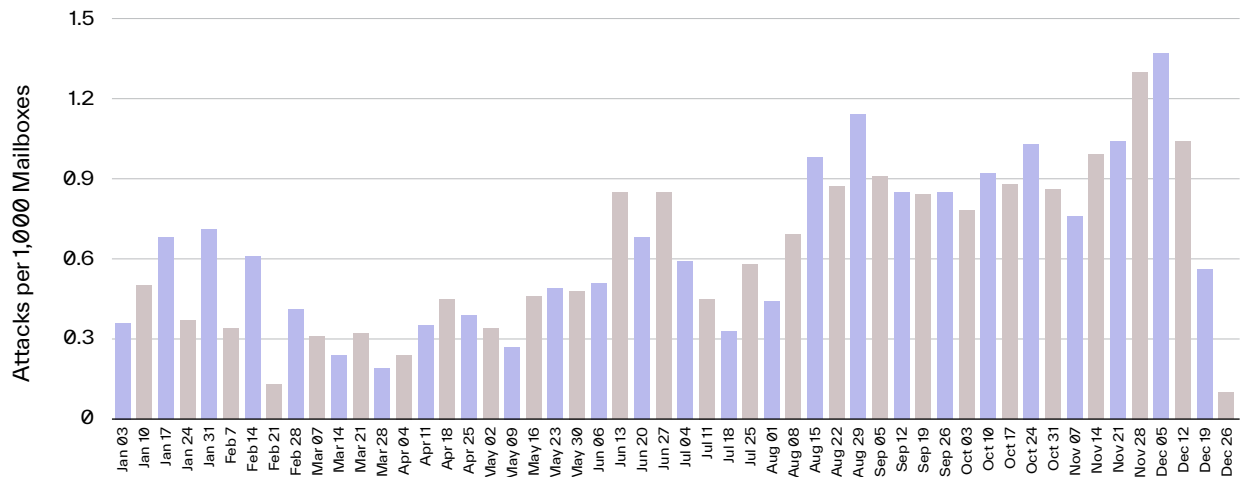
Business Email Compromise Increases as Cybercriminals Turn to High-Value Attacks

Despite increased awareness of business email compromise (BEC), threat actors continue to see success. According to the FBI, financial losses from the crime have increased by 44% since 2018, accounting for \$1.86B lost in 2020. And according to all trends, this number is going to increase in 2021.

Significant Increase in Business Email Compromise Attacks

While BEC attacks make up only a small percentage of all advanced attacks, they are especially concerning because they use impersonation of an employee or trusted partner to establish rapport with the victim and convince them to engage in actions such as paying fake invoices, buying gift cards, or providing access to sensitive data. This half, there was an astounding 84% increase in these attacks over the previous half of the year.

Median Weekly BEC Attacks per 1,000 Mailboxes



By sheer numbers, business email compromise attacks are not that common—with an average of only .44 attacks per 1,000 mailboxes in the first half of the year. That said, the number of attacks climbed to .82 per thousand mailboxes in the second half of 2021. One interesting note is that there were six weeks over the half where there was at least one attack per thousand mailboxes—peaking at 1.37 attacks in early December.

And it's important to remember that volume does not equal value when it comes to business email compromise. One successful attack could have dire financial or reputational consequences for an organization.

84%
 increase in the number of business email compromise attacks in H2 2021.

Small Businesses Receive Most BEC Attacks per Mailboxes

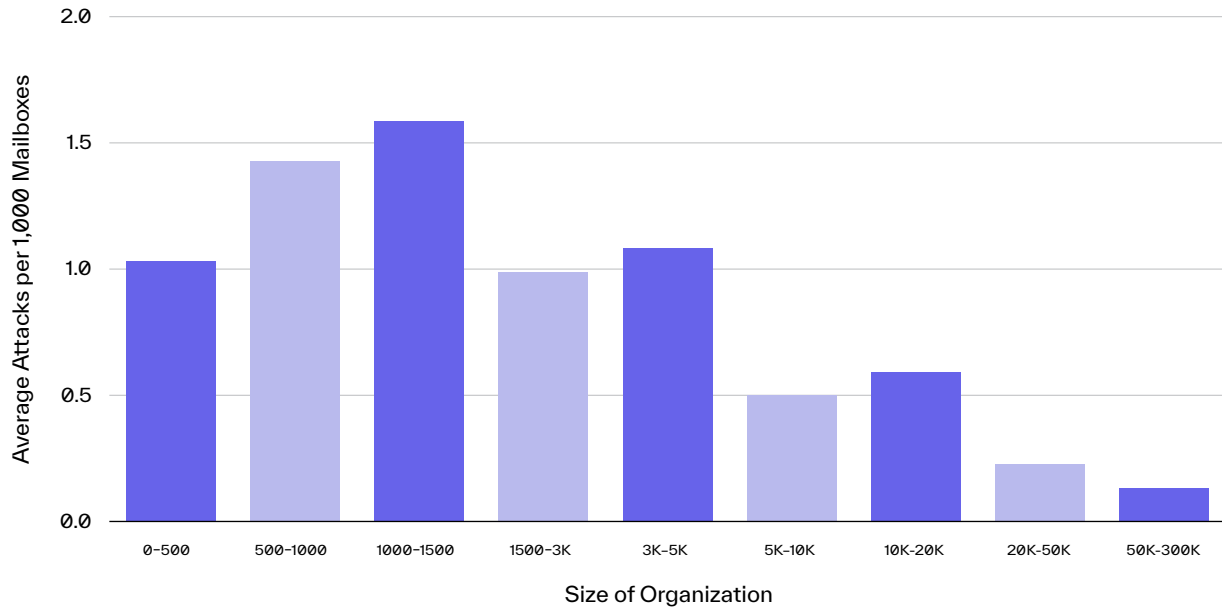
Because business email compromise is highly targeted, it does not necessarily grow alongside the size of the organization like more broad-based attacks. Instead, a pattern where the number of attacks decreases as the organization gets larger indicates that the attackers are targeting specific roles, often executives and those in the finance department.

95%

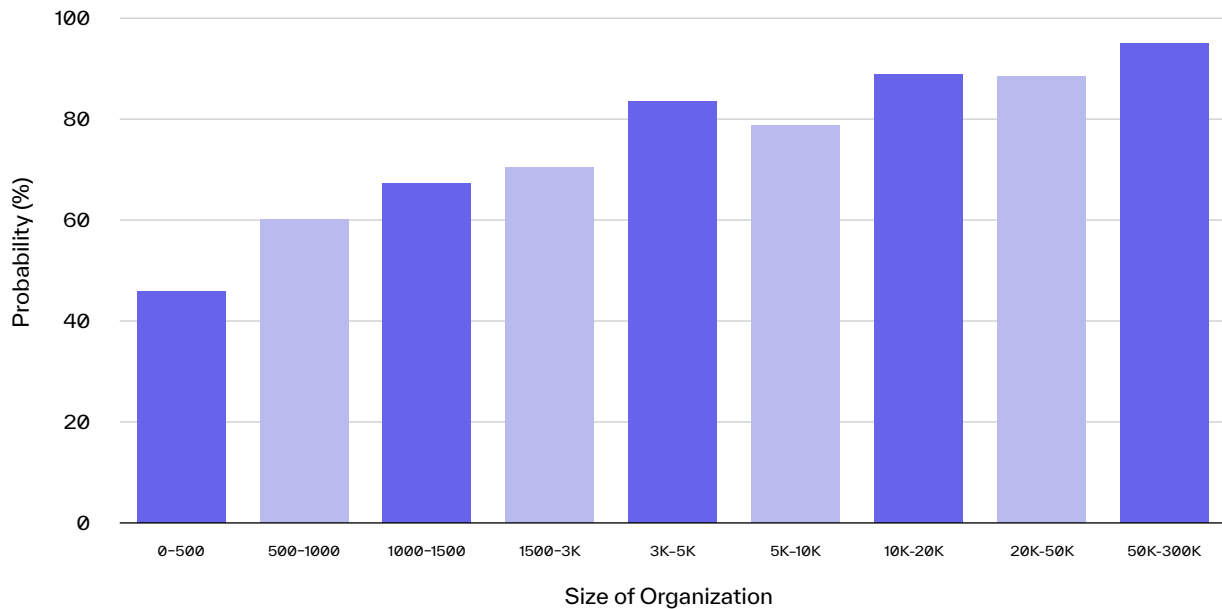
chance of receiving a BEC attack each week for organizations with 50,000+ employees.

This half, organizations under 5,000 employees received the most attacks, with those between 1,000-1,500 employees receiving 1.59 per 1,000 mailboxes each week. In contrast, organizations larger than 50,000 employees received only .13 BEC attacks per 1,000 mailboxes each week—highlighting the fact that cybercriminals target specific roles as part of these schemes. That said, due to sheer volume of mailboxes, those organizations with more employees have a higher probability of receiving at least one attack each week, with the largest organizations peaking at 95% chance of attack.

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



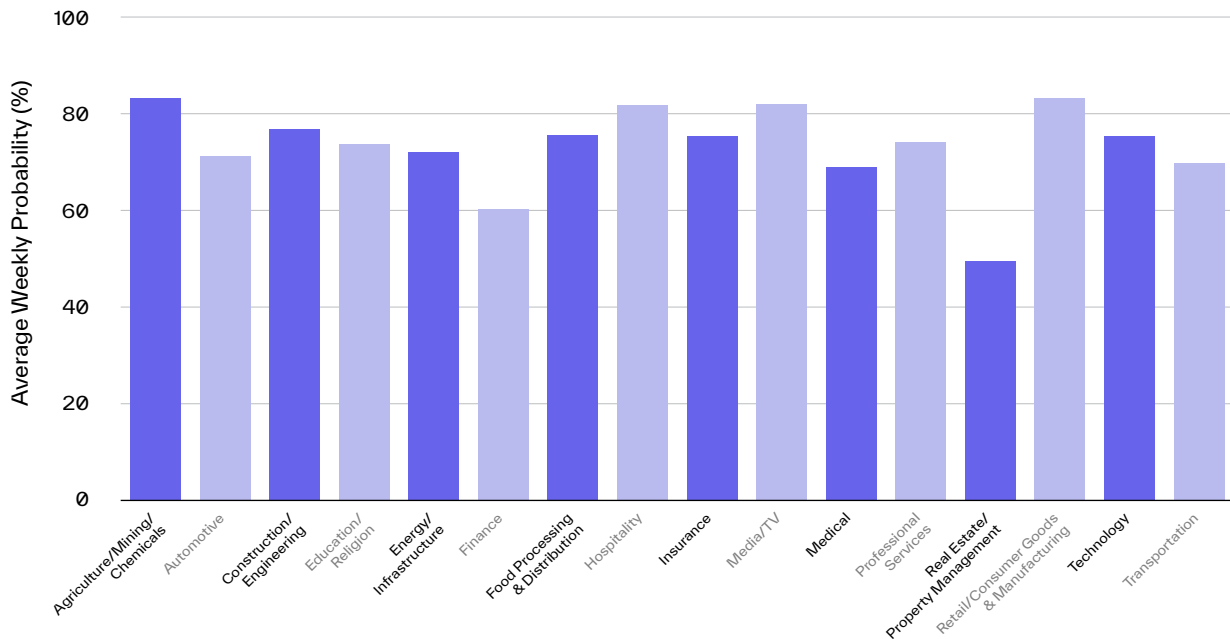
Average Weekly Probability of Receiving a BEC Attack by Organization Size



Retail and Agriculture at Highest Risk for Business Email Compromise

Four industries received more than one attack per 1,000 mailboxes each week: professional services, technology, construction and engineering, and retail and consumer goods. But when it comes to probability of attack, retail and agriculture take the top spot—both with a 83.2% chance of receiving at least one BEC attack each week.

Average Weekly Probability of Receiving a BEC Attack by Industry



One interesting note is that finance and real estate, two industries that are typically some of the most targeted, were at the bottom of the list—with only a 60% and 50% chance of attack, respectively.

1.48

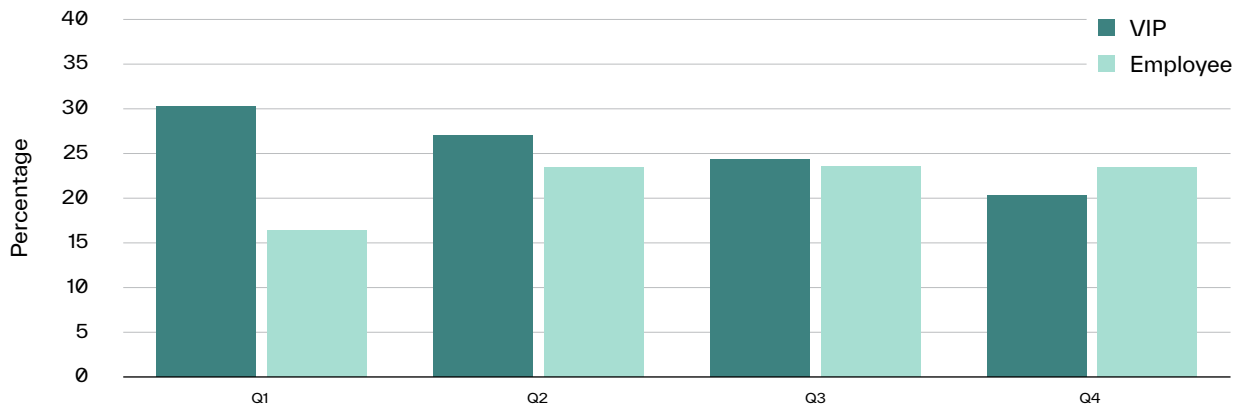
BEC attacks per week received by employees in the professional services industry.

VIPs Impersonated Less, But Attacked More

With business email compromise, it’s common to see executives and other important names impersonated in an effort to use name recognition to convince the target to complete the request. However, as more end users become aware of this tactic, threat actors seem to be shifting their impersonation strategy.

This half, executives were targeted less frequently as a percentage of all attacks, continuing a downward trend that started in the first half of the year. And while they are still one of the most commonly impersonated parties in BEC attacks, they lost the top spot to impersonations of general employees in H2 2021, perhaps as cybercriminals turn to less obvious impersonation tactics to trick unsuspecting victims.

Attacked Parties as Percentage of BEC Attacks

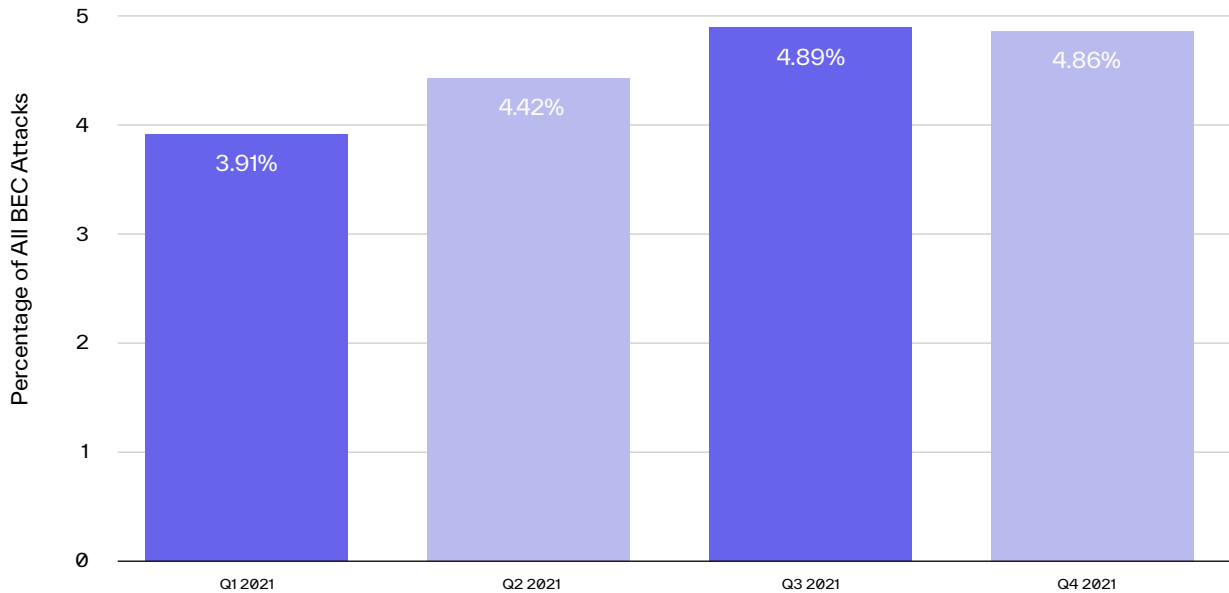


One interesting note here is the move from impersonating the VIPs to targeting them, with a 23.9% increase in executive targeting between the first and last quarters of the year—indicating a significant shift in strategy. What did stay consistent is the fact that the most common party impersonated in attacks that target executives is actually other executives, such as the CFO being impersonated in an email to the CEO.

Executives

are the most common impersonated party in attacks that target other executives.

Percentage of Business Email Compromise Attacks Targeting Executives



Cybercrime is an evolving game. As organizations and employees become more aware of one tactic, the strategy will shift in an effort to stay one step ahead of email security platforms and security awareness training. This change is one indicator that those shifts are already occurring, and that we can expect to see more in the future.

87.7%

of all business email compromise attacks target general employees.

Expect an Increase in Modern Attacks

It's clear that modern email attacks like business email compromise and supply chain fraud will continue to be a threat to organizations worldwide, as cybercriminals shift tactics to stay ahead of both technology and humans. And the new focus on phone fraud scams shows that these threat actors will try all types of tricks to make money.

What all these email attacks have in common is that they are almost exclusively text-based in an effort to bypass traditional email security tools that look for malicious attachments and links. When those traditional indicators of compromise are not included, these attacks reach inboxes where they can cause significant financial losses and data breaches.

While we expect all types of modern attacks to continue to increase, both in volume and severity, they can be stopped with the right solution—one designed to detect identity, context, and content to understand normal behavior and block those emails that deviate from the baseline. With a layered defense, you can ensure that your employees and your executives are protected from the attacks that matter most.

Abnormal

Abnormal Security provides a leading cloud-native email security platform that leverages AI-based behavioral data science to stop socially-engineered and never-seen-before email attacks that evade traditional secure email gateways. Abnormal delivers a fundamentally different approach that precisely detects and protects against the widest range of attacks including phishing, malware, ransomware, social engineering, spam and graymail, supply chain compromise, and internal account compromise.

The Abnormal platform delivers inbound email security, internal and external account takeover protection, and full SOC automation. Abnormal's API-based approach enables customers to get up and running in 15 minutes and can augment a SEG or be used standalone to enhance native Microsoft security protection. Abnormal Security is based in San Francisco, CA.

More information is available at abnormalsecurity.com

Interested in Stopping Modern Email Attacks?

Request a Demo:

abnormalsecurity.com →

Follow Us on Twitter:

@AbnormalSec 