Abnormal

H2 2022
EMAIL THREAT REPORT

Threat Actors Impersonate 265 Different Brands in Credential Phishing Attacks

Executive Summary

Over the past three decades, malicious emails have evolved from low-impact threats like spam and simple phishing to targeted high-impact attacks like ransomware and business email compromise. Because they evade traditional security solutions like secure email gateways and yield significant ROI for threat actors, these socially-engineered attacks aren't going anywhere. In fact, based on our data, advanced email threats are increasing substantially and will only become more sophisticated, pervasive, and damaging.

Threat Actors Exploit Well-Known Brands in Credential Phishing Attacks

Credential phishing attacks have become progressively more intricate and, therefore, more convincing. With increasing frequency, cybercriminals are impersonating well-known brands to leverage their familiarity and reputation and fool targets into providing login credentials.

Believing their account has been compromised and/or they're at risk of losing access, employees deliver sensitive information directly to the attackers. Over the first half of 2022, we saw 265 individual brands impersonated in phishing emails. Social networks, Microsoft products, and ecommerce and shipping solutions were favored most by attackers, accounting for nearly 70% of all impersonated brands.

Risk of Business Email Compromise Continues to Grow

For seven straight years, business email compromise (BEC) has been the most financially devastating cybercrime. The reason? It works. While these threats may not account for a large percentage of all advanced attacks, threat actors only need a BEC attack to be successful once to acquire the information or funds they seek. Between the second half of 2021 and the first half of 2022, BEC attacks grew by almost 60%. Even more remarkable: they increased by more than 150% year-over-year.

60%

Increase in the number of business email compromise attacks over the past year.

89%

Probability of a large enterprise receiving a financial supply chain compromise attack each week.

32%

Of credential phishing attacks involved the impersonation of a social network.

83%

Probability of an advertising/marketing agency receiving a business email compromise attack in H1 2022.

Abnormal™

Table of Contents

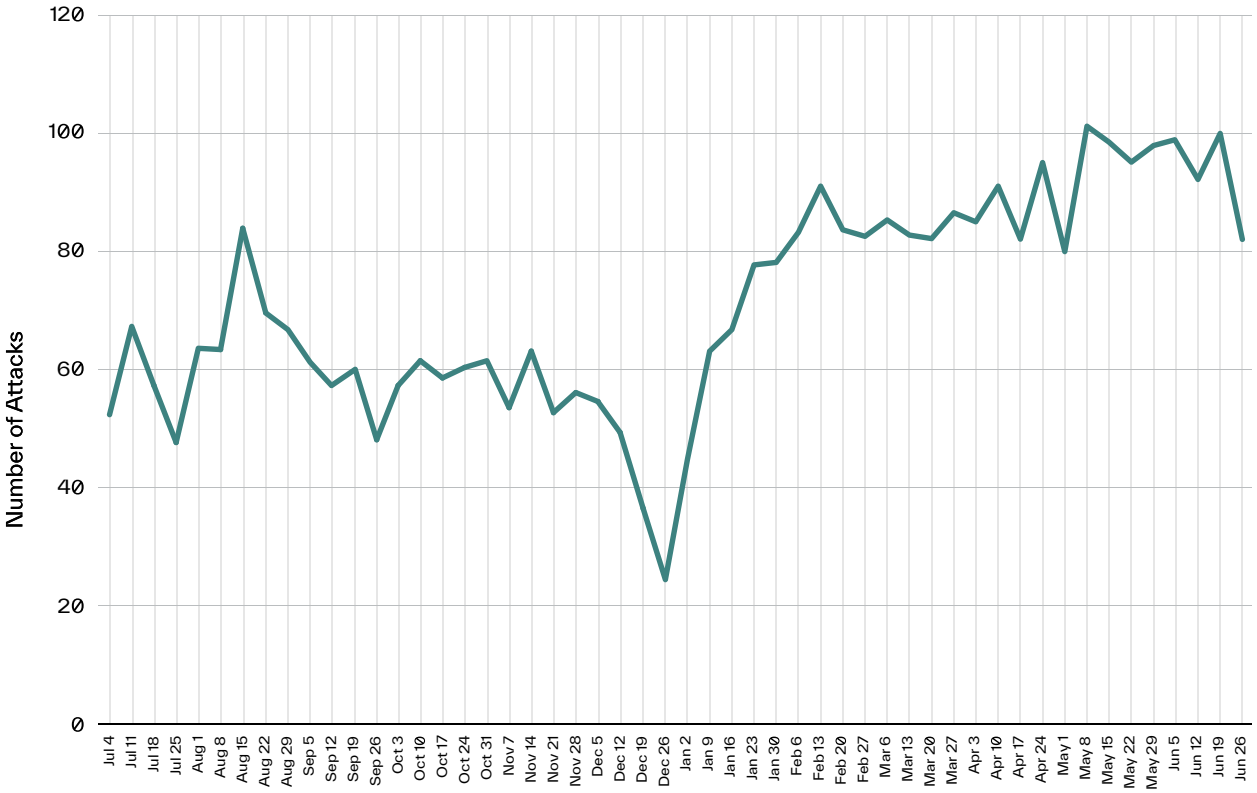
Email Reinforces Its Position as Top Vector for Malicious Threats

Because email is a universal communication medium, threat actors have seen consistent success in utilizing it as an attack vector. Email attacks are highly lucrative at a relatively low cost and as a result, it's safe to assume that email will continue to be an attractive vehicle for cyberattacks.

Attack Volume Increases by Nearly 50%

Over the course of the past two halves, overall attack volume increased by 48%, from an average of 57.5 attacks per 1,000 mailboxes to an average of 85.1.

Attacks per 1,000 Mailboxes



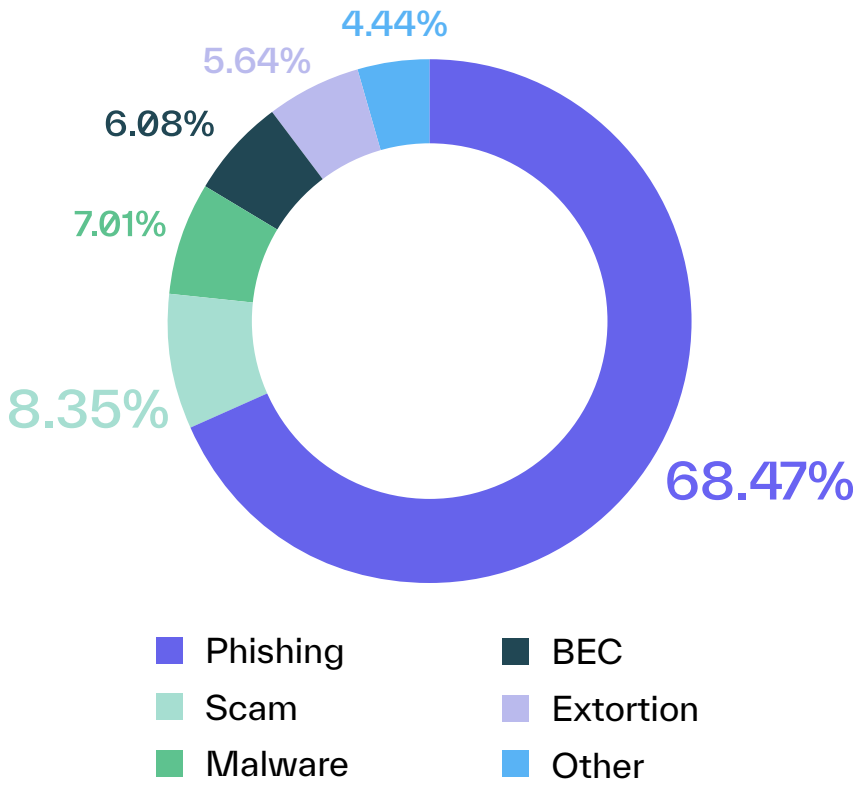
As discussed in our previous report, attack volume declined around the holiday season. Threat actors recognize that a high percentage of professionals are on PTO during this time, which means the likelihood of an employee engaging with a malicious email is lower. Accordingly, cybercriminals also tend to take a break in late December—perhaps to spend time with their own families and enjoy the holiday season.

But as employees began turning off their out of office replies at the start of the new year, attack volume quickly increased. By mid-January, the average number of weekly incidents was already 170% higher than the average recorded in the last week of 2021. And starting in February, attack volume never dipped below 80 attacks per 1,000 mailboxes.

Abnormal™

Taking a look at the breakdown by attack type, credential phishing remains the popular choice for cybercriminals, accounting for nearly 70% of all advanced attacks. This snapshot reflects the broader threat landscape as, according to the FBI's Internet Crime Complaint Center (IC3), phishing has been the most common cybercrime for the past three years.

Percentage of Advanced Attacks by Type



In addition to being the most common attack type, credential phishing also has the potential to open the door to more damaging attacks. Phishing emails are often the first step to compromising employee email accounts, from which far more damaging attacks can be sent.

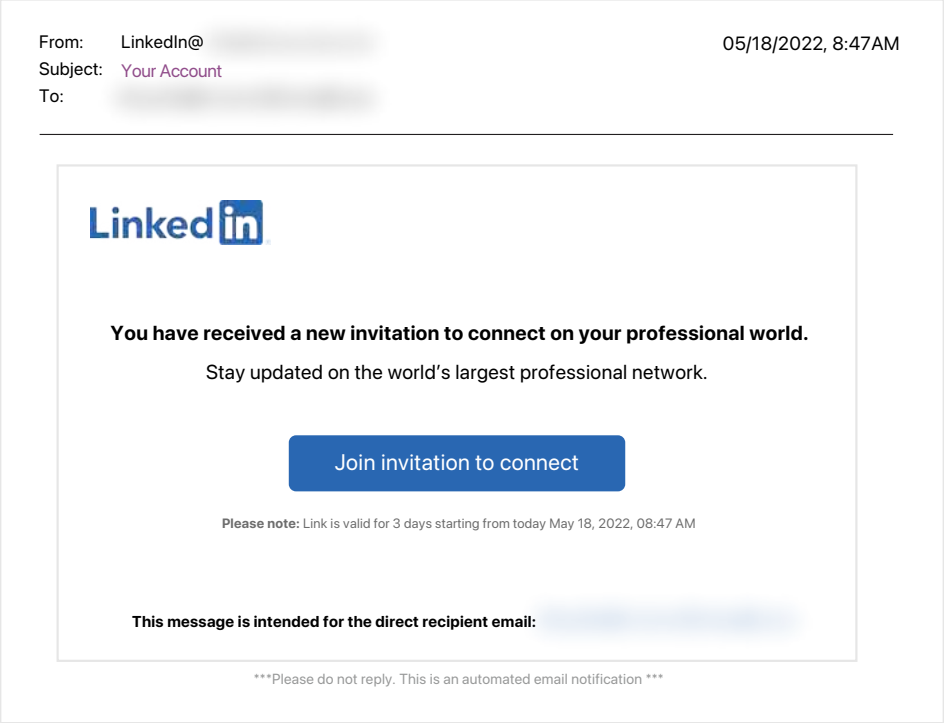
Threat Actors Opt for Brand Impersonation in Credential Phishing Attacks

Credential phishing attacks represent a huge threat to organizations as a well-crafted (or even somewhat realistic-looking) phishing email can trick an employee into providing login credentials. But what makes phishing particularly dangerous is that once a threat actor has access to an internal account, they can launch even more sophisticated and costly attacks.

Abnormal™

Brands Remain King of Credential Theft

As with most modern email threats, credential phishing attacks have become increasingly more intricate in recent years and, consequently, more believable. Threat actors impersonate well-known brands and create a sense of urgency to fool employees into believing their account has been compromised and/or they're at risk of losing access.



From: LinkedIn@ [redacted] 05/18/2022, 8:47AM
Subject: Your Account
To: [redacted]

LinkedIn

You have received a new invitation to connect on your professional world.

Stay updated on the world's largest professional network.

Join invitation to connect

Please note: Link is valid for 3 days starting from today May 18, 2022, 08:47 AM

This message is intended for the direct recipient email: [redacted]

***Please do not reply. This is an automated email notification ***

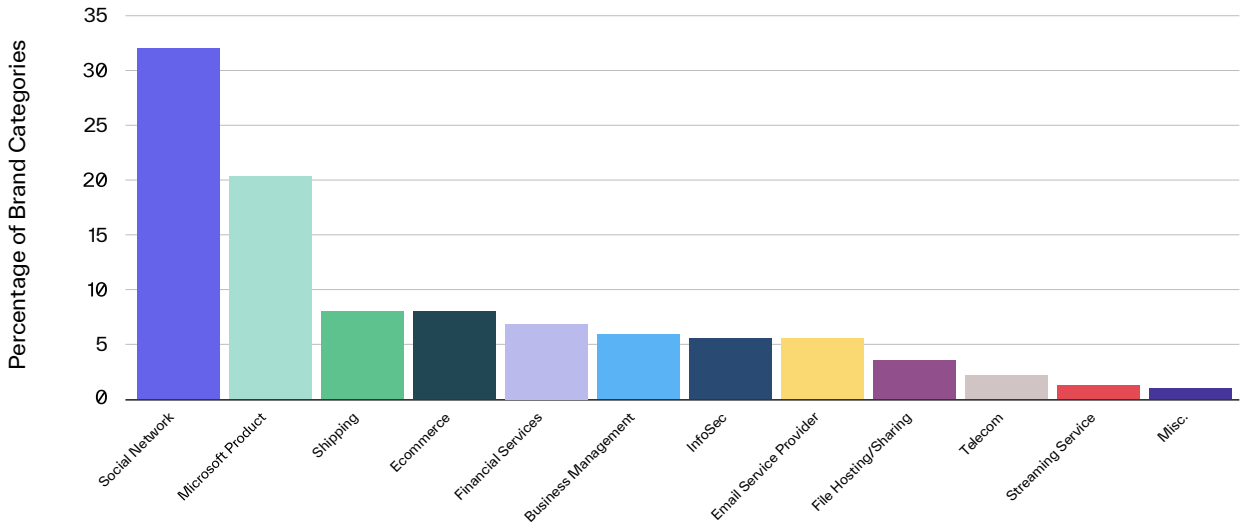
To make things even easier for attackers, the number of platforms and apps we use is always growing—as is the number of accounts we create for online portals. A report from LastPass found that employees at large enterprises manage an average of 25 passwords; at smaller organizations that number jumps to 85. And, as much as employers discourage it, the report revealed that employees reuse one password an average of 13 times.

Every software and website that requires you to provide your email address for access represents a phishing opportunity for cybercriminals—and they know it. And once they have access to the account, they can use it for all types of nefarious activities, from infiltrating additional platforms to stealing money from the account to buying products using your credit card.

Social Networks and Microsoft Products Most Impersonated in Credential Phishing Attacks

Of the more than 425,000 credential phishing attacks in which a brand was impersonated in the first half of 2022, 32% involved the impersonation of a social network, with LinkedIn being the most impersonated platform.

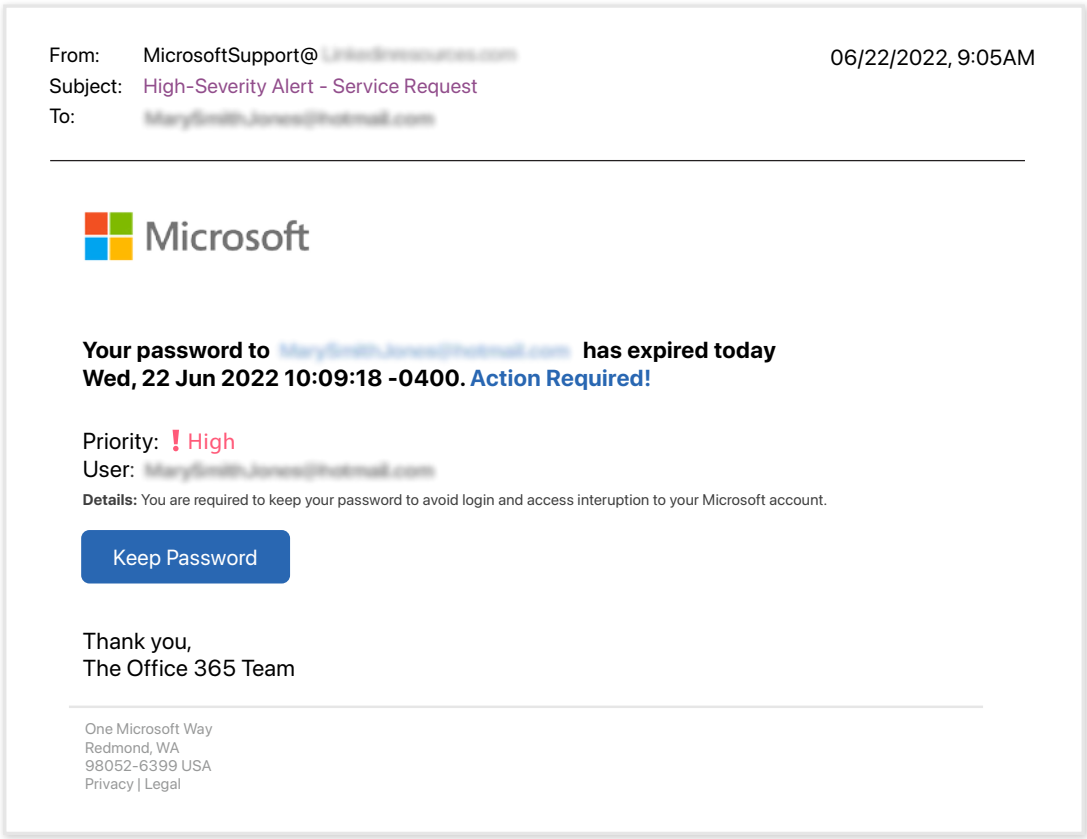
Percentage of Brand Categories Impersonated in Credential Phishing Attacks



Because LinkedIn often sends emails with updates about profile views and search results, users are accustomed to receiving occasional, unsolicited emails from the platform. This means that in addition to more standard phishing emails that claim there is a problem with the account, threat actors can also recreate these other types of LinkedIn emails and include a link to a phishing site.

Abnormal™

After social networks, Microsoft products were the second most impersonated, with Outlook, OneDrive, Microsoft 365, and the parent company appearing in 20% of incidents. One of the reasons organizations use Microsoft is that the company provides a large suite of solutions applicable to every business use. The downside of this is that attackers will leverage that ubiquity and authority to convince employees they're at risk of losing access to their inbox or important files. And perhaps most concerning about Microsoft credential theft is that compromise of these accounts allow bad actors to use that email address to send other email attacks, impersonating real employees and hijacking ongoing conversations to redirect payments or request new fund transfers.



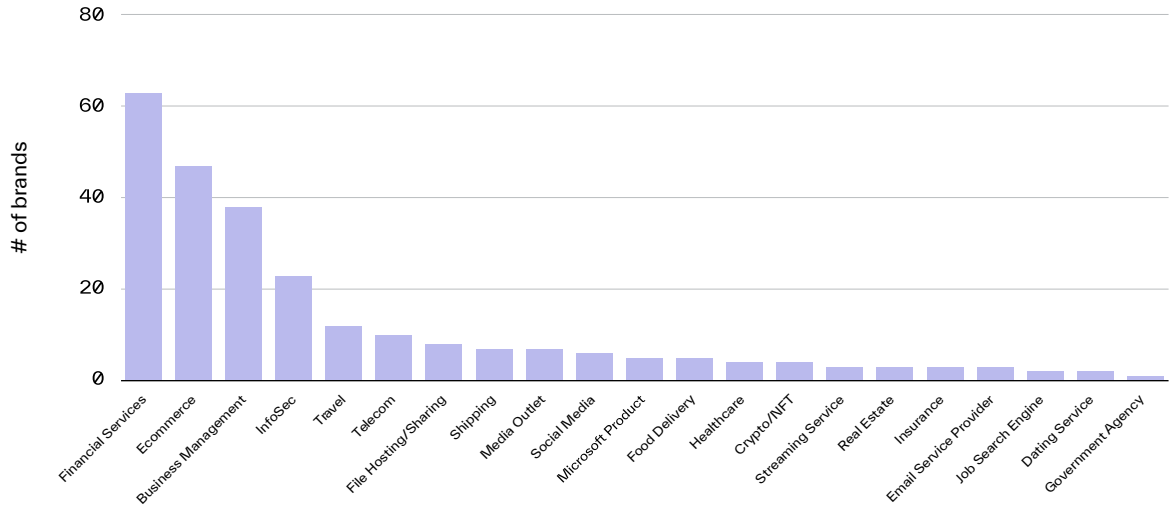
Tied for third in phishing attacks involving brand impersonation were shipping services and ecommerce platforms, appearing in a combined 16% of incidents. This is relatively unsurprising, considering online shopping grew by more than 50% between 2019 and 2021, and our collective dependence on Amazon made it the most impersonated ecommerce brand in these attacks.

Attackers Favor Impersonating Brands with Best Potential ROI

Of the 265 individual brands that attackers impersonated, nearly one in four were in the financial services industry—including banks, credit card providers, and online payment processors. Fan favorites included American Express, PayPal, and Wells Fargo.

While this is somewhat unsurprising, it is still concerning. Gaining access to an organization's banking or payment portal allows threat actors to transfer money to their own accounts, redirect incoming payments, send fraudulent payment requests, and steal sensitive financial information to use in future attacks.

Number of Brands Impersonated in Each Category



Further, victims of such attacks may not be able to easily resolve the situation, and their accounts could be closed permanently. Not only does this impact their ability to use any other platforms connected to the account, such as billing and accounting software, but the company will also have to dispute fraudulent charges with their bank and pay any additional fees that result from the attack.

One other interesting thing to note is that of the approximately 25,000 attacks in which a business management software provider was impersonated, 27.4% involved a document management solution brand like DocuSign. From the target's point of view, receiving an email with a request to log in to view or sign a document is far from unusual. And from an attacker's point of view, gaining entry into an organization's digital document repository means they have access to a wealth of proprietary and sensitive information.

Threat Actors Utilize Different Tactics for Different Industries

While the types of brands being impersonated were fairly similar no matter which industry was the target, there were some notable outliers. For example, of all the industries studied by Abnormal, the transportation industry was the only one that did not receive a majority of attacks that impersonated a social network or Microsoft product.

Customer Industry	1st Most Impersonated	%	2nd Most Impersonated	%	3rd Most Impersonated	%
Advertising/Marketing	Microsoft Products	28.77%	Social Network	23.10%	Ecommerce	19.22%
Agriculture/Mining/Chemicals	Microsoft Products	47.18%	Social Network	12.45%	Shipping	5.63%
Automotive	Microsoft Products	28.97%	Social Network	28.43%	Shipping	11.06%
Construction/Engineering	Social Network	25.41%	Microsoft Products	24.91%	Ecommerce	11.33%
Education/Religious Organizations	Social Network	50.14%	Microsoft Products	7.05%	Ecommerce/Shipping	6.80%
Energy/Infrastructure	Microsoft Products	27.71%	Social Network	26.86%	Shipping	6.24%
Finance	Microsoft Products	31.81%	Social Network	14.04%	Shipping	9.66%
Food Processing & Distribution	Social Network	27.71%	Microsoft Products	27.06%	Shipping	5.05%
Government	Social Network	57.07%	Microsoft Products	24.77%	Shipping	4.02%
Hospitality	Social Network	30.69%	Microsoft Products	27.53%	Shipping	7.78%
Insurance	Microsoft Products	31.51%	Social Network	15.04%	Ecommerce/Shipping	5.27%
Media/TV/Entertainment	Social Network	52.96%	Microsoft Products	10.66%	Ecommerce	7.12%
Medical	Microsoft Products	37.19%	Social Network	12.87%	Shipping	7.07%
Professional Services	Microsoft Products	25.69%	Social Network	23.25%	Shipping	9.66%
Real Estate/Property Management	Social Network	30.36%	Microsoft Products	18.94%	Shipping	7.33%
Retail/Consumer Goods & Manufacturing	Microsoft Products	30.69%	Social Network	18.50%	Ecommerce/Shipping	11.10%
Sports	Microsoft Products	53.99%	Ecommerce	28.17%	Social Network	5.63%
Technology	Microsoft Products	27.98%	Social Network	15.33%	Ecommerce/Shipping	8.17%
Transportation	Ecommerce	35.72%	Microsoft Products	22.93%	Social Network	11.59%

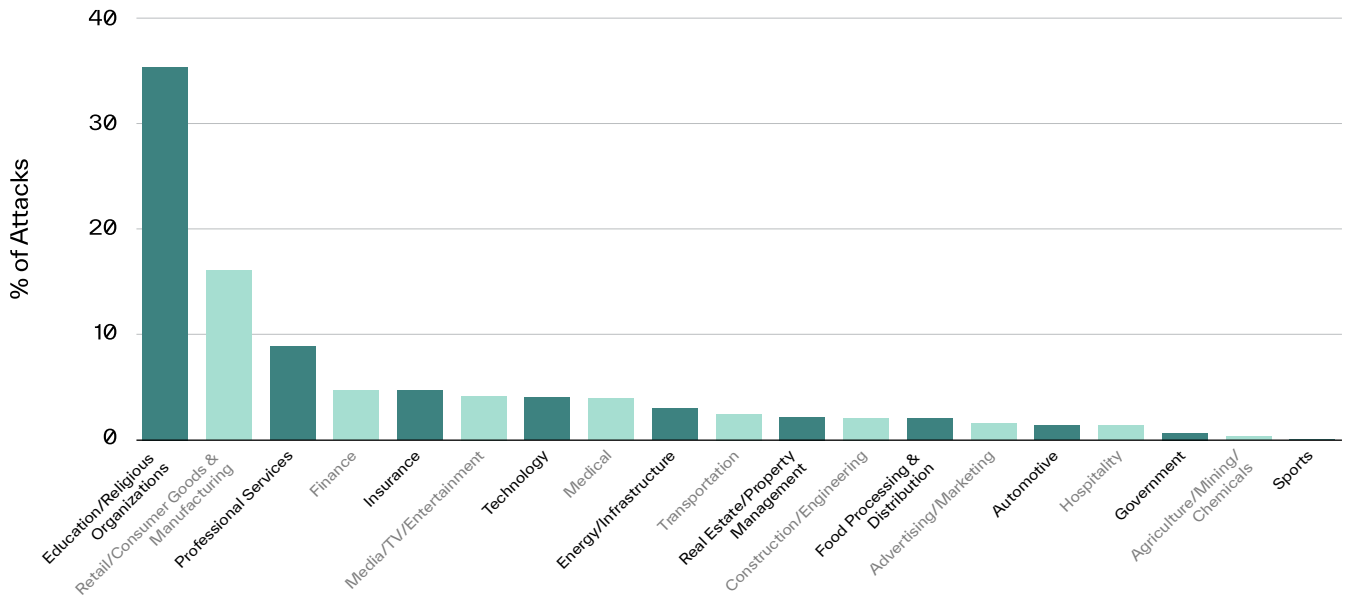
And while all other industries saw this pattern, the percentage of those attacks varied widely. For example, the front offices of professional sports teams received emails pretending to be from Microsoft, Outlook, OneDrive, or Office 365 in 54% of phishing attacks. And 47% of attacks targeting agricultural companies included the impersonation of a Microsoft product.

Social networks are by far the most impersonated in attacks targeting government agencies, educational and religious organizations, and companies in the entertainment industry Impersonations of LinkedIn, Facebook, Instagram, and Twitter were involved in more than half of the phishing attacks these organizations received. Perhaps most interesting is the fact that over half of all brand impersonation attacks targeting government employees impersonated social networks, possibly in an effort to gain access to the platform and post on behalf of the organization.

Educational Institutions and Religious Organizations Most Targeted

While all industries are targeted by credential phishing attacks that use brand impersonation, educational and religious organizations experienced the largest percentage of these attacks. For the most part, brand impersonation was the tactic of choice in 2-5% of all attacks, with a handful of outliers.

Percentage of Total Attacks by Industry



On the other hand, of all the attacks received by education and religious organizations, over 35% of them involved brand impersonation. The second closest, retailers and manufacturers of consumer goods, received these impersonations in only 16% of all attacks, and rounding out the top three was professional services at 8.9% of all attacks.

For educational and religious organizations, a lack of budget for email security tools makes for an easy target and is a likely explanation for the high volume of attacks. For retailers and manufacturers of consumer goods, gaining access to databases filled with customer credit card numbers and vendor account information is quite the draw for cybercriminals. And for professional service providers like lawyers and accountants, a successful credential phishing attack allows threat actors to take advantage of the valuable information stored in the client database or reroute payments for expensive services.

Business Email Compromise Attacks Continue to Increase in Frequency

There's a reason business email compromise has been the most financially devastating cybercrime for seven straight years: it works. Free of traditional indicators of compromise, these text-based, socially-engineered attacks are nearly impossible for traditional email security solutions to detect and thus yield a significant ROI for cybercriminals.

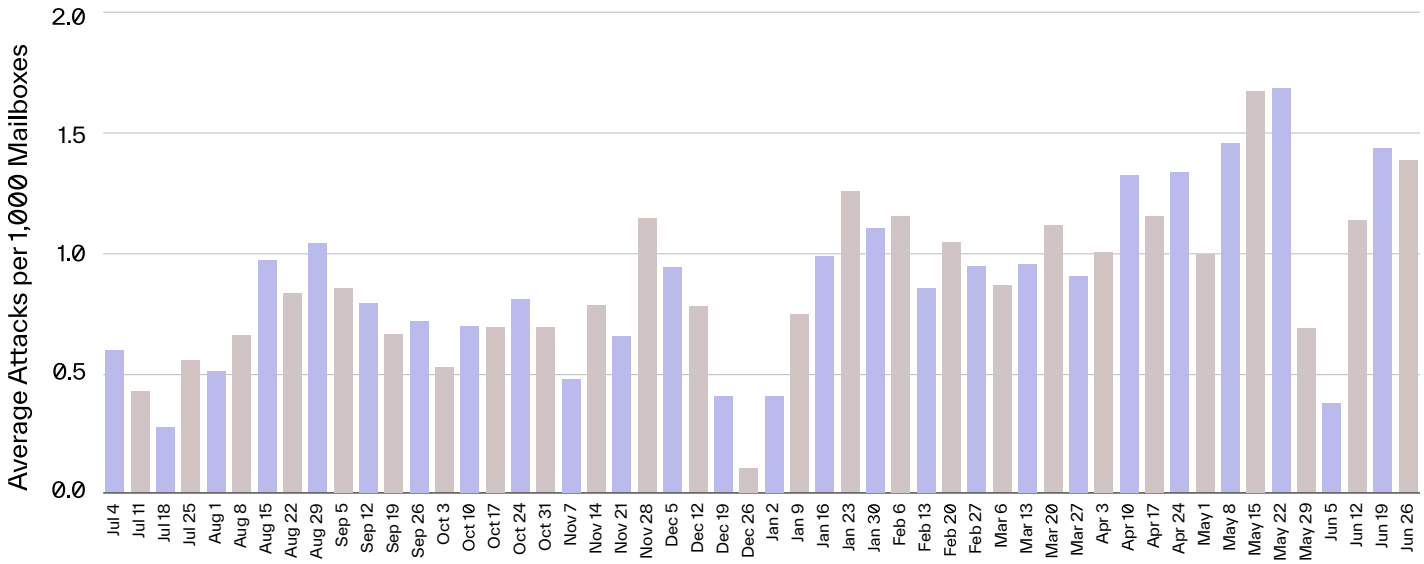
Risk of Business Email Compromise Sees Steady Growth

Unlike spam and simple phishing campaigns that rely on sending millions of emails with little regard for targeting or personalization, business email compromise (BEC) attacks are successful because they do the opposite. Threat actors impersonate an executive or third-party vendor, gain the target's trust, and then convince them to pay fake invoices or provide access to sensitive data. So while they make up a small percentage of all email attacks, the value they provide to the attacker is massive.

Over the past two halves, BEC attacks grew by almost 60%, from 0.671 attacks per 1,000 mailboxes to 1.07. In addition, there were 15 weeks where there was at least one attack per 1,000 mailboxes—peaking at 1.68 in late May.

Similar to what we saw in December 2021, there was a noticeable dip in BEC attacks during the week of Memorial Day and the following week, as cybercriminals opted to take the holiday off like their targets. However, attack volume quickly rebounded, and the number of BEC attacks was back in line with the average by mid-June.

Median Weekly BEC Attacks per 1,000 Mailboxes

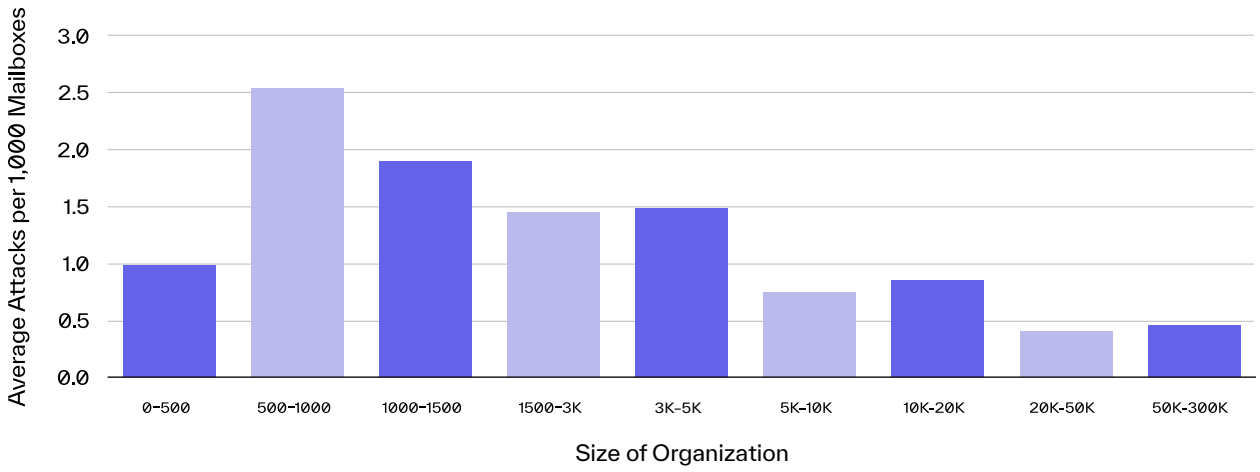


Smaller Organizations Continue to Receive Most Attacks per Mailboxes

Over the first six months of the year, organizations with fewer than 5,000 employees experienced the most business email compromise attacks per mailbox, with an average of 1.65 attacks per thousand mailboxes. In contrast, companies with more than 50,000 employees received only 0.45 BEC attacks per 1,000 mailboxes each week. Still, due to the sheer number of mailboxes, organizations with more employees have a higher probability of experiencing at least one attack each week, with the largest companies peaking at a nearly 99% chance of attack.

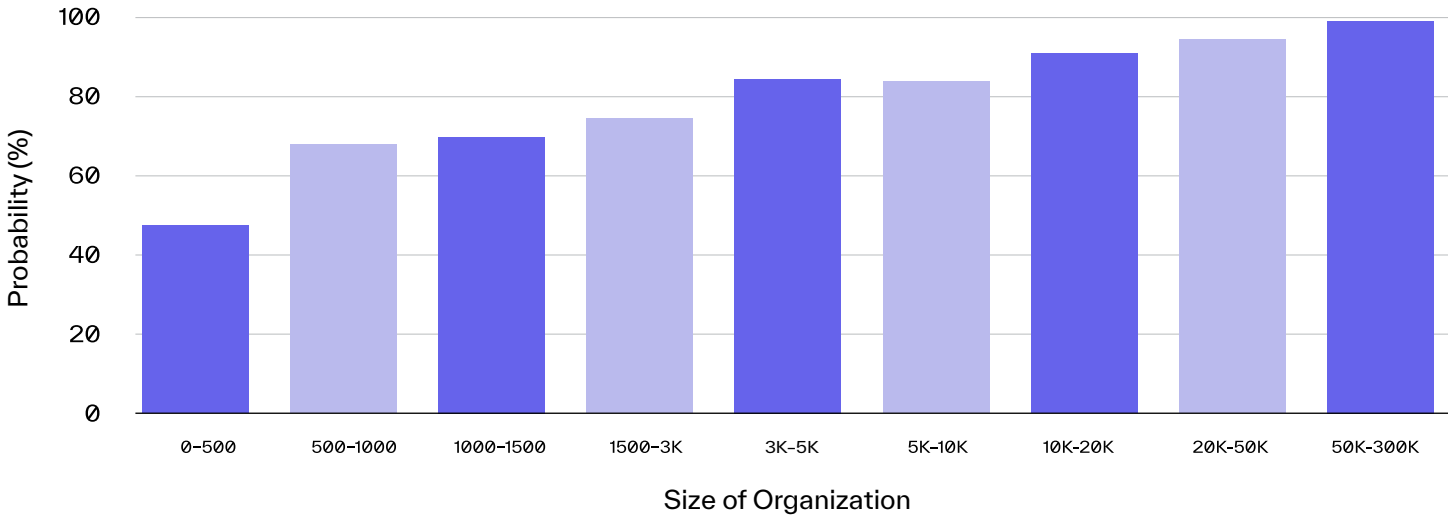
Interestingly, organizations with under 500 mailboxes saw a 54% half-over-half increase in business email compromise, and companies with 500-1,000 mailboxes recorded more than double the number of BEC attacks. This demonstrates that even the smallest organizations are at a growing risk of becoming a victim of business email compromise. Threat actors aren't just targeting giant global companies; they're going after whichever organizations they believe will provide the information or funds (or both) they desire.

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



Abnormal™

Average Weekly Probability of Receiving a BEC Attack by Organization Size

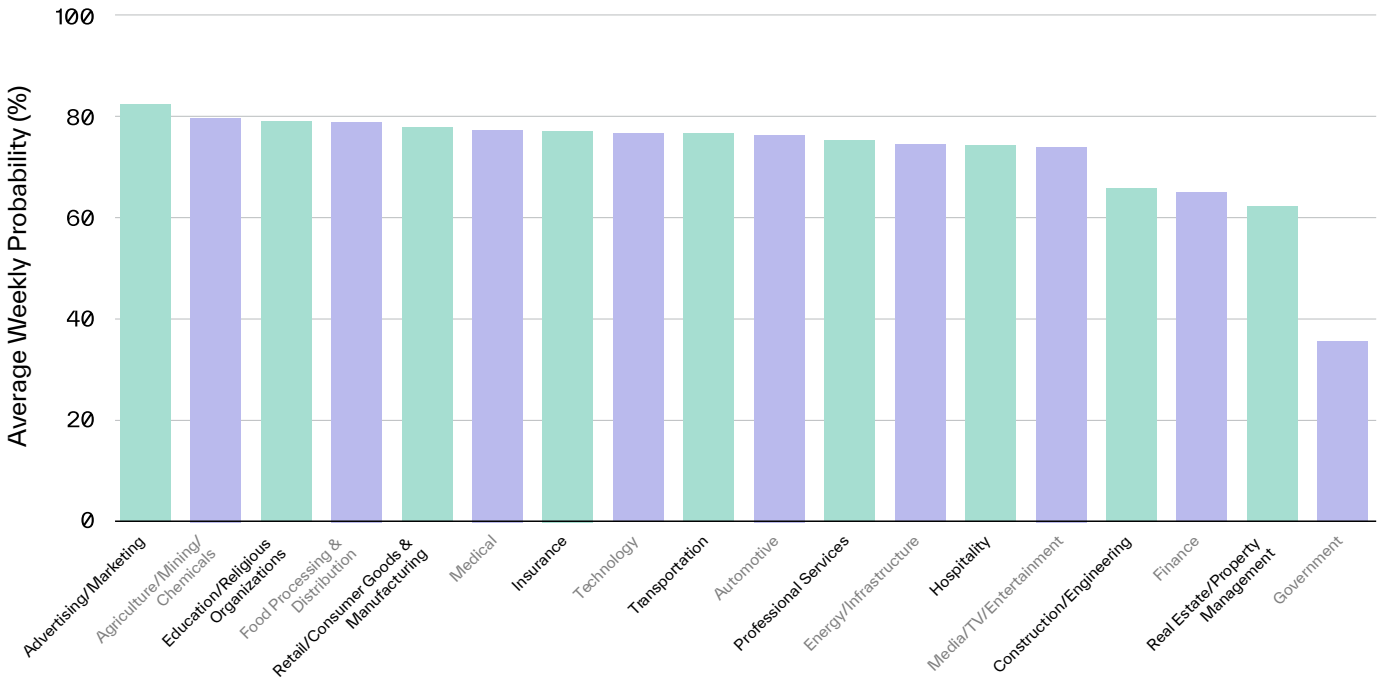


One point to note here is that because business email compromise is highly targeted, the number of BEC attacks doesn't necessarily grow at a rate proportionate to the size of the company. Rather, because attackers focus on specific roles, often executives and those who manage the company's finances, we see the opposite trend where the number of attacks decreases despite the increase in size.

Abnormal™

Advertising and Marketing Agencies at Highest Risk

Average Weekly Probability of Receiving a BEC Attack by Industry



Organizations in the advertising and marketing industry recorded the highest probability of experiencing business email compromise in the first half of 2022. Advertising and marketing agencies tend to have above-average turnover, and it's common for employees to take on duties outside of their normal responsibilities. Knowing that these employees may be more stressed than average, or that they are used to last-minute requests, threat actors may find them particularly vulnerable to their attacks.

Additionally, the advertising/marketing industry as a whole has seen a massive surge in business since the pandemic as consumers spend more time looking at screens. This increase in potential audience size means an increase in revenue, making these organizations even more appealing to cybercriminals. This logic related to an increase in demand may also hold true for some of the other industries most targeted by BEC, including agriculture and mining, food processing and distribution, and retail and consumer goods manufacturing.

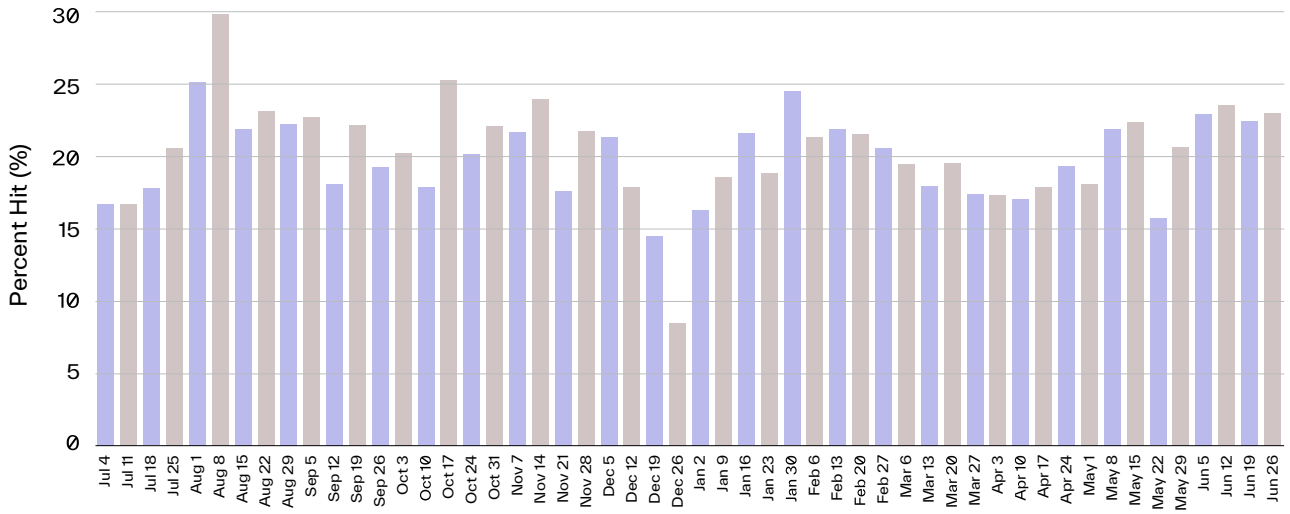
Financial Supply Chain Compromise Endures as Evolving Threat

The CEO fraud that dominated the last few years is not nearly as successful as it used to be. As a result, attackers are moving away from internal impersonation and instead focusing on impersonating third parties, giving rise to what we call financial supply chain compromise.

Risk of Financial Supply Chain Compromise Still Steady

Much like traditional BEC attacks, a financial supply chain compromise attack requires the use of a trusted identity to run the scam. In these attacks, however, the person being impersonated is an external third party rather than an internal executive or another employee.

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



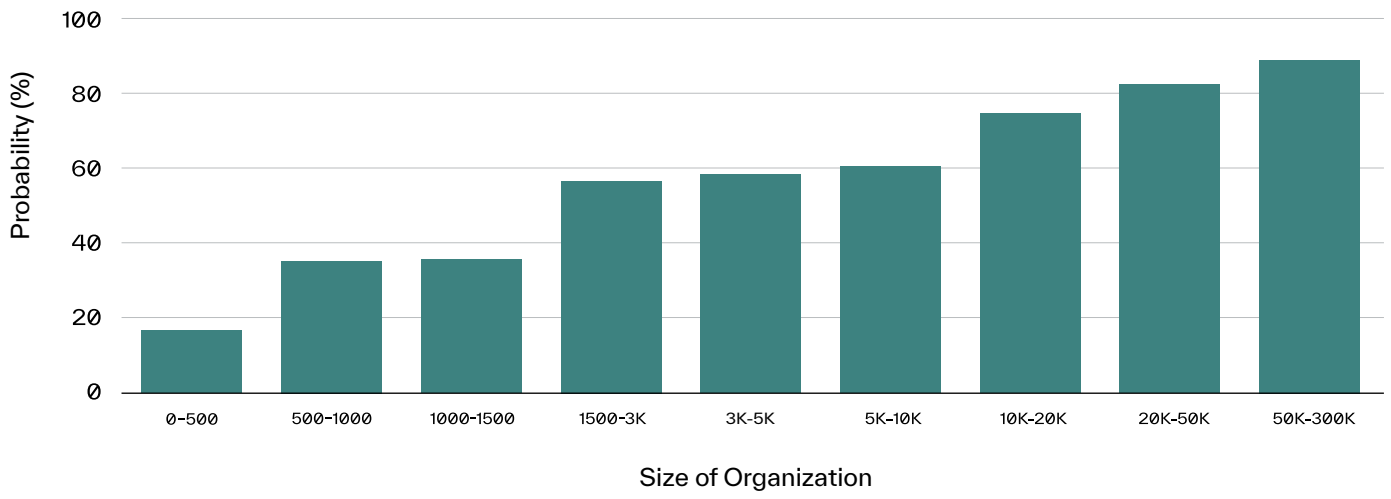
Impersonating known vendors, threat actors request that invoices be paid, billing account details be updated, or wire transfers be completed. And because the number of vendors working with a company is much, much higher than the number of CEOs within that same organization, the results are astounding.

In the first half of the year, one in five Abnormal customers was the target of a financial supply chain compromise attack each week, continuing the trend of this growing threat that we saw in 2021. By exploiting the trust in the impersonated identity and the implicit authenticity of business email, these kinds of attacks can result in heavy losses for victims.

Larger Organizations Remain at Greatest Risk

As with other types of BEC attacks, organizations with more employees have a higher probability of experiencing a financial supply chain compromise attack. Companies with 10,000 mailboxes or more are likely to receive a financial supply chain compromise attack at least three weeks out of four, and organizations with more than 50,000 mailboxes will experience an attack nearly every week of the year. Even medium-sized businesses will receive an attack at least every other week.

Probability of Receiving a Financial Supply Chain Compromise Attack by Organization Size



Undoubtedly, one reason for this is that more employees equals more targets. But another factor to consider is that larger companies have substantially more suppliers and distributors that can be compromised. Cybercriminals are no longer reliant on impersonating executives to run their scams, which means every vendor relationship is a channel threat actors can exploit.

The decision of attackers to transition away from internal impersonation and instead focus on impersonating third parties represents a major evolution in the business email compromise threat landscape. With benign attachments like invoices and without known malicious signatures to flag, these attacks are more likely to bypass legacy infrastructure and trick end users, which is why we expect this trend to continue.

Stopping Advanced Email Attacks

The vast majority of cybercrime today is successful because it hijacks the people behind the keyboard. It's clear that email threats are only going to grow in complexity, and as cybercriminals evolve and optimize their strategies, it will become increasingly more difficult to recognize attacks.

While security awareness training remains an important tool in the cybersecurity toolbelt, the best way to prevent your workforce from falling victim to these increasingly sophisticated attacks is to stop them before they reach employees. Being proactive about protection and taking advantage of innovative technologies are key to reducing your organization's risk.

There is little denying that email attacks will continue to increase in both volume and severity, but they can be stopped with the right solution—one that uses a behavioral AI-based approach and evaluates identity, context, and content to establish a known good baseline. By understanding what is normal within the organization, the right cloud email solution can block any messages that deviate from it. And with the right technology in place, you can be confident that your employees are protected from all types of attacks, whether they impersonate your favorite social media platform or your most high-profile executive.

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