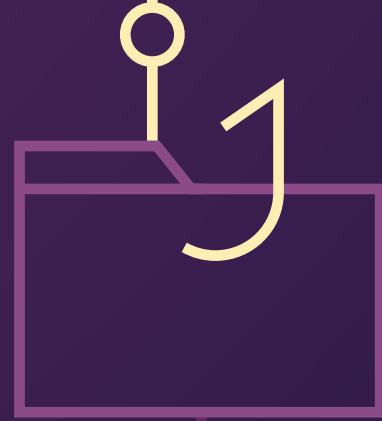


Abnormal



Bait and Switch

File-Sharing Phishing
Attacks Surge 350%

H2 2024 THREAT REPORT

Executive Summary

350%

Year-over-year growth in file-sharing phishing attacks

As the only universally adopted platform across every industry and region, email is a vital business communication channel. However, it also presents significant cybersecurity challenges, as it is inherently intrusted despite being inherently insecure.

While real-time collaboration tools like Slack, Zoom, and Microsoft Teams have skyrocketed in popularity, email remains the go-to channel for asynchronous communication. As our universal dependence on email is unlikely to end anytime soon, it will continue to be an attractive vehicle for cyberattacks.

60%

Percentage of file-sharing phishing attacks sent using legitimate domains

Threat Actors Exploit Familiarity and Trust in File-Sharing Phishing Attacks

The well-known hallmarks of phishing attacks are starting to fade away, as cybercriminals leverage legitimate business tools and dark web resources to create malicious emails that appear indistinguishable from safe ones.

51%

Half-over-half increase in business email compromise attacks

In file-sharing phishing attacks, threat actors exploit popular platforms and plausible pretexts to impersonate trusted contacts and trick employees into disclosing private information or installing malware. A complex and escalating threat, file-sharing phishing attacks increased by 350% year-over-year, with financial organizations and built environment firms being the most targeted.

BEC and VEC Attacks Endure as Evolving Threats

Business email compromise (BEC) and vendor email compromise (VEC) are specifically designed to circumvent both users' common sense and conventional security measures. Utilizing social engineering and text-based emails with no traditional indicators of compromise allows cybercriminals to evade legacy email security solutions and manipulate targets. This one-two punch has brought attackers continued success and is likely why BEC and VEC have maintained their momentum.

41%

Percentage of Abnormal customers targeted by VEC each week

Between H2 2023 and H1 2024, BEC attacks grew by more than 50%. VEC remained steady, with an average of 41% of Abnormal customers being targeted by VEC each week during January–June 2024.

Table of Contents

Cyberattackers Capitalize on Email's Vulnerabilities	4
Phishers Exploit Legitimate File-Sharing Platforms to Amplify Attack Impact	7
Business Email Compromise Persists as Popular Attack Strategy	21
Risk of Vendor Email Compromise Stays Steady	24
Securing Your Organization Against Modern Threats	27
About Abnormal	28



Cyberattackers Capitalize on Email's Vulnerabilities

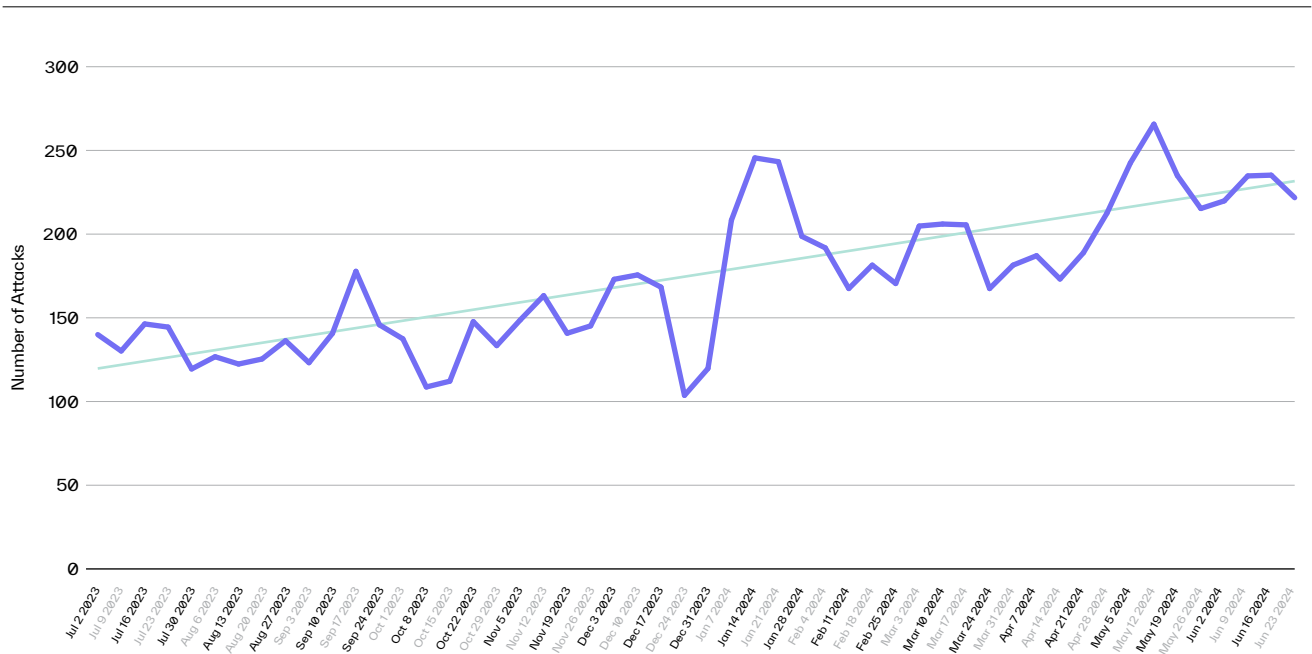
When email was first introduced, the idea that bad actors would infiltrate inboxes or exploit email to engage in cybercrime wasn't even a consideration. The focus was merely on establishing a reliable, universal communication channel.

Complicating this lack of native security is the fact that the inbox has evolved into the hub for just about everything the average professional needs to do their job. Thus, although multiple security protocols have been added over time, email remains a challenge to secure and, as a result, a vulnerable entry point.

Attack Volume Increases by Nearly 50%

Over the past 12 months, the volume of advanced attacks increased by 49.6%, from a median of 139 attacks per 1,000 mailboxes during July–December 2023 to 208 during January–June 2024.

Attacks per 1,000 Mailboxes



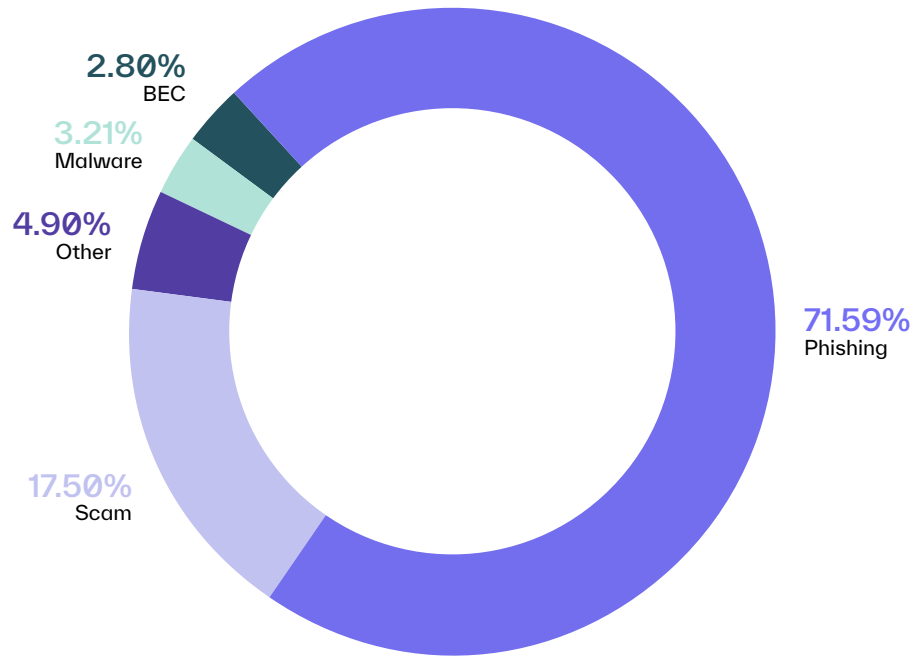
In line with the trends we've seen in recent years, attack volume dropped precipitously the week of Christmas, decreasing by just about 40% week-over-week. This is presumably due to two factors: threat actors recognize that most of their potential targets will be offline during this period, reducing their chances of success, and/or they wish to take a break to enjoy the holiday with their families.

Then, as expected, attack volume rebounded dramatically at the start of the new year, jumping by more than 100% during the first week in January. Since then, attacks have yet to dip below 165 attacks per 1,000 mailboxes. To help put this trend in perspective, just two years ago, during the time period of January–June 2022, the median number of attacks per 1,000 mailboxes was 85.



Examining the breakdown by attack type, credential phishing has maintained its position as the most popular choice for cybercriminals, accounting for approximately 72% of all advanced attacks.

Advanced Attacks by Type



Perhaps due to its versatility as the first step in a variety of crimes, phishing far outpaces other types of attacks. The FBI's Internet Crime Complaint Center (IC3) documented 298,878 phishing incidents in 2023—five times as many as the second most common cybercrime.

The phishing emails of the past usually contained several indicators that the message was malicious, such as numerous misspellings, poor grammar, and less-than-convincing impersonations. Now, today's threat actors have a wealth of free tools at their disposal that allow them to generate messages that can trick even the most eagle-eyed employee. Attackers also spoof email addresses of trusted parties, hiding their true identities behind usernames and URLs with minor misspellings or character substitutions that are easily overlooked.

In short, bad actors have learned how to create phishing emails that wouldn't raise any level of suspicion in the majority of employees—one of the reasons it's the most prevalent cybercrime.



Phishers Exploit Legitimate File-Sharing Platforms to Amplify Attack Impact

The telltale signs of phishing attacks are rapidly disappearing, as bad actors take advantage of legitimate business tools and dark web resources to craft malicious messages that, for all practical purposes, are identical to safe emails.

In file-sharing phishing attacks, a sophisticated and growing threat, cybercriminals exploit trusted platforms and convincing pretexts to impersonate well-known brands and manipulate targets into revealing private information or downloading malware.



File-Sharing Phishing Attacks: A Modern Trojan Horse

Every phishing attack involves the impersonation of a trusted contact or brand with the goal of deceiving a target into divulging sensitive information or installing malicious software. However, not all phishing attacks are created equal.


A file-sharing phishing attack is a unique type of phishing threat in which a cybercriminal poses as a known colleague or familiar file-hosting or e-signature solution and sends a target a malicious email containing a link to what appears to be a shared file or document. Should the recipient click on the link, it initiates the second phase of the attack, which varies depending on the cybercriminal's desired outcome—e.g., stealing login credentials or infecting the target's device with malware.

On the surface, this may sound like a run-of-the-mill phishing attack that happens to have a particular motif. But when we dig into the unique characteristics of file-sharing phishing attacks, it becomes clear how devious these threats truly are.

The Art of Deception

First, sharing files and documents via email is a common practice for organizations in every industry. While the themes of some phishing attacks are likely to raise at least a little suspicion (such as unsolicited, too-good-to-be-true job offers or an email from the CEO requesting \$500 in gift cards), the pretext of file-sharing phishing attacks is perfectly ordinary and, therefore, inherently believable. Depending on their approach, an attacker often doesn't even need to invest considerable effort in establishing a plausible pretense beyond selecting a relevant name for the bogus file.

It's also becoming progressively easier for threat actors to convincingly impersonate the individuals and brands they're imitating.



Generative AI tools enable attackers to craft personalized emails with perfect spelling, grammar, and syntax in the recipient's native language. This eliminates the most obvious signs of a malicious message that employees are used to seeing. Bad actors can also purchase phishing templates on the dark web that are nearly indistinguishable from the real emails sent by popular file-hosting or e-signature platforms. Additionally, GenAI and dark web resources allow cybercriminals to produce compelling malicious emails at a remarkably faster rate, facilitating the creation of large-scale phishing campaigns in a fraction of the time.

File-sharing phishing attacks also make extensive use of social engineering. A primary component of these threats is leveraging the target's familiarity with the impersonated party or service to lower their defenses. In addition, the attacks capitalize on the fact that employees recognize file-sharing platforms are generally used for higher-priority and time-sensitive documents, which increases not only the semblance of legitimacy but also the sense of urgency. On top of that, the subject lines and/or document names used in file-sharing phishing attacks refer to topics that are likely to pique the target's curiosity or induce FOMO ("fear of missing out")—for example, references to vacation policy changes or compensation package updates.

Hiding in Plain Sight

Perhaps the most devious aspect of file-sharing phishing attacks is that a significant percentage don't just impersonate a legitimate file-hosting or e-signature service but actually use the service itself to deliver the email, malicious link/payload, or both.

Because popular solutions like Dropbox, ShareFile, and DocuSign offer either free registration or no-charge trials, any individual (including attackers) can create and send emails via the platform. This means cybercriminals can craft and dispatch malicious messages that are essentially identical to a normal, genuine notification. The sender's address, email body, and embedded link are all legitimate. It is only after the target leaves the email environment and engages with the shared file or document that they are exposed to the malicious content or payload.

Even if they opt not to exploit a legitimate platform's infrastructure, the threat actors behind file-sharing phishing attacks can use multiple techniques to obfuscate the malicious nature of the embedded link.

For example, some attackers utilize URL shorteners to mask the link to the phishing page. Others take advantage of open redirect vulnerabilities and append the malicious site to a trusted website's URL. Then, when a target clicks the embedded link, they are first directed to the legitimate website before being immediately redirected to the malicious site, making it more difficult to notice the phishing attempt. Because traditional security solutions only analyze the top-level domain and not the entire URL or its final destination, these tactics decrease the chances of the link being flagged by legacy tools as malicious.

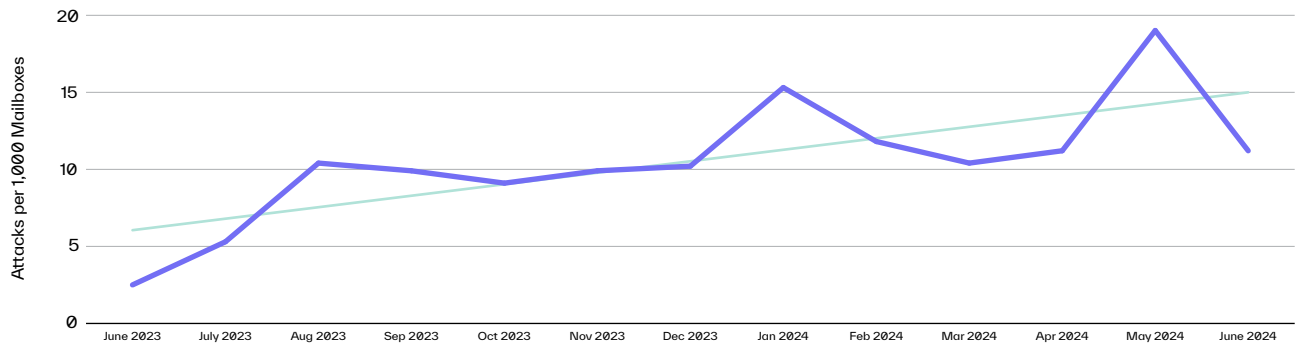
All of these elements combined result in email threats that are all but guaranteed to bypass traditional security measures and have an exceptionally high probability of deceiving employees.

Given this, minimizing your organization's vulnerability to file-sharing attacks starts with understanding the breadth of the issue, the key attributes of these threats, your organization's risk level, and which of your employees are most likely to be targeted.

File-Sharing Phishing Volume More Than Triples Year-over-Year*

File-sharing phishing attacks would be a pressing issue regardless of volume, as one single successful attack can have costly consequences. But considering that these attacks increased by 350% between June 2023 and June 2024, it's clear that blocking these threats is rapidly becoming more critical than ever.

File-Sharing Phishing Attack Volume



The rise of remote work and hybrid workforces have led to a corresponding increase in the use of file-sharing services for business communications and collaboration. Never a group to ignore an opportunity to capitalize on broad changes in work habits, attackers have clearly taken advantage of this accelerated adoption.

Additionally, today's threat actors are always on the lookout for tactics that allow them to reach a broader audience without sacrificing the quality of the email content (since that would impact their success). Utilizing legitimate file-hosting platforms is a cost-effective and scalable way for cybercriminals to launch attacks, as they can easily send convincing emails containing malicious links without having to develop and maintain their own infrastructure.

Moreover, as previously mentioned, generative AI tools and phishing-as-a-service kits are widely accessible, significantly lowering the barrier to entry into the world of cybercrime. This increased availability is likely to result in a higher number of cybercriminals and, in turn, an escalation in the volume of attacks.

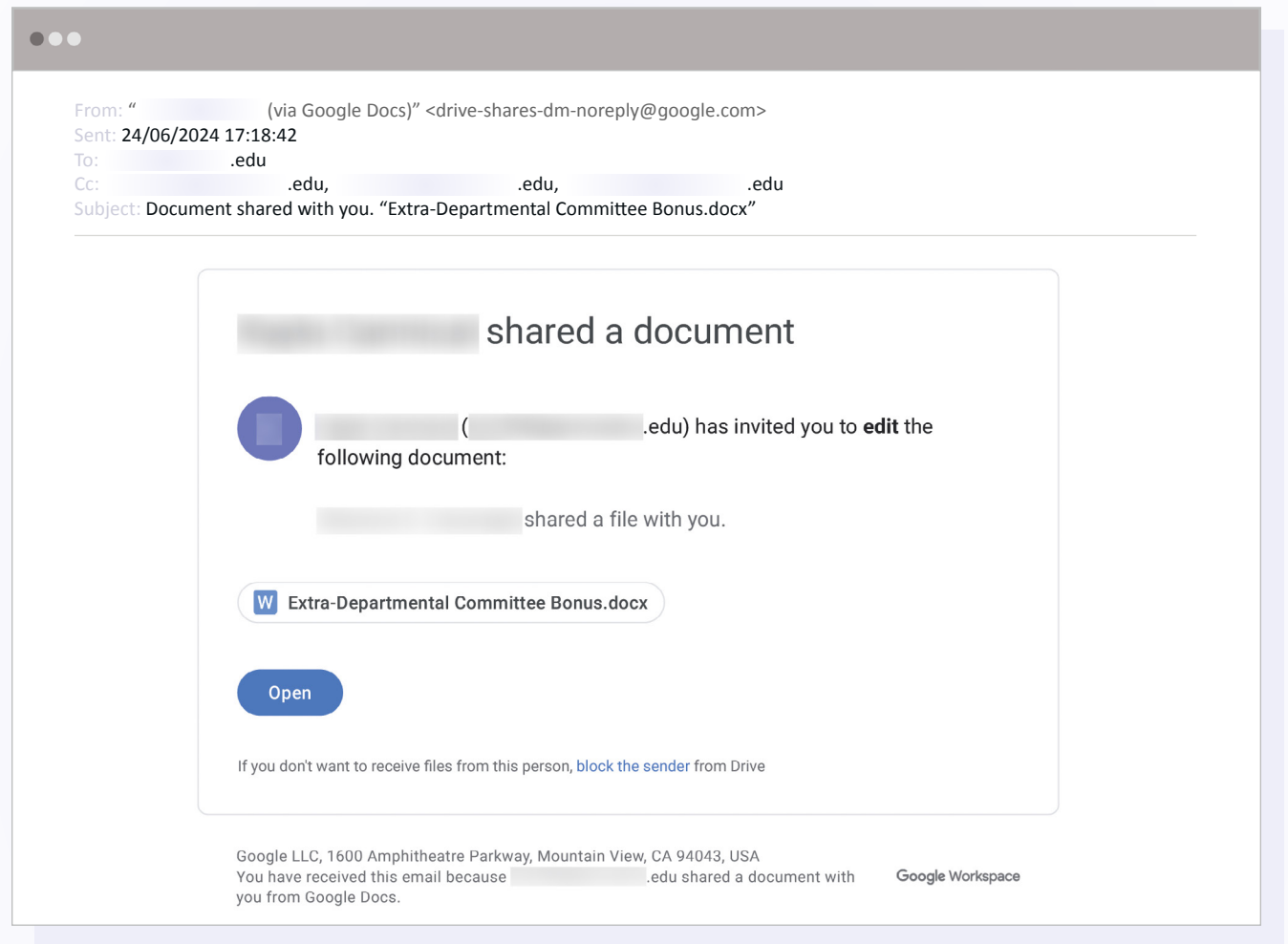
*Note: We focused specifically on the most sophisticated file-sharing phishing attacks, in which recipients were prompted to enter login credentials after clicking on a link contained within the malicious message.



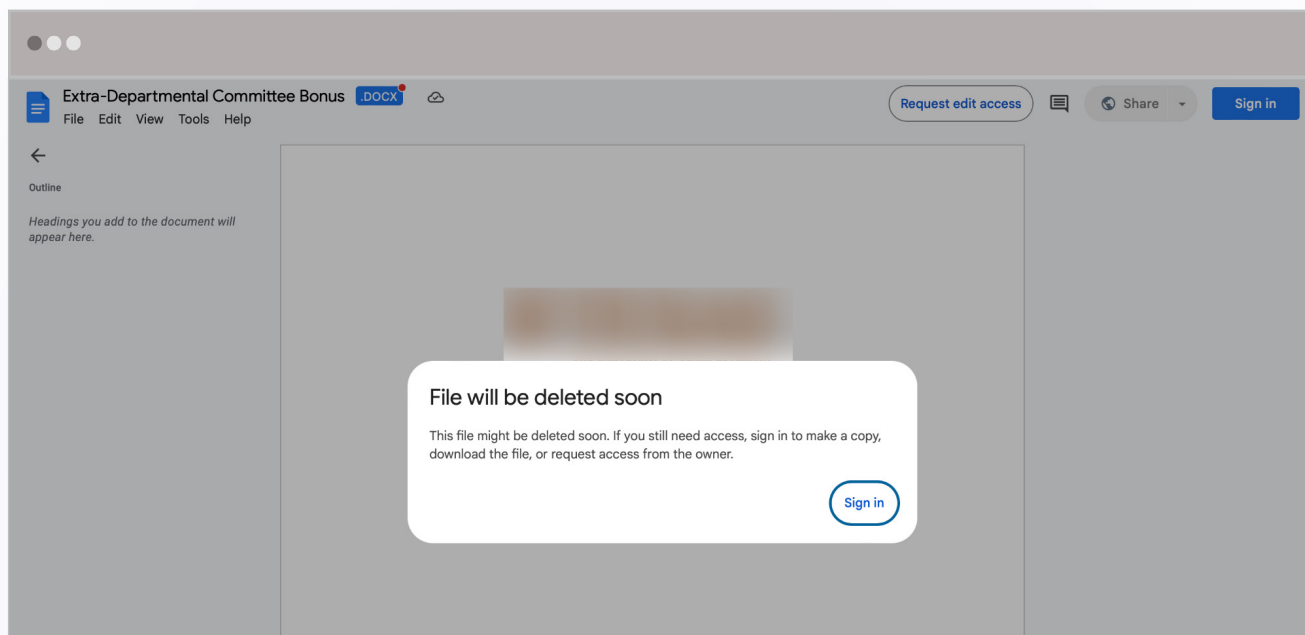
Real-World Example of a File-Sharing Phishing Attack

The example below illustrates how a threat actor can launch a file-sharing attack exclusively using legitimate platforms and still accomplish their goal of stealing login credentials.

First, the attacker compromises a university student's account and uses it to create a Google Doc, which they then share with the targets—faculty members at another university.

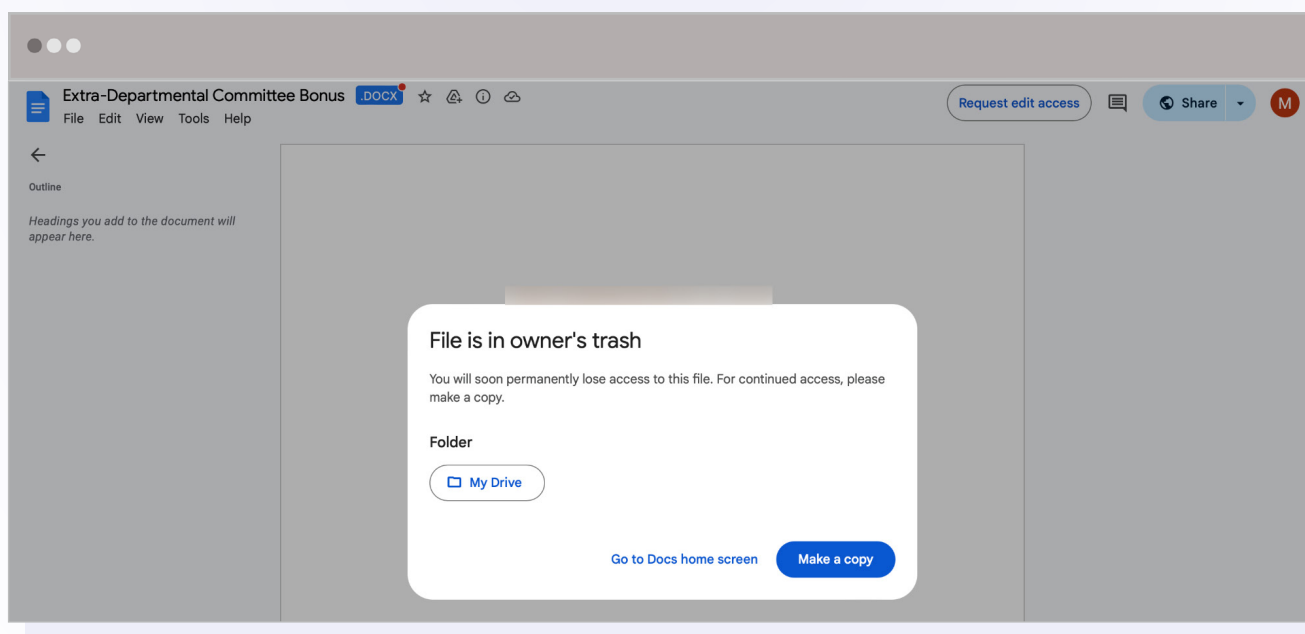


The threat actor's decision to give the file a name related to financial compensation is a smart one, as it is likely to pique the recipients' interest. If one of the faculty members clicks the Open button to view the document, they will be redirected to the impersonated student's Google Drive account.

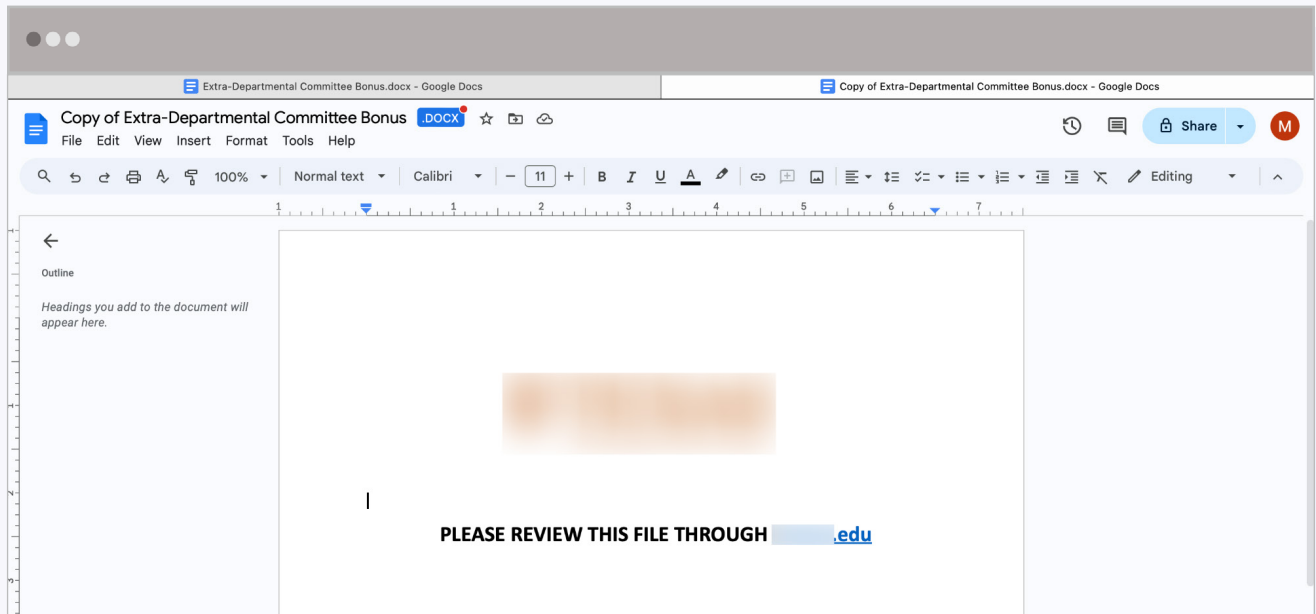


Interestingly, the attacker has hidden the linked file in the university student's trash, which accomplishes three things: 1) it prevents the student from discovering the document, 2) it increases the appearance of legitimacy by requiring the target to log in to their Google account, and 3) it manufactures a sense of urgency for the recipient since, if they do not act quickly, they will seemingly lose access to the file.

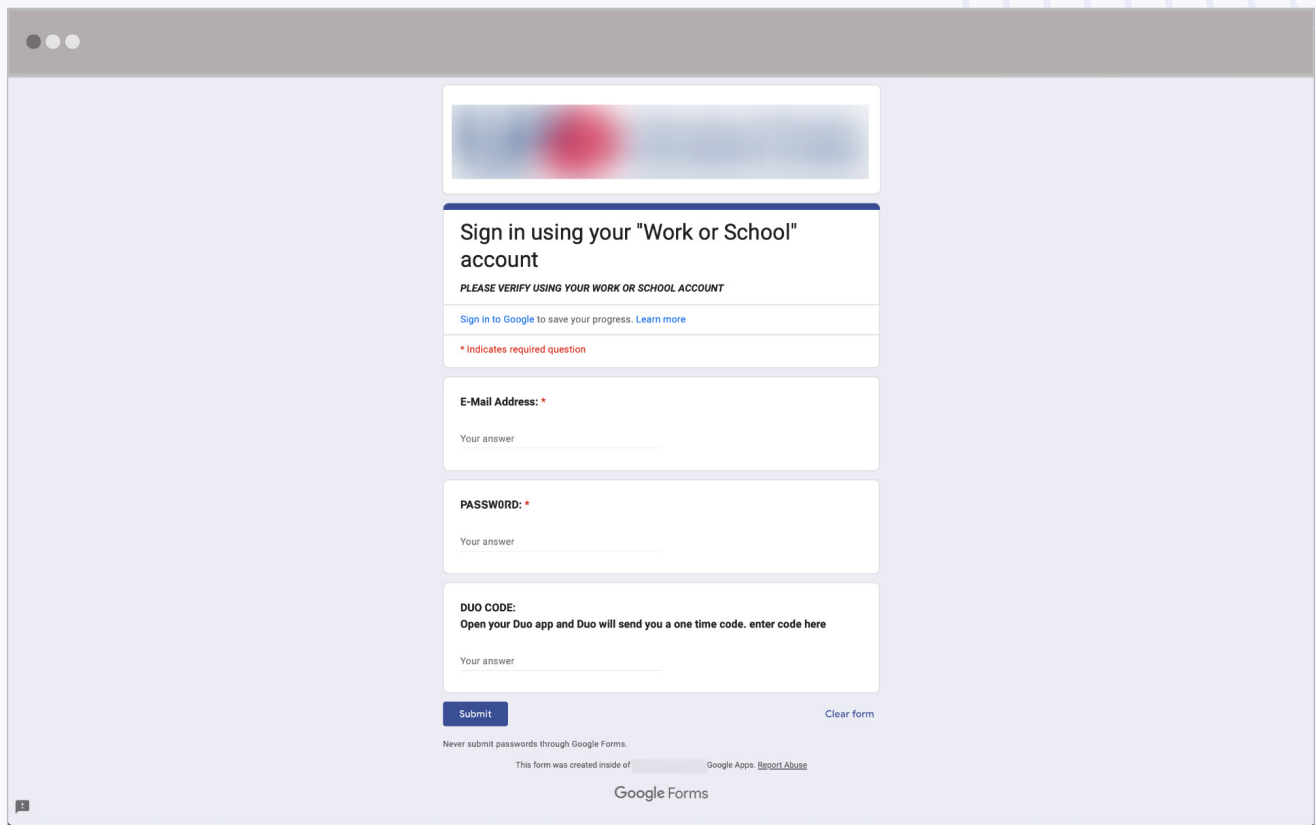
Once the target signs into their Google account, they are presented with the option to make a copy of the shared document.



After making a copy, they can view the full document, which features the logo of the university at which the faculty member works to add to the semblance of authenticity. It also includes an invitation to review what can only be assumed to be the file referenced in the original email.



Although the hyperlinked text is the domain for the target's university, the actual link is to a form hosted on Google Forms.



This is where the attacker apparently became a little sloppy, as the logo on the form is for another university, albeit one located in the same state as the faculty member's employer. What is likely the case is they executed a similar attack on another university and reused the form without updating it first.

The form requests that the recipient verify their identity by entering their email address, password, and the authentication code from Duo, a multi-factor authentication (MFA) solution. However, because the Google Forms Terms of Service states that the product cannot be used to "solicit or collect sensitive data such as passwords," a form that includes the word "password" as part of the question might be flagged. To circumvent this, the attacker spells "password" with a zero instead of an O and a symbol from the Cherokee syllabary that resembles an R.

Should the target enter the requested information, including the authentication code, the attacker will be able to sidestep MFA and immediately access the faculty member's account.

While the threat actor may have been mildly careless with their personalization of the Google Form, at no point in the attack was there an obvious indicator of compromise. The initial email originated from a legitimate domain—google[.]com. The shared file was created using Google Docs, a legitimate software, utilizing a real Google account belonging to a real university student. The phishing page was hosted on Google Forms, another legitimate platform.

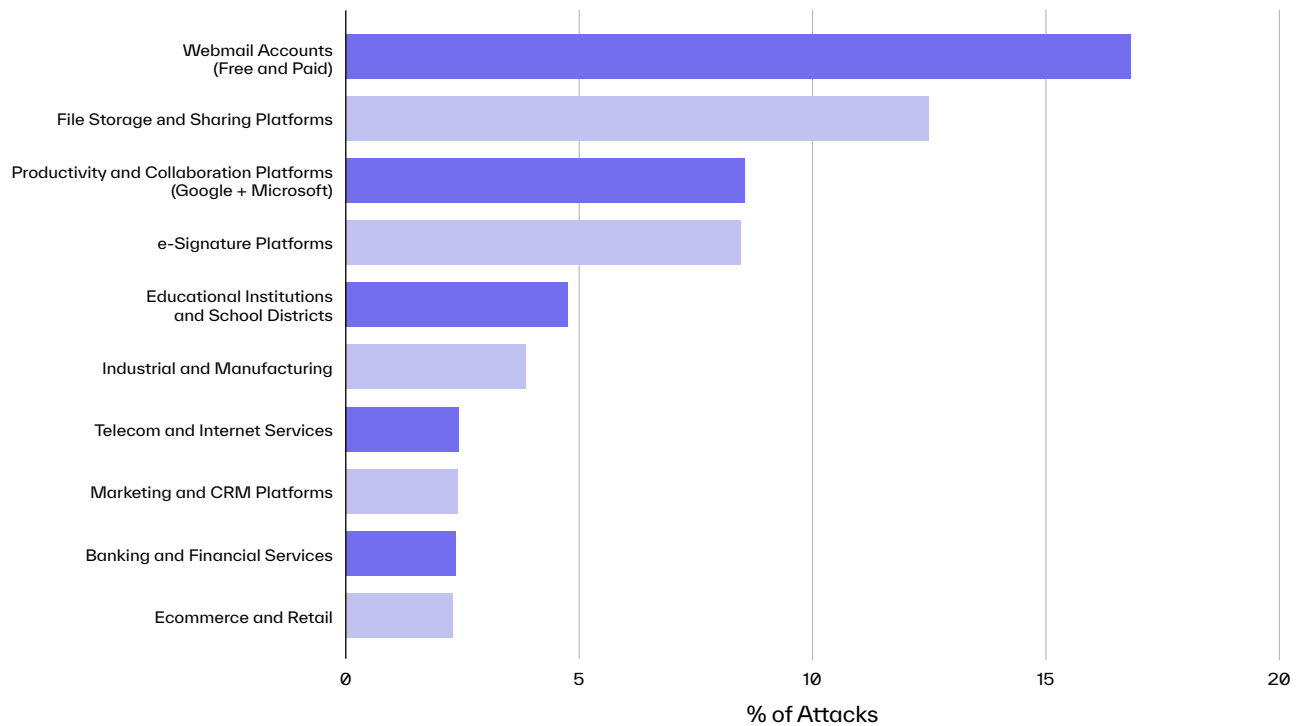
In short, identifying this as an attack is not possible without the ability to understand the context and intent.



Inspecting Legitimate Sending Domains Used in File-Sharing Phishing

Though not every file-sharing phishing attack originates from a legitimate sending domain (i.e., one that was registered more than five years ago), more than 60% do, accounting for nearly 3.5 million attacks in the first half of 2024.

Top Categories of Legitimate Domains Used in File-Sharing Phishing Attacks



In examining the top 10 categories of legitimate domains used to send file-sharing phishing attacks, the four most common are unsurprising. Webmail accounts, such as Gmail, iCloud, and Outlook, are popular options for attacks of all types. The category of Productivity and Collaboration Platforms represents the domains used for notifications from Google's and Microsoft's respective solutions. Because most of the platforms in these suites are available to anyone and their sending domains are automatically trusted, they are highly attractive to cybercriminals. Finally, file storage and sharing platforms like Dropbox and e-signature solutions like DocuSign are ideal for file-sharing phishing attacks due to their built-in plausible premises.

Educational Institutions and School Districts, the first domain category unrelated to email services or business solutions, also ranks high for several reasons.

First, almost every student brings multiple personal devices to campus, each one connected to the university network and representing a security vulnerability for attackers to exploit. Second, while student email addresses frequently stay active after graduation to allow alumni continued access, not every account is accessed regularly (if at all), leaving many dormant accounts vulnerable to compromise. Similarly, the high turnover rate in student email accounts due to transfers and withdrawals can lead to security gaps as accounts might not be monitored as closely once students leave. Moreover, emails from these institutions are generally assumed to be genuine, which means they can be used to both launch internal attacks and target individuals at external organizations.



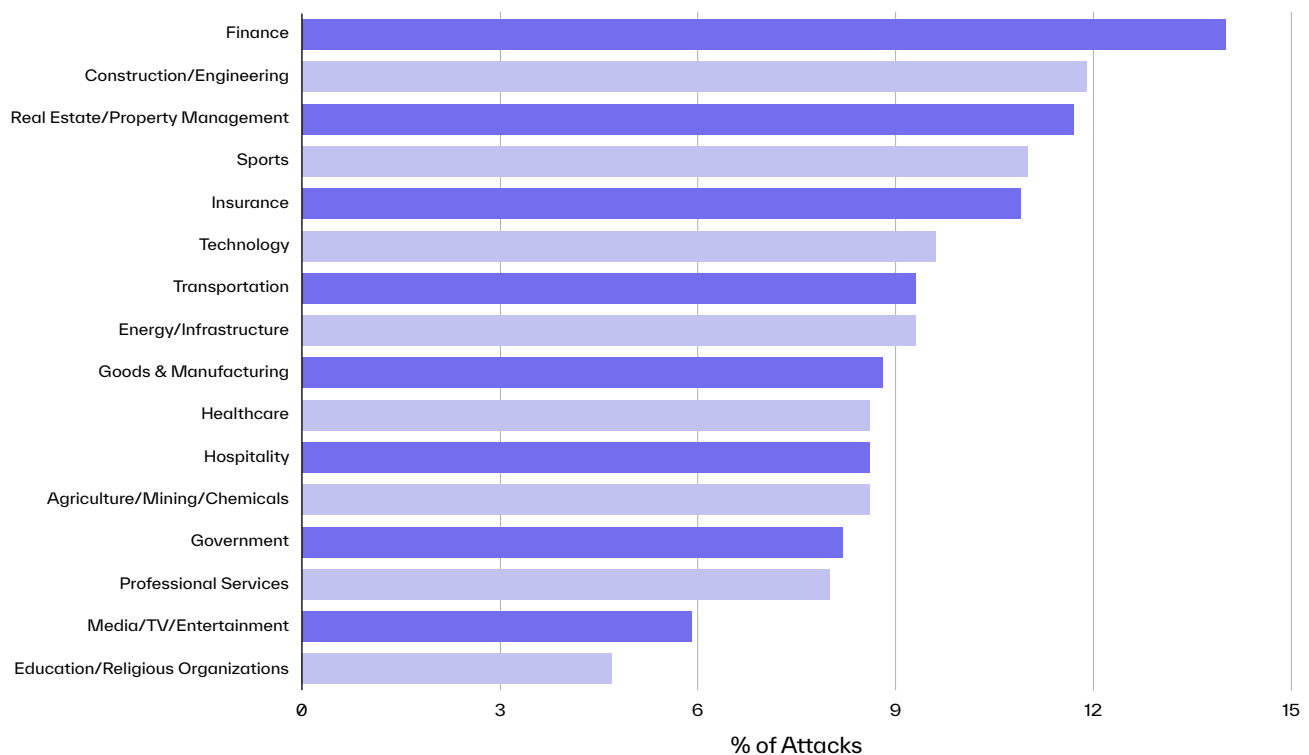
Ultimately, the inherent trust and widespread utilization of these domains make them irresistible for threat actors looking to compromise organizations through seemingly innocuous emails. This exploitation of established domains not only facilitates the success of file-sharing phishing attacks but also complicates the task of distinguishing between legitimate and malicious communications.



Financial Organizations and Built Environment Firms Most Targeted

While organizations in every industry are targeted by file-sharing phishing attacks, the proportion of total attack volume attributed to these threats varies by industry.

% of All Attacks Classified as File-Sharing Phishing Attacks by Industry



The finance industry experiences the highest ratio of file-sharing phishing attacks, with more than one in 10 advanced attacks classified as such. Financial institutions rely on file-sharing platforms to securely exchange documents with clients, partners, and regulatory bodies. As a result, attackers have ample opportunities to slip in a fraudulent file-sharing notification among the sea of invoices, contracts, investment proposals, and regulatory updates.



Incidentally, the need to adhere to regulatory requirements can put financial organizations at increased cybersecurity risk. In the interest of avoiding penalties and legal consequences, financial institutions often prioritize meeting compliance standards that prescribe specific procedures and controls, which regulatory bodies don't necessarily adjust in response to new cybersecurity threats. This rigidity can limit an organization's ability to keep pace with the rapidly evolving attack landscape.

Construction and engineering firms, along with real estate agencies and property management companies, have the second and third-highest ratios of file-sharing phishing attacks, respectively. This alignment is logical, as operations in these industries share certain characteristics that make them desirable targets.

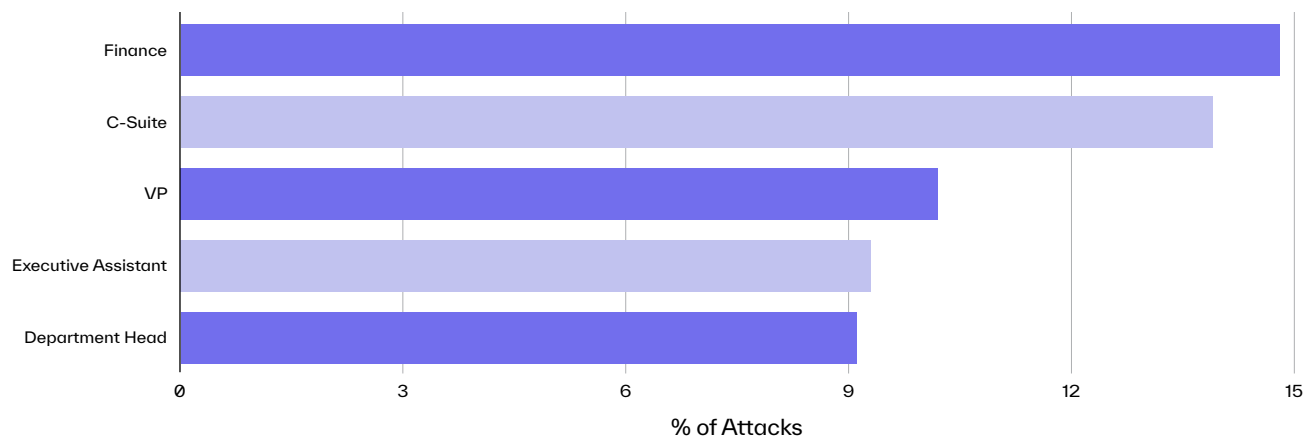
Similar to financial institutions, built environment firms rely heavily on frequent document transfers via file-sharing platforms. Further, both construction projects and real estate transactions are time-sensitive, involve extensive communication among multiple parties, and require rapid decision-making. Attackers can exploit the urgency, complexity, and volume of these exchanges by sending file-sharing phishing attacks that appear time-critical and blend in seamlessly with legitimate emails.



Finance Employees See Highest Ratio of File-Sharing Phishing Attacks

Traditionally, when analyzing attack trends by employee role, staff members in finance positions have not been the most targeted. However, that is not the case with file-sharing phishing attacks.

% of All Attacks Classified as File-Sharing Phishing Attacks by Employee Role



Employees in finance and accounting positions (e.g., accountant, payroll manager, financial analyst, etc.) recorded the highest ratio of file-sharing phishing attacks, even surpassing members of the C-Suite, who are frequently the most targeted by advanced attacks.

Financial documents, such as invoices, purchase orders, and account statements, are among the most common types of business documents sent via file-sharing platforms in general. Additionally, these employees often work directly with external vendors, clients, and regulatory bodies, necessitating the use of file-sharing platforms to securely exchange other business documents, including licensing agreements, strategic planning documents, and regulatory filings. Consequently, finance and accounting personnel would conceivably be more likely to open file-sharing links without suspicion since these emails are part of their daily workflow.

In addition to being in roles that are highly relevant to the premise of file-sharing phishing attacks, finance department employees have access to valuable financial data and personally identifiable information (PII) of employees and clients. Successfully compromising the account of one of these employees would allow a threat actor to steal this data and either sell it on the dark web or use it to commit fraud or identity theft.





Business Email Compromise Persists as Popular Attack Strategy

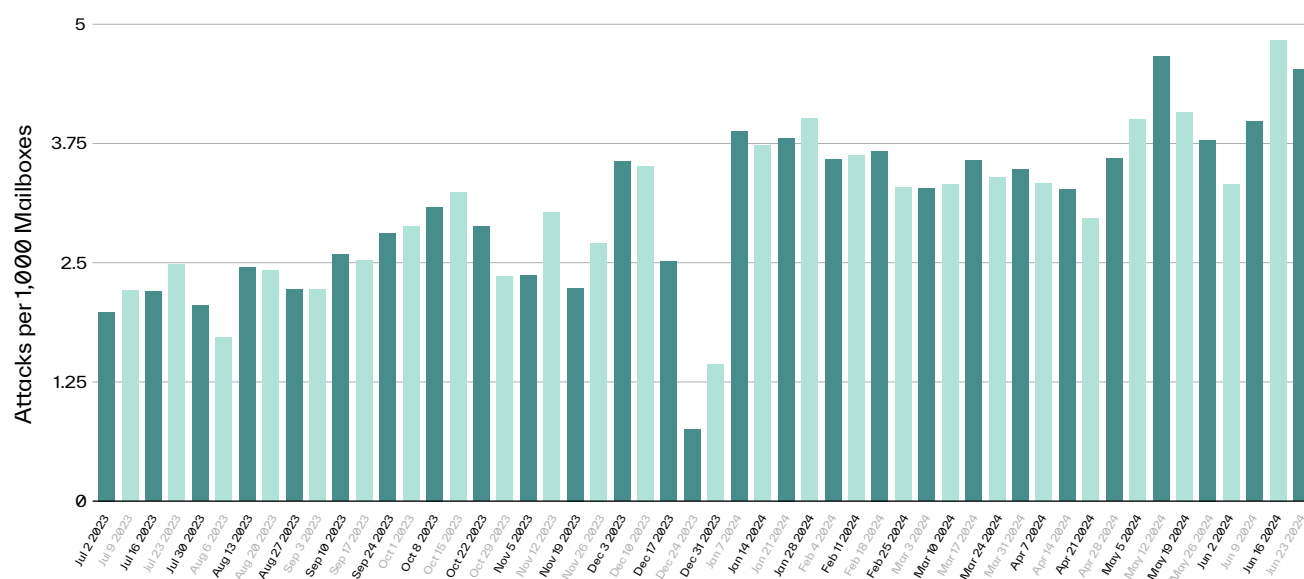
Of the more than \$12.3 billion in losses reported to the FBI IC3 in 2023, nearly 25% were directly attributable to business email compromise (BEC). Since its initial inclusion in the 2015 IC3 report, losses due to BEC have skyrocketed more than 1000%, totaling \$14.3 billion over the last eight years.

The most recent FBI IC3 report revealed that there were 21,489 victims of BEC attacks in 2023, costing organizations an average of more than \$137,000 per incident.

Business Email Compromise Attacks Continue to Increase

Business email compromise (BEC) attacks grew by more than 50% between H2 2023 and H1 2024, from 2.46 attacks per 1,000 mailboxes to 3.72.

Median Weekly BEC Attacks per 1,000 Mailboxes



In BEC attacks, threat actors meticulously select their targets and conduct thorough research, leveraging publicly available information to customize their malicious messages. They impersonate individuals with whom the target has an established partnership or who hold a position of authority, allowing them to capitalize on the implicit trust within the relationship. Then, they apply social engineering tactics to exploit the natural tendency of humans to be helpful to deceive targets into divulging sensitive information or completing fraudulent financial requests.

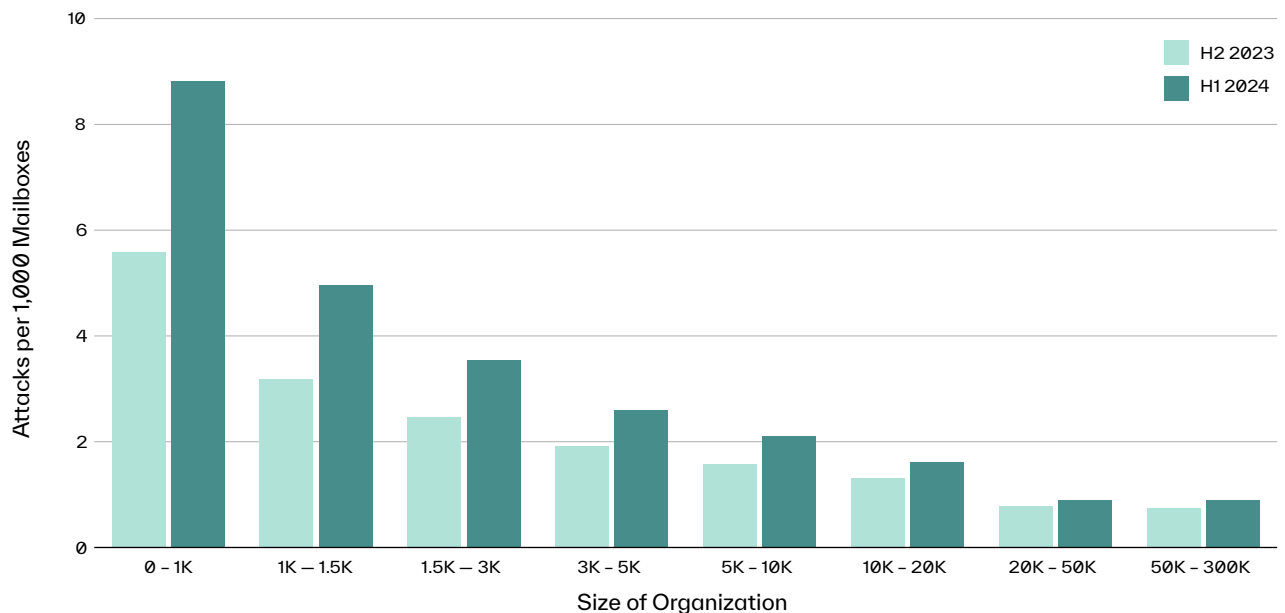
While these threats may not account for a large percentage of all advanced attacks, bad actors only need a BEC attack to be successful once in order to acquire the information or funds they seek.

Additionally, because these emails rarely contain obvious indicators of compromise, such as malicious links or attachments, they are difficult for legacy security solutions to detect. This leaves employees—notoriously the weakest link in the cybersecurity chain—as the last line of defense.

BEC Attacks on Smaller Organizations Rise Nearly 60%

As has consistently been the case for the past several years, BEC attacks targeting smaller organizations (i.e., those with 1,500 employees or fewer) are increasing at a significantly faster rate than those targeting larger organizations.

BEC Attacks by Organization Size (H2 2023 vs. H1 2024)



Between H2 2023 and H1 2024, BEC attacks on smaller organizations jumped by nearly 60%, from 5.6 attacks per 1,000 mailboxes to 8.8.

It's clear that the threat of business email compromise isn't just a problem for global enterprises; smaller organizations are also at risk. Although security incidents at large companies are what make the news, smaller businesses are actually a prime target for cybercriminals. This is partly because smaller companies often have limited budgets, which can mean less money is spent on cybersecurity measures and employee training.

Moreover, even though larger companies might experience fewer BEC attacks per 1,000 mailboxes, this doesn't indicate they are less at risk. BEC is highly targeted, focusing on employees who handle financial operations or have access to critical data. Therefore, the frequency of BEC attacks does not necessarily correlate with the size of the company.





Risk of Vendor Email Compromise Stays Steady

Much like traditional BEC, vendor email compromise involves the exploitation of a trusted identity. In these attacks, however, the person being impersonated is an external third party rather than an internal employee.

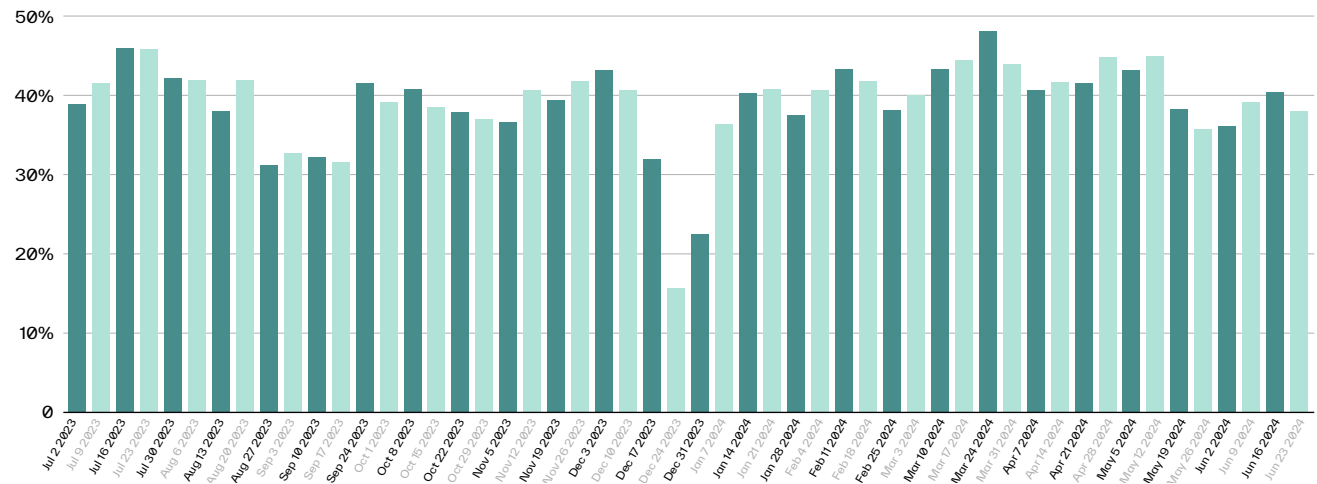
Posing as suppliers, distributors, or service providers, threat actors attempt to deceive targets into making payments for fake invoices, initiating fraudulent wire transfers, or updating banking details for future transactions.



Vendor Email Compromise Attacks Retain Velocity

Vendor email compromise (VEC) tends to occur at a lower rate than other threats like phishing for a few reasons. Primary among those is that cybercriminals will always choose the path of least resistance, and VEC, though lucrative, is a high-effort attack type.

Percentage of Organizations Receiving a VEC Attack Each Week



That being said, plenty of threat actors have deemed the effort worth the reward, as an average of 41% of Abnormal customers were targeted by VEC each week between January–June 2024. This represents a slight increase over the second half of 2023, when the average was 37%.

Although compromising employees is the most direct way to infiltrate your enterprise, every vendor is a potential entry point. If a vendor lacks sufficient security controls and a threat actor compromises an account in their ecosystem, that account can be used to attack your employees.

The emails, originating from a legitimate account with no history of suspicious behavior, would bypass signature-based security solutions. The targeted employee would likely not suspect fraud, as the emails would appear to be from the actual vendor. With access to previous correspondence, the attacker could also hijack ongoing conversations or mimic vendor communications exactly, making it nearly impossible for the average employee to identify the emails as malicious.



Retail, Consumer Goods, and Construction at Greatest Risk for VEC

Every organization is susceptible to vendor email compromise, as even the smallest businesses work with at least a handful of vendors. However, due to the nature of their operations, organizations in certain industries are more likely to be targeted for VEC than others.

Industry*	Percentage of Companies Targeted by VEC
Retail/Consumer Goods & Manufacturing	69.53%
Construction/Engineering	68.07%
Transportation	57.69%
Professional Services	54.76%
Energy/Infrastructure	52.50%

*Includes only industries with ≥ 100 companies

Nearly 70% of construction and engineering firms, as well as retailers and consumer goods manufacturers, received at least one VEC attack during January–June 2024.

Retailers and consumer goods manufacturers operate within complex and interconnected supply chains, where each vendor email account serves as a potential gateway for attackers. The high volume of email communications necessary for these operations further increases the risk by providing ample opportunities for malicious actors to blend in with legitimate interactions.

Similarly, modern construction projects depend on a network of digital systems spread across multiple job sites and offices, resulting in an extensive attack surface. In addition, coordinating major projects requires the ongoing exchange of confidential and proprietary information, including financial data, among a wide ecosystem of vendors, contractors, and subcontractors. This creates numerous chances for threat actors to intercept and exploit these communications.



Securing Your Organization Against Modern Threats

As the threat landscape continues to evolve, the inadequacy of legacy solutions like secure email gateways (SEGs) becomes increasingly obvious. File-sharing phishing attacks, in particular, highlight the shortcomings of signature-based security solutions with respect to modern threats.

These traditional systems rely on the concept of “if this, then that” and flag emails based on whether or not they are sent from a suspicious domain or contain known malicious components. However, file-sharing phishing attacks are crafted so they appear to originate (or actually originate) from trusted senders. The content of the email is also safe, and the message is often just the first stepping stone in a series that leads to the malicious link or payload, which frequently exists entirely outside the email environment. The architecture of file-sharing attacks necessitates an ability to not only understand the context and intent of every message but also evaluate elements beyond the inbox.

Where legacy email security solutions utilize rules and policies to identify attacks, a cloud-native, API-based email security platform takes a fundamentally different approach. The API-based architecture ingests extensive behavioral data across the email platform, enabling a deep understanding of individual and organizational behavior patterns and context. The platform then uses advanced AI techniques like computer vision and natural language processing for nuanced threat detection, understanding the content and tone of communications to identify anomalies. This allows it to precisely detect and then automatically remediate email threats.

Today’s threat actors know how to “hack the human” and are continually developing new strategies for manipulating employees. 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 mistake.



Abnormal

Abnormal Security is the leading AI-native human behavior security platform, leveraging machine learning to stop sophisticated inbound attacks and detect compromised accounts across email and connected applications. The anomaly detection engine leverages identity and context to understand human behavior and analyze the risk of every cloud email event—detecting and stopping sophisticated, socially-engineered attacks that target the human vulnerability.

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. Additional protection is available for Slack, Workday, Salesforce, ServiceNow, Zoom, Amazon Web Services and multiple other cloud applications.

Interested in Stopping Modern Email Attacks?

[Request a Demo →](#)

[Follow Us on X →](#)