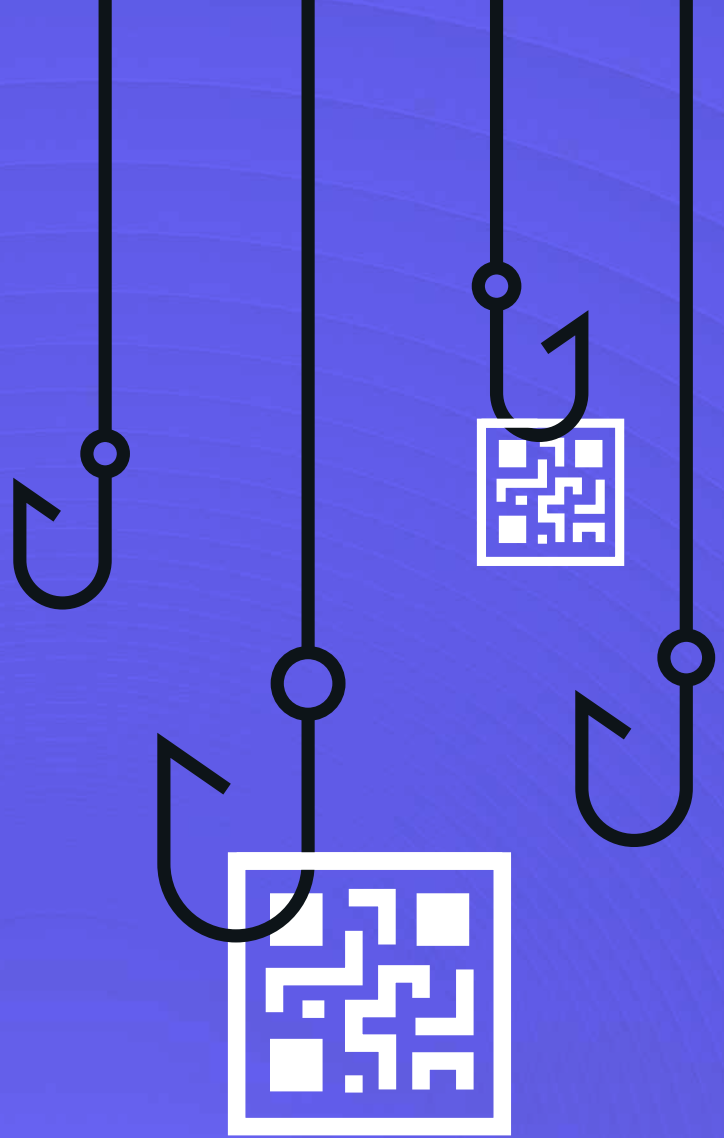


Abnormal



Phishing Frenzy:

C-Suite Receives
42x More QR Code
Attacks Than
Average Employee

Executive Summary

89.3%

Percentage of QR code attacks that are credential phishing attempts.

27%

Percentage of all quishing attacks that impersonate MFA notifications.

108%

Year-over-year increase in BEC attacks between 2022 and 2023.

98.9%

Probability of organizations with a minimum of 50,000 employees receiving at least one BEC attack every week.

Threat actors are opportunistic and enterprising, continually looking for new ways to evade organizational security measures and manipulate targets. Indeed, it's repeatedly been proven that if an element of email can be utilized for nefarious purposes, cybercriminals will learn how to exploit it.

The result has been a decades-long cat-and-mouse game in which every advancement in email security has given rise to a corresponding shift in strategy from attackers.

QR Code Attacks Make a Splash

QR code phishing ("quishing"), the newest iteration of phishing, tricks targets into interacting with malicious QR codes and unwittingly revealing private information that can be used to compromise accounts and launch additional attacks.

Although every employee is a potential quishing target, C-Suite executives receive 42 times more QR code attacks than the average employee. Cybercriminals also seem to have a favorite industry to target, with construction and engineering organizations experiencing quishing attacks at a rate 19 times higher than any other vertical.

BEC and VEC Attacks See Sustained Upward Trend

While QR code phishing is undeniably gaining momentum as a novel threat, cybercriminals have by no means abandoned their tried-and-true attack strategies. Business email compromise still stands as one of the most financially devastating cybercrimes, and the frequency of vendor email compromise continues to increase each year. In these attacks, threat actors leverage social engineering to manipulate recipients into sharing confidential data or completing fraudulent financial requests.

Between 2022 and 2023, BEC attacks skyrocketed, increasing by 108%. VEC also rose substantially year-over-year, recording 50% growth.

Table of Contents

Threat Actors Drawn to Email's Versatility as Attack Vector	4
Phishers Embrace the Use of QR Codes in Cyberattacks	6
Business Email Compromise Sustains Its Momentum	17
Risk of Vendor Email Compromise Continues to Rise	20
Defending Against New and Emerging Threats	23
About Abnormal	24





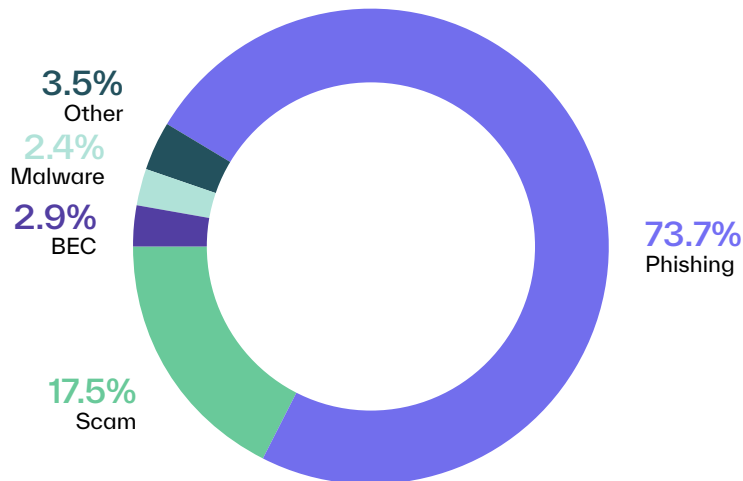
Threat Actors Drawn to Email's Versatility as Attack Vector

Business communication relies on email, as it is the only universally adopted platform across every industry and location. Unfortunately, email's ubiquity is one of the reasons why it's been a preferred attack vector for nearly four decades. Moreover, the versatility of email as a communication medium means it can be exploited by threat actors for a variety of malicious purposes. And with millions of individuals joining the workforce every year, threat actors always have new people (and new organizations) to target.

Phishing Remains the Most Popular Attack Strategy

Examining the distribution of attack types, it is unsurprising to see that credential phishing has maintained its position as the most prevalent cybercrime, accounting for more than 73% of all advanced attacks. This trend aligns with the broader threat landscape, as phishing has been ranked the most common cybercrime by the FBI's Internet Crime Complaint Center (IC3) for the past four years.

Percentage of Advanced Attacks By Type



It's true that, in terms of total losses, phishing falls squarely in the bottom third of all attack types tracked by the IC3. However, what security leaders must remember is that phishing is frequently just the first step in a variety of crimes and is often used more as a "foot in the door" technique rather than the end goal.

An email account acts as the hub for just about everything the average professional needs to do their job. Employees use their email to log into applications, link business accounts, and reset passwords. This means if a threat actor steals login credentials via a successful phishing attack, they can use those to compromise the employee's email account and gain access to nearly every other account that he or she has within the entire application ecosystem.

Phishing accounts for nearly 3/4 of all advanced inbound email attacks.





Phishers Embrace the Use of QR Codes in Cyberattacks

Although phishing emails have grown in sophistication and complexity over time, the end goal has stayed the same: trick targets into divulging private information. In the latest iteration of phishing, threat actors use social engineering to manipulate targets into interacting with malicious QR codes and unwittingly disclose details that enable the attacker to compromise accounts and launch further attacks.



Quishing Emerges as Latest Malicious Innovation by Threat Actors

Bad actors have been using phishing emails to steal sensitive data for three decades. Impersonating a trusted individual or brand and manufacturing a sense of urgency, attackers deceive targets into providing private information like login credentials or bank account details.

Because email wasn't initially designed with security in mind, early email platforms lacked the native functionality to proactively detect and block phishing attacks. Additionally, threat actors had the benefit of end-user naivete—targets had no reason to believe the sender was anyone other than the person or company they claimed to be. Over time, however, as email security tools evolved and end users became more aware of common attack ploys, cybercriminals had to adjust their tactics and adopt more sophisticated approaches.

Hook, Line, and Cybercrime: The Growth of Quishing

This evolution in strategy is part of the broader history of phishing, which is characterized by opportunistic threat actors capitalizing on innovations in communication that have led to an increasingly interconnected world.

For example, spear phishing, a more targeted form of phishing that began to emerge at the turn of the millennium, became a viable option when bad actors realized they could make their attacks more personalized (and more convincing) by harvesting the wealth of data available online. Similarly, the rise of voice phishing (vishing) and SMS phishing (smishing)—two attack strategies that started gaining prominence in the 2010s—was facilitated by the pervasiveness of cell phones and the popularity of texting.

QR code phishing, the newest iteration of phishing, is the latest in a long line of malicious initiatives designed by enterprising attackers to evade organizational security measures and manipulate targets.

Quishing is a type of social engineering phishing attack in which a threat actor attempts to trick a target into interacting with a malicious QR code. The QR code is linked to what appears to be a legitimate website (often an emulation of a Google or Microsoft login page) with a prompt to enter login credentials or other sensitive details. Unfortunately, any information provided can then be used by the perpetrator to compromise the target's account and launch additional attacks.

Why Cybercriminals Exploit QR Codes for Phishing

While malicious QR codes sent via email can be used for a variety of purposes, they are primarily utilized for credential phishing. Indeed, 89.3% of QR code attacks detected by Abnormal are credential phishing attacks. This precipitous rise of bad actors using malicious QR codes to steal sensitive data is driven by multiple factors.

First, consider the fact that for the past three and a half years, QR codes have been everywhere. Although this technology was invented in 1994, at no point pre-2020 did QR codes have anywhere near the omnipresence they do now. We scan QR codes to view menus at restaurants, check in at appointments, and make contactless payments. As a result, receiving an email with a request to scan an embedded QR code to reset an expiring password or access important documents is now unlikely to raise any red flags—and attackers know this.

Receiving an email with a request to scan an embedded QR code to reset an expiring password or access important documents is now unlikely to raise any red flags—and attackers know this.

Second, a pillar of cybersecurity awareness training is to emphasize to end users why they should avoid clicking on links in emails they weren't expecting to receive. Utilizing QR codes accomplishes the same goal of redirecting targets to a phishing page but makes the circumstances just different enough that the message may not set off alarms for the target the way a standard link-based phishing attack might.

From a technology standpoint, threat actors recognize that replacing hyperlinks with QR codes in phishing attacks improves the likelihood of the message bypassing legacy email security solutions. Unlike traditional email threats, quishing attacks contain minimal text content and no obvious URL, which significantly reduces the number of signals available for legacy security tools to analyze and use to detect an attack.

Further, a link-based phishing attack keeps the target on the same device, within the purview of the organization and its security controls. Using a QR code, on the other hand, moves the attack to the target's mobile device, which lacks the lateral protection and posture management available in a cloud-based business environment.



For these reasons, quishing will remain an ongoing threat and will likely continue to evolve in response to increased awareness and advancements in security solutions. While organizations of all sizes and across every industry can be targeted by QR code attacks, our research uncovered several noteworthy trends of which security leaders should be aware.

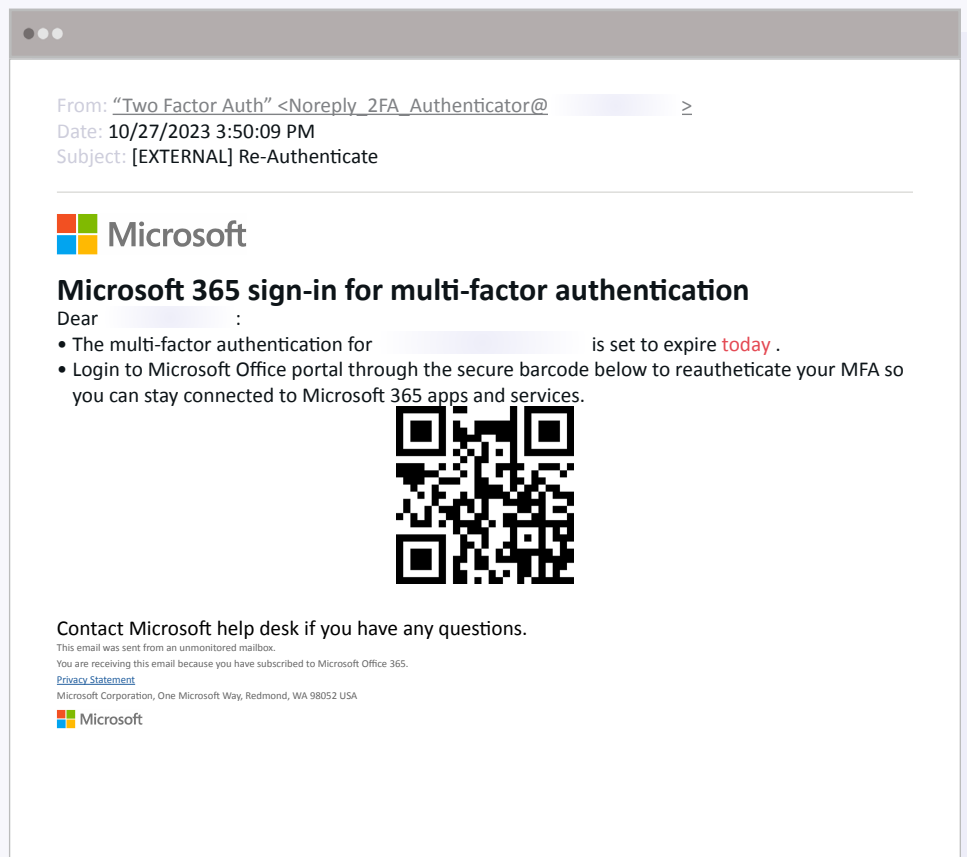


MFA and Document Sharing Stand Out as Preferred Attack Themes

Based on data collected during the second half of 2023, cybercriminals heavily favored two strategies in QR code phishing attacks. The first, accounting for approximately 27% of all phishing attacks, involved fraudulent notices related to multi-factor authentication (MFA). The other preferred approach, which was used in approximately 21% of all QR code attacks, was to send targets fake notifications of a shared document.


Below are four real-world QR code phishing attempts detected and blocked by Abnormal that illustrate the most common ways bad actors execute phishing attacks.

In this first example, the perpetrator states the target's MFA method is expiring that day and needs to be reauthenticated so they do not lose access to Microsoft 365 applications.



The threat actor in this second phishing attack attempts to compel the target to scan the malicious QR code by claiming it is the first step in setting up the multi-factor authentication required by their organization.

From: "IT Dept - 2FA Security" <accidentreporting@ >
Date: 11/9/2023 7:20:04 PM
Subject: General Mandatory Action: 'Authenticator App' update settings is required on or before Friday 10th November, 2023.


 Microsoft

Your organization requires you to set up the following methods to keep your email secure.

Method 1 of 2: App

Microsoft Authenticator
Scan the QR Code

Use your phone camera to scan the Microsoft Authenticator app.
This will start a process to connect your Microsoft Authenticator with your account.
After you scan the QR code, login your email account to complete setup.

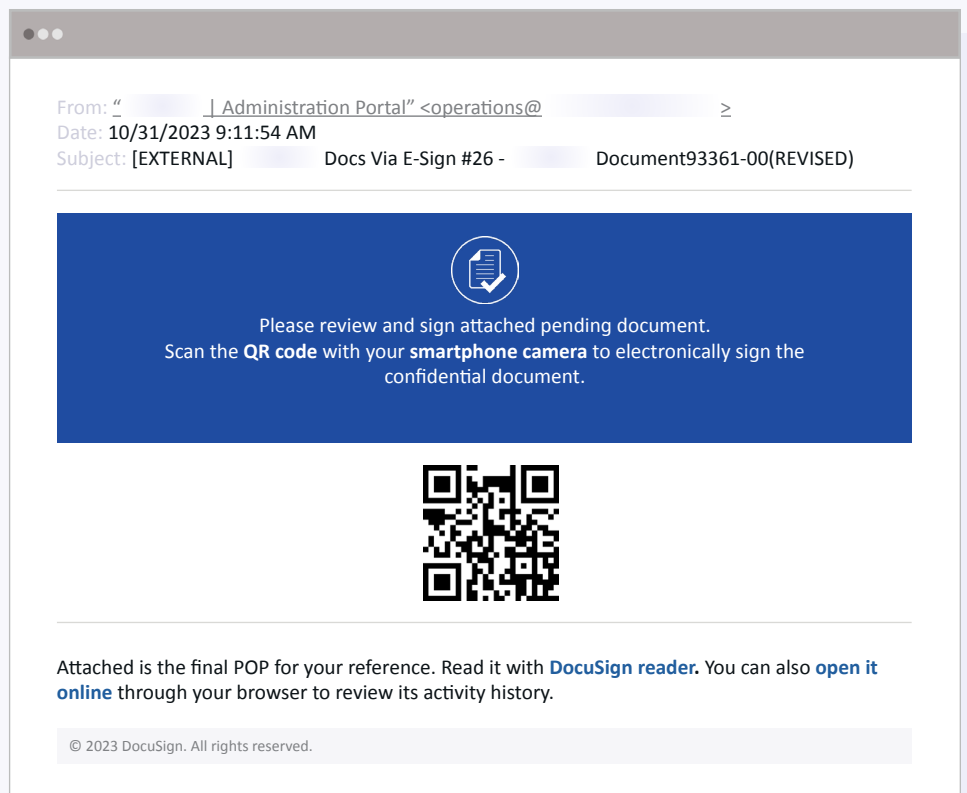
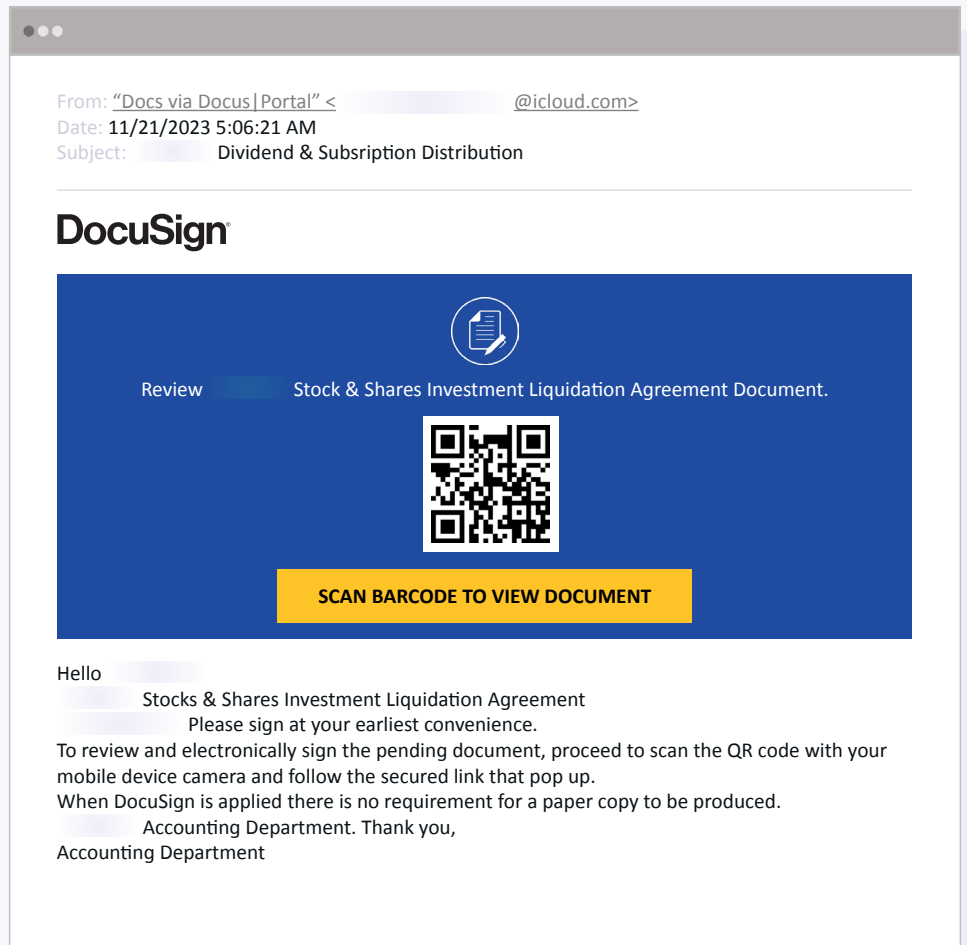


[Can't scan image?](#)

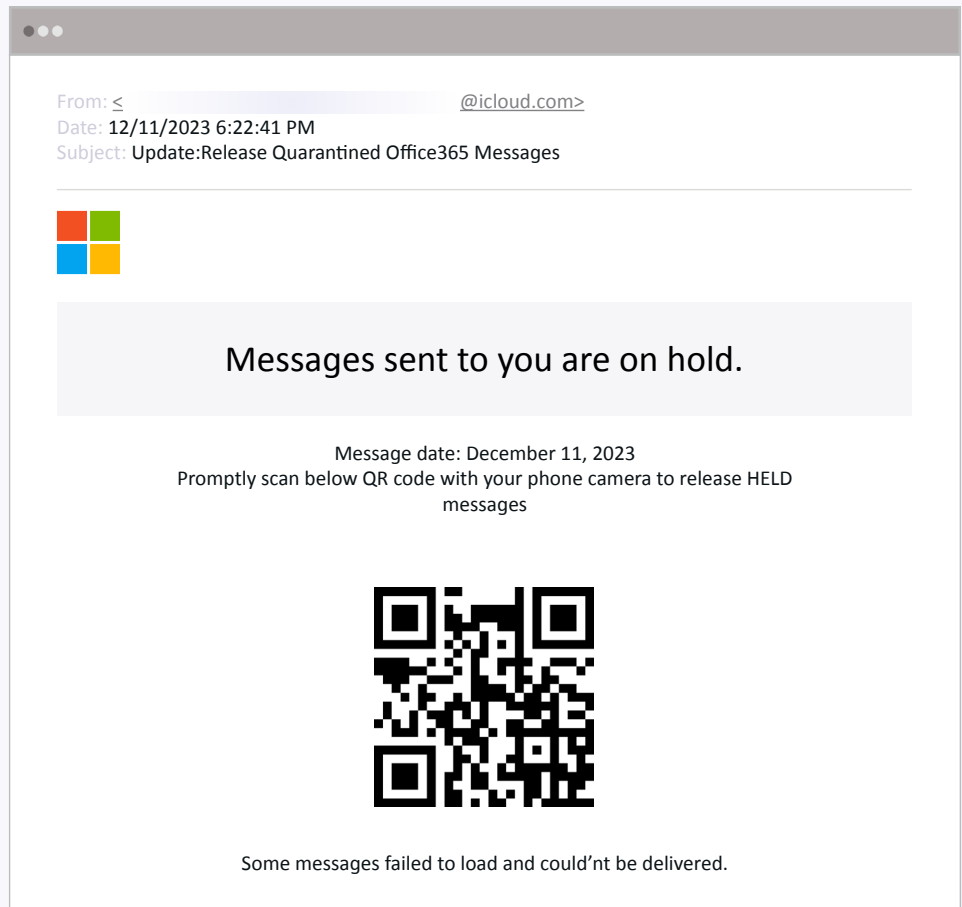
[Next](#)

[I want to set up a different method](#)

In both of the examples on this page, the attackers impersonate DocuSign and inform the target their signature is required on a pending document. The emails state the target can view and sign the document by scanning the included QR code.



While the most prevalent attack themes center on multi-factor authentication and notices of shared documents, these certainly aren't the only tactics bad actors use in quishing attacks. Another recurring, albeit less common, strategy we observed is sending targets an email claiming they have messages that have been quarantined by Microsoft 365, as in the example to the right.



In each of the examples above, the perpetrators utilize social engineering to establish trust and manufacture a sense of urgency. For example, they all integrate some level of the impersonated company's branding into the messages. The threat actors in the first three examples even go one step further and incorporate the attack motif into the sender names. To instill worry and spur action, the MFA-themed attacks claim the target is at risk of losing access to important applications. And because the use of DocuSign is generally reserved for important and/or confidential documents, cybercriminals know posing as that company and claiming financial documents are in need of attention will likely convince the target to act quickly.

Additionally, many of the QR code attacks stopped by Abnormal are sent from an iCloud address, as in the last example. Because iCloud.com is a legitimate sender domain, the emails pass SPF, DKIM, and DMARC checks, which improves the likelihood of a legacy security solution marking the email as safe.



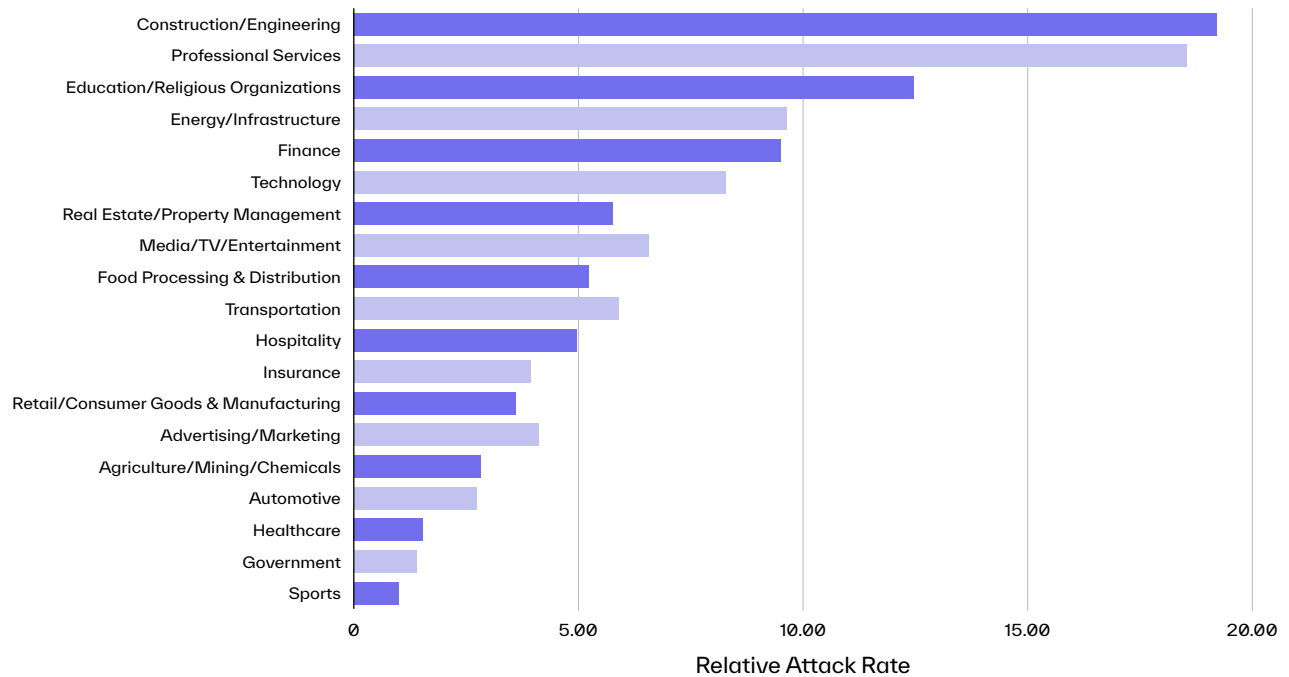
These attacks demonstrate just a few of the tactics threat actors use to bypass traditional email solutions and increase the appearance of legitimacy of their malicious messages to defraud employees.



Construction and Professional Services Most Targeted Industries

Due to the nature of their operations, two industries have considerably higher rates of QR code attacks than any other vertical: construction/engineering and professional services.

QR Code Attack Rate by Industry



According to our data, construction/engineering firms and professional service providers are up to 19.2 times and 18.5 times, respectively, more likely to receive QR code attacks than organizations in other industries.

Construction and engineering enterprises are especially vulnerable to cyberattacks in general due to the industry's historical reluctance to adopt robust data security and privacy regulations. For professional service providers like lawyers, accountants, and business consultants, cybercriminals recognize that gaining entry to their accounts means gaining access to highly confidential data that can either be sold, ransomed, or leveraged for additional attacks.



In the context of QR code attacks, organizations in these sectors are attractive targets for several reasons. Due to the prevalence of remote work among employees in construction and engineering firms, there is a substantial reliance on mobile devices for accessing project details and sharing documents with other stakeholders. Likewise, professional service providers often work from phones and tablets, necessitating on-demand access to various cloud software solutions via these devices.

Therefore, the expiration of multi-factor authentication for these employees can inhibit their ability to do their jobs, and, depending on the context, those delays can be exceptionally costly. As a result, receiving an email claiming imminent MFA expiration would likely spur them to act quickly without first confirming the authenticity of the message. Additionally, both construction and engineering professionals as well as professional service providers receive notifications of shared documents like contracts and invoices almost daily—if not multiple times a day.



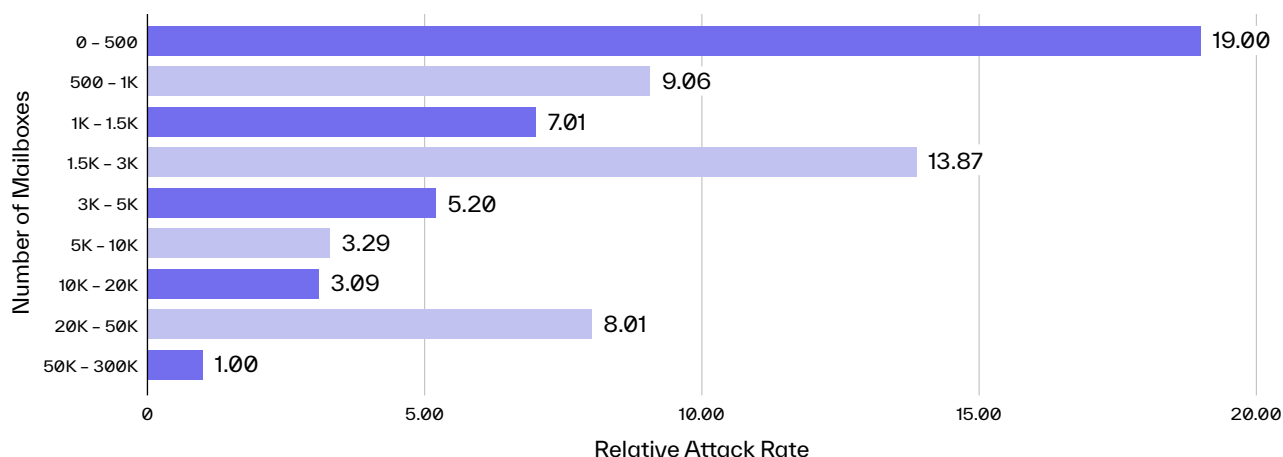
This means attackers have ample opportunities to send a malicious email that blends in nearly seamlessly with legitimate communications.



Smaller Organizations Record Highest Quishing Attack Rate

When comparing QR code attack rates across different business sizes, the data reveals that the smallest organizations (those with 500 or fewer mailboxes) experience quishing attacks at a rate up to 19 times higher than any other size company.

QR Code Attack Rate by Organization Size



There are a number of possible explanations for why this is the case. Larger organizations often have more advanced technology infrastructures and dedicated IT teams. Threat actors may recognize that smaller organizations, on the other hand, often have limited resources to invest in cybersecurity and therefore have fewer tools to detect and prevent quishing attacks. Accordingly, they may perceive smaller organizations as easier targets due to their potentially weaker security infrastructure and be more inclined to launch attacks against them.

Moreover, smaller organizations may not have the capacity to conduct comprehensive training and education programs. This can create gaps in security awareness and protocols, enabling cybercriminals to manipulate employees into falling victim to QR code phishing attacks.



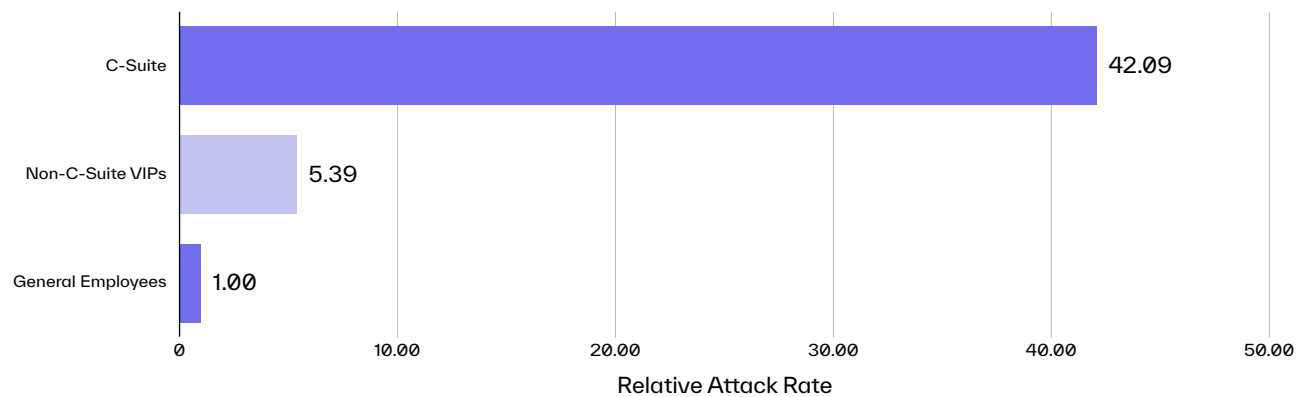
Finally, smaller organizations may have less developed incident response capabilities, making it challenging for them to detect and quickly contain the threat. This delayed response time can give perpetrators more time to carry out their malicious activities.



C-Suite Receives Most QR Code Attacks by Far

Another interesting trend we explored was the correlation between an employee's role in an organization and the likelihood of them being targeted by QR code attacks.

QR Code Attack Rate by Role



Our research revealed that members of the C-Suite were 42 times more likely to receive a QR code phishing attack than a non-executive employee. Non-C-Suite VIPs, such as executive vice presidents, senior vice presidents, and department heads, were also heavily targeted, with an attack rate more than five times that of non-executive employees.

Acquiring the login credentials of one of these individuals yields substantial benefits to an attacker. Besides the IT Director, executives likely have the highest level of app permissions of any member of the organization. They also have direct access to a wealth of confidential and valuable information. In other words, a successful QR code phishing attack on an executive would give a bad actor the “keys to the kingdom,” allowing them to infiltrate every inch of an organization’s network.

Not only that, using the executive’s compromised account, a cybercriminal could send fraudulent requests to internal and external parties who might not think twice about completing the requests since they seemingly came from a VIP. Threat actors also recognize that often multiple people have access to an executive’s inbox, such as executive assistants. Consequently, every individual who knows the login credentials for a VIP’s inbox represents a potential entry point that can be exploited by an attacker.



The background features a series of concentric dashed circles of varying radii, centered on the right side of the page. A solid circle is positioned in the lower right quadrant, partially overlapping the dashed lines. A vertical line and a diagonal line intersect at the center of the dashed circles.

Business Email Compromise Sustains Its Momentum

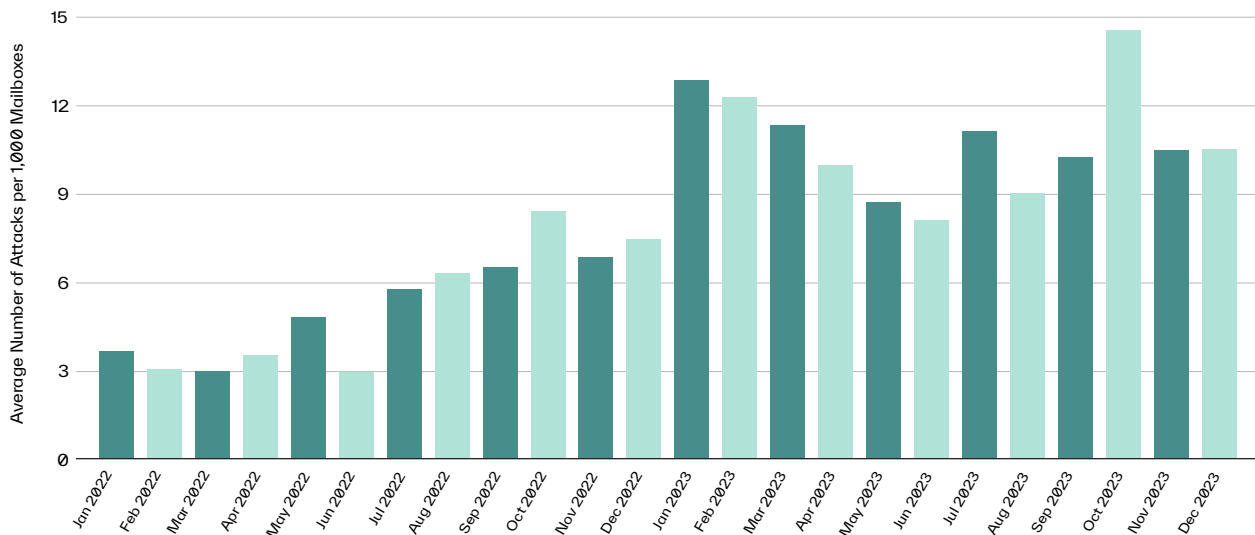
Business email compromise stands as one of the most financially devastating cybercrimes, resulting in losses of \$2.7 billion in the previous year alone. Using text-based emails with no traditional indicators of compromise, cybercriminals easily evade legacy email security solutions that lack the functionality to detect novel threats. By leveraging social engineering techniques to establish trust, threat actors can manipulate recipients into divulging sensitive information or completing fraudulent financial requests.



BEC Attack Frequency Doubles from 2022 to 2023

In 2023, BEC attacks skyrocketed, with monthly attacks per 1,000 mailboxes more than doubling to 10.77, a staggering 108% increase compared to 2022. The rate of these attacks peaked in October with a monthly average of 14.57 attacks per 1,000 mailboxes.

Median Monthly BEC Attacks per 1,000 Mailboxes



According to FBI IC3 data, the average cost of a successful business email compromise attack is more than \$125,000. Thus, while BEC accounts for a smaller percentage of all email attacks, it can yield a massive ROI for cybercriminals.

The fact that the rate of BEC attacks consistently increases year after year demonstrates that threat actors are continuing to achieve their objectives with this approach. And now, with the democratization of generative AI, threat actors can make BEC attacks even more sophisticated, convincing, and effective.



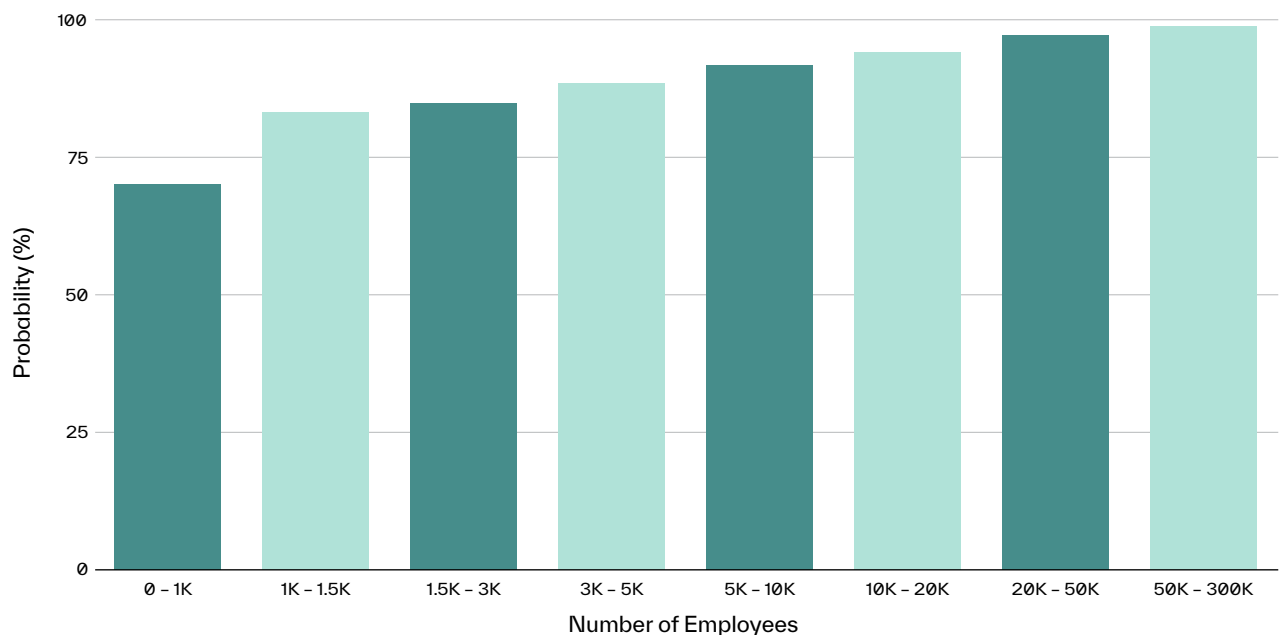
With no signs of slowing down, organizations must urgently prioritize robust email security and employee awareness training to combat this evolving threat.



Larger Organizations Have Highest Probability of BEC Attack

Organizations with 50,000 employees or more have a nearly 100% chance of experiencing at least one BEC attack every week—the highest probability of any organization size.

Average Weekly Probability of Receiving a BEC Attack by Organization Size



Although the largest enterprises recorded the highest weekly probability of receiving a BEC attack, the data shows that organizations of every size are all at considerable risk of business email compromise. Organizations with a minimum of 1,000 employees have anywhere from an 83% to 97% chance of being targeted by BEC each week.

Even the smallest organizations with fewer than 1,000 employees have a 70% weekly probability of experiencing at least one BEC attack per week. This is a testament to the fact that no organization is beyond the scope of a bad actor launching BEC attacks. Interestingly, this percentage has consistently risen year-over-year since 2021, which means if it continues to increase, it won't be long until every organization has upwards of a 90% weekly probability of receiving a BEC attack.





Risk of Vendor Email Compromise Continues to Rise

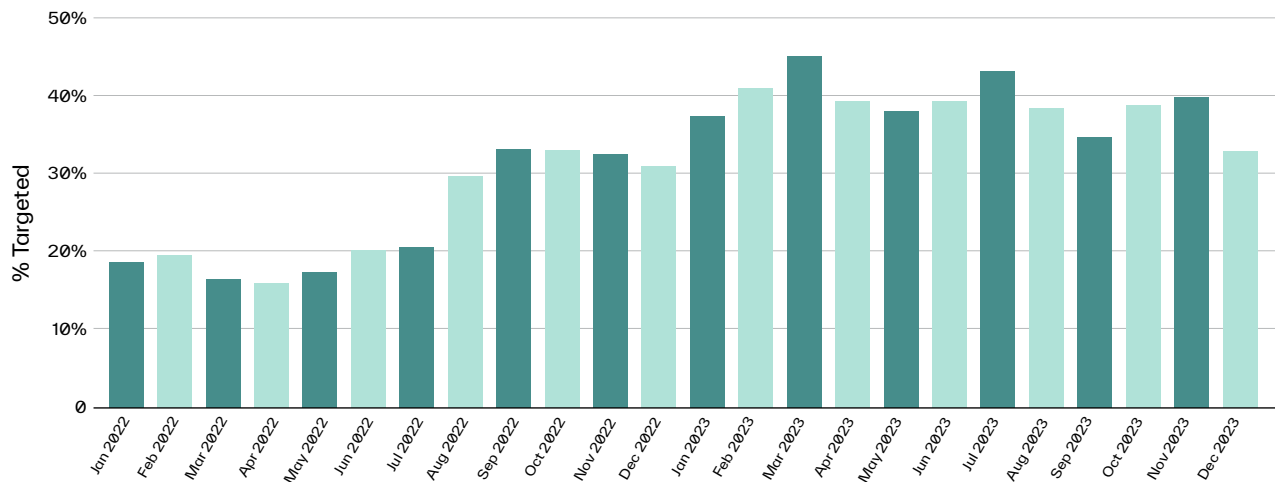
A subset of BEC, vendor email compromise (VEC) involves the impersonation of legitimate vendors to deceive targets into making payments for fake invoices, initiating fraudulent wire transfers, or updating banking details for future transactions. In the most sophisticated VEC attacks, threat actors will send an email from a compromised vendor email account to add credibility. Given that vendor communications frequently revolve around payments, distinguishing these attacks from genuine emails can be extremely challenging.



Vendor Email Compromise Jumps 50% Year-over-Year

In 2022, a quarter of Abnormal customers were the target of at least one vendor email compromise attack each month. In 2023, this value increased by 50%, with nearly 40% of Abnormal customers experiencing a monthly VEC attack.

Percentage of Abnormal Customers Targeted by VEC Each Month



The vendor-customer dynamic has an inherent financial element built into it, and invoices, billing accounts, and upcoming payments are often discussed via email. Consequently, malicious emails seemingly from vendors requesting payment for overdue invoices or changes to bank account information may not be immediately flagged as suspicious.

Furthermore, even small businesses usually work with at least one vendor, and larger multinational enterprises often have contractual agreements with hundreds or even thousands of distributors and suppliers. Employees in larger organizations may also have limited visibility into the entire vendor ecosystem, especially when compared to their familiarity with the company's executive team.

Considering these factors, it becomes evident why threat actors increasingly choose to impersonate external third parties in their attacks.

The percentage of organizations targeted by VEC each month in 2023 never dropped below 32%.



Attackers Target Construction and Retail Industries for VEC

Attackers clearly had their preferred targets for VEC in the second half of 2023. Organizations in the construction and engineering industry topped the list, with 76% of Abnormal customers in this vertical receiving at least one vendor email compromise attack. Not far behind were retailers and consumer goods manufacturers, 66% of which were targeted by VEC during July–December 2023.

Industry	Percentage of Abnormal Customers Targeted by VEC
Construction/Engineering	76.00%
Retail/Consumer Goods & Manufacturing	66.14%
Automotive	61.29%
Energy/Infrastructure	58.97%
Transportation	58.14%

Modern construction projects rely on a network of numerous digital systems dispersed across multiple job sites and offices—creating an expansive attack surface. The seamless coordination of major projects also involves a continuous exchange of confidential and proprietary information, including financial data, among a wide network of vendors, contractors, and subcontractors. This provides ample opportunities for threat actors to hijack conversations.

Retailers and consumer goods manufacturers often have complex and interconnected supply chains, and every vendor email account represents an entry point for an attacker to infiltrate. Additionally, operating these organizations typically involves a high volume of email communication that can create opportunities for attackers to blend in with legitimate communication.

Unfortunately, regardless of your industry, your organization is always at risk of experiencing a vendor email compromise attack. It's only a matter of time before threat actors identify the best person to impersonate and the target they can most easily deceive.



Defending Against New and Emerging Threats

The emergence of malicious QR codes in phishing emails underscores one of the unfortunate truths of cybersecurity: if threat actors can determine how to exploit something fundamentally harmless for malicious purposes, they will. Time and time again, cybercriminals have demonstrated their impressive ability to identify new ways to leverage everyday communication tools as mechanisms for deceiving employees into disclosing private information and completing fraudulent requests.

History has shown that threat actors are versatile and adaptable, continually responding to increased awareness and improvements in email security with novel attack strategies. The proliferation of generative AI tools has now made it even easier for cybercriminals to craft sophisticated phishing, business email compromise, and vendor email compromise attacks that bypass traditional security solutions and trick end users.

With each new development in the attack landscape, it becomes increasingly evident that legacy systems like secure email gateways (SEGs) are ill-equipped to defend against the evolving tactics of cybercriminals. Organizations must recognize the limitations of SEGs and invest in modern solutions that use AI-native detection engines to stop new and emerging threats like QR code phishing.

AI-native security platforms are not only able to detect QR codes in emails and parse the associated link but also utilize behavioral signals to spot anomalies in email patterns that indicate a potential attack. This allows the solution to block sophisticated threats before they reach employee inboxes. By leveraging advanced behavioral science and risk-adaptive detection, organizations can enhance their security posture and stay one step ahead of an ever-expanding array of threats.



Abnormal

Abnormal Security provides the leading behavioral AI-based email 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 and messages—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, with additional protection available for Slack, Teams, and Zoom.

More information is available at abnormalsecurity.com.

**Interested in Seeing How Abnormal
Can Help You Protect More, Spend Less,
and Secure the Future?**

See Your ROI →

Request a Demo →