FORTRA™

2023 BEC Trends, Targets, and Changes in Techniques

Table of Contents

The volume of nefarious emails impersonating enterprises has reached a crescendo in 2023, with threats such as BEC making up nearly 99% of reported threats. Cybercriminal preference of email impersonation is by design, as social engineering continues to prove effective at deceiving both end users and the security tools designed to protect them.

While the fundamentals of BEC attacks have largely remained the same, criminals continue to optimize tactics to increase their success rate. Third party targeting, AI, and phishing-as-a-service (PhaaS) has enhanced what was already working, putting the pressure on security teams to identify and mitigate text-based threats before employees fall victim.

Detection of BEC is increasingly nuanced despite the lack of technical exploitation within a message, with even the most effective gateways often failing to flag attacks. And because BEC campaigns do not require the technical savvy needed to execute payload-based attacks, even the most inexperienced criminals can launch highly-convincing campaigns.

In this report, we use data from Fortra's Agari and PhishLabs solutions to examine current attack techniques and infrastructure used in BEC and other email impersonation threats. For purposes of this report, email impersonation attacks are defined as messages that rely solely on social engineering as their means of success and do not deliver malicious code via attachment or URL.

Key Findings:

Threats in Corporate Inboxes Hit New Highs
A quarter of all reported emails are classified as Malicious or Untrustworthy

Email Impersonation Threats are by far the Most Difficult to Block
99% of threats observed in corporate inboxes are response-based or credential theft attacks.

BEC Actors Move Towards Intercepting Payments
Instead of requesting an explicit amount, attackers ask for an unspecified sum owed.

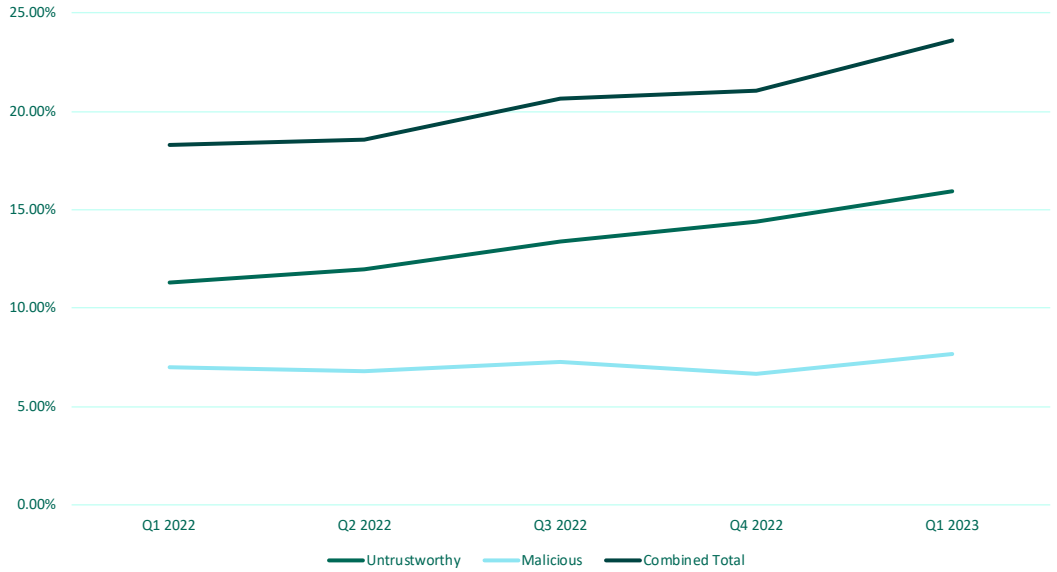
Office 365 Phish Trending Up
Phishing attack volume targeting O365 credentials doubles in Q1

Hybrid Vishing Outpaces BEC and 419 Scams
Hybrid Vishing attacks make up more than 45% of response-driven attack volume

"Malicious emails are messages that use language, links, or attachments to intentionally cause harm."

Untrustworthy Email Volume Continues to Grow

User Reported Malicious and Untrustworthy Email Volume



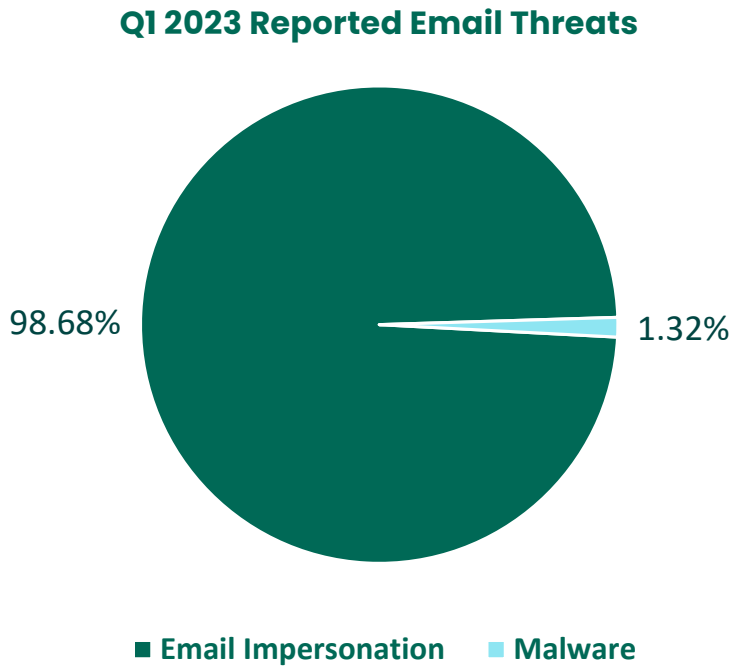
In Q1 2023, the percentage of emails classified as malicious or untrustworthy reached nearly a quarter of all messages reported by corporate users. This is the highest combined percentage since Fortra began reporting this data.

Looking at each category separately, malicious emails represented 7.7% of volume in Q1. This is the greatest percentage of share of reported emails since 2021. Messages considered untrustworthy also reached their highest share since tracking this category, making up nearly 16% of total share. Untrustworthy emails are suspicious messages that require interaction with the sender to verify malicious intent, and therefore should not be engaged with by users.

Just over 76% of reported emails contained no threat to recipients.

> ***"Untrustworthy emails are suspicious messages that require interaction with the sender to verify malicious intent, and therefore should not be engaged with by users."***

Email Impersonation Threats Found in Corporate Inboxes



In Q1 2023, the number of malicious emails classified as impersonation attacks climbed to nearly 99% of total reported volume. While email impersonation attacks have historically been the majority of threats reported in user inboxes, this is the largest percentage we've observed since we began tracking this data point. The most common types of email impersonation include BEC, credential theft, and hybrid vishing.

Malware reports declined for the third consecutive quarter, representing only 1.32%.

Email Sender Spoofing Classifications and Volume

Most threat actors modify the display name or sending domain in an email impersonation attack to enhance the perceived legitimacy of their message. The most four most common imposter types are the following:

Compromised Account - The legitimate individual's account has been compromised through phishing or password reuse and is used to impersonate that individual.

Brand Display Name Imposter - The email address is irrelevant. The attacker is relying on the fact that most mail clients only display the name portion of the From: header to impersonate a well-known brand.

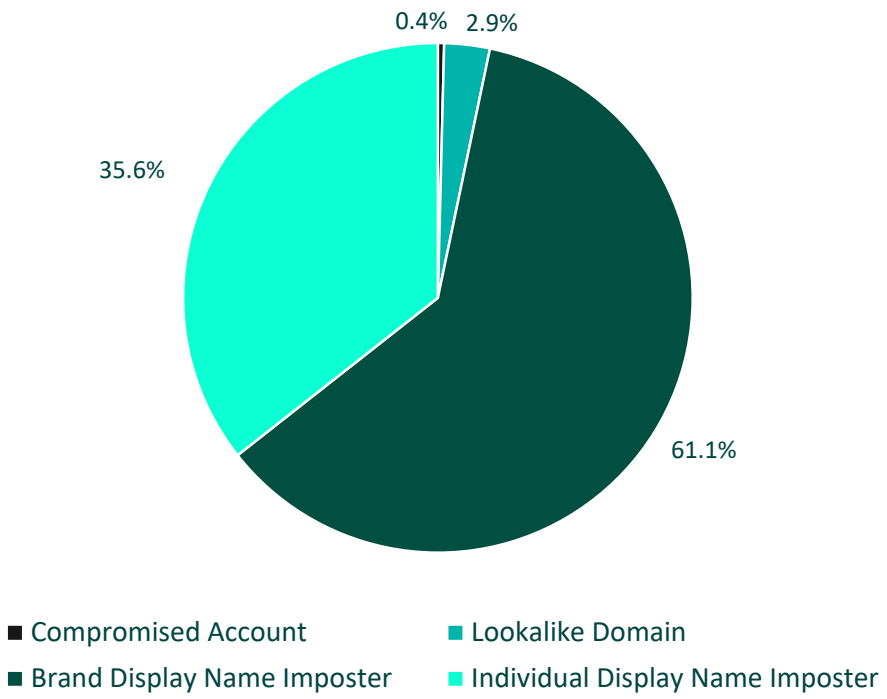
Lookalike Domain - The attacker uses an email domain that is similar to the actual domain of the organization they are trying to impersonate.

Individual Display Name Imposter - The email address is irrelevant. The attacker is relying on the fact that most mail clients only display the name portion of the From: header to impersonate an individual.

When looking at email impersonation attacks over the course of a two-week period, more than 60% of emails impersonated a well-known brand in the display name. This includes trusted and commonly used brands such as Microsoft and Google.

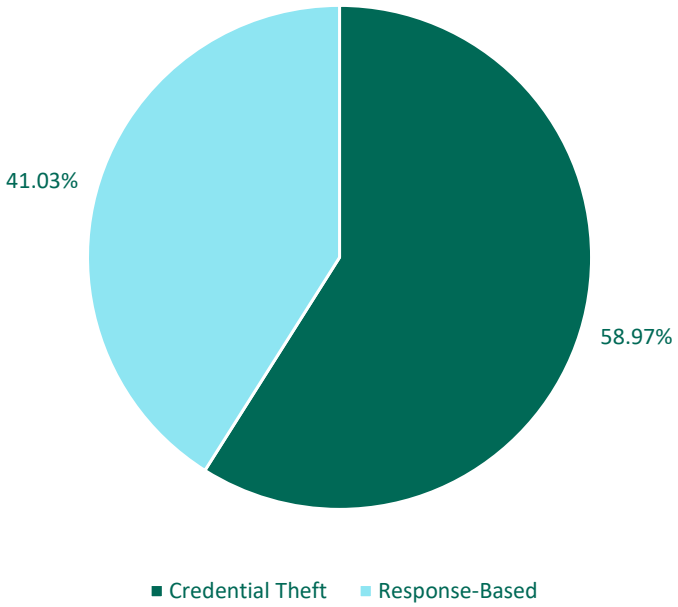
Nearly 36% of email display names are altered to a more granular level and pose as specific individuals. These messages are tailored to inspire urgency in addition to the false sense of legitimacy associated with the sender, most often impersonating a high-ranking officer within the company or a 3rd party vendor.

Email Impersonation Attacks by Imposter Type



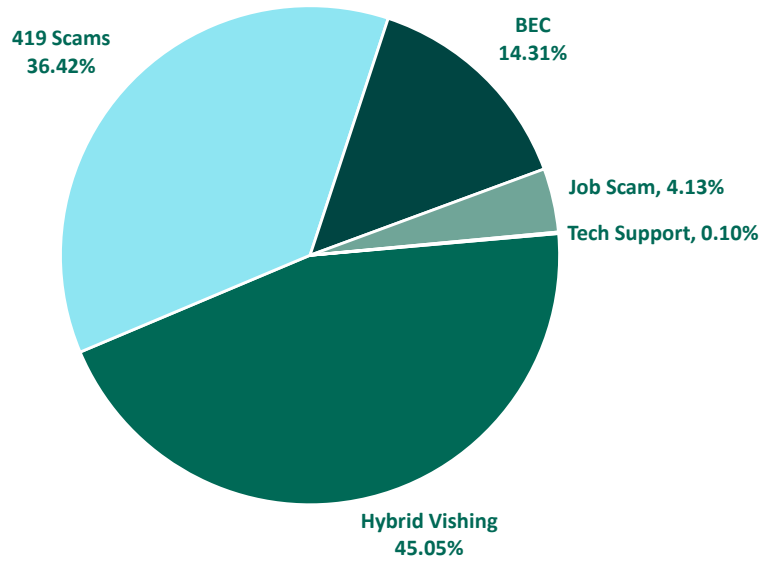
Types of Email Impersonation

Email Impersonation Threat Types



Q1 Volume

Response-Based Attack Volume



Q1 Volume

Email impersonation is fractioned into two categories: Credential Theft and Response-Based. Credential Theft emails redirect victims to malicious websites by way of phishing links or attachments. Response-Based attacks require the victim to communicate directly with the sender via additional messages or phone. In Q1, Response-Based represented the majority of email impersonation attacks.

The Response-Based category is comprised of five different threat types. In this report, we have isolated our analysis to Response-Based threats BEC and Hybrid Vishing, in addition to Credential Theft.

Business Email Compromise

The greatest losses from email impersonation are associated with BEC. Historically, these attacks impersonate an organization's CEO or high-level executive to trick recipients into initiating large financial transactions. Increasingly however, threat actors are expanding their target list to include vendors associated with the intended victim. By compromising a third party or business partner, the victim organization is prone to highly realistic emails that often contain key insider information, significantly enhancing the legitimacy of an attack.

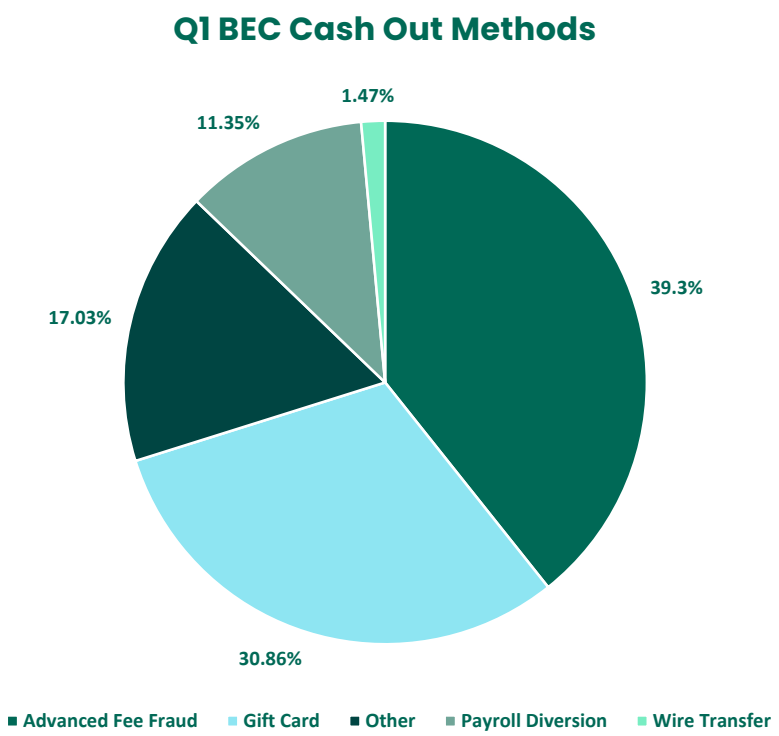
Generative AI is also trending among cybercriminals. Large language models such as ChatGPT give criminals the tools to craft well-written messages at scale and avoid the poor spelling and grammar that frequently mark phishing attacks.

Despite criminal innovation into BEC tactics, secure email gateways (SEGs) continue to advance in the identification of this threat-type. BEC was reported less in Q1 2023 when compared to other impersonation attacks such as hybrid vishing.

As a whole, BEC attack volume has remained steady over the past year, representing more than 14% of share of Response-Based volume in Q1. This is a 2% increase over the same time last year.

When looking at a snapshot of BEC activity in Q1, the most common cash out method was Advanced Fee Fraud, making up nearly 40%. Gift Cards followed close behind, used by criminals 30.86% of the time.

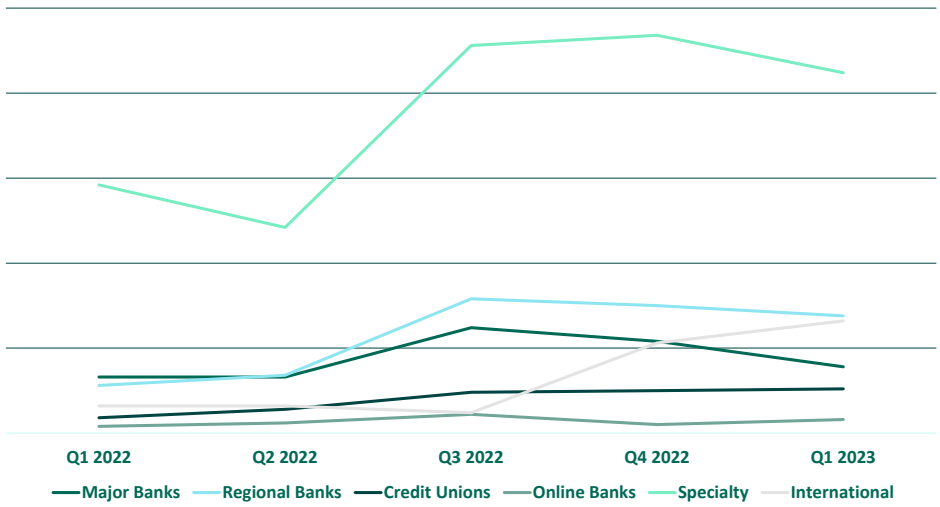
While wire transfers made up only 4% of the preferred cash out methods, there was a significant shift in tactics in Q1. Instead of asking for a specific payment, BEC actors have begun asking the victim to provide "the outstanding balance" or "owed amount." This technique attempts to redirect payment of an unpaid invoice that has already been fully or partially approved by the appropriate internal stakeholders. Businesses often require new invoices or purchase orders go through multi-step approval process prior to payment being scheduled. But once an invoice has been approved and scheduled for payment, changes outside of the payment amount may have a less robust approval process (if any at all). BEC actors can exploit this by impersonating an established vendor that is likely to have at least one invoice already approved and awaiting payment.



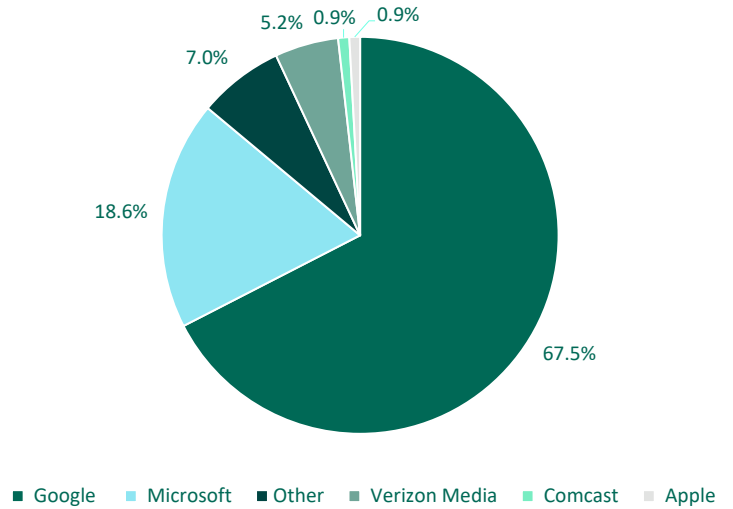
Specialty accounts such as prepaid debit cards are consistently the top means of transferring funds, with 61% of cybercriminals choosing this method in March. Regional Banks were used 13% of the time, with National Banks and International Banks tying for third.

The majority of BEC attacks are sent from email addresses hosted on free webmail providers. In Q1 2023, Google led all other providers, so far accounting for 67.5% of total free webmail volume. Microsoft is the second most abused, contributing to 18.6% of BEC campaigns. Verizon, Comcast, and Apple rounded out the top five.

Type of Financial Institution used in Payroll Diversion



Free Webmail Providers used in BEC Attacks



Q1 Free Webmail Providers

Hybrid Vishing

Hybrid vishing attacks have shown significant growth, with share of reported volume nearly doubling over the course of 2022. In Q1 2023 hybrid vishing was the top reported Response-Based threat type with 45% of total volume, despite declining 6% of share. This is the second consecutive quarter hybrid vishing has surpassed all other threat types within this category.

Hybrid vishing attacks use phone numbers and the stolen intellectual property of trusted brands to evade gateways and convince users of their legitimacy. These messages take on the appearance of unexpected invoices or bills for products with a telephone number as the point of contact. The most commonly impersonated brands in these attacks are online payment services such as Paypal and digital security software such as Norton or McAfee products.

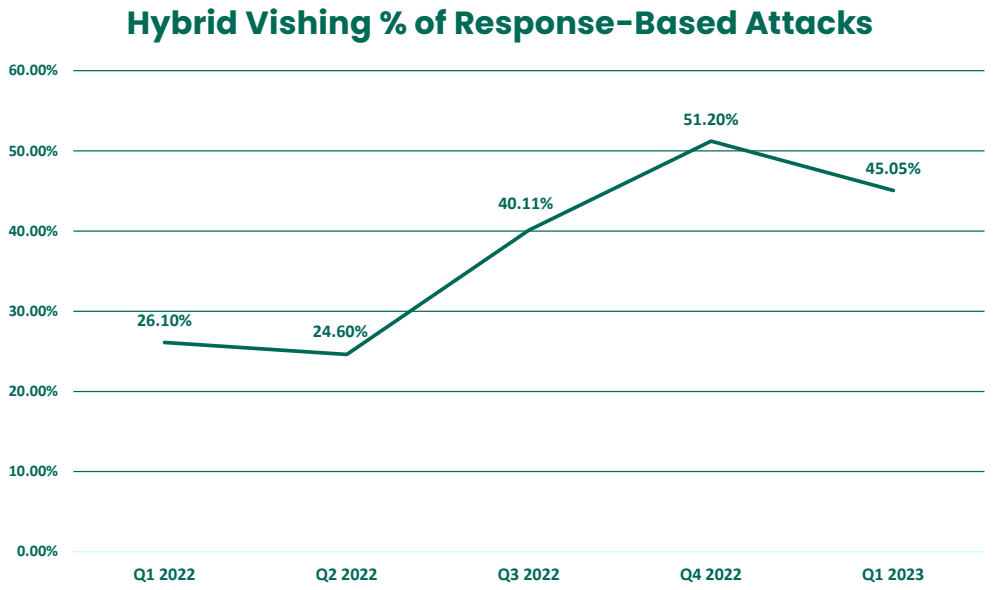
If the victim calls the phone number within the message, there are several ways criminals will attempt to monetize the attack:

ID Theft: The criminal confirms that they will cancel the fake charge, provided the victim verify personal details such as their SSN, home address, mother's maiden name, and more.

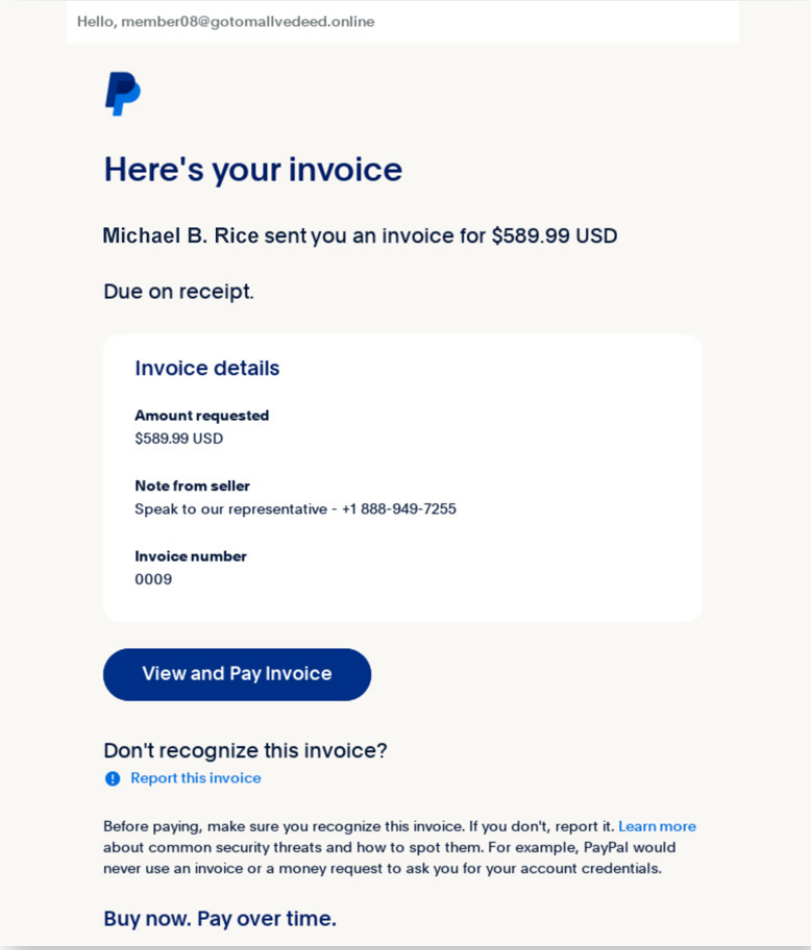
Credit Card Fraud: The victim is asked to disclose their credit card number, expiration date, CVV code, and home address in order to receive a refund.

Malware Implant: The criminal requests access to the victim's computer to remove fake software and prevent future charges.

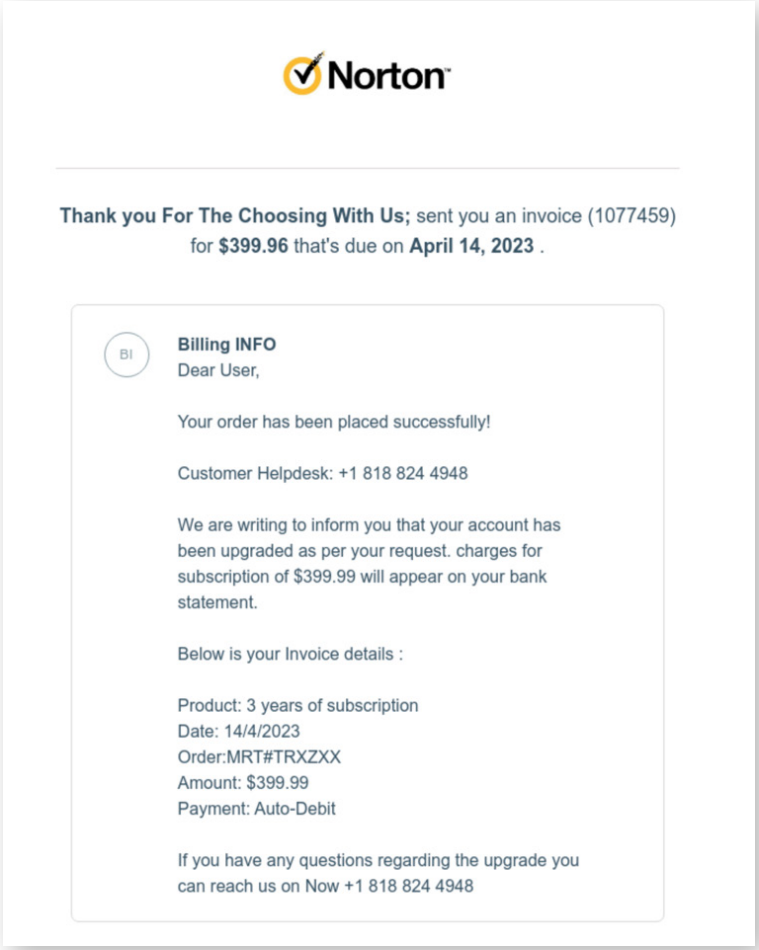
> ***"Hybrid vishing attacks nearly double in share during 2022"***



Below are common examples of hybrid vishing attacks reported through PhishLabs' Suspicious Email Analysis.



Hybrid vishing attack impersonating Paypal



Hybrid vishing attack impersonating Norton

Credential Theft

Credential Theft attacks are back on the rise after declining the second half of 2022. In Q1, Credential Theft led all email impersonation threat types. Driving the increase were Microsoft O365 phish, which experienced the largest quarter-over-quarter jump in share since we began reporting the datapoint. Phishing emails impersonating Microsoft products grew 10% in share over Q4 and made up nearly 41% of all Credential Theft phish.

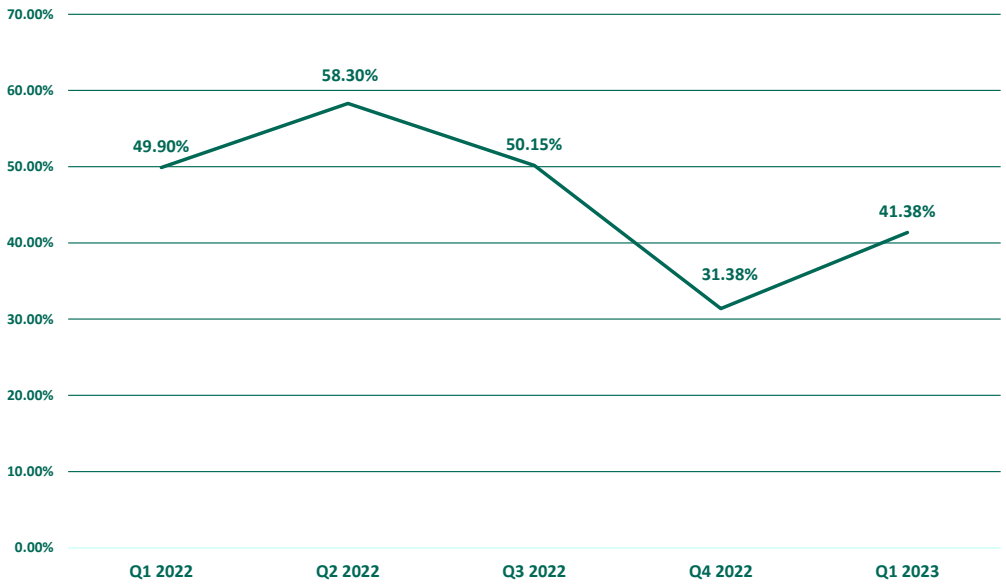
The Microsoft suite of products has long been a favorite target of cybercriminals due to its ubiquity among organizations. The average windows user has a conditioned trust of the Microsoft brand, using email, Sharepoint, Onedrive and more to perform a variety of business functions. Microsoft notifications are common and expected, aiding in the criminal's need to dampen suspicions.

Stolen Microsoft credentials are especially damaging to organizations and can equate to an open door to the enterprise. Everything the user has access to, including partner communications and single sign on (SSO), is open to exploitation.

The potential impact that Microsoft credentials carry with them makes O365 phish especially desirable options for attackers. Phishing-as-a-service (PhaaS) operations sell kits tailored to actors keen on launching O365 campaigns, helping with targeting, page customization, and published lures. PhaaS operations are increasingly improving resources and offering competitive pricing, allowing criminals with little money or expertise to launch attacks.

> ***"O365 attacks jump 10% quarter over quarter"***

O365 % of Credential Theft Attacks



Conclusion

Social engineering has opened the door to some of the most effective and undetectable threats organizations face. As security teams prioritize measures to protect their people and assets, understanding how to identify a threat that relies solely on impersonation will be the greatest challenge.

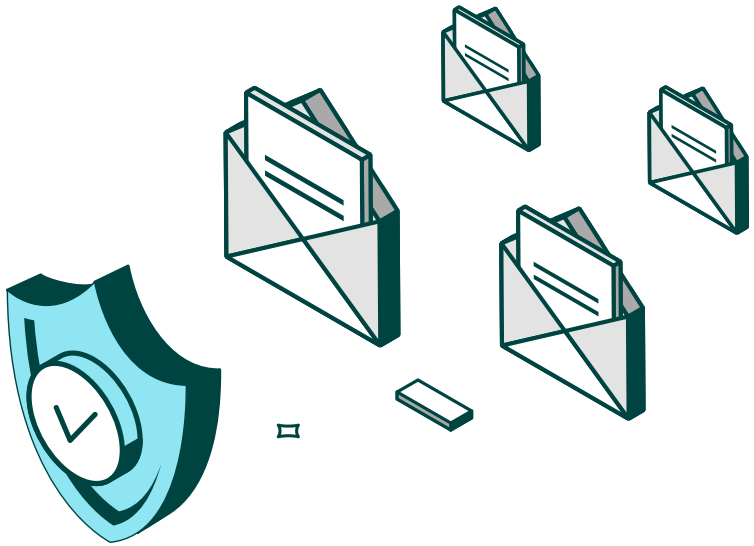
In 2023, email impersonation represents nearly all malicious activity reported in employee inboxes. The greatest losses associated with an email impersonation attack are tied to BEC, with roughly 14% of all threats reported as this threat type.

Cybercriminals most often choose advanced fee fraud and gift cards as their cash out methods in BEC attacks, with specialty accounts such as debit cards the most used for payroll diversion. Regional banks are the second most used. Of the BEC email address hosted on free webmail accounts, Google represents nearly 70% of volume.

Office 365 phish remain a significant threat to organizations. O365 volume is trending up so far in 2023, with incident counts doubling in Q1. Widely available kits and tools make it simple for actors to launch this type of attack, and security teams should prioritize the detection of O365 threats as well as the resources used to build their infrastructures.

Hybrid vishing attacks experienced a slight dip in volume this year, yet remain one of the top threat types to organizations. Hybrid vishing can be monetized in multiple ways, including stolen PII, card credentials, and more. A vishing attack can also result in malware delivery.

Impersonation attacks are forcing organizations to rethink how to defend against threats that consistently get past traditional email security controls. The two key recommendations to combat these threats are emphasizing current impersonation techniques in Security Awareness Training and implementing additional email security layers that are optimized to detect and respond to advanced email threats. Applying algorithms through machine learning that assist in the detection of anomalies and patterns will be increasingly necessary to thoroughly and accurately inspect email. By building models that can recognize patterns and make predictions, organizations will be able to accurately detect these signatureless threats at scale.



FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

ag-gd-0623-db