Abnormal

RESEARCH REPORT

5 Emerging Email Attacks to Watch For in 2024

Executive Summary

The cybersecurity landscape is poised for significant evolution in 2024, marked by the emergence of new and refined threat vectors, as well as an increase in the tried and true attacks of the past.

76%

of all advanced email threats aim to steal credentials.

Abnormal Data, 2023

$43 billion

in exposed losses due to business email compromise since 2016.

FBI Internet Crime Complaint Center, 2023

17%

of all attacks in the last quarter of 2023 included a QR code.

Abnormal Data, 2023

97.3%

of organizations expect AI to be moderately or extremely important to their email defenses in the next year.

Osterman Research: The Role of AI in Email Security

Attackers have spent years honing their techniques, making social engineering tactics more nuanced and personalized. These advanced attacks are already adept at exploiting human vulnerabilities, often leveraging trust and familiarity to deceive recipients and make it challenging for conventional security measures and humans alike to discern malicious intent. But the rise of new technologies, and especially generative AI, makes the attacks coming in 2024 more dangerous than those of the past.

For example, the usage of QR codes for various legitimate purposes such as making payments, accessing websites, or joining Wi-Fi networks has grown significantly. As the public became more familiar with them, attackers saw how to exploit them—using similar themes to encourage their targets to provide credentials, money, or sensitive information.

But not every new attack is truly brand new... sometimes all it takes is a new variation.This is especially true of business email compromise (BEC) and its sub-categories, as attackers continue to move away from the CEO fraud of the past and lean more into vendor compromise and impersonation to trick victims. In the coming year, we expect this vendor fraud to increase as more threat actors leverage partner relationships to increase the success rate of their attacks.

While we do not have a crystal ball and cannot predict the future with complete accuracy, we are confident about one thing: email attacks are more sophisticated than ever before, and they will continue to evolve in 2024. To help prepare organizations against them, we've gathered five specific attack types that we expect to increase in the coming year. These real-world email attacks, sent to Abnormal customers in 2023, illustrate how attackers are constantly changing their tactics and showcase why security leaders must take the necessary steps today to safeguard their email infrastructure from these continuously-evolving threats.

© 2023 Abnormal Security Corporation. All rights reserved.

Table of Contents

© 2023 Abnormal Security Corporation. All rights reserved.

The Ever-Evolving Email Threat Landscape

Email remains a prevalent attack vector due to its ubiquitous nature and widespread adoption for both personal and professional communication. And despite advancements in cybersecurity, malicious actors consistently exploit vulnerabilities in email systems, leveraging a variety of techniques to compromise sensitive information and steal money.

The email threat landscape has continued to evolve and grow year over year. One of the primary reasons behind the persistent growth of email threats is the sheer volume of emails exchanged daily. With billions of emails sent globally, attackers have a vast pool of potential targets. Further, the integration of email platforms with other technologies and services has created more entry points for exploitation, amplifying the attack surface for cybercriminals.

The continuous success of email attacks can also be attributed both to the lack of safeguards within email itself and to the reliance on humans to discern when an email may be malicious. Unfortunately, despite increases in security tool spend and security awareness training efforts, attackers have learned how to bypass security platforms and users still fall victim to well-crafted, socially-engineered emails.

As we look ahead to 2024, several factors suggest that email attacks will continue to grow in **both** volume and sophistication. Business email compromise alone is the cause of one-fourth of all cybercrime losses for the past three years, and the number of attacks seen daily is only continuing to increase. Add generative AI into the mix, and cybercriminals have the perfect arsenal from which they can launch millions of attacks each day—at least some of which are bound to succeed.

To combat these ever-advancing threats, organizations will need to adopt a modern cybersecurity solution that utilizes the power of AI to baseline known behavior and detect anomalous activity. As attackers learn new tactics and stop relying on traditional attacks, security leaders must stay one step ahead to keep their email (and their employees) protected. Utilizing defensive AI is the only way forward to ensure that attacks are detected before they reach inboxes and that employees stay safe from the latest socially-engineered threat.

© 2023 Abnormal Security Corporation. All rights reserved.

5 Email Attacks to Prevent in 2024

Last year, Abnormal detected and blocked millions of advanced email threats across the full spectrum of attacks—from generic scams to highly-targeted vendor fraud threats. In doing so, we've uncovered how attackers are shifting their attention and what new threats may be on the horizon.

The following threats are real-world examples sent to Abnormal customers in 2023. They showcase our predictions of how the threat landscape will evolve in the coming year and provide insight into what types of attacks organizations must be prepared to detect and defend against in 2024.

© 2023 Abnormal Security Corporation. All rights reserved.

01 Internal Systems Impersonation

33 million

email credentials were stolen in 2021 alone, and this number continues to increase year-over-year.

Verizon 2023 Data Breach Investigation Report

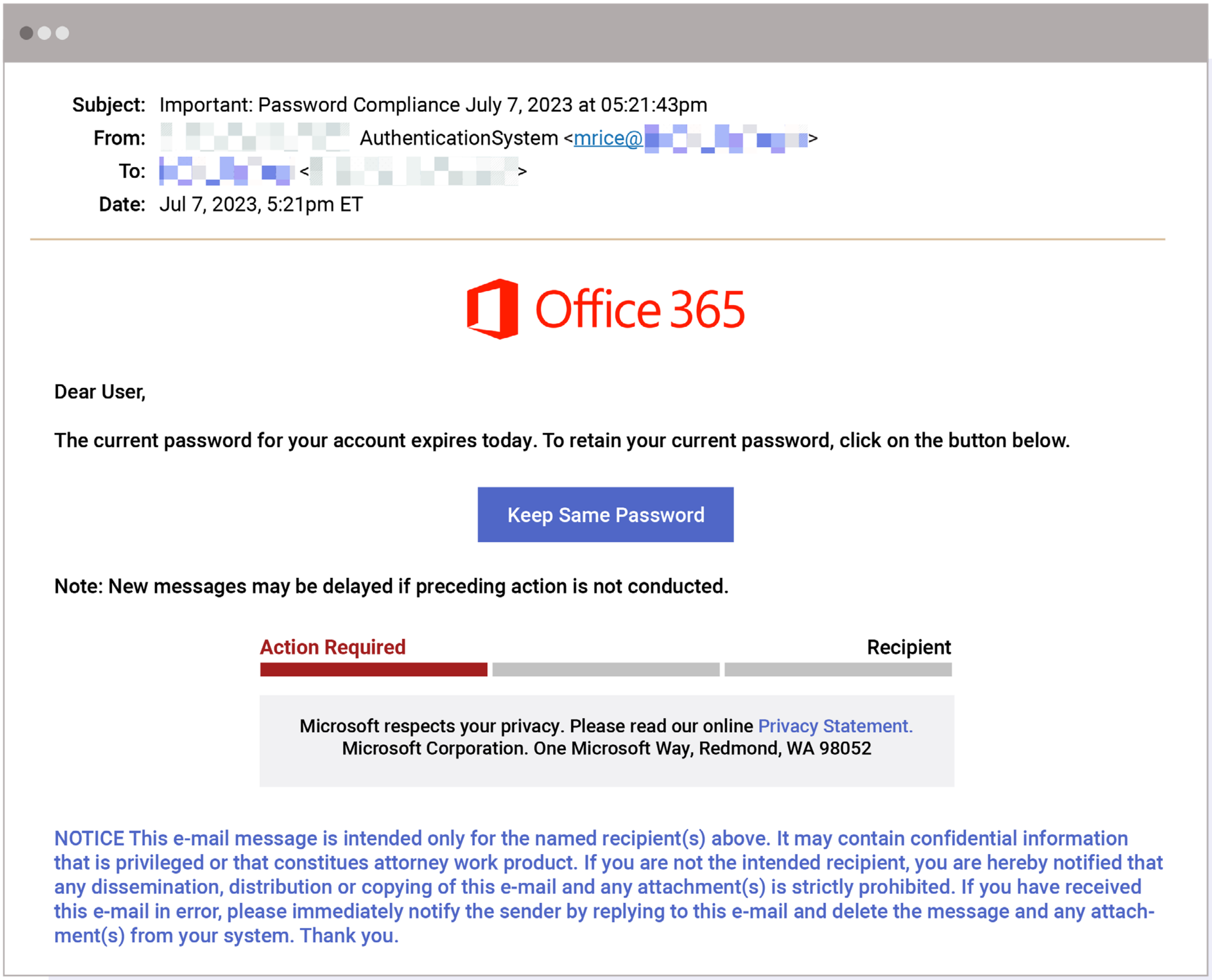
Though credential phishing attacks are nothing new, they are becoming increasingly sophisticated and appear more like legitimate emails than ever before. In fact, credential phishing is the number one email attack by volume, responsible for 76% of all advanced attacks received by Abnormal customers.

In these attacks, threat actors use seemingly trusted identities to trick employees into clicking on phishing links. The subsequent fraudulent phishing sites are often crafted to look identical to real sign-in pages, making it nearly impossible for employees to discern a malicious page from a real one. **But while brand impersonation has long been a threat actor favorite, we anticipate a continued rise in the impersonation of internal systems in an effort to phish credentials.** By impersonating an internal entity, typically the IT department, the threat actor can convince the recipient to click the link and enter their credentials.

The sophistication of this is illustrated by the following real-world attack in which a threat actor impersonates an internal IT system and asks the recipient to change their login credentials for Microsoft Office 365. The email comes from the domain of the company impersonated, and the display name includes “Company AuthenticationSystem,” which improves the likelihood that the message could be mistaken for official communication.

The email itself includes what appears to be the Office 365 logo and a corresponding password change notice, but is actually a single PNG image that links out to a malicious landing page. By replacing the content of the email with an image, the attack can bypass legacy security tools that cannot discern malicious images from legitimate ones. And despite the fact that this email comes from an internal IT administrator, the Microsoft branding is included to bolster the credibility of the message. In addition, the attacker includes an official-sounding confidentiality notice at the bottom of the email—a common practice among many large organizations that deal with proprietary information.

© 2023 Abnormal Security Corporation. All rights reserved.



Subject: Important: Password Compliance July 7, 2023 at 05:21:43pm
From: [redacted] AuthenticationSystem <mrice@[redacted]>
To: [redacted] <[redacted]>
Date: Jul 7, 2023, 5:21pm ET

Dear User,

The current password for your account expires today. To retain your current password, click on the button below.

Note: New messages may be delayed if preceding action is not conducted.

Microsoft respects your privacy. Please read our online Privacy Statement.
Microsoft Corporation. One Microsoft Way, Redmond, WA 98052

NOTICE This e-mail message is intended only for the named recipient(s) above. It may contain confidential information that is privileged or that constitues attorney work product. If you are not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this e-mail and any attachment(s) is strictly prohibited. If you have received this e-mail in error, please immediately notify the sender by replying to this e-mail and delete the message and any attachment(s) from your system. Thank you.

Detecting Internal Impersonation Attacks

This particular credential phishing technique is effective and difficult to detect because it preys on the human tendency to trust established and reputable identities, and specifically their internal teams. Because the attack appears to come from a legitimate sender and includes a message that the recipient would expect IT to send, it makes it more difficult for a user to discern that it is in fact malicious.

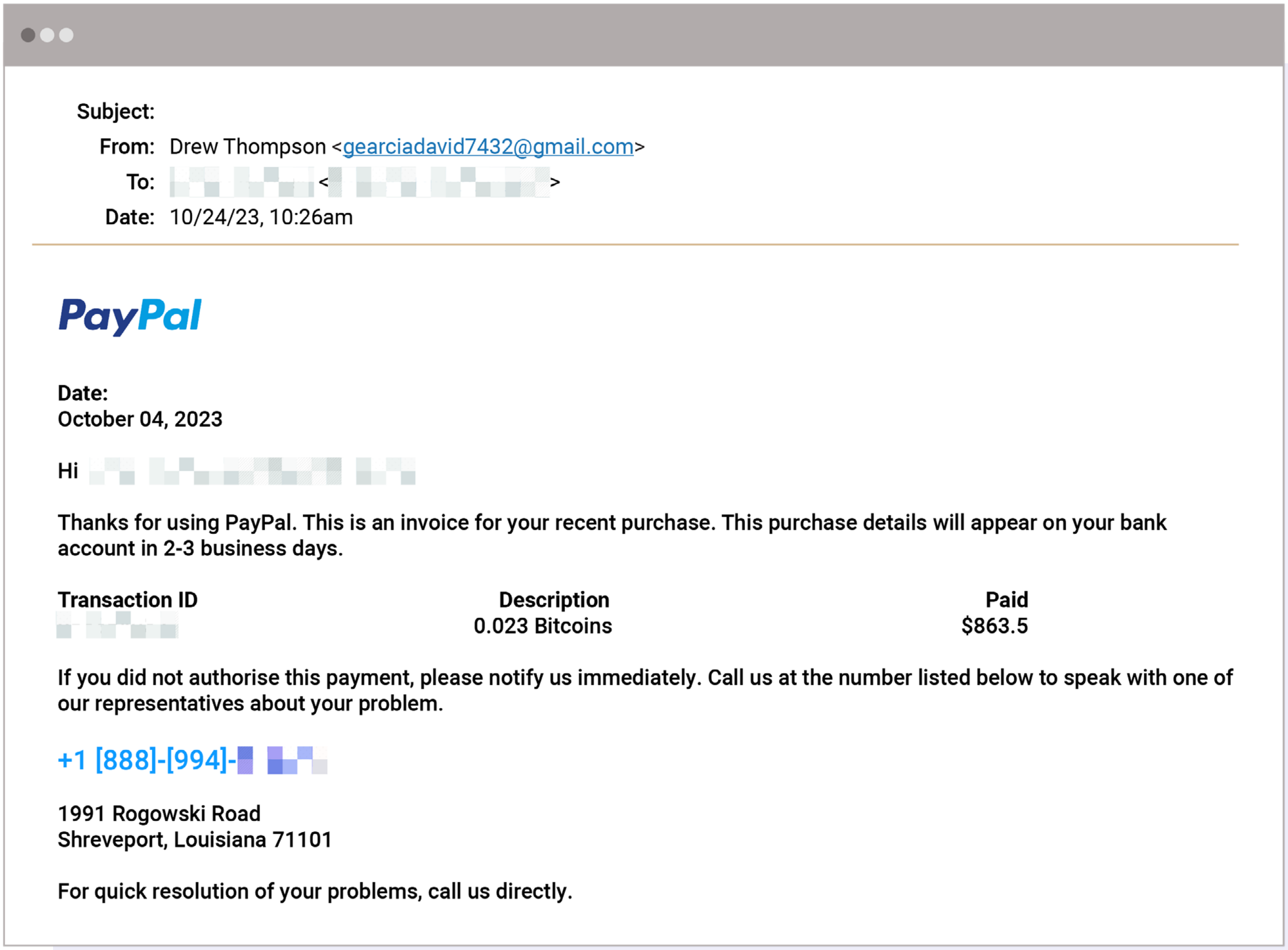
This attack was flagged by Abnormal due to the malicious link included and the discrepancy between the display name of "[Company Name] AuthenticationSystem" and the personalized sender email of "mrice@ companydomain.com. Abnormal also noted that the sender had never before sent mail to this recipient, and flagged that the image impersonated Microsoft—a common theme in credential phishing attacks.

02

Payloadless Malware

Payloadless malware attacks, also known as fileless or non-malware attacks, have emerged as a significant trend over the past year. Unlike traditional malware, payloadless attacks operate without the need for a malicious executable file, making them stealthier and harder to detect by traditional email security tools. In most of these attacks, the email itself contains no links or attachments, but instead provides a fake payment receipt or upcoming payment request and tells the recipient to call the number provided to reverse or stop the transaction. When they do so, the target receives a file to download, which contains the malware.

In this real-world attack, the email appears to be an invoice from PayPal for a recent cryptocurrency purchase. The email was sent from a Gmail account and includes transaction details such as the ID number and amount paid—$863.50 (0.023 Bitcoin).



Subject:
From: Drew Thompson <gearciadavid7432@gmail.com>
To: [redacted] <[redacted]>
Date: 10/24/23, 10:26am

PayPal

Date:
October 04, 2023

Hi [redacted]

Thanks for using PayPal. This is an invoice for your recent purchase. This purchase details will appear on your bank account in 2-3 business days.

Transaction ID	Description	Paid
[redacted]	0.023 Bitcoins	$863.5

If you did not authorise this payment, please notify us immediately. Call us at the number listed below to speak with one of our representatives about your problem.

+1 [888]-[994]-[redacted]

1991 Rogowski Road
Shreveport, Louisiana 71101

For quick resolution of your problems, call us directly.

© 2023 Abnormal Security Corporation. All rights reserved.

35%

of attackers disseminating malware deliver it almost exclusively through email.

Verizon Data Breach Investigation Report

The email goes on to state that if the recipient did not authorize the purchase, they should notify the sender immediately by calling a "representative" at the phone number provided.

If the user were to fall for this and call the helpline, the attacker could easily install malware, which then enables them to download malicious applications, open unsafe web pages, and steal information.

Detecting Payloadless Malware

By avoiding the use of easily recognizable malware signatures, payloadless attacks can circumvent traditional security solutions and allow threat actors to execute sophisticated and persistent campaigns.

This specific attack is difficult to identify because the email is text-based, without any other indicators of compromise. There is little for a secure email gateway to use to determine malicious intent. The email was sent from a Gmail account, a free webmail service available to anyone. As a result, there is no bad domain reputation for traditional security providers to discover, and the email passes all authentication checks for SPF, DKIM, and DMARC.

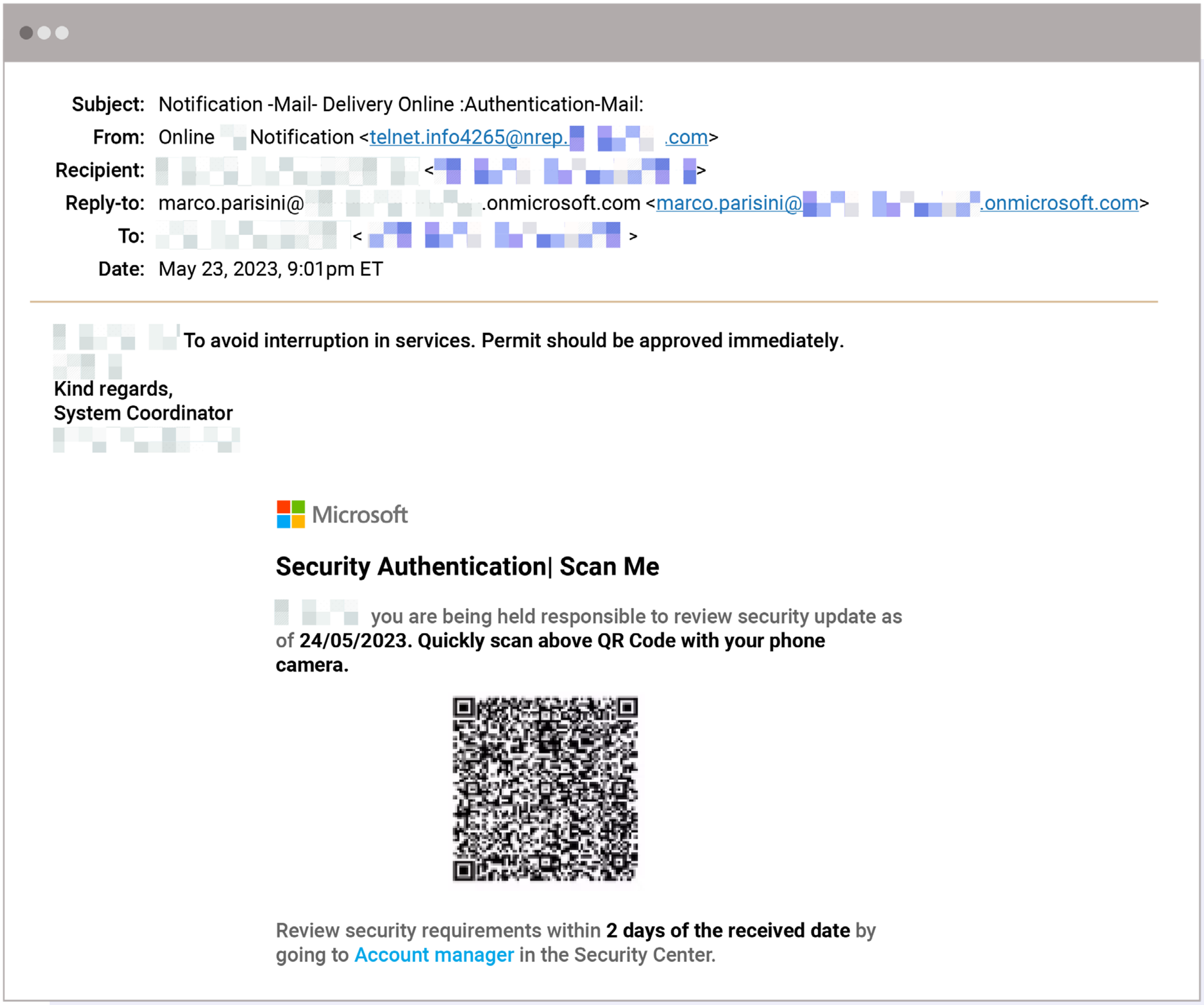
Abnormal detected this attack with behavioral AI and content analysis, which understand the tone of the email and the included phone number. Lookalike content is also helpful in analyzing how this attack relates to other phone-based text attacks, which have seen increased popularity in recent months due to their continued success.

03

QR Code Phishing (aka Quishing)

QR codes have become increasingly popular over the past few years, both for their convenience and contactless nature. While they are often used for beneficial purposes, from marketing campaigns to restaurant menus, QR codes have recently become a frequent tactic for malicious actors. In fact, Abnormal data shows that 17% of attacks that bypassed native spam filters in 2023 utilized QR codes, and this is expected to continue increasing in 2024.

The following attack illustrates how threat actors are exploiting QR codes to bypass traditional security methods. In this case, the attacker impersonates a systems administrator at the recipient's employer and informs them that a permit requires immediate approval in order to prevent service interruption.



Subject: Notification -Mail- Delivery Online :Authentication-Mail:
From: Online [redacted] Notification <telnet.info4265@nrep.[redacted].com>
Recipient: [redacted] <[redacted]>
Reply-to: marco.parisini@[redacted].onmicrosoft.com <marco.parisini@[redacted].onmicrosoft.com>
To: [redacted] < [redacted] >
Date: May 23, 2023, 9:01pm ET

[redacted] To avoid interruption in services. Permit should be approved immediately.
[redacted]
Kind regards,
System Coordinator
[redacted]

Microsoft

Security Authentication| Scan Me

[redacted] you are being held responsible to review security update as of **24/05/2023. Quickly scan above QR Code with your phone camera.**

Review security requirements within **2 days of the received date** by going to Account manager in the Security Center.

© 2023 Abnormal Security Corporation. All rights reserved.

80%

of malicious QR codes are used to execute credential phishing and invoice payment fraud attacks.

Abnormal Data, 2023

The short email includes Microsoft branding and a QR code, which leads to a malicious phishing website posing as a legitimate Microsoft login page. The landing page encourages the recipient to enter the login credentials for their Microsoft account, which the attacker could then use to compromise the email account and move laterally through connected Microsoft systems.

Detecting Quishing Attacks

Detecting QR code phishing attacks can be challenging due to the limited text content and heavy reliance on images. When paired with social engineering tactics like shown above, the lack of traditional indicators of compromise makes it difficult for legacy email security solutions to identify and extract malicious intent.

Threat actors are knowingly exploiting this vulnerability and continuing to find ways to increase the sophistication of their quishing attacks. In this particular case, the attacker spoofed a legitimate, four-year-old domain, and named it something similar to what a real administrator would use. To increase perceived authenticity, the attacker also utilizes a Microsoft feature that creates a backup domain as the reply-to address, ".onmicrosoft[.]com," which at first glance could be mistaken for a genuine communication from Microsoft.

In order to combat quishing attacks, Abnormal is continuing to make detection enhancements and can now follow the links enabled by QR codes. Here, Abnormal identified that the email was sent from an unusual sender and domain, neither of which the recipient had previously interacted with. Then, Abnormal parsed the QR code, which flagged the resulting link as malicious.

© 2023 Abnormal Security Corporation. All rights reserved.

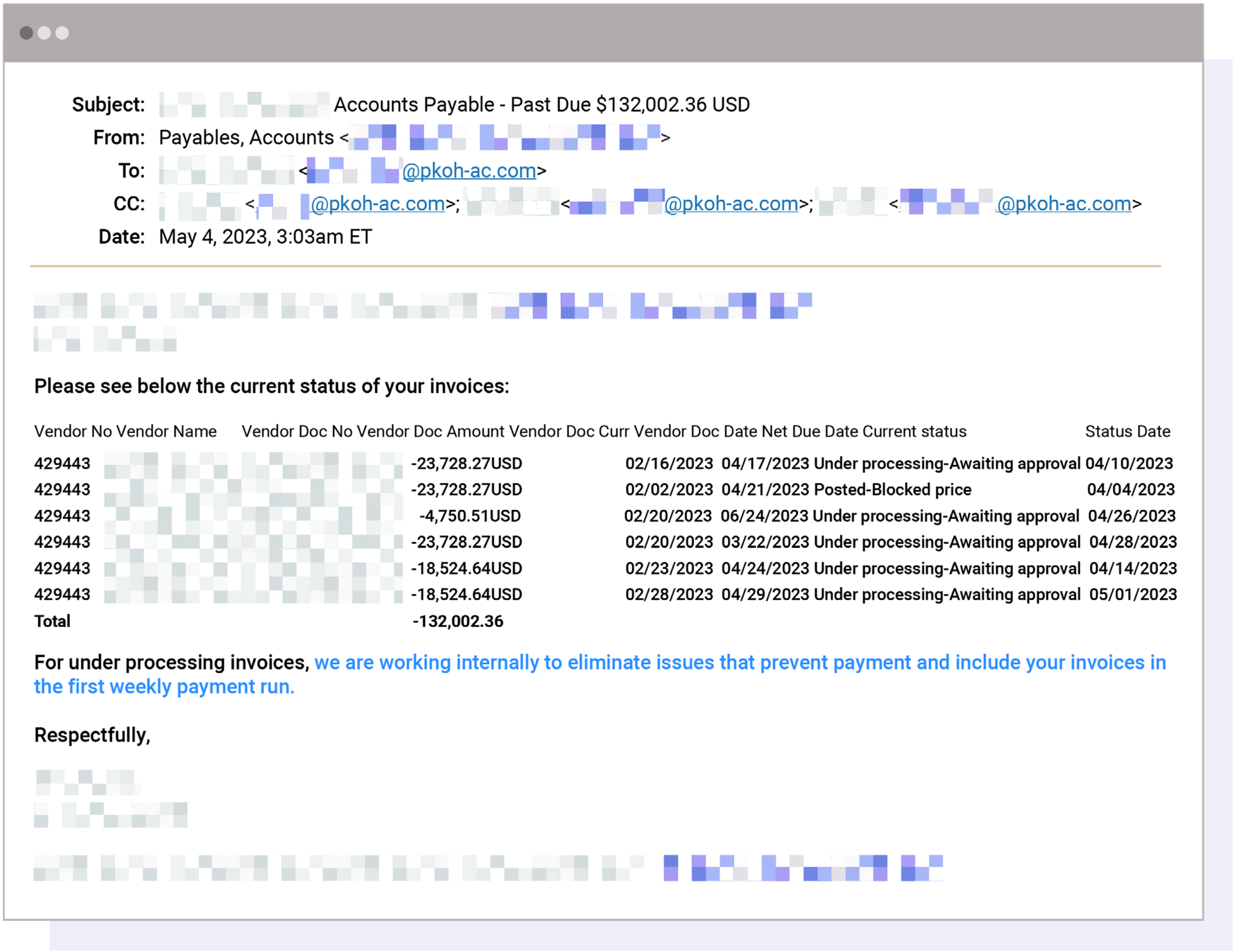
04

Vendor Email Compromise (VEC)

While not a new type of attack, vendor email compromise has picked up in frequency over the last year. According to Abnormal data, 48% of organizations received a VEC attack in the first half of 2023, which is notable as these attacks can only occur when a vendor account has been truly compromised.

Threat actors typically view small vendors as the easiest target and will often use real vendor accounts to target larger companies. For example, in order to get information or steal money from a large multinational corporation, they may simply compromise the account of the local janitorial service and use the control of that account to gain access to their larger target.

The following example illustrates the sophistication of these modern VEC attacks. This first legitimate email first outlines the current status of unpaid invoices and requests $132,000 from the recipient.



Subject: [redacted] Accounts Payable - Past Due $132,002.36 USD
From: Payables, Accounts <[redacted]>
To: [redacted] <[redacted]@pkoh-ac.com>
CC: [redacted] <[redacted]@pkoh-ac.com>; [redacted] <[redacted]@pkoh-ac.com>; [redacted] <[redacted]@pkoh-ac.com>
Date: May 4, 2023, 3:03am ET

[redacted]

Please see below the current status of your invoices:

Vendor No	Vendor Name	Vendor Doc No	Vendor Doc Amount	Vendor Doc Curr	Vendor Doc Date	Net Due Date	Current status	Status Date
429443	[redacted]	[redacted]	**-23,728.27USD**		**02/16/2023**	**04/17/2023**	**Under processing-Awaiting approval**	**04/10/2023**
429443	[redacted]	[redacted]	**-23,728.27USD**		**02/02/2023**	**04/21/2023**	**Posted-Blocked price**	**04/04/2023**
429443	[redacted]	[redacted]	**-4,750.51USD**		**02/20/2023**	**06/24/2023**	**Under processing-Awaiting approval**	**04/26/2023**
429443	[redacted]	[redacted]	**-23,728.27USD**		**02/20/2023**	**03/22/2023**	**Under processing-Awaiting approval**	**04/28/2023**
429443	[redacted]	[redacted]	**-18,524.64USD**		**02/23/2023**	**04/24/2023**	**Under processing-Awaiting approval**	**04/14/2023**
429443	[redacted]	[redacted]	**-18,524.64USD**		**02/28/2023**	**04/29/2023**	**Under processing-Awaiting approval**	**05/01/2023**
Total			**-132,002.36**					

For under processing invoices, we are working internally to eliminate issues that prevent payment and include your invoices in the first weekly payment run.

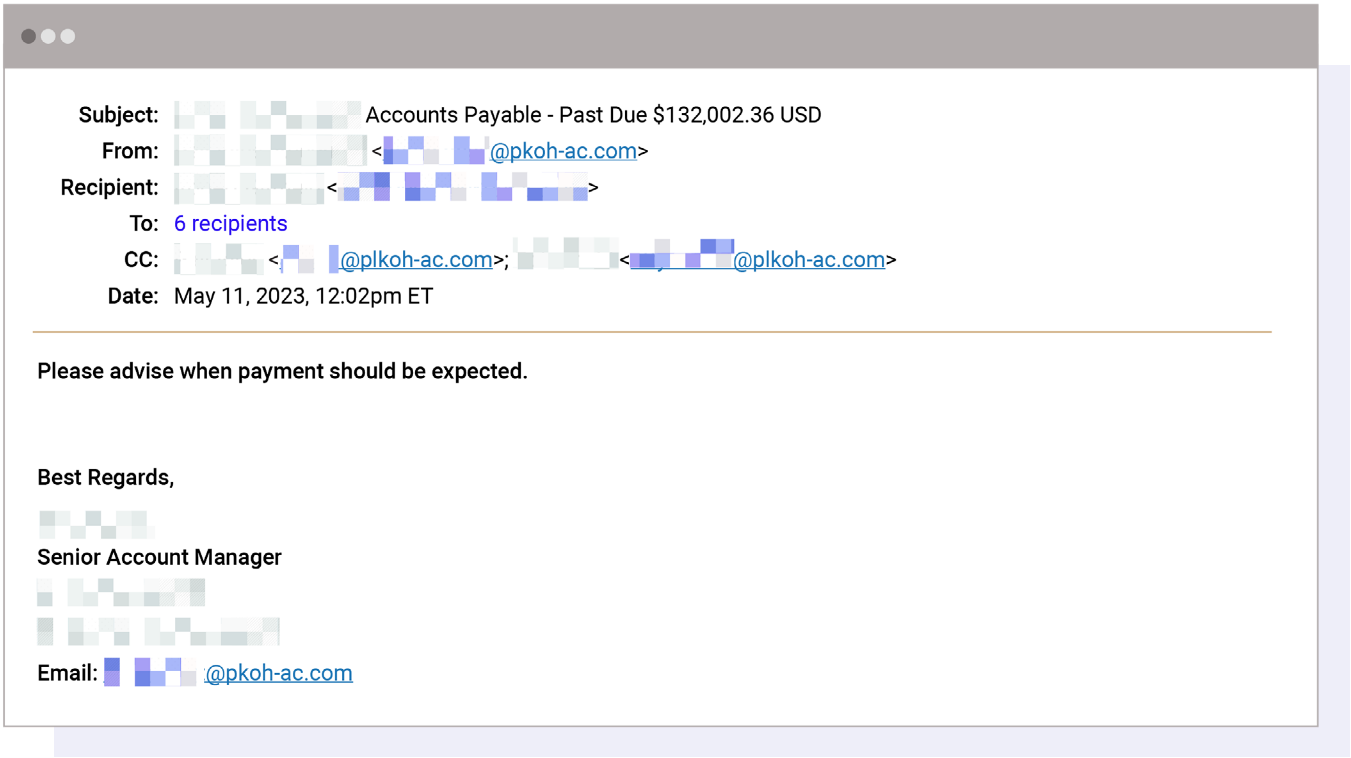
Respectfully,

[redacted]

[redacted]

© 2023 Abnormal Security Corporation. All rights reserved.

Nothing is abnormal... until a week later. Having compromised the vendor account, an attacker then sends a follow-up email, asking when payment can be expected. In this follow-up, they cc two individuals from the first email with one difference: a “l” has been added to the domain, creating a lookalike domain that is nearly impossible to detect by the average employee.



Subject: [redacted] Accounts Payable - Past Due $132,002.36 USD
From: [redacted] <[redacted]@pkoh-ac.com>
Recipient: [redacted] <[redacted]>
To: 6 recipients
CC: [redacted] <[redacted]@plkoh-ac.com>; [redacted] <[redacted]@plkoh-ac.com>
Date: May 11, 2023, 12:02pm ET

Please advise when payment should be expected.

Best Regards,

[redacted]
Senior Account Manager
[redacted]
Email: [redacted]@pkoh-ac.com

By including the lookalike domain, the attacker can then answer from that email address in the future—enabling them to take the attack out of legitimate inboxes where they may get caught. From here on, the legitimate recipients will never receive a response.

© 2023 Abnormal Security Corporation. All rights reserved.

The largest vendor fraud attack caught by Abnormal to date requested

$36 million

from the recipient.

Abnormal Data

Detecting Vendor Email Compromise

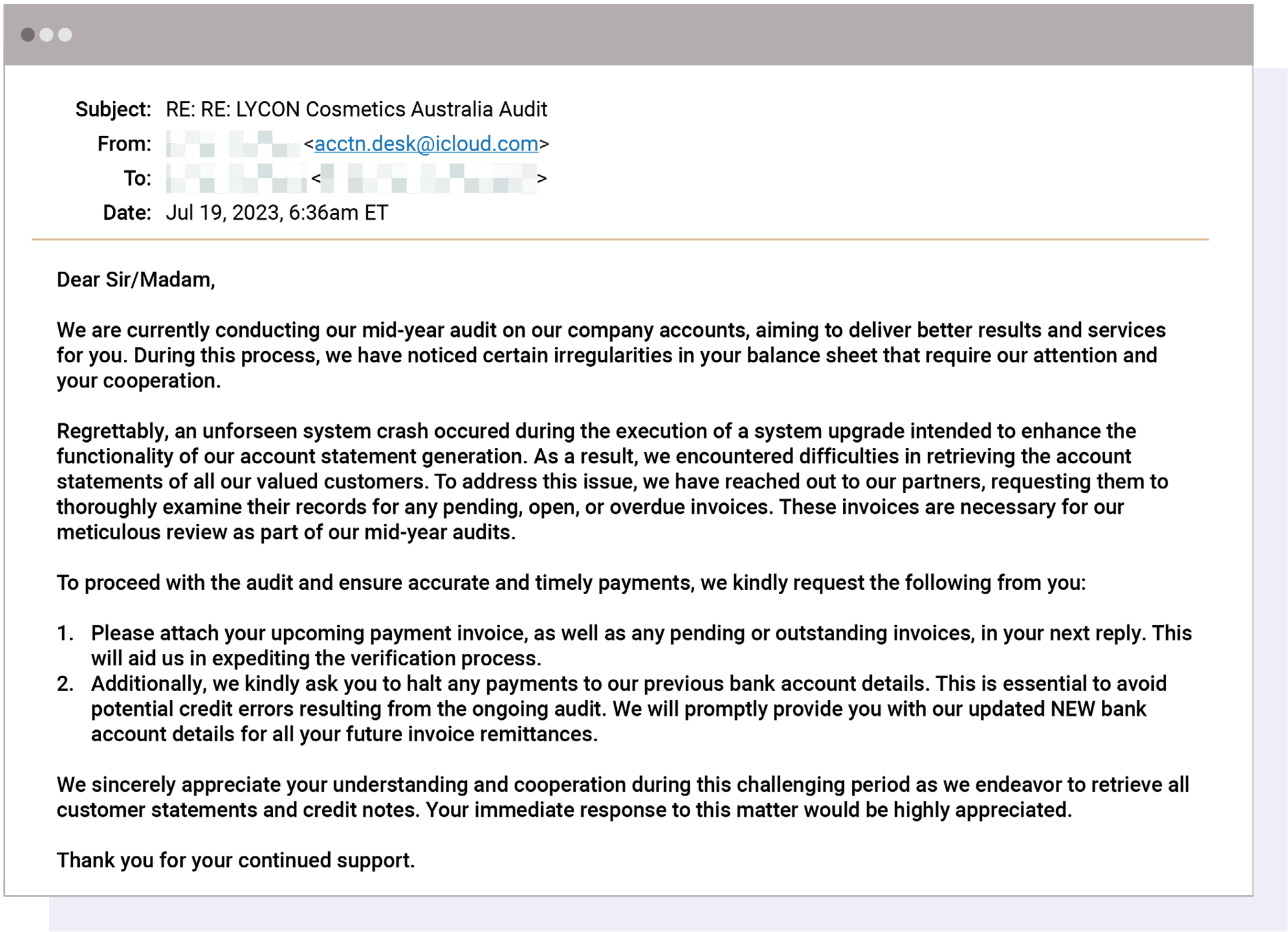
This type of attack can be especially difficult to detect because threat actors are using real vendor accounts to carry out their malicious activity, meaning that their emails will bypass all normal checks. The attackers then employ a variety of techniques, including changing reply-to addresses, adding mail forwarding rules, and hijacking existing email threats to request invoice payments or updates to banking details.

There is also a lack of identifying information in the email header, making it likely that this attack would bypass a traditional security solution. The advanced, AI-powered platform used by Abnormal, however, has the ability to evaluate vendor risk through VendorBase, highlight the addition of the look-alike domain, and understand the tone and financial language used in the email. When combined with other factors, these elements allow Abnormal to detect this as malicious and block it from reaching employee inboxes.

05 AI-Generated Attacks

Over the past year, advancements in generative AI technology have enabled cybercriminals to generate unique content rapidly—elevating the sophistication of social engineering attacks and email threats. Additionally, threat actors have started creating their own malicious forms of generative AI (like WormGPT) to deploy advanced attacks. We've already started to see cybercriminals take advantage of this technology, and advancements in artificial intelligence are expected to increase in 2024, making these attacks a growing security risk.

This is illustrated by the following fraudulent billing scam. The attack, likely generated by artificial intelligence, involves an impersonation of a business development manager from the Australian cosmetics company LYCON. The attacker claims that a mid-year audit uncovered various issues demanding urgent attention, citing irregularities in the recipient's balance sheet and a system crash hindering the retrieval of account statements.



Subject: RE: RE: LYCON Cosmetics Australia Audit
From: [redacted] <acctn.desk@icloud.com>
To: [redacted] <[redacted]>
Date: Jul 19, 2023, 6:36am ET

Dear Sir/Madam,

We are currently conducting our mid-year audit on our company accounts, aiming to deliver better results and services for you. During this process, we have noticed certain irregularities in your balance sheet that require our attention and your cooperation.

Regrettably, an unforseen system crash occured during the execution of a system upgrade intended to enhance the functionality of our account statement generation. As a result, we encountered difficulties in retrieving the account statements of all our valued customers. To address this issue, we have reached out to our partners, requesting them to thoroughly examine their records for any pending, open, or overdue invoices. These invoices are necessary for our meticulous review as part of our mid-year audits.

To proceed with the audit and ensure accurate and timely payments, we kindly request the following from you:

1. Please attach your upcoming payment invoice, as well as any pending or outstanding invoices, in your next reply. This will aid us in expediting the verification process.
2. Additionally, we kindly ask you to halt any payments to our previous bank account details. This is essential to avoid potential credit errors resulting from the ongoing audit. We will promptly provide you with our updated NEW bank account details for all your future invoice remittances.

We sincerely appreciate your understanding and cooperation during this challenging period as we endeavor to retrieve all customer statements and credit notes. Your immediate response to this matter would be highly appreciated.

Thank you for your continued support.

© 2023 Abnormal Security Corporation. All rights reserved.

97%

of security stakeholders express apprehension about the dangers posed by generative AI.

Osterman Research: The Role of AI in Email Security

The attacker then urges the recipient to send any pending or outstanding invoices and advises them to cease payments to previously provided bank account details. This scam aims to deceive the recipient into divulging sensitive financial information and rerouting payments to the attacker's bank account.

Detecting AI-Generated Attacks

Generative AI enables threat actors to dynamically craft emails with varying structures, wording, and contextual nuances—without the typos and grammatical errors that have been indicative of attacks of the past. The diversity in content makes it difficult for traditional security systems to recognize patterns or signatures associated with known malicious text strings, as each attack instance may appear distinct, and the lack of errors makes it much more believable to the recipient.

This particular attack would be challenging to detect as it was sent from a legitimate email service provider, is entirely text-based, and relies on social engineering to compel the recipient to take action. Further, there are no traditional indicators of compromise, such as a bad domain reputation or malicious link, for legacy email solutions to detect.

However, using AI, Abnormal was able to establish a baseline for normal behavior within the organization and then detect and block activity that deviated from this baseline—noticing the mismatched display name and email address, the unique sender, and the financial language included in the email. After detecting the attack, further analysis by CheckGPT shows that it was likely AI-generated.

© 2023 Abnormal Security Corporation. All rights reserved.

Predictions for 2024 and Beyond

As you can see from these example attacks, cybercriminals are becoming more sophisticated every single day. This is compounded by the exploitation of technologies like generative AI and QR codes, making cybersecurity a bigger challenge than ever before.

Looking ahead, we expect several trends to shape the email threat landscape over the next few years:

Increased Adoption of Malicious AI: As cybercriminals discover how to use ChatGPT and its malicious counterparts to their advantage, we will see an increased volume of attacks. With the ability to create unique malicious content in seconds, there will be millions more emails sent in the coming year—making it harder for SOC teams to manually review each attack.

Increased Sophistication of Social Engineering: Cybercriminals will also continue to exploit generative AI technology to carry out highly targeted and sophisticated email attacks, which will pose a greater challenge for traditional email security systems and humans alike. By inputting targeted information into these systems, attackers will be able to socially-engineer humans like never before.

Need for AI-Native Platforms: As generative AI takes off for cybercriminals, the cybersecurity community will need to rely more on defensive AI to counter the increased attacks. While these platforms have been available for the past few years, AI-native solutions that use machine learning and natural language processing to detect and block attacks will be the only option available that will truly stop these constantly-evolving threats.

While there is no crystal ball and no one can predict the future, one thing is certain: **cybercrime will not stop in 2024**. Instead, it will only continue to increase, so security professionals must find better ways to protect their organizations and their employees from these threats. As threat actors continue to innovate, Abnormal Security does too—ensuring that our customers stay protected from the attacks of the past, the present, and the future.

© 2023 Abnormal Security Corporation. All rights reserved.

Conclusion

As we navigate the ever-evolving digital landscape, the potential risks associated with email attacks in 2024 are both diverse and formidable. The real-world threats outlined in this report underscore the increasing sophistication of cybercriminals, and the direction in which they are headed.

In the face of advanced phishing attacks, malware threats, supply chain vulnerabilities, AI-driven attacks, and more, organizations must implement a heightened level of awareness and diligence. The dynamic nature of these threats demands continuous adaptation and the adoption of cutting-edge AI-powered technologies to stay one step ahead. Staying informed, remaining vigilant, and implementing proactive measures to prevent these threats will be key to safeguarding sensitive information, preventing financial fraud, and maintaining the integrity of digital communication channels in 2024 and beyond.

© 2023 Abnormal Security Corporation. All rights reserved.

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.

Interested in Preventing Email Attacks in 2024?

Get a Demo →

See Your Abnormal ROI →