THREAT REPORT

Inbox Under Siege:

5 Email Attacks You Need to Know for 2025

Abnormal

Executive Summary

Few issues are as far-reaching as cybersecurity. Every business, from sole proprietors to global conglomerates, faces cyberattack risks, with threat actors targeting industries across both niche markets and essential sectors.

While cybercriminals can (and do) infiltrate organizations by exploiting software vulnerabilities and launching brute force attacks, the most direct—and often the most effective—route is via the inbox. As the front door of an enterprise and the gateway upon which employees rely to do their jobs, the inbox represents an ideal access point for attackers. And it seems that, unfortunately, cybercriminals aren't lacking when it comes to identifying new ways to sneak in.

$5.8B

Total losses due to cryptocurrency fraud reported to FBI IC3

2024 IC3 FBI Cryptocurrency Fraud Report

350%

Increase in file-sharing phishing attacks between June 2023 and June 2024

Abnormal AI Internal Data

261 Days

Required to resolve breach resulting from a phishing attack

IBM Cost of a Data Breach Report, 2024

98%

Share of security leaders concerned about cybersecurity risks of AI

Abnormal AI Internal Data

Cryptocurrency fraud exploits the decentralized and irreversible nature of blockchain transactions, targeting individuals unfamiliar with its nuances. File-sharing phishing schemes leverage legitimate platforms like Google Drive and Dropbox to evade detection, while multichannel phishing broadens the attack surface, incorporating text messages, phone calls, or messaging apps to shift interactions to less secure personal devices. Generative AI enables attackers to craft convincing business email compromise (BEC) campaigns at scale, empowering even novice threat actors to launch sophisticated attacks. Email account takeover is among the most dangerous threats, providing cybercriminals with direct access to corporate systems and enabling subsequent attacks like BEC, vendor email compromise, and lateral phishing.

The potency of these attacks lies in their ability to exploit trust. Whether impersonating known contacts, abusing compromised accounts, or weaponizing trusted platforms, attackers manipulate trust to breach defenses at every stage of an attack. The result is a threat landscape in which legacy security solutions, such as secure email gateways, are increasingly ineffective at detecting complex campaigns.

This white paper underscores the urgent need for AI-native defenses capable of identifying anomalies and analyzing context in real time. By gaining a deeper understanding of how attackers innovate and adopting solutions designed to counter these evolving methods, organizations can safeguard their systems, data, and people from the rising sophistication of email threats.

Table of Contents

5 Advanced Email Attacks to Watch For in 2025 04

- Cryptocurrency Fraud 05
- File-Sharing Phishing 08
- Multichannel Phishing 12
- AI-Generated Business Email Compromise 15
- Email Account Takeover 18

Predictions for 2025 and Beyond 21

Defending Against New and Emerging Threats 22

About Abnormal AI 23

INTRODUCTION

5 Advanced Attacks to Watch For in 2025

EMAIL IS THE CORNERSTONE OF BUSINESS COMMUNICATION, UNIVERSALLY ADOPTED ACROSS INDUSTRIES AND LOCATIONS.

Unfortunately, its ubiquity is one reason it has been a preferred attack vector for nearly four decades. Email's versatility as a communication medium further compounds the issue, as threat actors can leverage it for a variety of malicious purposes.

Opportunistic and enterprising, cybercriminals are continually seeking 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, threat actors will learn how to exploit it.

The following are real-world examples of threats that Abnormal customers received in 2024. They demonstrate the anticipated evolution of the threat landscape in the coming year and offer critical insights into the attack strategies organizations must be ready to detect and defend against in 2025.

ADVANCED EMAIL ATTACKS TO WATCH FOR IN 2025 \\

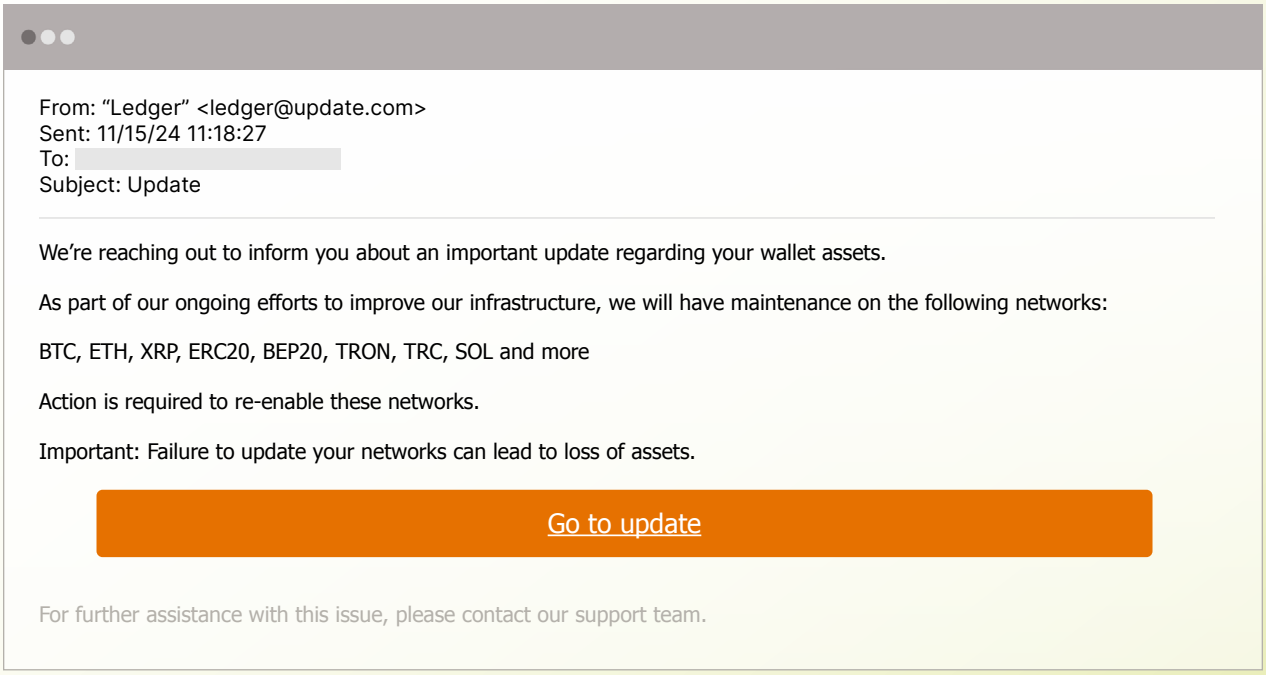
Cryptocurrency Fraud

Cryptocurrency was initially developed to be more secure than traditional money, utilizing blockchain technology to enable decentralization and immutable transactions. However, these same qualities can facilitate fraud, as the lack of centralized oversight and the speed of irreversible transactions provide considerable opportunities for exploitation. Additionally, its novelty and esoteric nature make it attractive to less financially experienced individuals drawn to its perceived potential, while also posing challenges for even the most financially savvy to fully understand. Combined, these characteristics have made cryptocurrency a popular theme for cyberattacks.

Cryptocurrency fraud has certainly not shown any signs of slowing. And with an incoming administration that has generally been more supportive of cryptocurrency and the value of Bitcoin surging as we near the end of the year, we anticipate the volume and sophistication of these threats to continue growing throughout 2025.

Real-World Example of Cryptocurrency Fraud

Receiving a request to provide your mother's maiden name or the name of your first pet would instantly raise red flags for the average individual. We all recognize these details as the answers to standard security questions and know not to share them. But a recovery phrase of 12-24 words is a much less common authentication mechanism, which means being asked to supply this information wouldn't necessarily set off the same alarm bells. This is what the threat actor in this attack example is banking on.



From: "Ledger" <ledger@update.com>
Sent: 11/15/24 11:18:27
To:
Subject: Update

We're reaching out to inform you about an important update regarding your wallet assets.

As part of our ongoing efforts to improve our infrastructure, we will have maintenance on the following networks:

BTC, ETH, XRP, ERC20, BEP20, TRON, TRC, SOL and more

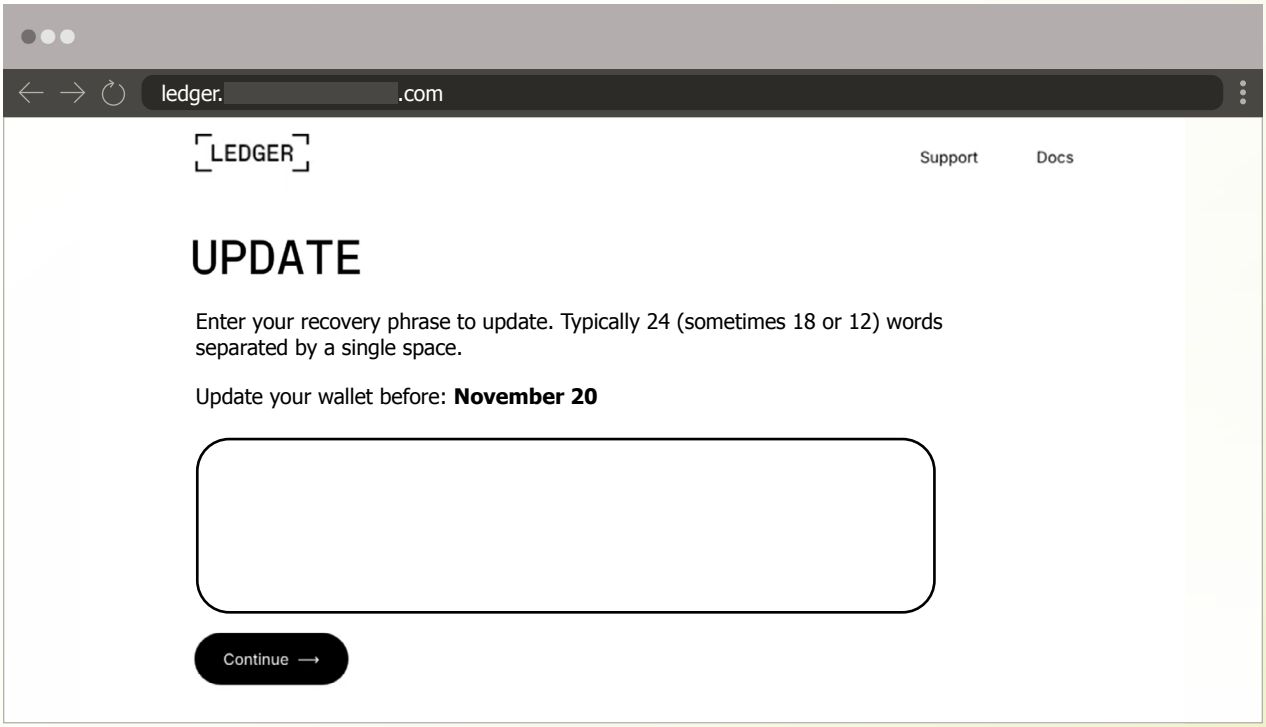
Action is required to re-enable these networks.

Important: Failure to update your networks can lead to loss of assets.

Go to update

For further assistance with this issue, please contact our support team.

Posing as Ledger, a provider of digital asset security solutions, the attacker claims that several popular cryptocurrency networks are undergoing maintenance. To re-enable the target's access to these networks, they must use the provided link to update their account; otherwise, they risk losing their assets. Should the recipient click on the link, they are redirected to a page with a prompt to input their recovery phrase.



If they enter the recovery phrase for their digital asset wallet and click "Continue," the page simply redirects to a real page on Ledger's website. This is likely intended to make the target believe that they have completed the requested update successfully. However, what they don't know is that they have handed their recovery phrase directly to the attacker. Using any compatible wallet software, the threat actor can input the recovery phrase to derive the wallet's private keys and restore access to the wallet's funds.

Detecting Cryptocurrency Fraud

Traditional security solutions like secure email gateways (SEGs) struggle to identify this email as malicious for a few reasons. First, the sending domain the attacker uses was initially registered 30 years ago, which can trick legacy systems that often equate age with trustworthiness. Additionally, the domain on which the phishing page is hosted is legitimate and belongs to a UK-based business. Plus, the sender has never communicated with the recipient before—a challenge for SEGs, which often struggle to assess the risk of new senders accurately.

Abnormal's AI detection engine recognizes that the sending domain doesn't match the domain of the link in the email body and also flags the embedded URL as suspicious. Further, its content analysis algorithms evaluate the text and identify multiple questionable elements: an attempt to engage the recipient without prior communication, an apparent financial request, and language referencing cryptocurrency transactions. Due to these factors, the email was marked as malicious.

$5.8B

Total losses due to cryptocurrency fraud reported to FBI IC3

2024 IC3 FBI Cryptocurrency Fraud Report

ADVANCED EMAIL ATTACKS TO WATCH FOR IN 2025 \\

File-Sharing Phishing

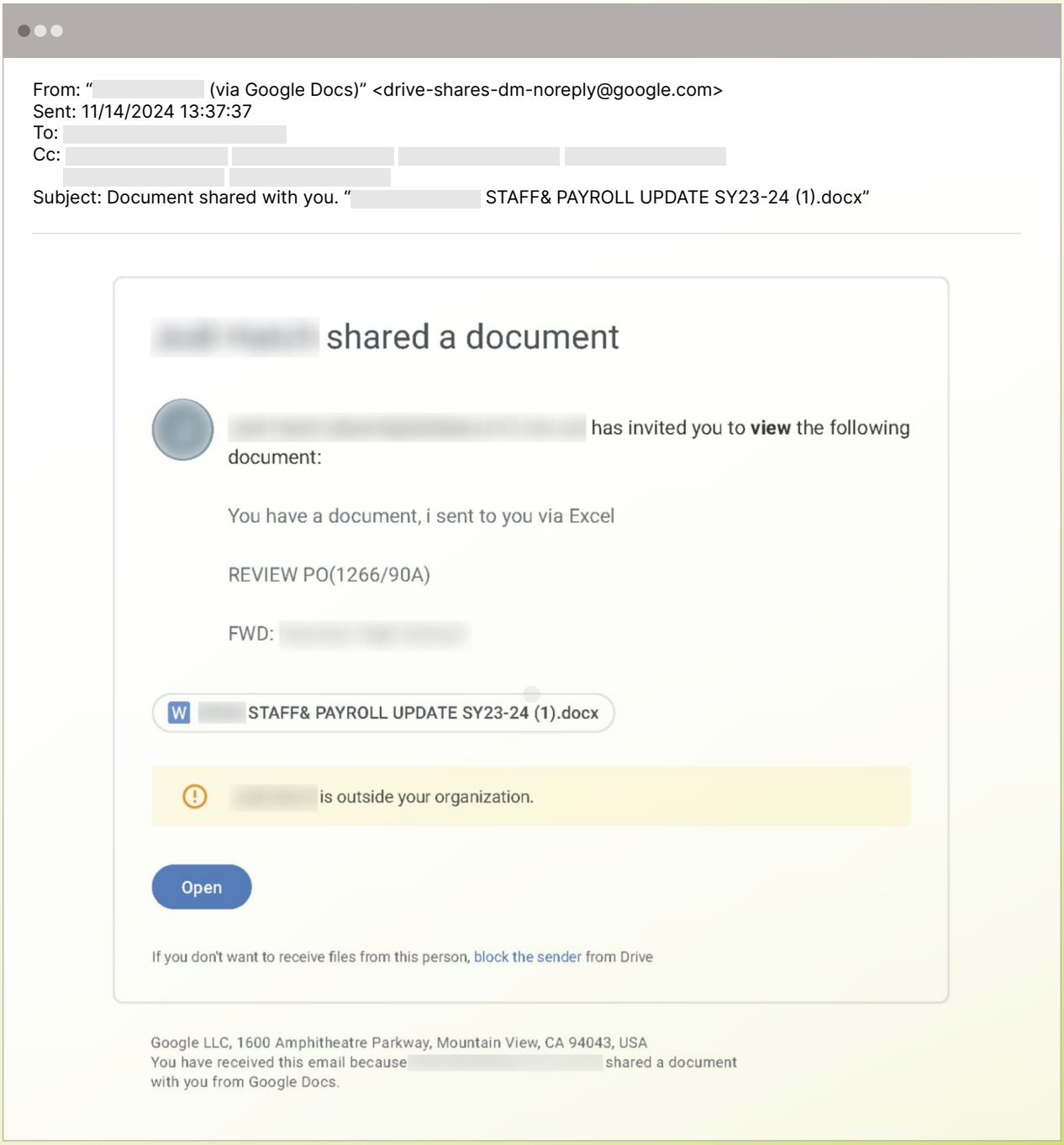
A file-sharing phishing attack is a unique type of phishing threat in which a threat actor exploits a legitimate file-hosting or e-signature solution to deceive targets. Because popular solutions like Dropbox, ShareFile, and Docusign offer either free registration or no-charge trials, and are API-enabled, any individual (including cybercriminals) can create and send emails at scale via the platform.

Consequently, bad actors can craft and dispatch malicious messages that are essentially identical to a normal, genuine notification because the sender's address, email body, and embedded link are all legitimate. This also means that, unlike the vast majority of phishing attacks, the malicious link isn't contained within the email. It exists within a separate document hosted on a genuine file-hosting service, and it's only after the target leaves the email environment and engages with the shared file that they're exposed to the phishing link.

Real-World Example of File-Sharing Phishing

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 creates and shares a Google Doc with faculty members at a public high school. As in most file-sharing phishing attacks, the document's name is related to a topic designed to pique the recipients' interest—in this case, a payroll update.



From: " (via Google Docs)" <drive-shares-dm-noreply@google.com>
Sent: 11/14/2024 13:37:37
To:
Cc:
Subject: Document shared with you. " STAFF& PAYROLL UPDATE SY23-24 (1).docx"

shared a document

has invited you to **view** the following document:

You have a document, i sent to you via Excel

REVIEW PO(1266/90A)

FWD:

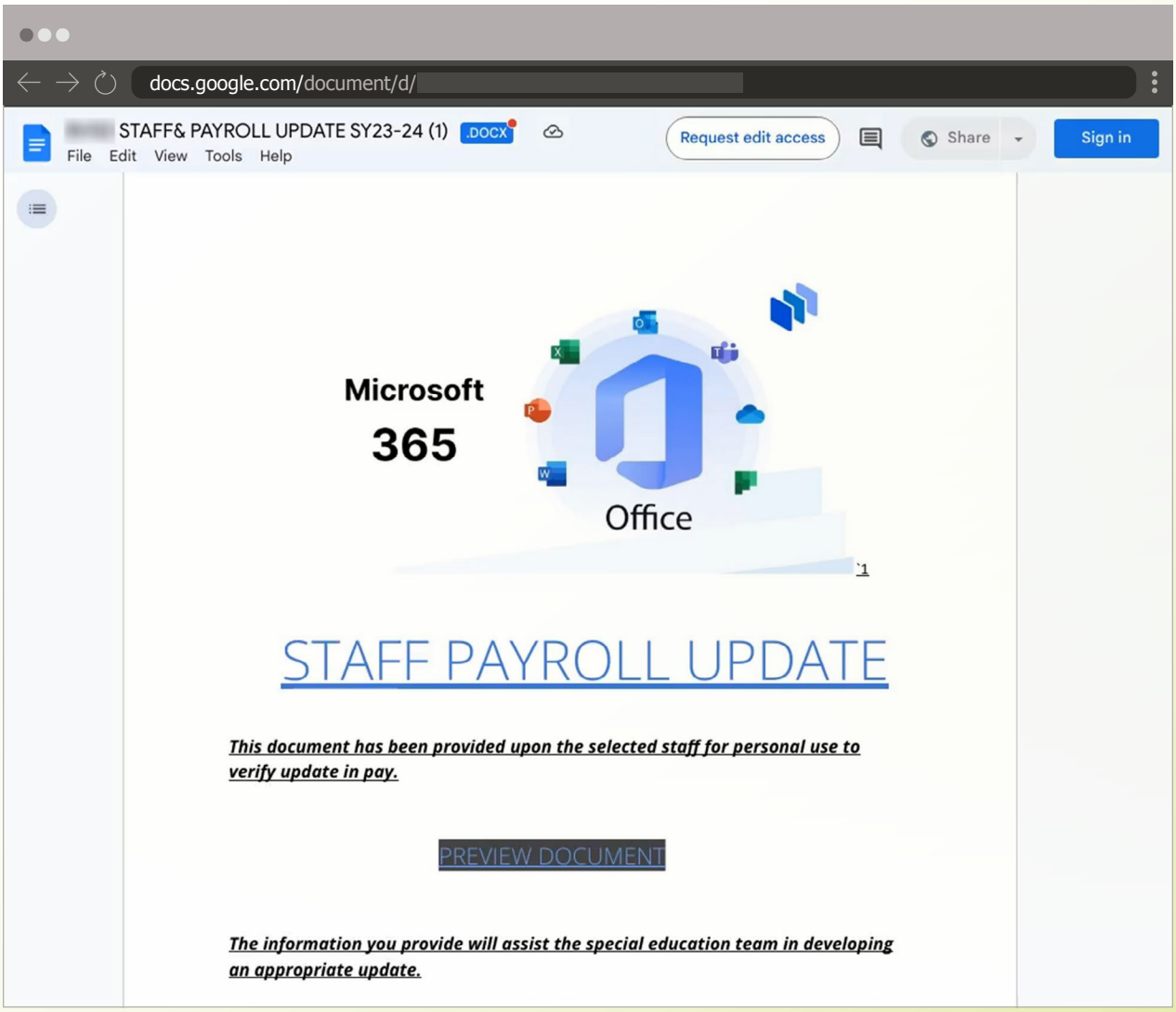
STAFF& PAYROLL UPDATE SY23-24 (1).docx

is outside your organization.

Open

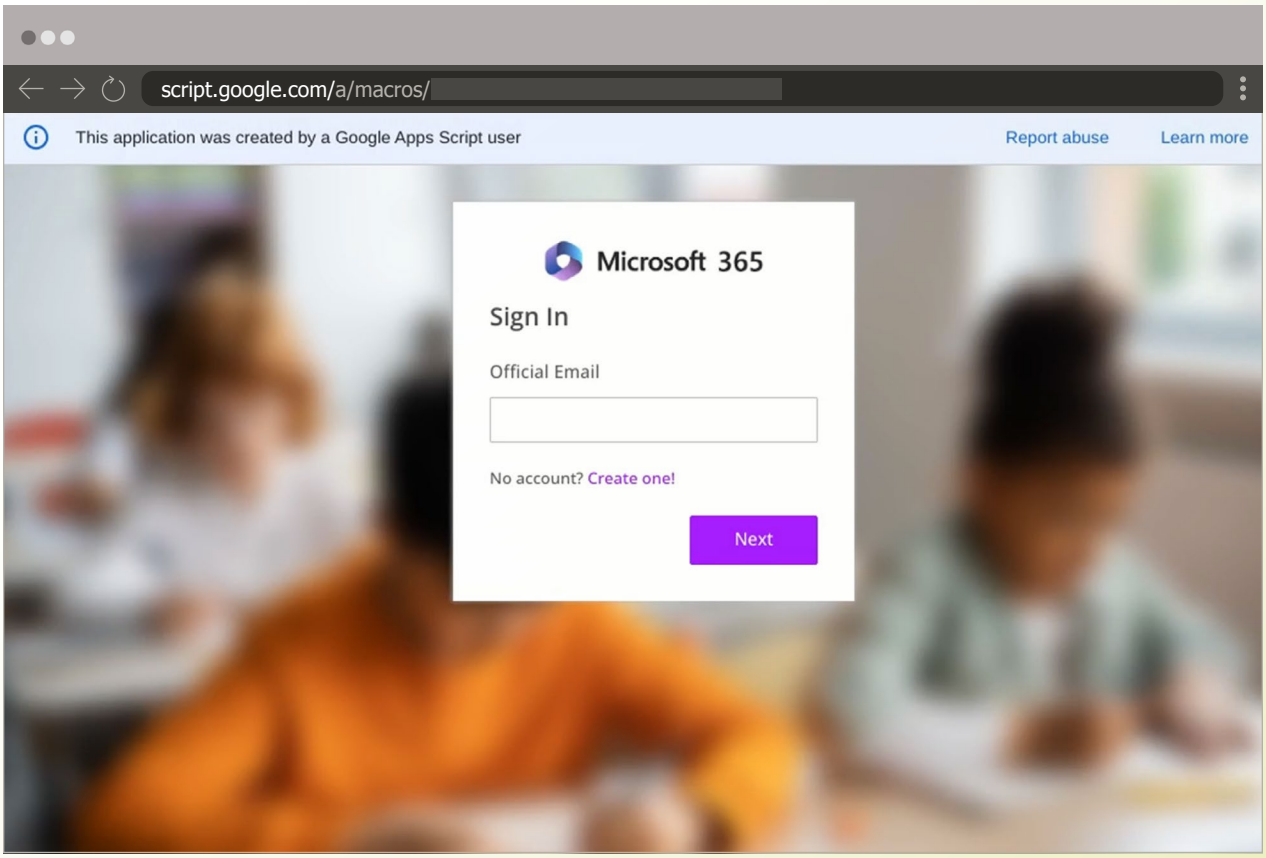
If you don't want to receive files from this person, block the sender from Drive

Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
You have received this email because shared a document with you from Google Docs.



The Google Doc, which features the latest Microsoft 365 branding to increase the appearance of legitimacy, informs the recipients that the document linked within the file should be used to verify an update in their compensation.

Clicking on “PREVIEW DOCUMENT” redirects the targets to a login screen hosted on script.google.com, the domain for Google Apps Script, a cloud-based JavaScript platform that enables users to integrate with Google services and develop web applications.



To enhance the ruse, the attacker cleverly uses a stock photo of children in a classroom as the background, reinforcing the idea that the login portal is meant for educators. However, any information entered into the page will be stolen by the cybercriminal and used to launch additional attacks.

Detecting File-Sharing Phishing

Legacy security tools operate on a simple "if this, then that" logic, flagging emails based on factors like suspicious sending domains or known malicious components.

However, at no point in the attack was there an obvious indicator of compromise. The initial email originated from a legitimate domain—google.com. Additionally, the message serves as simply the first stepping stone in a series that leads to the malicious link, which is located completely outside the email ecosystem. The shared file was created using Google Docs, a legitimate software, utilizing a real Google account belonging to a real person. The phishing page was hosted on Google Apps Script, another legitimate platform. In short, identifying this as an attack requires an ability to understand the message's context and intent—something only an AI-native solution like Abnormal can achieve.

350%

Increase in file-sharing phishing attacks between June 2023 and June 2024

Abnormal AI Internal Data

ADVANCED EMAIL ATTACKS TO WATCH FOR IN 2025 \\

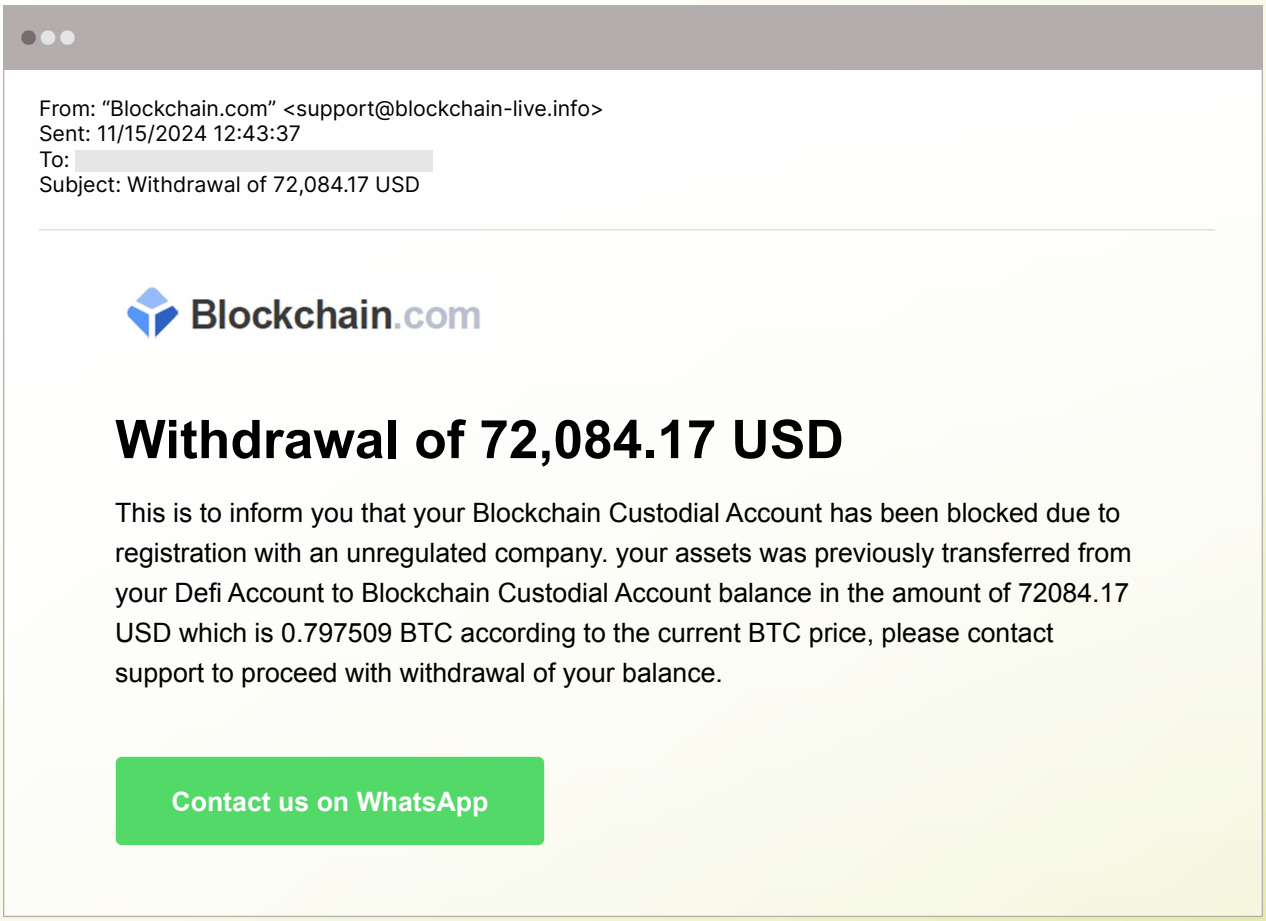
Multichannel Phishing

Multichannel phishing represents an evolution of phishing tactics, leveraging multiple communication platforms to manipulate victims more effectively. Unlike traditional phishing, which relies exclusively on email, multichannel campaigns initiate contact through email but then steer the conversation to other channels, such as text messages, phone calls, or third-party messaging apps like WhatsApp or Telegram.

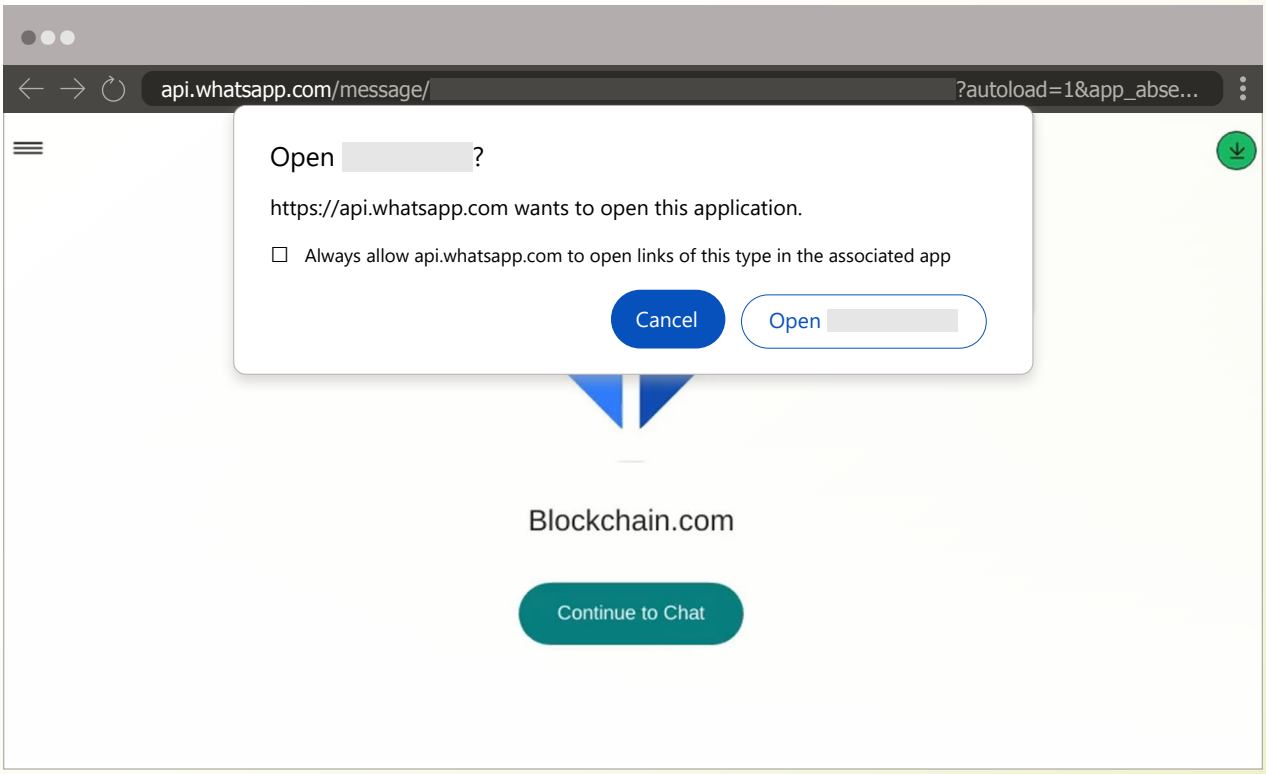
This strategy serves a variety of purposes. First, it fosters a sense of urgency by transitioning from an asynchronous channel to a real-time medium. Next, it increases the probability of deceiving employees since security awareness training primarily focuses on the email environment—not external channels. Finally, by moving the interaction from the recipient's company-managed laptop to their personal mobile device, attackers circumvent enterprise-level security controls. This shift exposes the victim to greater risk, as personal devices typically lack the same rigorous security configurations and oversight found in business environments.

Real-World Example of Multichannel Phishing

In this multichannel phishing attack, the threat actor impersonates Blockchain.com, a popular cryptocurrency exchange, and informs the target that access to their account has been blocked due to transactions with an unregulated entity and they must withdraw their balance. The email instructs them to use the embedded link to contact the support team.



Should the recipient click on the button labeled "Contact us on WhatsApp", they will be redirected to a WhatsApp URL featuring Blockchain.com's branding.



Clicking on "Continue to Chat" opens the impersonated business' profile on the WhatsApp app. If the target begins a conversation with someone they believe is part of the support team for Blockchain.com, they will initiate the next stage of the attack, which most likely involves convincing the target to provide sensitive information or grant access to their digital wallet.

Detecting Multichannel Phishing

As with the previous two examples, the challenge for legacy systems with respect to this attack is that so many elements of the initial email are legitimate. The sending domain, albeit a parked domain, is an actual website, and the address passes both SPF and DKIM authentication. All of the links in the email are to trusted websites, including real Blockchain.com pages. In other words, there's no known bad for a SEG to detect.

Abnormal, on the other hand, leverages machine learning and behavioral AI to identify multiple suspicious features. For example, not only does the sending domain not match any domains found in body links, but it is also inconsistent with the sender's display name. It also leverages natural language processing to understand and extract topics from the content, including a suspicious financial request and language often found in cryptocurrency attacks. While traditional security tools may not flag any of these aspects, Abnormal recognizes these as all signs that the email is malicious.

261 Days

Required to resolve breach resulting from a phishing attack

IBM Cost of a Data Breach Report, 2024

ADVANCED EMAIL ATTACKS TO WATCH FOR IN 2025 \\

AI-Generated Business Email Compromise

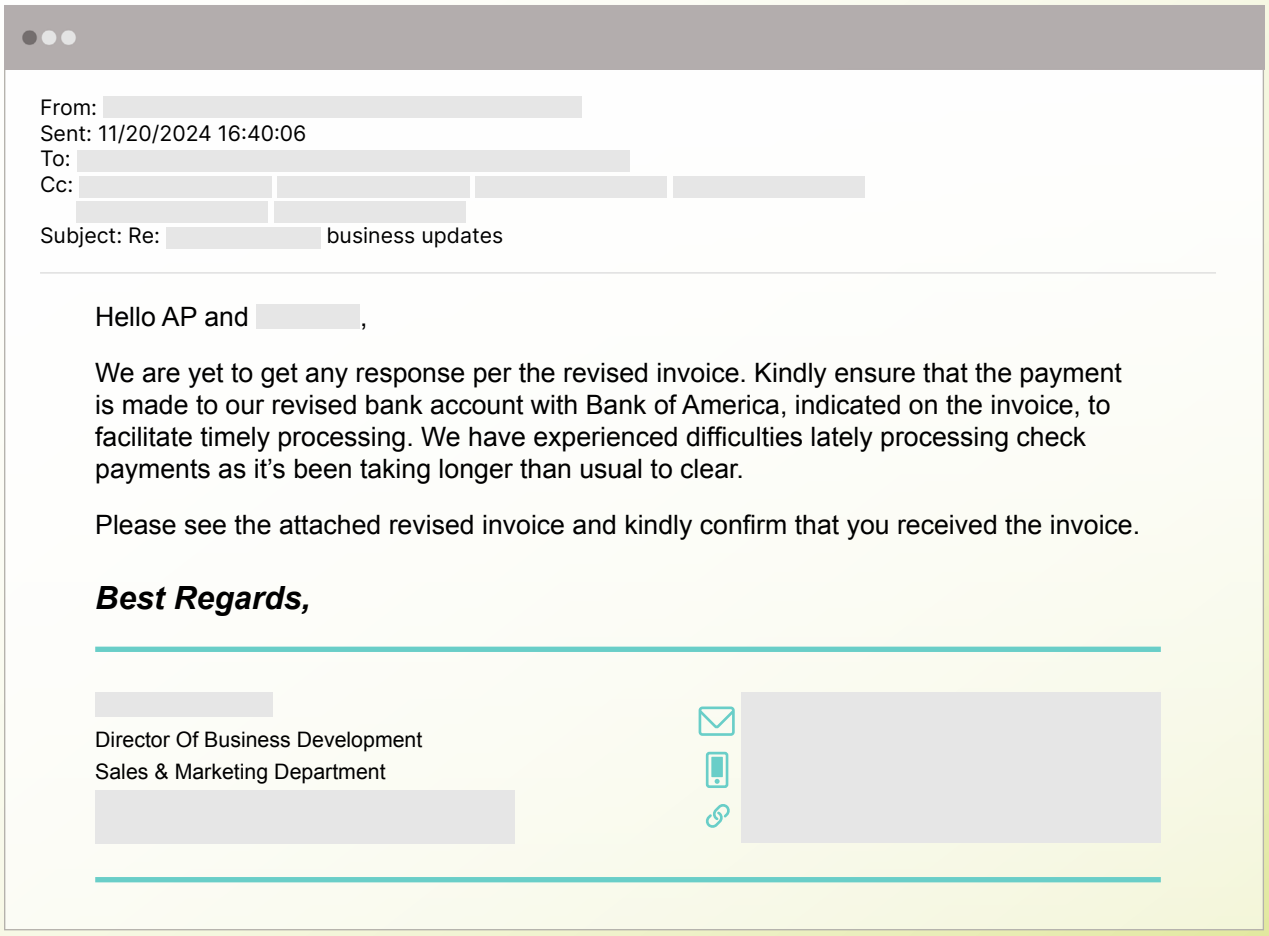
Business email compromise (BEC) attacks leverage social engineering to deceive recipients into divulging sensitive information or completing fraudulent financial requests. Threat actors impersonate trusted partners or authority figures, allowing them to capitalize on the implicit trust within the relationship.

BEC had already established itself as a leading cyber threat, but the emergence of AI has complicated matters. By analyzing vast volumes of data from social media, online activity, and past interactions, AI-powered platforms can generate hyper-personalized messages that convincingly mimic the writing style of the impersonated individual. This makes the emails more difficult for traditional security measures to detect and more likely to deceive unsuspecting recipients. And while legitimate tools like ChatGPT have built-in measures to prevent malicious use, these can be circumvented. Plus, malicious versions like FraudGPT are designed specifically for criminal use, empowering even novice threat actors to up-level their attacks.

Real-World Example of Likely AI-Generated Business Email Compromise

Much like traditional BEC, vendor email compromise (VEC) 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.

Both BEC and VEC attacks can involve spoofing sender addresses or using look-alike domains to deceive employees into believing the sender is who they claim to be. But the especially nefarious (and difficult to detect) attacks utilize the actual account of the individual being impersonated, as is the case with this example.



From:
Sent: 11/20/2024 16:40:06
To:
Cc:
Subject: Re: business updates

Hello AP and ,

We are yet to get any response per the revised invoice. Kindly ensure that the payment is made to our revised bank account with Bank of America, indicated on the invoice, to facilitate timely processing. We have experienced difficulties lately processing check payments as it's been taking longer than usual to clear.

Please see the attached revised invoice and kindly confirm that you received the invoice.

Best Regards,

Director Of Business Development
Sales & Marketing Department

After compromising the account of the Director of Business Development at a renewable energy manufacturer, the attacker hijacks an existing thread discussing a purchase order and invoice for battery parts. Likely utilizing generative AI, the cybercriminal drafts an email requesting confirmation that an attached invoice with updated banking information has been received and that future payments will be sent to the new account.

Thanks to GenAI, the email has no misspellings and uses acceptable grammar, punctuation, and syntax. And because it was sent from the director's real account, the recipients have no reason to believe the request is fraudulent. Should the targeted accounts payable team transfer funds to the account listed on the doctored invoice, they would wire more than $230,000 directly to the attacker.

Detecting Likely AI-Generated Business Email Compromise

Traditional email security tools can effectively block basic attacks that contain obviously malicious links or embedded code, include suspicious attachment types, use known bad phrases, or originate from domains with negative reputations. This is because a signature-based solution like a SEG relies on preexisting knowledge of threats rather than adaptive analysis—i.e., it can only detect an attack when the message has characteristics already known to be harmful.

But this email contains no malicious links or code, and the only attachment is a PDF. Further, it's sent from a trusted account with a positive reputation, and the attacker likely leveraged generative AI to make the text unique. Once again, there is nothing for a SEG to latch onto. In contrast, Abnormal builds a behavioral baseline across all cloud entities in an organization, which enables the platform to flag anomalies that indicate a threat. For this attack, Abnormal detected the inclusion of a recently registered lookalike domain in the threat actor's response, the use of suspicious language indicative of attempted vendor fraud, and an unexpected change in sender behavior that aligns with VEC attacks identified by Abnormal in the past.

98%

Share of security leaders concerned about cybersecurity risks of AI

Abnormal AI Internal Data

ADVANCED EMAIL ATTACKS TO WATCH FOR IN 2025 \\

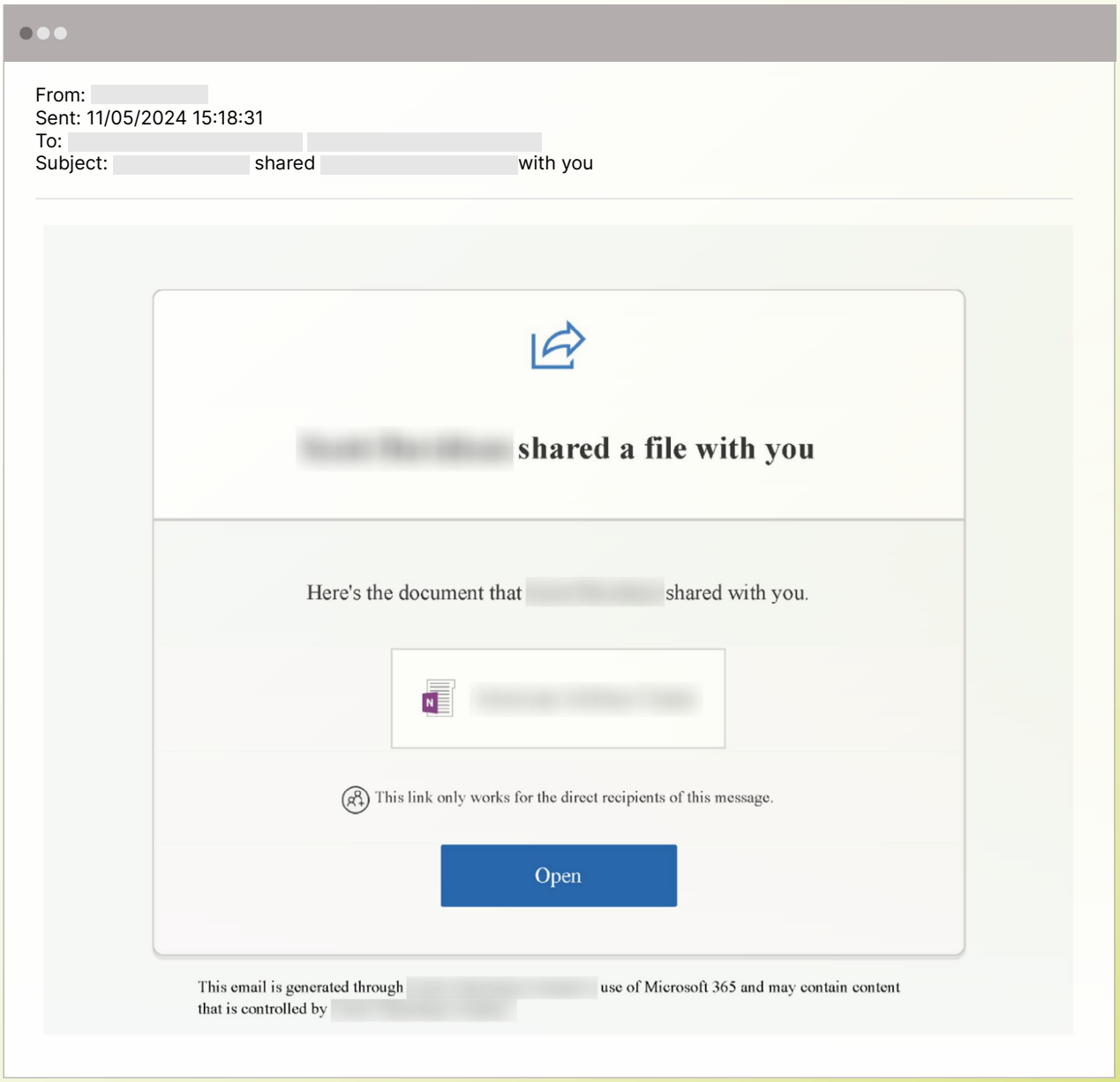
Email Account Takeover

Email account takeover (ATO) may be the most dangerous email threat that organizations face, as it provides threat actors with unparalleled access to the company's network and internal systems. It can be initiated using various methods, including phishing, social engineering, password stuffing, or session hijacking via authentication token theft or forgery.

These attacks are especially insidious because they enable bad actors to weaponize an account's existing reputation, making malicious activities more difficult to detect. By compromising a legitimate email account, cybercriminals can bypass traditional security measures and exploit the trust inherently placed in the account's communications. The result is a highly effective and versatile attack vector, capable of facilitating further compromise or fraud across an organization's network. Email ATO is among the most damaging attack types, with the average cost of a data breach caused by compromised credentials totaling $4.81 million.

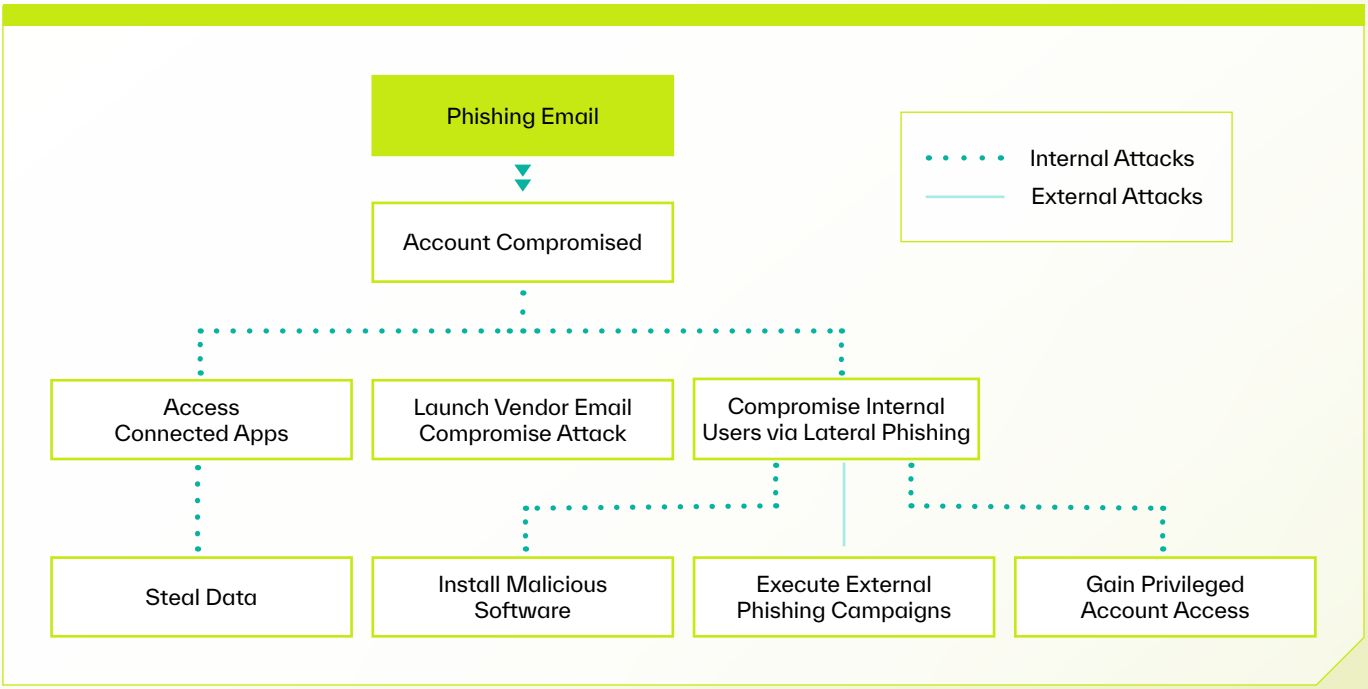
Real-World Example of Email Account Takeover

If an account takeover is initiated via phishing, the initial malicious message typically looks like any other modern phishing email. For instance, in the example below, the attacker exploits Microsoft 365 to share a OneNote file that contains a link to a phishing site designed to steal login credentials.



What the attacker does after fraudulently acquiring the target's login information is what makes account takeover potentially so devastating. Once an account has been compromised, attackers can perform a variety of malicious acts, such as exfiltrating sensitive data, infiltrating connected applications, or using the account to send additional email attacks to coworkers, partners, and customers.

The diagram below illustrates the flow of a typical email ATO attack initiated via phishing. First, a threat actor sends the target a phishing email designed to steal their login credentials like the example above. Upon successfully capturing the username and password for the target's account, the bad actor logs in.



With unrestricted access to the target's inbox and all connected applications, the attacker can search for and steal confidential business data, personal information of customers and employees, and private communications. They can also hijack existing email threads and send new attacks to people on the target's contact list, including colleagues and vendors. Email account takeover is a critical enabler of cyber threats—often preceding business email compromise and vendor email compromise, and always driving lateral phishing attacks.

Detecting Email Account Takeover

While threat actors can utilize compromised accounts to attack external entities, they generally focus on targeting other internal users and systems. Because SEGs are deployed at the perimeter and lack native API integrations with the cloud email providers' infrastructure, they have limited to no visibility into internal email patterns and the contextual signals that are critical to detecting and preventing internal email threats like account takeovers or lateral phishing attempts.

Abnormal baselines normal user behavior across multiple factors, including location, devices, browsers, login frequency, and authentication methods. This allows it to identify suspicious activities such as unusual MFA device registrations or mail filter rule changes. Using natural language understanding, it compares messages against typical communication patterns to flag anomalies. In the event of a compromise, Abnormal automatically disarms affected accounts and blocks internal-internal phishing to prevent lateral movement.

$4.81M

Average cost of a data breach caused by compromised credentials

IBM Cost of a Data Breach Report, 2024

Predictions for 2025 and Beyond

A Surge in Financially Motivated Email Attacks Leveraging AI

In 2025, financially motivated email attacks are expected to escalate significantly, driven by the adoption of AI technologies that enhance both the scale and sophistication of these campaigns. By leveraging AI-powered tools, threat actors can craft highly personalized and convincing malicious emails, maximizing their ROI while simultaneously reducing the likelihood of detection.

These AI-generated attacks will integrate real-time data from sources such as social media, business websites, and previous breaches, allowing cybercriminals to deliver highly targeted and contextually relevant messages with a level of precision previously unattainable. As these techniques grow more advanced, even vigilant recipients may struggle to distinguish between legitimate and malicious communications, posing significant challenges for organizations that continue to rely on legacy email security systems.

Rising Exploitation of Legitimate API-Enabled Services in Attack Infrastructure

Bad actors are expected to increasingly exploit legitimate API-enabled services to build, obfuscate, and scale their attack infrastructure. Platforms such as cloud services, communication APIs, and online collaboration tools will be co-opted to streamline malicious operations, enabling attackers to blend seamlessly into legitimate traffic and evade detection.

The misuse of APIs will facilitate the automation of a wide range of malicious activities, including the bulk creation of phishing sites and rapid scaling of attack campaigns. As the boundary between legitimate and malicious usage becomes increasingly blurred, security teams must adopt more advanced behavioral analysis tools that leverage AI and machine learning to mitigate these evolving threats.

The Imperative for AI-Native Solutions to Counter Emerging Threats

With each new development in the attack landscape, it becomes increasingly evident that legacy systems like secure email gateways (SEGs) are ill-equipped to prevent advanced threats from reaching employee inboxes. And any time an employee has to assess whether or not an email is safe is an opportunity for them to make a mistake. Unfortunately, the data shows that employees are notoriously bad at distinguishing malicious messages from legitimate ones.

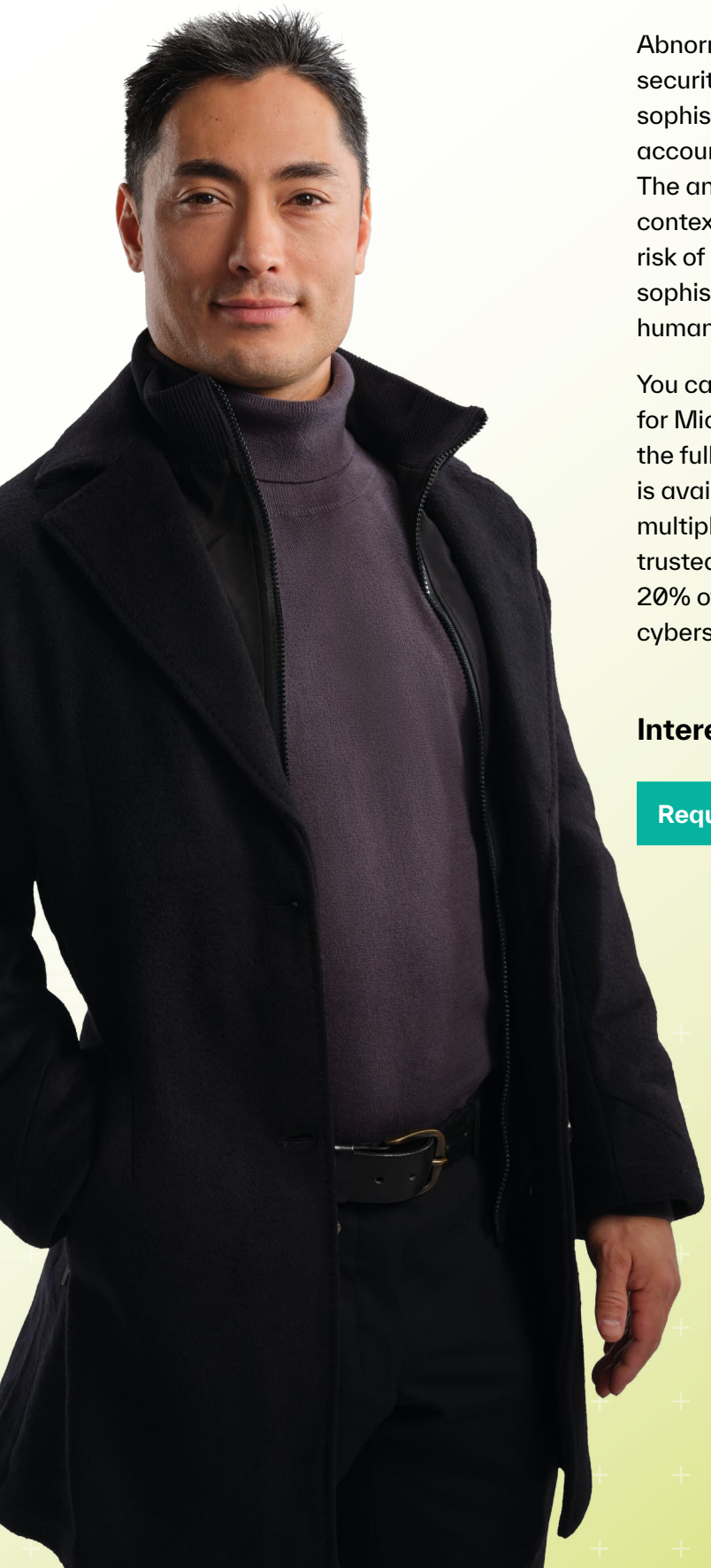
Unlike legacy systems reliant on static rules, AI-native tools excel at analyzing real-time data, detecting anomalies, and adapting to new attack vectors. These solutions are critical in addressing threats across expanding attack surfaces, such as APIs and cloud services, where speed and precision are paramount. By continuously learning and providing actionable insights, AI-native defenses empower organizations to stay ahead of cybercriminals, mitigating both known and emerging threats with agility and precision.

Defending Against New and Emerging Threats

Research reports and stakeholder surveys are increasingly drawing the same conclusion: employees remain the most vulnerable part of an organization's cybersecurity posture. While security awareness training is a critical component of a comprehensive defense strategy, the most effective way to protect your employees from ever-more complex attacks is to prevent malicious emails from reaching them in the first place.

There is little denying that email threats will continue to increase in both volume and severity. However, these attacks can be effectively neutralized with the right solution—one that leverages AI to analyze identity, context, and content and build behavioral baselines for every identity in your cloud environment. By understanding an organization's unique patterns of communication, a robust email security platform can identify and block anomalous messages before they become a threat.

With the right technology in place, you can be confident that your employees are protected from all types of attacks—even those that have yet to be observed.



About Abnormal AI

Abnormal AI 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, ServiceNow, Zoom, and multiple other cloud applications. Abnormal is currently trusted by more than 3,200 organizations, including over 20% of the Fortune 500, as it continues to redefine how cybersecurity works in the age of AI.

Interested in Stopping Modern Email Attacks?

Request a Demo ›

Follow Us on X/Twitter ›