

CYBERSECURITY AWARENESS MONTH 2025

Abnormal

Anomalies Everywhere!

Your Guide to Understanding Anomalous Activity



Meet the Anomalies

Free of traditional indicators of compromise and leveraging sophisticated social engineering tactics, modern threats are nearly impossible for traditional email security solutions to detect.

Silently lurking in your cloud environment, these alarming anomalies bide their time until they identify an opportunity to wreak havoc in your organization. And while they appear in many forms, they all have the same goal: exploit vulnerabilities to infiltrate your enterprise.



Credential Phishing

Reeler

Launched 77% of
all advanced email attacks

With numerous misspellings, poor grammar, and obvious impersonations, the phishing emails of the past were often easy to spot. Now, thanks to online translation services like Google Translate and AI tools like ChatGPT, today's threat actors can craft personalized messages with perfect spelling, grammar, and syntax. Attackers also spoof email addresses of trusted parties, hiding behind usernames and URLs with minor misspellings or easily overlooked character substitutions.

In short, bad actors can create phishing emails that wouldn't raise any level of suspicion in the majority of employees—one of the reasons it's the most popular attack type, accounting for 77% of all advanced email attacks.

CREDENTIAL PHISHING



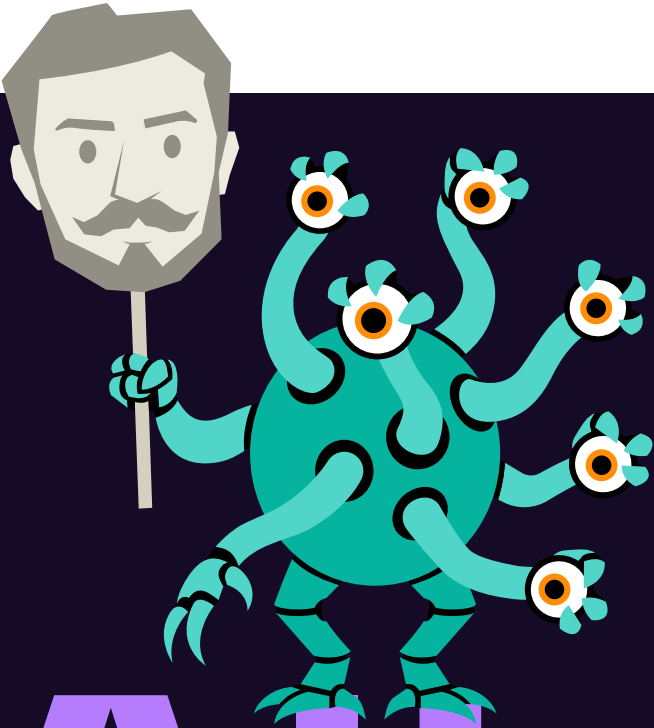
Business Email Compromise

Grifty Greta

Caused \$2.77 billion
in losses in 2024

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

BEC stands as one of the most financially devastating cybercrimes, resulting in losses of \$2.77 billion in the previous year alone.



**BUSI
NESS
EMAIL
COMPROMISE**



Vendor Email Compromise

Frauderick

44% of attacks drive further engagement

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. Given that the vendor-customer dynamic has an inherent financial element built into it, and invoices, billing accounts, and upcoming payments are often discussed via email, distinguishing these attacks from genuine emails can be extraordinarily challenging.

As a result, these attacks prove highly effective, with 44% of read VEC attacks triggering replies or forwards.



VENDOR EMAIL COMPROMISE



Malware and Ransomware

Malicious Malcolm

Executed 1,400 attacks on critical infrastructure

As the only universal communication vehicle, email is the easiest way for attackers to reach employees and compromise networks via malware. To bypass traditional email security tools, attackers often embed malware files within seemingly legitimate links or attachments. They also utilize a strategy known as payloadless malware, which involves sending targets a text-only email about a fabricated time-sensitive issue that includes a fake support phone number. If the target calls, they are instructed to download a file that, unbeknownst to them, contains a malicious payload.

An increasingly popular target, critical infrastructure providers experienced 1,400 attacks last year alone.



Account Takeover

Bobby Beaux-Gus

Average loss:
\$4.67 million per attack

Account takeovers may be the most dangerous email threat that organizations face, as they provide unparalleled access to a company's network. Once an account has been compromised, attackers can exfiltrate sensitive data, infiltrate connected applications, or use the account to send additional email attacks to coworkers, partners, and customers. Account takeovers can be initiated using various methods, including session hijacking via authentication token theft or forgery, phishing, social engineering, password stuffing, or brute-force attacks.

These attacks are among the most damaging, with the average cost of a data breach caused by compromised credentials totaling \$4.67 million.



ACCOUNT TAKE OVER



Generative AI Attacks

GenAimee

Connected to 1 out of
6 data breaches

The rise of AI-generated attacks marks a significant shift in cybercrime tactics, as AI empowers attackers to craft emails tailored to individual recipients with unprecedented precision. By analyzing data scraped from social media, online activity, and previous correspondence, AI tools can generate messages that believably mimic the writing style and behaviors of the impersonated party while also being hyper-personalized to the recipient. This sophistication makes detection more difficult and increases the chances of deceiving targets.

As a result, AI-powered threats have become increasingly pervasive, with one in six data breaches now involving generative AI.



QR Code Attacks

Olivia Obscura

Targets executives
42x more often

QR code attacks, the newest form of phishing, use social engineering to trick a target into interacting with a malicious QR code. The code is linked to what appears to be a legitimate website with a prompt to enter login credentials or other sensitive details. Unfortunately, the perpetrator can then use any information provided to compromise the target's account and launch additional attacks. With minimal text content and no obvious URL, QR codes easily evade detection by legacy security tools.

Executives face the brunt of this deception, enduring QR code attacks at 42 times the rate of their employees.



Third-Party App Attacks

Victor Vector

Involved in 30%
of data breaches

Though inbound email attacks are a mainstay for threat actors, cybercriminals are increasingly targeting third-party applications to access organizations' email environments. On average, enterprise organizations have more than 300 third-party applications integrated into their cloud environment. When employees authorize these apps, they grant them various permissions, and if an app is compromised, attackers can access sensitive company data. Each third-party application is a potential entry point, a side door attackers can use to compromise email accounts without detection.

Unfortunately, exploited third-party apps connected to the email environment contribute to 30% of data breaches.



Let's take a look at a real-world credential phishing email to showcase the problem.



Perfect Grammar

Unlike the phishing emails of the past, there is not a single misspelled word or grammatical error in this lengthy email.



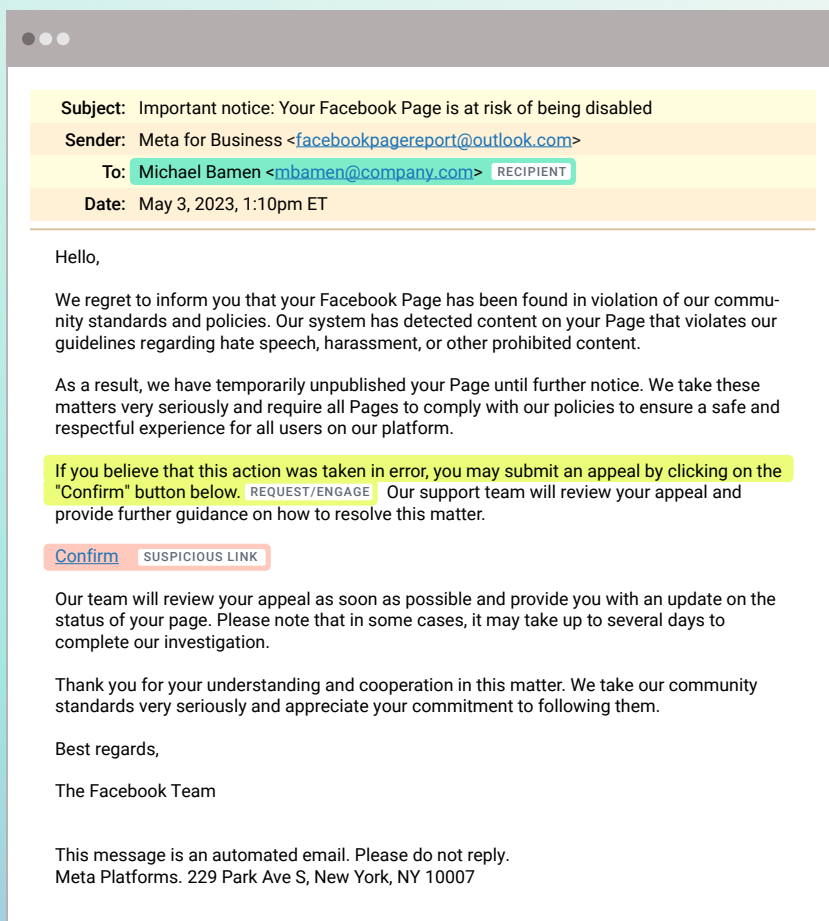
Relevant Topic

The email has been sent to the admin of the company's Facebook Page, stating that the Page has been temporarily unpublished.



Urgent Instructions

Using a tone expected of a business, the email states that the recipient should click on the included link to file an appeal.



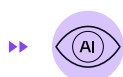
There is very little in this email to indicate an attack. Because it is sent from a legitimate domain, it will pass traditional authentication methods including SPF, DKIM, and DMARC. The lack of attachments means it will bypass malware checks. And the fact that this email is so well-crafted makes it difficult to detect by humans.

All of this underscores the increased need for email security that can understand anomalies to detect and block sophisticated attacks.



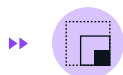
Keeping Anomalous Activity Out of Your Inboxes

So what do you do about these attacks? To counter these highly sophisticated cyber threats, organizations need the right security platform. The next generation of email security includes:



Behavioral Data Science Approach

The solution should use a fundamentally different approach that leverages behavioral data science and AI to profile and baseline good behavior and detect anomalies. It should use identity modeling, behavioral and relationship graphs, and deep content analysis to identify and stop emails that appear suspicious. Without the ability to understand normal behavior the solution will be unable to detect anomalous activity and stop the alarming anomalies.



API Architecture and Integrations

A solution that connects to Microsoft 365 and Google Workspace via an API and in doing so, provides access to the signals and data needed to detect suspicious activity. This includes unusual geolocations, dangerous IP addresses, changes in mail filter rules, unusual device logins, and more. More advanced solutions can also connect to other applications like Slack, Okta, Zoom, and CrowdStrike to understand identity and detect attempted multi-channel attacks.



Organizational and Supply Chain Insights

A solution that understands both formal and informal organizational hierarchy and maps internal and cross-organizational relationships to understand typical communication patterns and behavior across the ecosystem. It should include a focus on vendor relationships to protect against business email compromise, account takeovers, and other types of fraud throughout the supply chain.



With these capabilities, the solution can use thousands of signals to detect anomalous activity so that sinister cyber threats can be thwarted before they reach the inbox.



Beware of Anomalies All Year Long

Unfortunately, anomalous activity won't stop after Cybersecurity Awareness Month ends. Be sure to stay ahead of the threat by implementing tools that can detect these anomalies and stop them in their tracks.

ADDITIONAL RESOURCES



ON-DEMAND WEB SERIES

THE CONVERGENCE OF AI + CYBERSECURITY

AI is both a tool for innovation and a weapon for exploitation—making it critical for security leaders to understand its dual nature. In our on-demand series, The Convergence of AI + Cybersecurity, experts examine the rise of AI-powered cyberattacks and the evolving strategies defenders are using to fight back. Watch now to gain insights into today's most pressing AI-driven threats.

[Watch Now >](#)



WHITE PAPER

CISO GUIDE TO DEFENSIVE AI

Defensive AI applies behavioral and intent-aware analysis to detect threats, model human communication, and adapt to emerging risks in real time—lightening the load on analysts. Download the guide to explore what true AI-powered defense looks like.

[Download Now >](#)



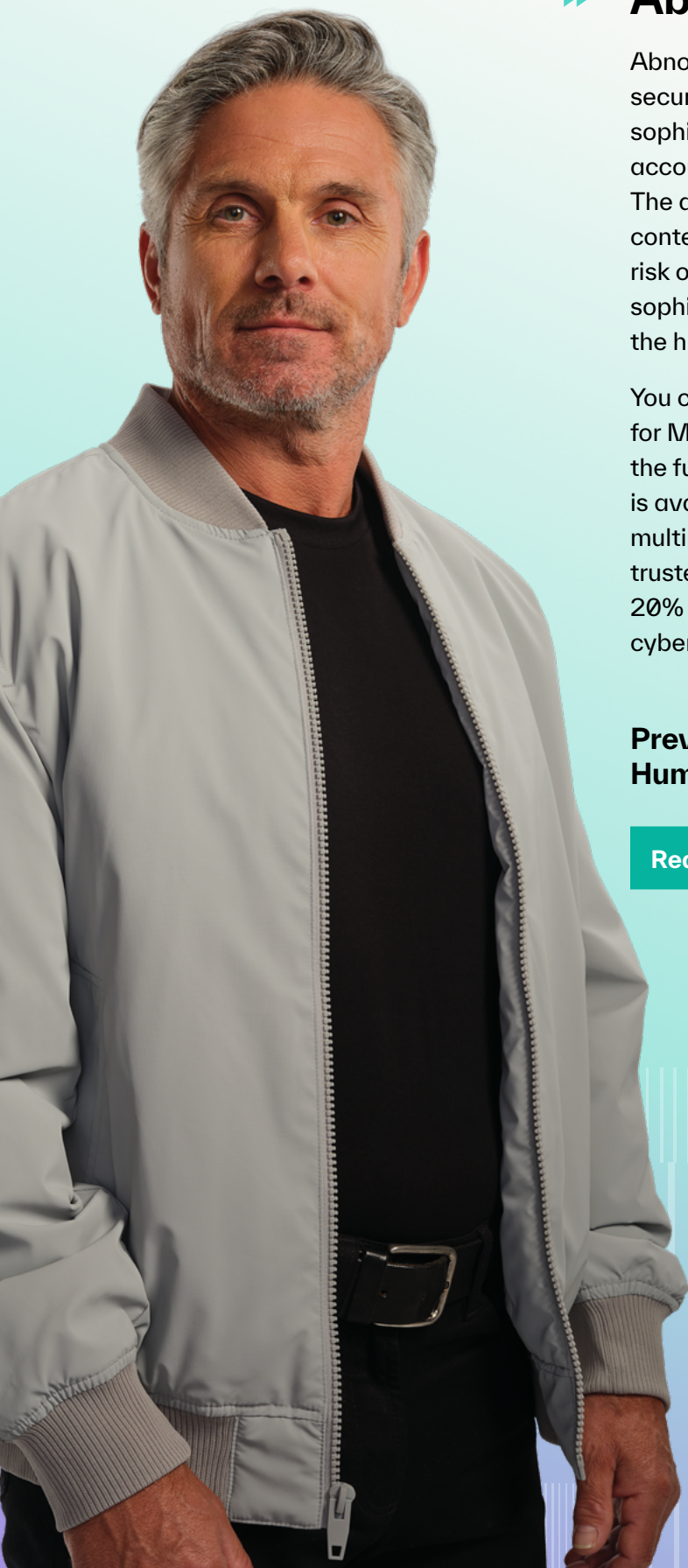
WHITE PAPER

INSIDE THE AI ARMS RACE: HOW CYBERCRIMINALS EXPLOIT TRUSTED TOOLS AND MALICIOUS GPTS

Generative pre-trained transformers (GPTs) are reshaping AI with human-like fluency—but the same capabilities that drive innovation are also being weaponized by attackers. Download this guide to learn how to defend against the next wave of AI-powered threats.

[Download Now >](#)





► 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.

Prevent Attacks Targeting Human Behavior Today

[Request a Demo >](#)[Discover the Products >](#)