Phishing Trends Report (Updated for 2026)

Get actionable insights from 4 million people's interactions with over 50 million phishing simulations and real attacks. This report provides the industry's chief reference point on real phishing attacks that bypass email filters, helping paint a clearer picture of evolving trends in the AI-boosted phishing landscape and its effect on human cyber behavior.

TABLE OF CONTENTS

Executive Summary

AI was coming. Now it's here.

AI Phishing Campaign Incidence

Callback Phishing

Most-Impersonated Entities and Domains

Recruitment Scams

Introduction

The **2026 Phishing Trends Report** is the industry's leading benchmark for phishing attacks that bypass security filters and trigger malicious clicks. Over 50 million data points were collected from the real and simulated threat reports of over 4 million Hoxhunt users around the world.

Connecting phishing simulation results to real threat detection outcomes unlocks new dimensions of analysis, insight, and intervention. These stats and trends help security awareness leaders deliver risk-relevant training, while CISOs can prioritize defensive measures against the top emerging threats.

Malicious .ics Calendar Invites: Four Times More Dangerous

Attachment Types

Impersonation campaigns leverage trusted brands

Campaign targets: Mostly business. But sometimes, it's personal

Malicious attachment campaigns

More engagement unlocks cyber behavior improvement

Cyber performance Success / Failure rate benchmark by industry

Failure rate improvement by industry

Security training performance by Job Role

Security training performance by country

Security training performance by continent

Security training performance by phishing theme

Conclusion

Report methodology & key terms

ABOUT THE AUTHOR

Trends revealed in 2026 include a **14x end-of-year surge in AI-generated phishing attacks**, new malicious attachments such as SVG files and calendar invites, mobile and callback attacks, recruitment scams, and more.

→ This report also provides a map to better security outcomes. User behavior data on tens of millions of real and simulated threats shows that the right training to the right person at the right time improves cyber performance and helps protect organizations against even the most sophisticated social engineering attacks.

Executive Summary

A Phishmas Anti-Miracle

One might call the cyber threat forecast for the first 11 months of 2025 "Cloudy with a chance of Skynet." Contrary to headlines and hyped-up marketing campaigns, Hoxhunt analysis revealed that under 5% of attacks on our 4 million users each month were AI-generated.

Until Christmas, that is.

In December, the forecast darkened into a thunderhead. Hoxhunt analysts uncovered a **14x surge in AI-generated phishing attacks** that bypassed email filters and landed in inboxes. Their share of all reported attacks across the Hoxhunt global threat detection network soared from **4% to 56% over the holiday season**.

Talk about coal in your Christmas stocking. Several CISOs confirmed to us that they were inundated over the holidays with a new breed of AI phish. And that trend has held steady into 2026.



Eliot Baker
Director of Content Marketing, Hoxhunt



Maxime Cartier
Head of Human RIsk, Hoxhunt

SHARE THIS GUIDE

How the Grinch stole Phishmas...with AI: a story in a single bar graph

AI was coming. Now it's here.

This is a remarkable development, but expected. It was only a matter of time before the dozens-fold post-ChatGPT increase in malicious messages hitting email filters translated into more than the trickle of AI phish we were seeing slip into inboxes.

These AI-generated phish are concerning, but they are not yet Skynet-level terminators. Rather, we are seeing more polished, more targeted versions of previously recognized phishing messages.

And they are no longer strictly hitting desktop devices or inboxes. Social engineering attacks are continuously expanding into a variety of communication channels, on both desktop and mobile.

Still the most common data breach vector, and the most costly, at an estimated **$4.88M per phishing breach** (IBM *Cost of a Data Breach Report 2025*), phishing continues to be our biggest cyber risk. The Comcast Business Cybersecurity Threat Report says **80–95% of breaches are initiated by a phishing attack.**

→ The good news is that phishing and social engineering risk can be measurably reduced when training is designed for behavior change and personalized to the employee's background and skill level. We must build

cyber muscles for self-defense skills, not force awareness exercises for compliance tick boxes.

After adopting a **security behavior change program** over a traditional SAT model (quarterly, manual, static trainings), employees recognize and report social engineering attacks with a **6x improvement in 6 months**, according to Hoxhunt data. They reduce the number of malicious clicks by **87%**.

The biggest human cyber risk is neglecting your humans. Leaving them unattended enlarges the greatest risk factor in cybersecurity.

This report shows the latest advances in the threat landscape and proves that good training tilts the advantage in favor of the good guys, even against the most sophisticated social engineering technologies and tactics. AI can be used for evil, but it must be adopted for good as well.

> **“AI is making social engineering faster and more scalable. When we keep training timely and relevant, people can adapt just as fast as the threats.”**

> **MAXIME CARTIER**
> VP of Human Risk

Key Phishing Statistics and Trends

Key Trends for 2026

AI GENERATED PHISHING CAMPAIGN SURGE

14x

December **increase in AI-generated phishing emails** that bypasses email security filters

20%

use open **redirects to mask** the malicious link from users and email filters

43%

of AI phishing emails use **malicious links**

11%

of AI phishing emails use **malicious attachments**

8%

impersonated HR teams & 8% included **scam invoices** from spoofed service providers

5%

of AI phishing emails included a **malicious phone number**, indicating callback phishing campaigns

19%

of AI phishing messages promoted **fraudulent offers & rewards**

13%

of AI phishing messages impersonated **financial** service providers

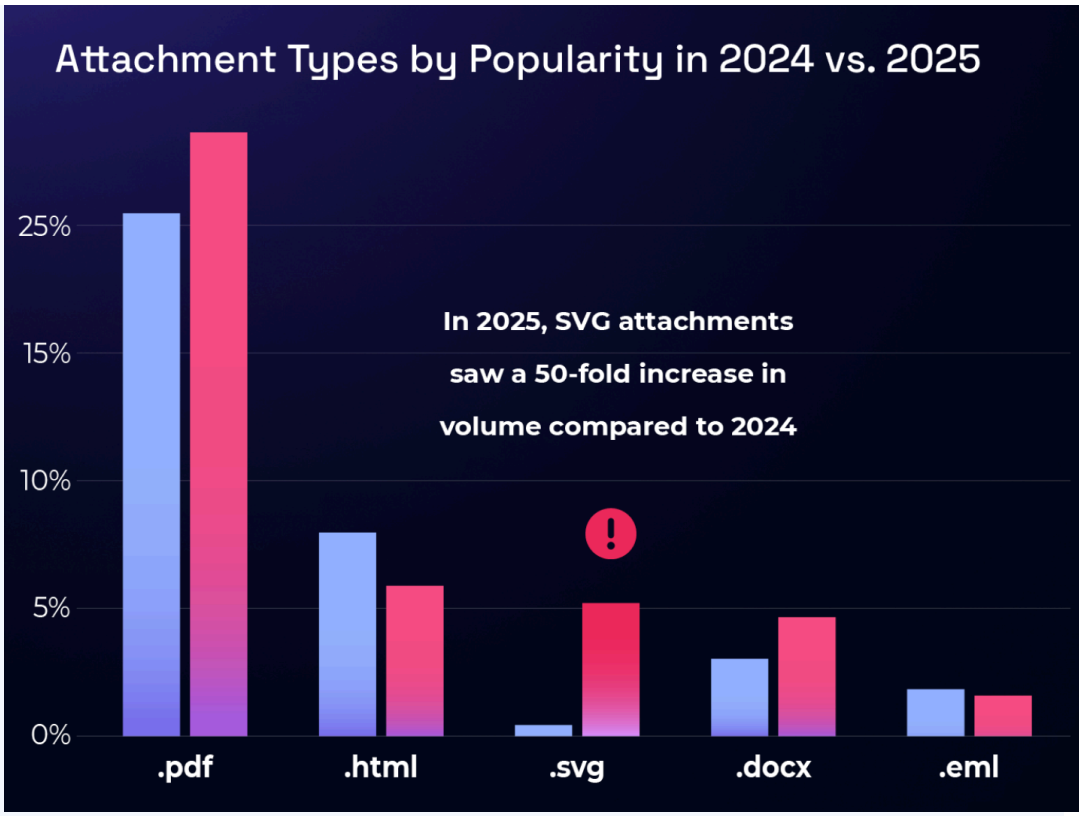
After holding steady at 1%-4% of all reported threats AI-generated phishing emails surged to 56% in December 2025 and dipped to 40% in January 2026.

Callback, maybe: The rise of callback phishing



Phone numbers are less likely to trigger alarms like attachments and malicious links will, which makes callback phish an attractive option.

Don't get attached: Malicious attachment trends



ATTACHMENTS & DELIVERY TACTICS

PDFs 24%: Still the most common at 1/4 of all malicious attachments

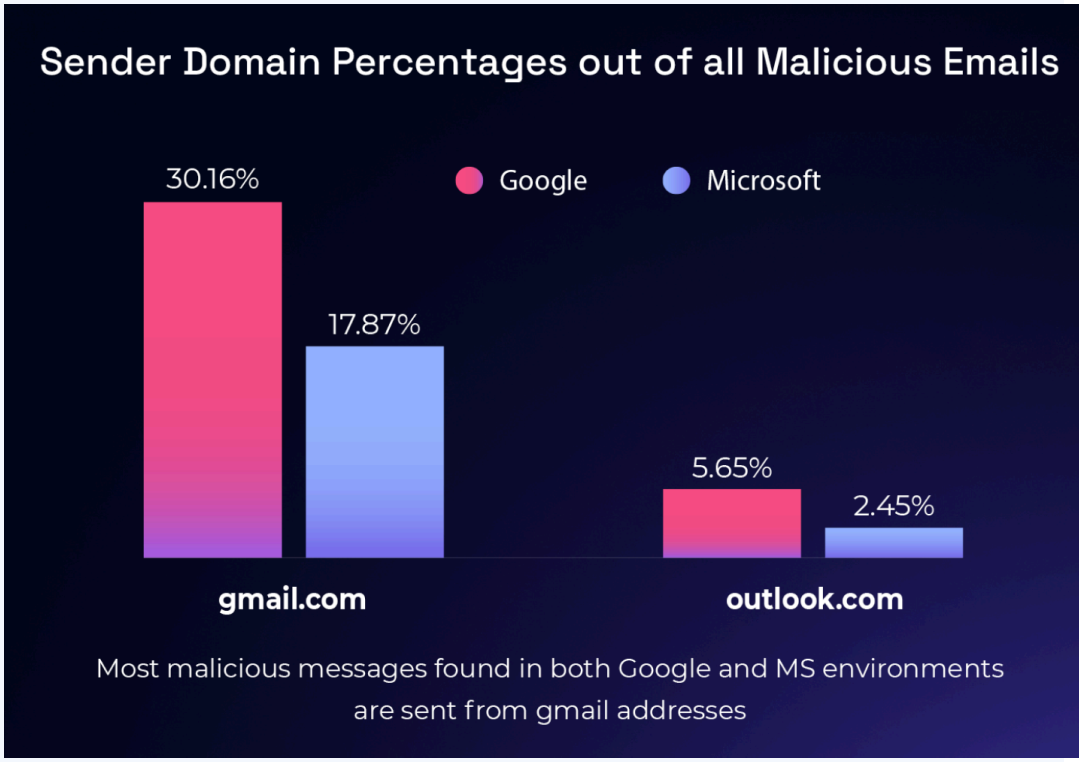
HTML fell by nearly half from 2024's 10% to 5.6% of all malicious attachments in 2025

24% failure rate on simulations of **surging malicious Calendar invites** (.ics), 4X the norm.

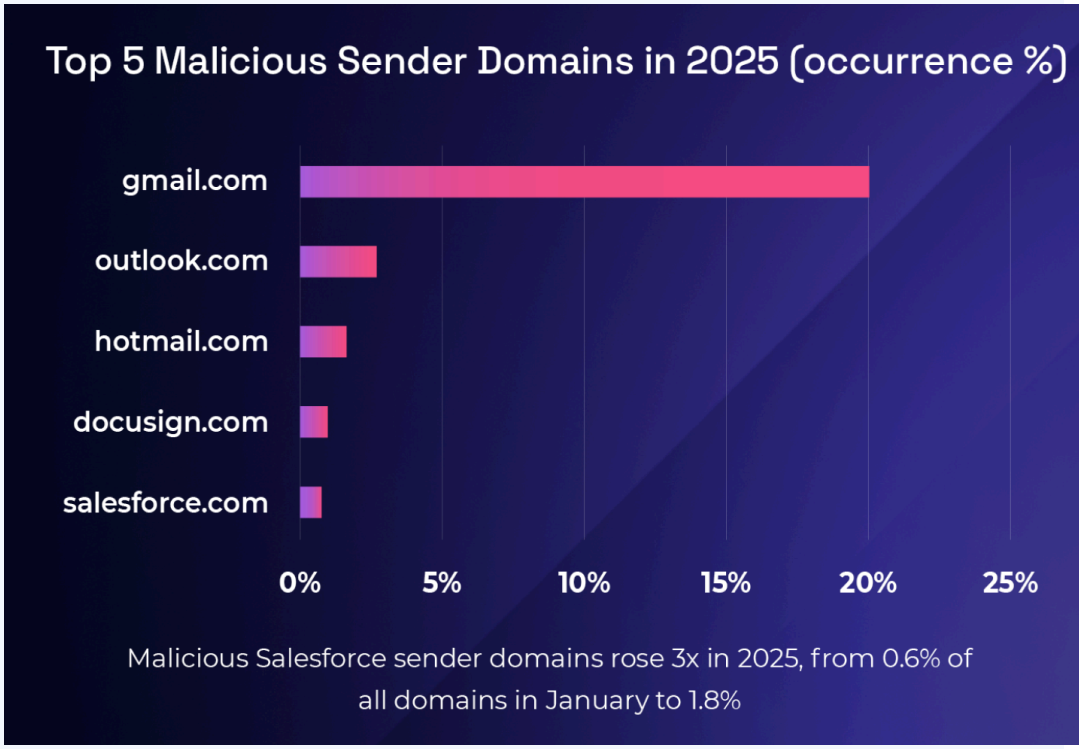
SVG files 50X surge in 2025

Malicious **QR codes declined** to under 2% of attacks in email bodies, but **re-surged hidden inside attachments, e.g. PDFs**

Google vs. Microsoft, and the top malicious domains



Most malicious messages found in both Google and MS environments are sent from gmail addresses



Malicious Salesforce sender domains rose 3x in 2025, from 0.6% of all domains in January to 1.8%

Part I: Phishing Trends & Statistics

Phishing is a multi-billion-dollar industry driven by an organized service model. Malicious actors use phishing-as-a-service tools that yield the greatest ROI with the lowest risk of getting caught. The technological barrier to entry is low, courtesy of easily available phishing kits.

Like any industry adopting a new technology, the disruption of cybercrime by AI was predicted to occur gradually and then all at once, as Clayton Christensen famously wrote about disruptive innovation.

Cheap, well-established phishing kits containing obvious errors continued to dominate the threat landscape until the end of 2025. But since December, AI-generated phishing campaigns have flooded inboxes with a **14x surge**, and now represent around half of all attacks reported by users.

So what do they look like? These mass campaigns are not deepfake agentic video calls or individualized spear phishing campaigns at scale.

Rather, Hoxhunt analysts observed traditional phishing campaigns becoming more polished throughout 2025, with improved grammar and slick graphics, aligning with the increasing availability and quality of generative AI tools. The landscape has shifted toward these polished lures while older templates are still in use, as detailed in the **Hoxhunt Cyber Threat Intelligence Report**.

Phishing attacks 2026

Business email compromise (BEC)	A staggering 64% of businesses report facing BEC attacks in 2024, with a typical financial loss averaging $150,000 per incident. These phishing attacks frequently target employees with access to financial systems, mimicking executives or trusted contacts.
Credential phishing	Around 80% of phishing campaigns aim to steal credentials, particularly targeting cloud-based services like Microsoft 365 and Google Workspace.

	With the growing reliance on cloud platforms, cyber attackers leverage realistic fake login pages to deceive users.
HTTPS phishing	An increasing number of phishing sites now use HTTPS to appear legitimate. In 2024, approximately 80% of phishing websites feature HTTPS, complicating detection for users.
Voice phishing (vishing)	Vishing attacks are growing in prevalence, with 30% of organizations reporting instances where threat actors used fake calls to impersonate officials or executives.
Quishing (QR code phishing)	QR code phishing attacks (quishing) increased by 25% year-over-year, as attackers exploit physical spaces like posters or fake business cards to lure victims.
AI-driven attacks	AI is powering phishing attacks, with deepfake impersonations increasing by 15% in the last year. These attacks often target high-value individuals in finance and HR.
Multi-channel phishing	Attackers are increasingly exploiting platforms like Slack, Teams, and social media. Around 40% of phishing campaigns now extend beyond email, reflecting a shift to these channels.
Government agency impersonation	Phishing emails mimicking government bodies such as the IRS or international tax agencies have increased by 35%. These often involve claims about overdue taxes or fines.
Phishing kits	The availability of ready-to-use phishing kits on the dark web has risen by 50%, enabling less sophisticated attackers to deploy high-quality phishing schemes.
Brand impersonation	Attackers frequently impersonate well-known brands like Microsoft, Amazon, and Facebook, leveraging user trust. For example, over 44,750 phishing attacks specifically targeted Facebook by embedding its name in domains and subdomains over the past year.

Stats above from TPro, Egress, UpGuard and Trend Micro News.



How much does phishing cost?

According to the 2024 IBM / Ponemon Cost of a Data Breach study, the average annual cost of phishing rose by nearly 10% from 2024 to 2023, from $4.45m to $4.88m. That's the biggest jump since the pandemic.

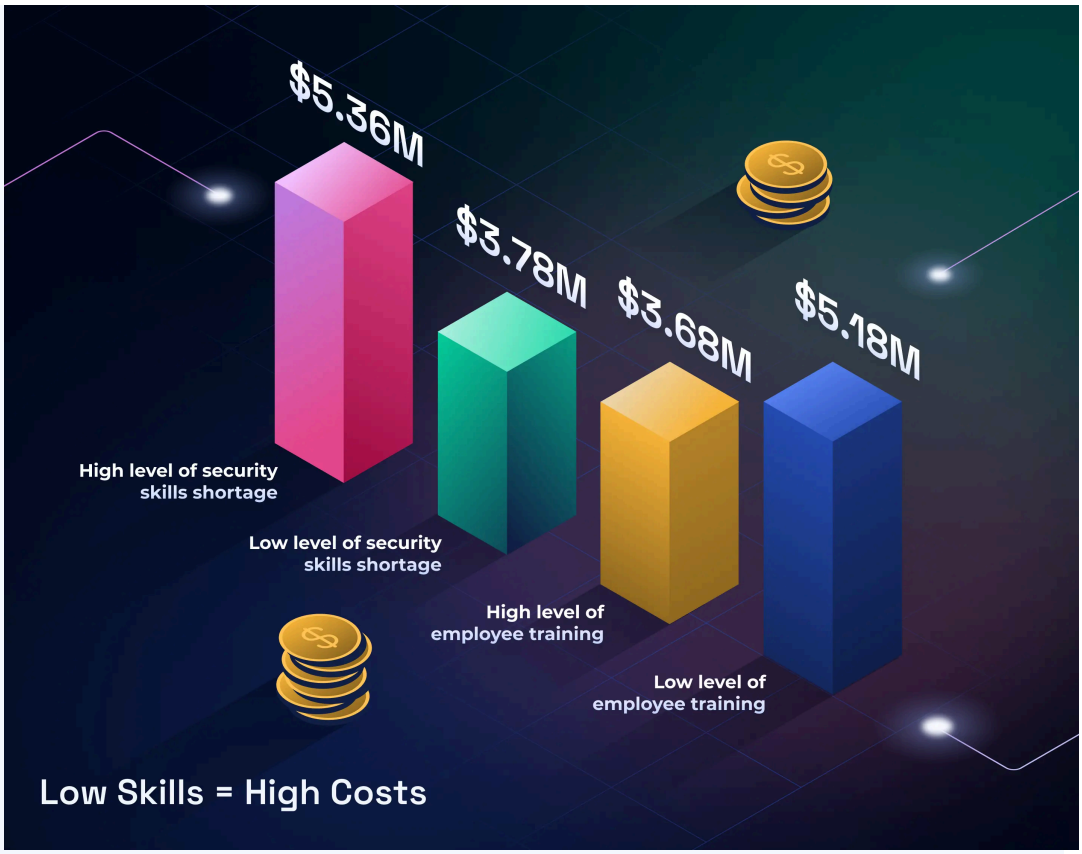
The IBM study reported the following costs:

- Phishing breaches: $4.88M
- Social engineering: $4.77M
- BEC: $4.67M

The above-listed categories of cyber security breach costs are all related to people-targeted attacks. BEC, social engineering, and stolen credentials often contain a phishing element.

Additionally, speed is essential. The report found a $1.2 million cost difference between breaches that were identified and contained before or after 200 days of initiation. The faster you can detect an incident, the faster you can limit the damage and prevent a catastrophic breach.

The same IBM study also found that poorly trained vs. well-trained employees were the biggest cost-amplifiers and cost-mitigating factors in breaches. Speed and skill in cybersecurity save companies millions.



And let's not forget the connection between ransomware, a form of encryption malware, and phishing. A survey by Statista found that ransomware infections were caused by:

- 54% Phishing
- 27% Poor user pactices / gullibility
- 26% Lack of cybersecurity training
- 14% Malicious websites

AI Phishing Campaign Incidence

Samples of phishing emails were observed in the Hoxhunt threat detection network in November, December, and January (2025–2026) and analyzed. In November's sample analysis, **4% of all reported phishing emails** had indicators of AI assistance in the email body or on the landing page.

In December, this proportion rose to **56%**. It decreased to **40% in January**.

November's sample size of phish was smaller than December's or January's but the **4% incidence** was consistent with the higher end of previous

monthly analyses. The **14x holiday surge in AI phishing attacks** was astonishing and aligned with anecdotal reports from security teams.

> *"AI is fueling a new era of social engineering tactics, but it can also be the white hat that helps us fight back. This report illustrates how AI-driven insights and automation can directly correlate higher employee engagement to reduced phishing risk."*
> – Pyry Åvist, Co-Founder and CTO, Hoxhunt



Methodology of AI Phishing Analysis

Samples of phishing emails observed in the Hoxhunt threat detection network in November, December, and January (2025–2026) were analyzed to determine what proportion of emails were possibly executed via generative AI.

The analysis focused on surface-level indicators of likely AI use in email-based phishing, as well as HTML-based hints in both email bodies and landing pages. This means the analysis does not capture more backend uses of generative AI such as reconnaissance or coding, nor how it might be used in voice phishing, deepfakes, or across other channels.

Clues of AI Assistance

The most common signs of AI-assisted phishing were generic templates impersonating a range of entities. Common elements included buttons, highlighted sections, headers, and footers.

The emails also contained HTML comments and generic section markers such as “Main Content” or “Click to Call,” embedded in the code and invisible to recipients but visible when inspecting the HTML. The repeated presence of these comments supports the assessment of AI-assisted template generation, as large language models commonly produce neatly structured HTML with descriptive labels.

Regardless of the impersonated entity, the emails shared several common elements, including:

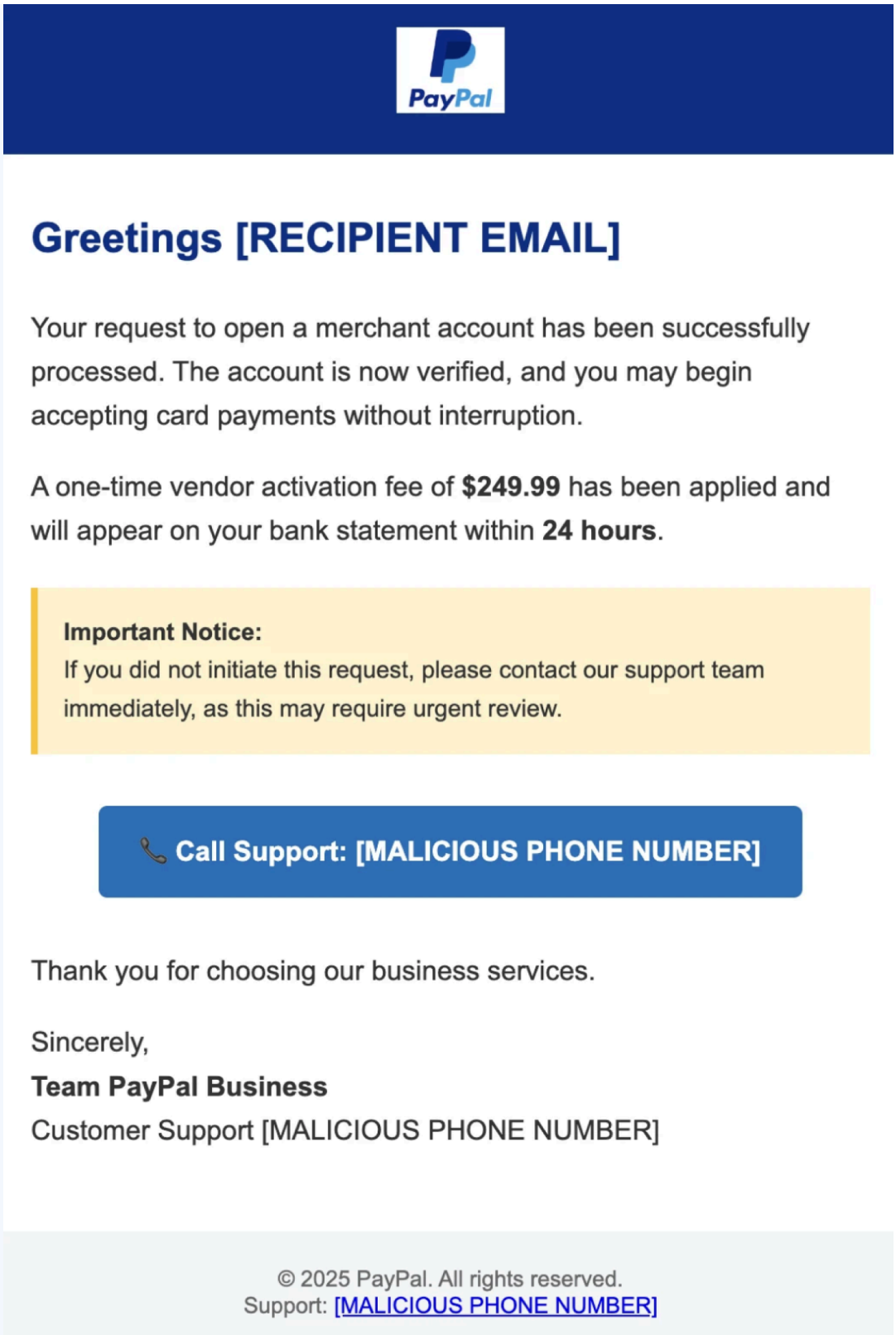
→ **Highlighted boxes** emphasizing the key issue or required action. The box usually included a thick left border in the same hue as the text, but a darker shade.

→ **Emojis emphasizing key actions**, such as:
“📞 Call Support…”
“🔎 See attached…”
“🔒 Secure documents…”

→ **Rounded corners** in buttons and boxes.

→ **Polished grammar and formal language.**

Depending on the impersonated entity, the emails were adapted to include brand colors and sometimes a brand logo.



Most Common Themes, Techniques, and CTAs

Deeper analysis of the likely AI-assisted phishing campaigns from November and December revealed the most common themes, techniques, and calls to

action used in the emails.

Themes

The most commonly observed themes were **fake offers and promotions, financial service impersonations, unpaid invoices, and HR impersonations.**

18.6% of AI-assisted threats promoted fraudulent offers such as free phones, car emergency kits, or airline rewards.

13.1% impersonated financial service providers, such as banks, insurance companies, or PayPal, often claiming the recipient must take action regarding security updates or available benefits.

8.3% included invoice lures, with impersonated parties ranging from career training consultants to supply chain partners.

8.2% impersonated HR teams, where the most common lures were related to performance reviews and salary updates (Figure 2).

Importantly, the popularity of these lures likely reflects the year-end timing of the sample campaigns, another reminder of the sophisticated timing and targeting of attacks.

Techniques

We found that **43.1% of the analyzed emails used links**, **11% used attachments**, and **20.3% used open redirects** to mask malicious links from both the human recipient and spam filters.

4.9% of the emails included a malicious phone number, indicating callback phishing campaigns (Figure 1).

The most commonly exploited emotion was **urgency**, for example claiming 24-hour deadlines for taking action (Figure 1, PayPal attack).

Other commonly exploited emotions included **greed and reward-seeking**, such as lures about increased benefits or recognition for performance from management (Figure 2, HR impersonation).

PERFORMANCE RECOGNITION

Annual Review Results

You Have Been Recognized

Dear [RECIPIENT FIRST NAME],

We are pleased to inform you of some exciting news.

Based on a review of performance data from the past year, our leadership team has identified you as one of our **top contributors**. Your hard work, positive attitude, and dedication have been acknowledged.

Your Recognition Package:

Bonus PTO Days	**+3 Days**
Wellness Credit	**$500**
Learning Budget	**$1,200**
Remote Work Upgrade	**Upgraded**
Performance Bonus	**Incorporated**

To review and activate your benefits package, please click the button below. The process takes approximately 2 minutes to complete.

ACTIVATE BENEFITS

> Please complete your enrollment by **January 16** to secure your benefits.

CONFIDENTIAL: This message contains sensitive information intended for [RECIPIENT FIRST NAME] only.

Thank you for being a valuable member of our team.

Best regards,
Human Resources Department

Calls to Action

The most commonly observed CTAs in the emails were:

- Clicking a malicious link
- Opening malicious attachments
- Replying to pretext messages

In other words, the CTAs were conventional. However, delivery mechanics (notably open redirects and occasional callback lures) indicate optimization for **reach and filtering evasion**, rather than innovation in user interaction.

Agentic Deepfakes and Spear Phishing: The Future of Social Engineering

The future of AI in social engineering attacks can be glimpsed through the work of a cybercrime “supergroup” formed in 2025: **Scattered Spider, LAPSUS$, and ShinyHunters**, who formed an alliance called **“The COM.”**

They specialize in highly targeted spear phishing campaigns equipped with **deepfake voice and video capabilities** for initial access, followed by malware or ransomware payloads.

Examples of their work include:

- The MGM casino breach
- The Jaguar / Land Rover breach
- High-profile breaches involving Salesforce
- Attacks against airline, retail, and financial companies

However, these attacks are **not yet representative of the AI-powered mass phishing campaigns** typically hitting employee inboxes.

The COM’s techniques still require human social engineers to make phone calls and target SSO platforms such as **Okta** to gain system access.

But just as we waited for AI-generated emails to emerge at scale, we are monitoring closely for **agentic spear phishing** to become the new normal.

GenAI and Automatic Personalization

Hoxhunt analysis shows that **AI-enabled automatic personalization is already fairly common**, but it is **not very good yet**.

These error-prone auto-personalized phishing templates use placeholders for target details (similar to spam marketing emails sent to large contact lists). When the replacement process fails, leftover placeholder text reveals how the campaigns are constructed.

Instead of simply showing a blank or an email address, these malicious templates sometimes expose internal variables such as:

“##victimdomain##”

This unsubtle placeholder exposes the attacker’s intent and raises obvious red flags, even for untrained users.

In 2025, we observed **no decline in placeholder artifacts**, suggesting that GenAI phishing **has not yet mastered personalization**. That is likely to change.

Callback Phishing

Callback phishing refers to phishing emails that include a fake alert (such as an invoice, subscription renewal, or security warning) that urges the recipient to **call a malicious phone number**.

Unlike malicious links or attachments, phone numbers typically **do not trigger filtering solutions**, allowing more callback phishing emails to bypass technical defenses.

During the call, attackers use social engineering to trick the recipient into:

- Sharing credentials
- Installing malicious software
- Making fraudulent payments

Industry data highlights the growing scale of this technique:

→ **500% increase in callback phishing campaigns in Q4 2025** (VIPRE Security Group)
→ **43% of BEC attacks contain a callback phishing lure** (LevelBlue, formerly AT&T Cybersecurity)

A Hoxhunt analysis of callback phishing campaigns from **October 2025 to January 2026** revealed the most common themes and emotional triggers used in these emails.

Callback Phishing Themes

The most commonly observed theme was **financial service impersonation**, including brands such as **PayPal, Venmo, and Bank of America**.

Most often, victims were threatened with a **bogus charge for an order they never placed**, unless they called the malicious number.

The second most common theme was **invoice phishing**, including:

- Fake subscription renewals
- Expiring subscription notices
- Fake order confirmations
- Unpaid invoice claims

Impersonated brands included **McAfee, eBay, and Zelle**.

27.1% of callback phishing emails were classified as financial service impersonations, while **26.6% were invoice-themed.**

Other themes included:

- HR impersonations
- Security alerts
- Suspicious login warnings
- Account verification requests

Most-Impersonated Entities and Domains

Our most widely used and trusted services tend to be the **most frequently spoofed by threat actors**.

Familiar brands make attractive phishing lures because **our guard naturally lowers when we see messages from services we trust**.

The Big 3: Microsoft, Docusign, and HR Impersonations

In the most popular **Microsoft impersonations**, the recipient is told that their account or multi-factor authentication is expiring. They are warned that unless they follow the attacker's instructions, such as clicking a link or downloading a file, they will lose access to their account.

In **Docusign impersonations**, recipients are often asked to review and sign documents. Sometimes attackers provide no details about the "document," while other times they claim it comes from a company administrator and may include alarming language such as "termination." Docusign has introduced a service that allows users to verify suspicious messages by forwarding them to **verify@docusign.com**.

In **HR impersonations**, recipients are most commonly asked to review salary updates or vacation plans, which arouse curiosity. HR communications often contain emotionally charged messaging around time-sensitive actions, benefits, or potential consequences. These elements are frequently exploited in phishing email campaigns.

Most-Spoofed Domains

In 2025, **gmail.com accounted for 20% of sender domains** in malicious emails, compared with **2.8% for outlook.com**, the second most popular origin domain.

Two factors likely contribute to Gmail's popularity with attackers:

- Gmail accounts are free and easy to create
- Google offers a single free consumer domain, while Microsoft distributes usage across multiple domains such as Outlook, Hotmail, and Live, including regional variants

	Microsoft	Google
% of reported emails confirmed malicious	34.7%	12.1%
Frequently observed domains	Third-party services such as docusign.net and salesforce.com	Campaign-specific domains were more common.
Top two sender domains of malicious emails	gmail.com **17.9%** outlook.com **2.5%**	gmail.com **30.1%** outlook.com **5.7%**

Most phishing emails come from gmail, regardless of the recipient's email environment.

Frequently Observed Domains

→ **Microsoft tenants:** Malicious emails often leveraged third-party services such as **Docusign** and **Salesforce** as part of the attack path.

→ **Google tenants:** Malicious emails more frequently used **campaign-specific domains** created primarily for a phishing or scam campaign.

Top Sender Domains of Malicious Emails

Microsoft tenants

- gmail.com – **17.9% of confirmed malicious emails**
- outlook.com – **2.5%**

Google tenants

- gmail.com – **30.1% of confirmed malicious emails**
- outlook.com – **5.7%**

Most malicious emails in both ecosystems are sent from the **"Big 2" email providers: Google and Microsoft**.

Discrepancies between confirmed malicious emails in Google and Microsoft environments may result from:

- Differences in spam filtering solutions
- Environment-specific phishing campaigns
- Variations in users' training tenure and reporting skills

Beyond the top domains, malicious emails originate from a variety of sources including:

- Other free webmail services (e.g., **hotmail.com**, iCloud)
- Compromised accounts
- Misused third-party services

Recruitment Scams

Hoxhunt found that **recruitment scams have ascended as a major new threat**, primarily targeting employees in sales and marketing departments with the allure of a better job at a prestigious company.

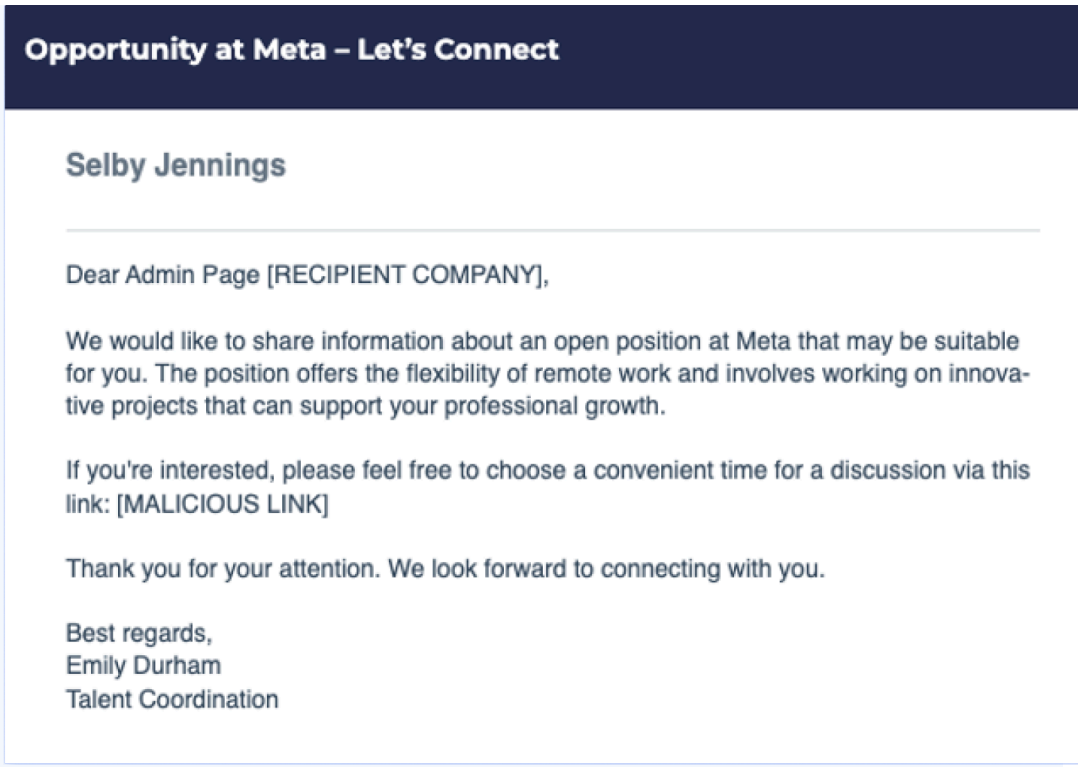
Campaigns have impersonated brands such as **Google, Coca-Cola, and Meta**, targeting marketers and social media administrators with fake job listing lures.

Targets are selected through **open-source intelligence gathered from social media profiles**. Recipients receive a personalized phishing message that directs them to a landing page impersonating **Calendly**, where they are prompted to authenticate using **Facebook**.

The attacker's goal is to trick the victim into signing up for an interview slot using a **Browser-in-the-Browser (BitB) credential harvester**, which displays a fake Facebook login window.

If credentials are entered, attackers may gain access to:

- Personal Facebook accounts
- Organizational social media accounts



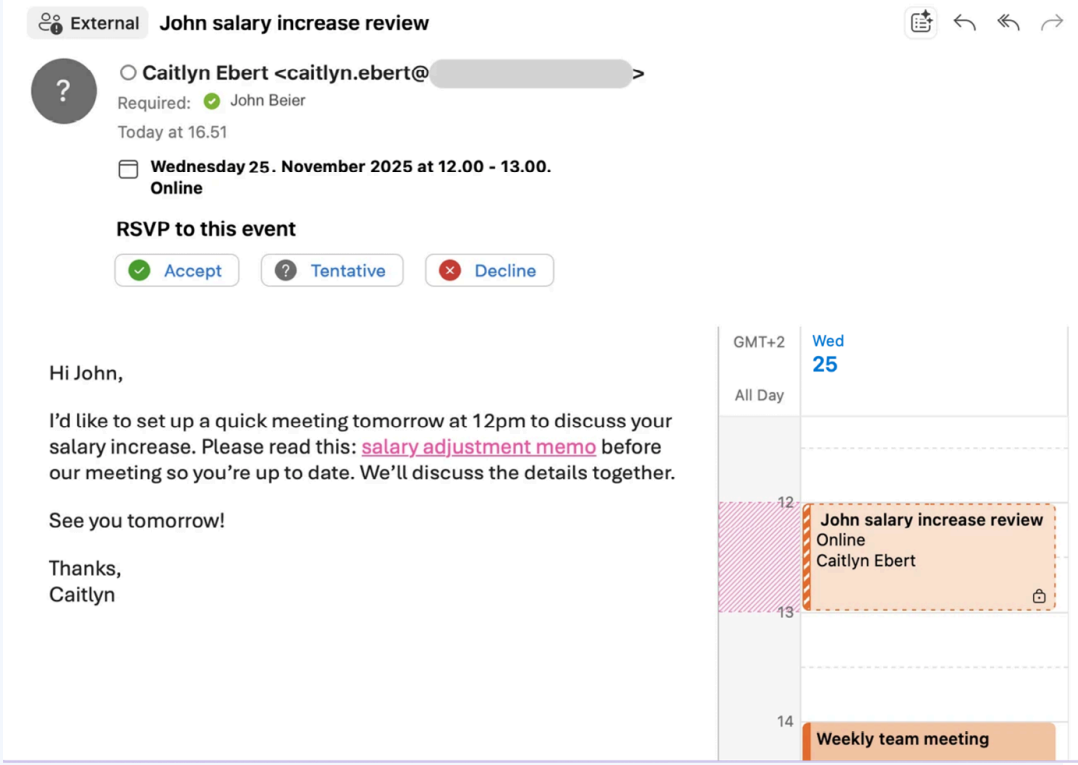
Malicious .ics Calendar Invites: Four Times More Dangerous

Hoxhunt monitored a surge in phishing attacks using **.ics calendar invite files**.

Following a spike in these attacks in late 2025, Hoxhunt quickly created phishing simulations using calendar invites. The results were concerning: **failure rates were 4–6 times higher than the global baseline**, reaching **24%**.

Attackers send phishing emails containing **.ics files**, a standard format for calendar invitations used by applications such as Outlook.

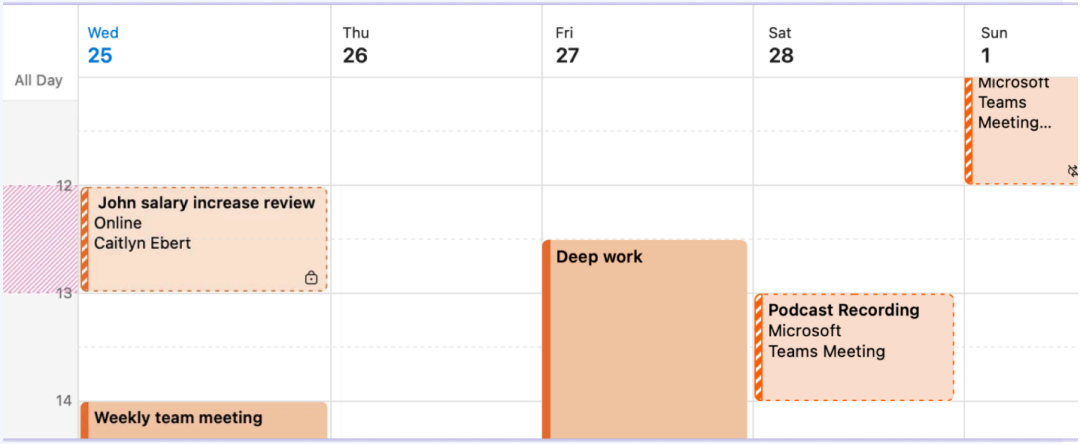
Many email environments automatically interpret these files as events and add them directly to the user's calendar when the email arrives.



From there, attackers rely on the user's routine behavior:

When you see a new meeting on your calendar, you naturally want to check the details. These invitations often appear legitimate, but the meeting links or attachments included in the event are malicious.

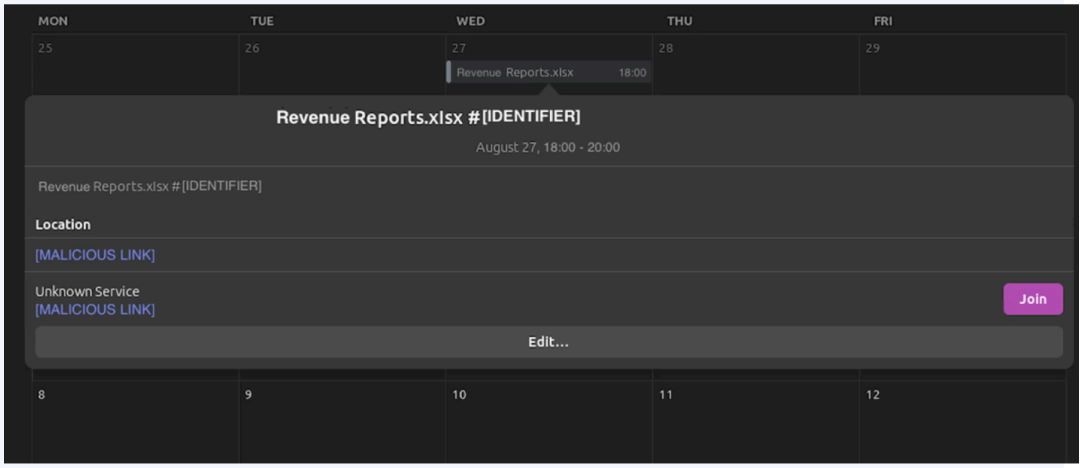
In some cases, reporting the suspicious email **does not remove the event from the calendar**. Most security tools and reporting buttons focus on email messages, not calendar objects.



Malicious calendar invites therefore **double the attacker's chances of success**. Even after reporting the email, users may forget about the calendar event itself.

Hours or days later, a user might notice the event and wonder, “What meeting was this again?” Calendar reminders may also trigger notifications, increasing the chance that the user clicks the malicious link.

For this reason, **the calendar event must be deleted separately**.



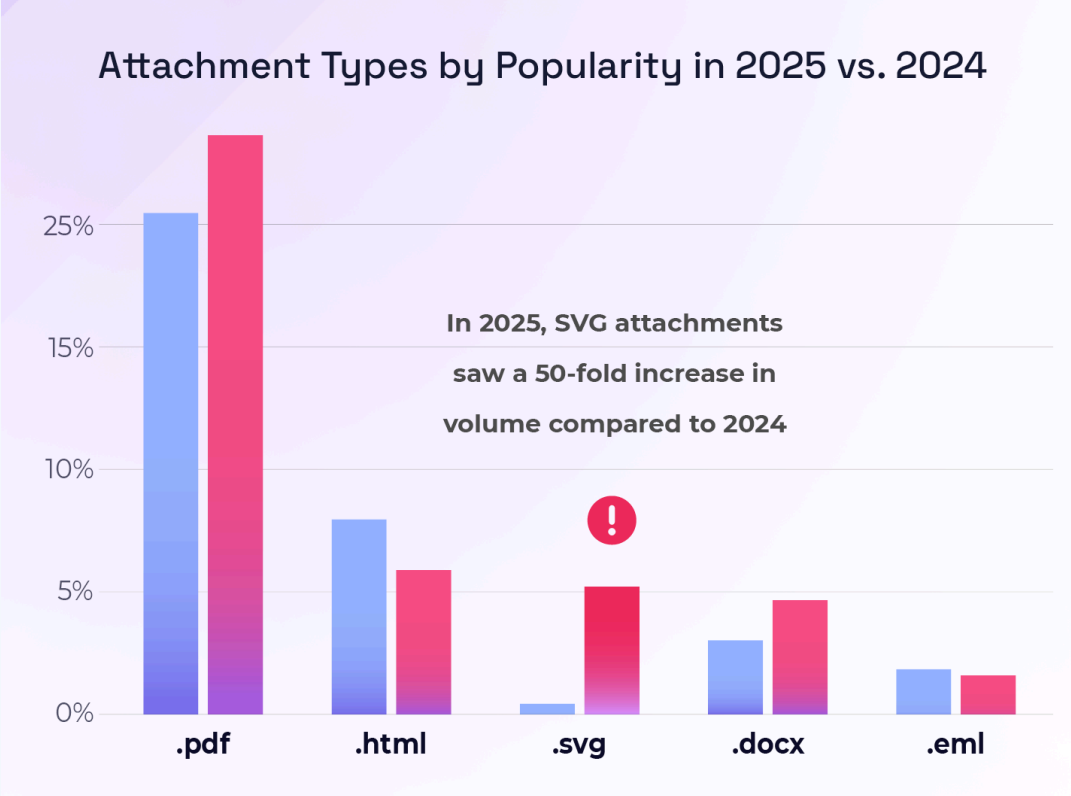
Attachment Types

In 2025, **PDF attachments remained the most common malicious file type**, accounting for **23.7%** of malicious attachments in the first half of the year.

These PDFs included:

- Fake invoices with fraudulent payment details
- Fake Europol letters
- Documents containing embedded links or additional attachments leading to credential harvesters

PDFs likely remain popular because they **bypass filters more easily and appear trustworthy to users**.



Malicious SVG Files

In 2025, malicious **SVG files increased fifty-fold compared to 2024**. They comprised 5% of all malicious attachments, the third most popular malicious file type and slightly second-lace HTML attachments.

SVG files appear to be harmless graphics but can bypass many anti-spam email tools, making them an attractive technique for attackers.

As of September 2025, **Microsoft stopped displaying inline SVG images** to mitigate increasing misuse such as cross-site scripting (XSS) attacks. However, **SVG attachments are still supported**, allowing the technique to persist.

Other Attachment Types

In 2025:

- **HTML attachments** ranked second at **5.6%**, down from **10% in 2024,** but still slightly ahead of third-place SVG files, which comprised 5% of malicious attachments**.**

- **Microsoft Word documents** accounted for **4.4%** of malicious attachments
- **EML files** accounted for **1.4%**

Other attachment types ranged from image files (such as fake invoices) to executable files.

However, because emails reported to Hoxhunt have **already bypassed email filters**, executable files, which are typically blocked by security systems, do not represent a significant portion of the dataset.

Impersonation campaigns leverage trusted brands

Our most used and trusted services tend to be the most-spoofed by threat actors. Familiar services make for attractive phishing lures because our guard lowers when we see a message from them.

Top 3 most-impersonated entities

- Microsoft
- Docusign
- Human resources

In the most popular **Microsoft impersonations**, the recipient is told that their account or multi-factor authentication is expiring. The recipient is told that unless they do as the attacker says - click a link or download a file - they will lose access to their account.

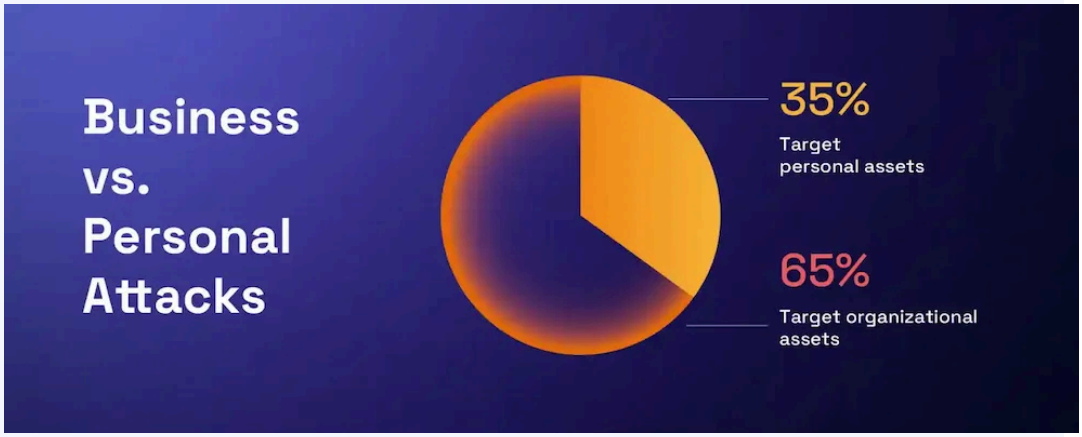
As for **Docusign impersonations**, the recipient is often asked to review & sign documents. Sometimes cyber attackers give no details about the “document”, and other times they may claim that it is coming from a company administrator. They might include words like “termination.”

In **HR impersonations**, the recipient is most commonly asked to review salary and vacation plans, arousing curiosity. HR comms often contain emotionally charged messages about e.g. time-sensitive actions that must be taken, benefits, and consequences; all common elements of phishing email campaigns.

Campaign targets: Mostly business. But sometimes, it's personal

The proportion of phishing attack targets varied between personal and organizational assets. Reasons for the variation are unclear, although the summer uptick in personal campaigns might indicate that threat actors are adjusting to summer vacation season.

- 2/3 of attacks target organizational assets.
- Typically, these cyber threats are credential harvesters and fraudulent invoices.
- 1/3rd target personal assets such as financial information.
- Common themes include postal service or financial institution impersonation.



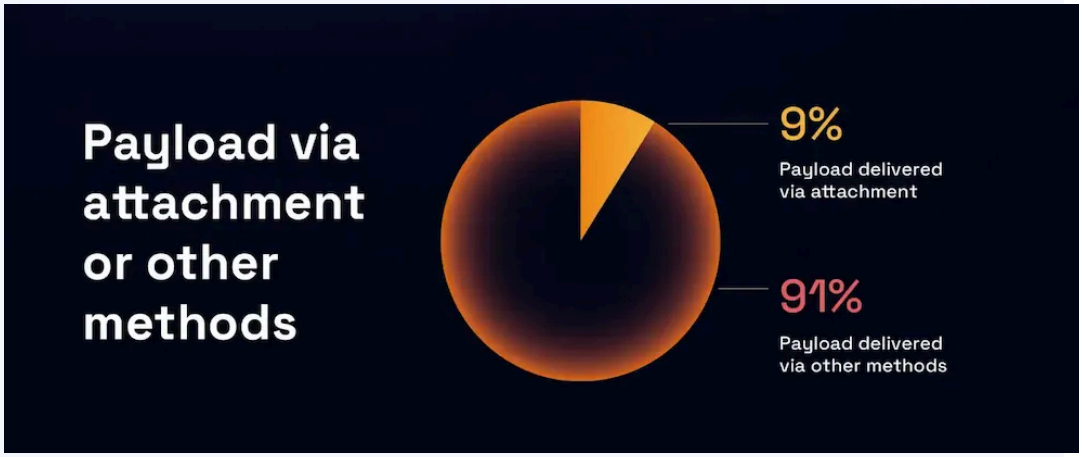
Malicious attachment campaigns

According to the 2024 Verizon DBIR, 94% of malware is delivered through email attachments. Malicious messages with attachments may contain a malware payload in the initial attachment, or a credential harvester or, more likely, lead users to the next step in a scam, where the ultimate payload might for example be:

- A credential harvesting site
- Malware
- A complex phishing scam with further social engineering across multiple channels, such as a phone call or video conference with an imposter
- A ruse to dupe people into handing over their multi-factor authentication (MFA) credentials

Of attacks that bypass email filters:

- Only around 10% of malicious payloads are delivered as attachments, and around 90% of the attachments contain deceptive links leading to a further payload, such as malware attacks or credential harvesting.
- The other 10% of attachments contain further social engineering, with the goal of further engagement from the recipient.



Malicious attachment campaigns are a common phishing technique because of their success.

Attachments arouse curiosity, and to the untrained email user, it can be hard to resist seeing what's inside.

Malicious attachment simulations: a success story

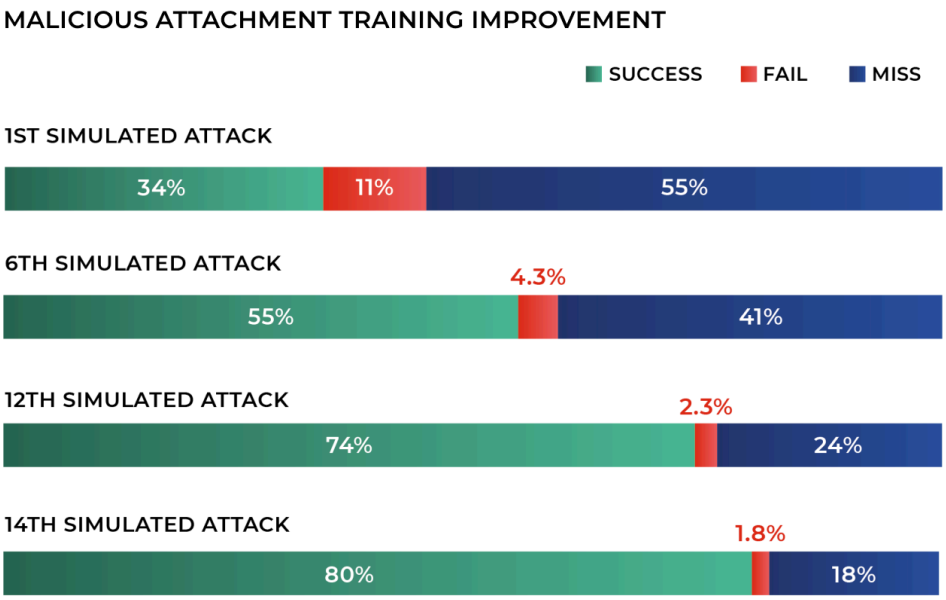
Even our training data reveals how dangerous malicious attachments can be relative to other phishing techniques.

And, interestingly, the training data reveals an important success story around malicious attachments. Behavior change on these particularly challenging phishing attacks is especially pronounced; reporting rates and malicious clicks decline significantly compared to other types of simulated attack types.

Before training, only 34% of users successfully report these phishing simulations, while an alarming 11% fail by opening the attachment or clicking a malicious link.

Failure rates are sliced by by 2.5 times within 6 months of phishing training. And after 12 months of phishing training, Hoxhunt sees success rate more

than double from 34% to 74% at 12 simulations, and climbs to 80% after 14 simulations.



Failure rate, meanwhile, plummets by 5.5x from 11% to below 2%.

The global averages for general success and failure after 12 months of training is 67% and 3% respectively.



The notable improvement in users at spotting and reporting simulated malicious attachments shows the impact of adaptive phishing training. With regular practice, people quickly learn to be instinctively suspicious of emails with attachments.

Part II: Phishing Training Performance Statistics

> “What we found was remarkable. When we examined the reporting rate of phishing emails, we found that users who had more recent training reported phishing emails at a significantly higher rate—about **21% against a base rate of 5%**, a **four times relative increase**.

> Given those results, the long-term strategy becomes **incentivizing employees to report**, and ensuring those reports are **as automated as possible in your workflow** in order to help block offending emails and links.”

> **VERIZON DBIR 2025**

A founding principle of the **Hoxhunt security behavior change model** is that a **threat report is the ideal outcome of a social engineering attack**. Reporting is therefore the key behavior to focus on in a training program.

It is encouraging to see these principles becoming more widely accepted across the industry. Similar sentiments are expressed in the **Verizon DBIR 2025**.

The **Verizon DBIR in 2024 and 2025** calculated a global benchmark for users who report phishing simulations at **around 20%**. While the participants and conditions of that benchmark are not entirely clear, the **20% reporting rate is encouraging** and higher than what many organizations might expect.

Most phishing simulations today are still delivered through **compliance-driven security awareness training (SAT)** programs.

Hoxhunt data shows a **roughly 10% reporting rate** among users engaged in quarterly SAT programs.

Threat reporting rates above 20% are typically associated with organizations that have implemented a **behavior change program and developed a mature security culture.**

More engagement unlocks cyber behavior improvement

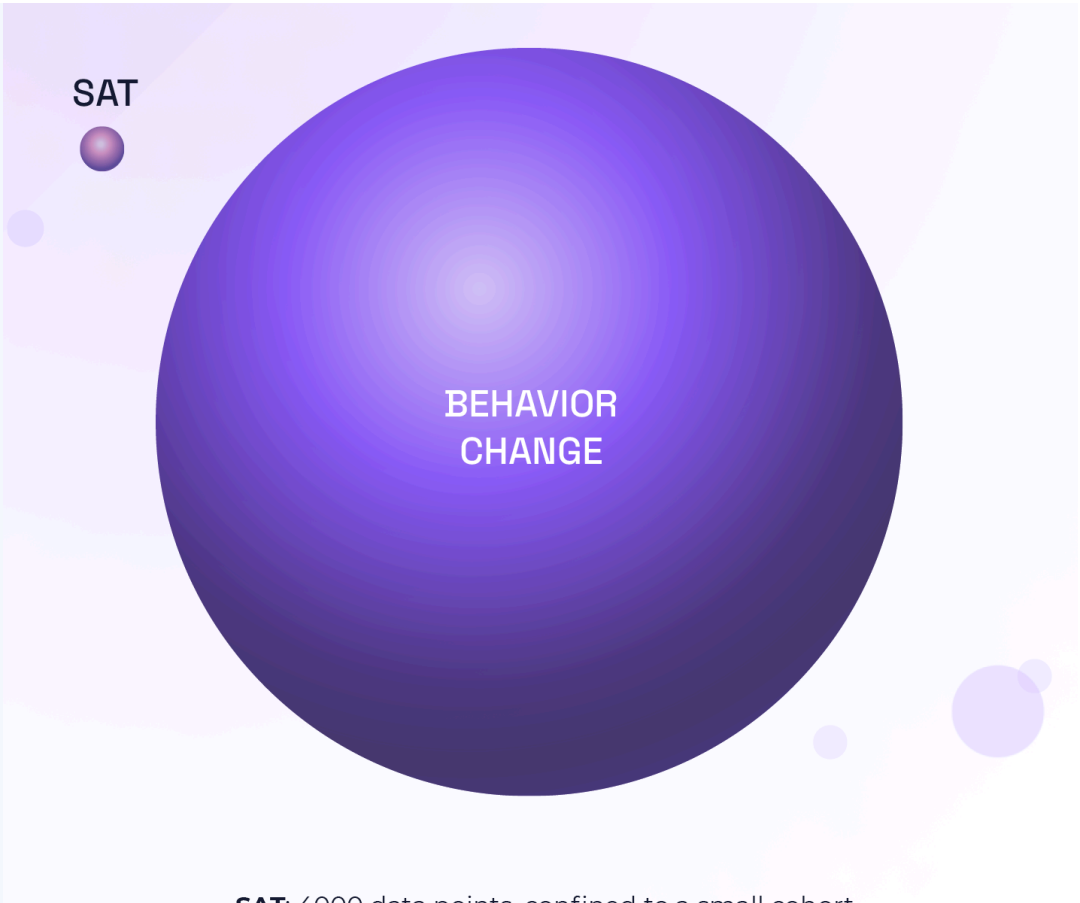
Behavior-based cyber training engagement unlocks peak cyber performance and reveals critical insights for human risk management. When employees are disengaged, exponentially fewer data points are available, especially when the primary SAT metric is **phishing simulation failure rate alone**.

In a hypothetical **10,000-person company**, the difference becomes clear.

An SAT tool that produces a **10% engagement rate** with **four simulations per year**, compared with a **security behavior change program (SBCP)** achieving a **50% engagement rate** with **36 simulations per year**, produces dramatically different levels of insight:

Quarterly SAT: 4,000 behavioral data points
SBCP: 180,000 behavioral data points

Moreover, high simulated threat reporting rates allow organizations to estimate with confidence the **actual incidence and deterrence of real phishing attacks** arriving in employee inboxes. The importance of this can't be overstated. When you have a security stack that is designed to unify simulated and real threat reporting outcomes, security teams can stop guessing and start making data-driven decisions on what threats to prioritize, and how.



SAT: 4000 data points, confined to a small cohort
Behavior Change: 180,000 data points, representing a statistically significant cohort

High simulated threat reporting rates let us estimate with confidence the actual incidence, and deterrence, of real phishing attacks that arrive in inboxes.

The Verizon DBIR for the first time in 2024 calculated a global benchmark for users who reported a phishing simulation: 20%. The participants in, and conditions of, that benchmark test aren't clear, but the 20% reporting rate is higher than what we'd expect.

Most phishing tests are part of compliance-driven security awareness training (SAT). Hoxhunt data shows a roughly 10% reporting rate by users engaged in quarterly SAT.

Elevated threat reporting rates above 20% are typically the result of a behavior change program and a mature security culture.

Global impact of adaptive phishing training for employees

The data after implementing Hoxhunt shows improvements in every relevant metric, from simulated phishing failure and success rates, to dwell time and real threat detection:



- **9x rise in simulated threat reporting**: Most programs neglect threat reporting and most users lack the knowledge, skills, and tools to report suspicious messages.
- **10X rise in real threat detection:** Nothing supports the value of training like a surge in real threat detection.
- **Median dwell time 1/3 faster**: Dwell time is the time elapsed between a phishing email landing in an inbox and a user reporting it. In cybersecurity, time is essential for mitigating risk.
- **Fastest 5% report threats in 39s**: the fastest 5% of reporters keep the whole organization safe by being the lighthouse that illuminates threats immediately, helping the SOC eliminate phishing campaigns from the system in minutes, rather than days.

- **2/3 report a real threat within first year**: There is no better proof of phishing training's real-world impact than a majority of users reporting real threats.

Training performance improvements over time

The standard, pre-Hoxhunt SAT performance baseline is 7% Success, 20% Failure, and 80% Miss rates (the figures don't add up to 100 due to separate data sets). Many enterprise organizations with legacy SAT models often have stagnant Success rates of about 10%, with limited visibility into real threat reporting and dwell time.

These metrics all drastically improve once onboarded with Hoxhunt and steadily improve over time, demonstrating sustainable engagement and resilience.

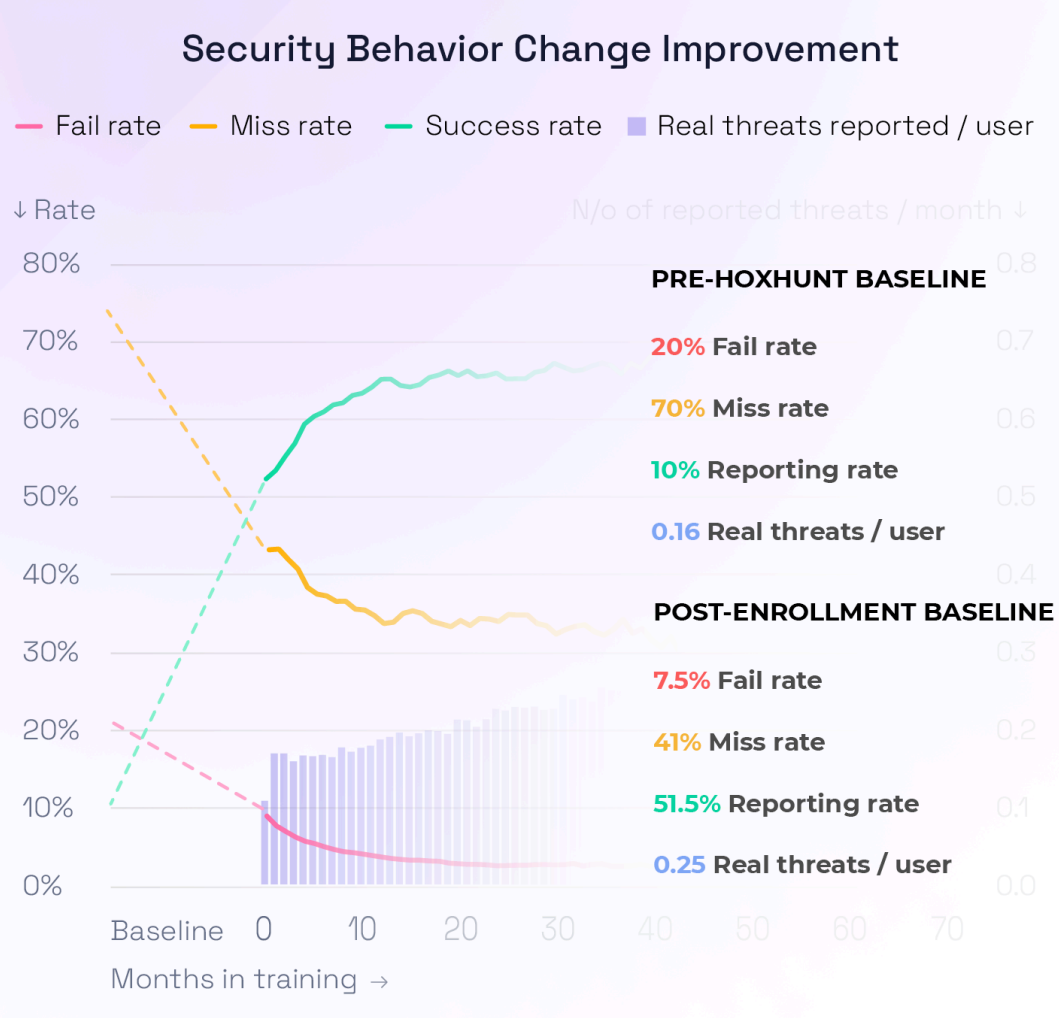
The below graph charts dramatic improvement that is the product of training that includes:

- AI-enabled customization
- Automatically adaptive training that adjusts to user skill and background level
- Gamification: Participation is rewarded and traced along a skills-building learning journey that invites healthy competition with other colleagues
- People-first
- Reward-based
- A dedicated Customer Success team that gets the program on track, and ensures it stays on track.

The blue histogram charts real threats detected, which is typically negligent or not tracked before organizations switch to Hoxhunt.But during onboarding with a security behavior change program, a phase change in threat reporting behavior occurs.

- Behavior-based engagement soars by over 6x.
- Failure rates are cut in half. And that's just with the onboarding.

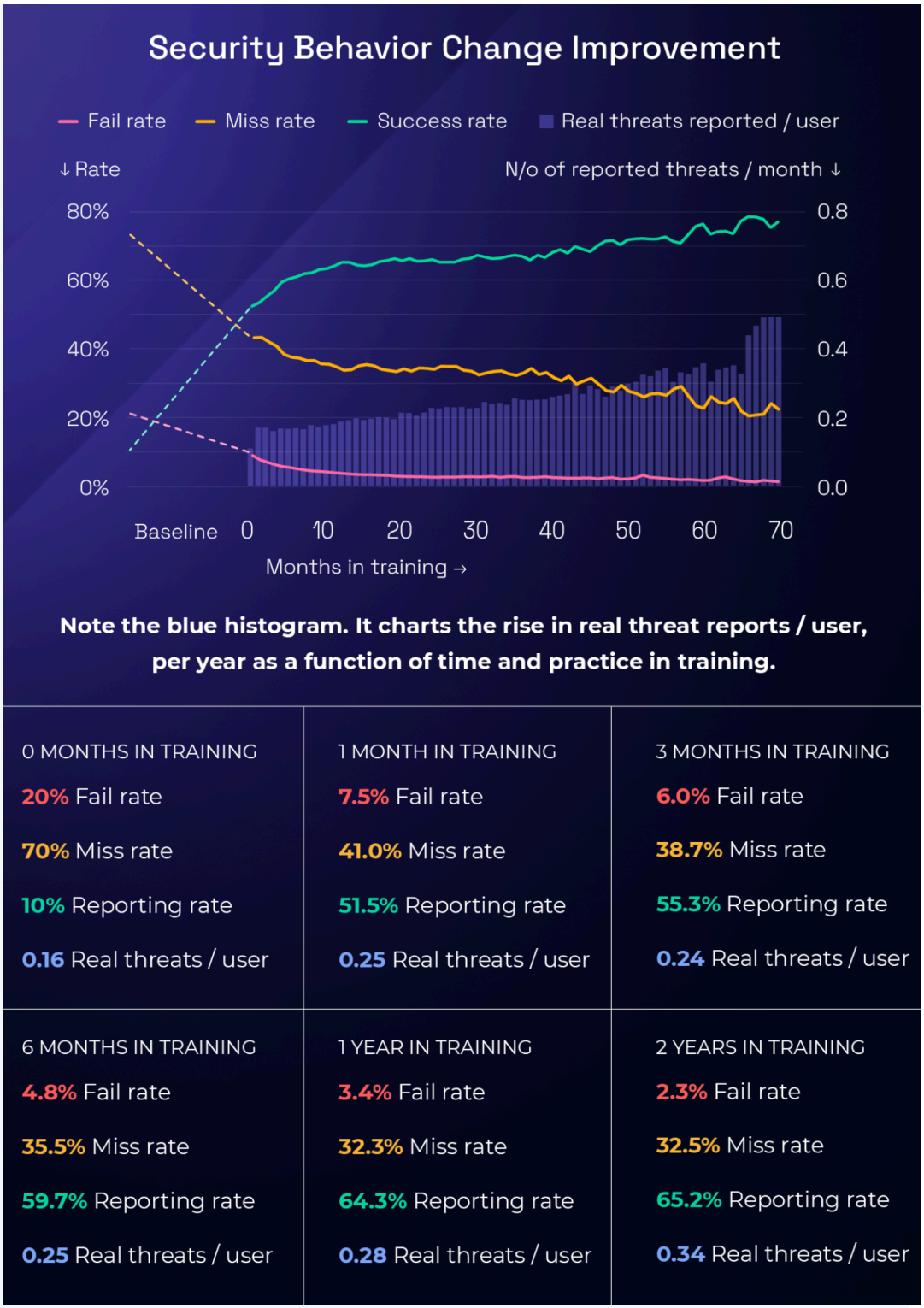
During onboarding, users are given a simple tool embedded in their email client to report phishing simulations. They learn how to use that tool while learning how to spot phishing attacks in gamified micro-trainings, along with communication from the security awareness manager.



Phishing simulations are sent every 10 days. They are designed via the adaptive learning model to get harder as the user's skill level improves. Notably, failure rates still continue to drop while threat reporting rates continue to climb.

Users stay engaged for years on end as the difficulty level of the training remains just hard enough to give people a sense of accomplishment with every threat report.

And those gains are locked in by the platform's Instant Feedback on real threat reports so people know immediately the impact they've made on their org's security.



Real threat detection rate improvements, when mapped to training performance improvements, prove the value of training. The percentage of users who have reported at least one real threat since the start of their training improves over time as thus:

Real threat detection improvement by organization

- 0 Months in training: 13%
- 1 Month in training: 26%

- 2 Months in training: 34%
- 6 Months in training: 50%
- 12 Months in training: 64%
- 24 Months in training: 71%

There is no better proof that training is making a real-world impact than an increase in real threats detected. The parallel rise in simulated and real threat reporting shows a powerful correlation between training performance and real-world impact. Half of employees report a real threat 6 months into training. 2/3 of employees report a real threat within one year of beginning training.

> *"With phishing simulation engagement rates reaching above 60 percent and failure rates dropping below 2 percent, Hoxhunt has helped us push our resilience into new territory, and surpass anything our legacy SAT tools could deliver."*
>
> – **Ryan Boulais**, VP & Chief Information Security Officer at Bunge

Cyber performance Success / Failure rate benchmark by industry

Industry	Reporting Rate (%)	Reporting Rank	Miss Rate (%)	Miss Rank	Fail Rate (%)	Fail Rank
Financial Services	66.4	1	31.5	1	2.04	1
Oil & Energy	64.6	2	33.1	2	2.31	2
Government	64.0	3	33.5	3	2.51	4
Utilities	59.5	4	37.6	4	2.84	7
Manufacturing & Construction	57.6	5	39.5	5	2.81	6
Entertainment	57.5	6	40.1	7	2.39	3
Legal & Business Services	56.9	7	39.8	6	3.33	12
IT, Software & Internet	56.7	8	40.2	8	3.12	10
Logistics & Supply Chain	56.4	9	40.6	9	2.96	9
Media Production	55.2	10	41.9	11	2.87	8
Travel & Tourism	54.1	11	41.7	10	4.18	14
Pharma & Healthcare	52.4	12	44.3	13	3.31	11
Retail	50.7	14	46.7	15	2.54	5
Education	50.1	15	44.2	12	5.72	15

There are signifiant differences between cyber performances by industry after one year of training. It's critical to target training to the factors that influence industry cyber performance, because that is exactly what attackers do. They understand, for instance, that hospital workers and retail professionals have high stress jobs that require rapidly switching between computer work and interactions with humans in situations that are naturally urgent. Government employees may be attacked with emails spoofing their bosses, whose personal details and schedules may be more easily obtained online for spear phishing attacks.

We can also see how certain departments tend to respond to training. The 0-month baseline is post-rollout with Hoxhunt, and factors in employees who have been enrolled in training and interacted with the first training experience.

Success Rate Improvement by Industry

Months in training	0	6	12
Financial Services	48%	69%	74%
Government	55%	68%	70%
IT, software, internet	54%	62%	66%
legal, professional, business services	49%	61%	64%
Logistics, supply chain	53%	63%	69%
Manufacturing, constuction	48%	64%	67%
Oil & energy	57%	68%	70%
Pharma & healthcare	52%	60%	62%
Retail	40%	58%	61%
Global Success rate	47%	63%	67%

Takeaways

- Global success rate goes up as months in training increase.
- FInancial services has the highest success rate after 12 months, at 74%, and healthcare and retail have the lowest, with 62% and 61% respectively
- The lower success rate for healthcare and retail may be due to the nature of the industries, as the employees spend less time on their computers and more time interacting with people in intense situations. This also leaves less time for going through emails and interacting with training.
- Note: with Hoxhunt adaptive training model, difficulty level of simulations increases over time

Failure rate improvement by industry



Months in training	0	6	12
Financial Services	4,6%	2,9%	2,1%
Government	6,4%	4,0%	4,2%
IT, software, internet	6,2%	4,2%	3,3%
legal, professional, business services	7,1%	5,0%	3,6%
Logistics, supply chain	3,8%	4,4%	2,8%
Manufacturing, constuction	6,5%	4,6%	3,7%
Oil & energy	4,5%	3,8%	2,5%
Pharma & healthcare	4,5%	4,8%	5,2%
Retail	5,2%	4,2%	2,7%
Global Fail rate	5,6%	4,2%	3,8%

Takeaways

- Employees' click rate decreases as the training period increases.
- Employees familiarize themselves with common aspects of phishing emails, and are able to recognize them more accurately whether they are AI-generated or not.
- Note: Fail rate = Click rate (simulations where the link or attachment has been clicked)
- Note: The Hoxhunt adaptive training model increases difficulty level of simulations over time as user skill improves. Even so, failure rate declines despite simulation difficulty increasing.

- As predicted by the behavioral science and behavior design principles, people “up their game” when challenged at the boundaries of knowledge and skill

Security training performance by Job Role

Different job roles contain different levels of access to sensitive information as well as different types of computer use and communications.

Moreover, certain job roles like IT are typically filled by people with higher or lower levels of computer and security knowledge.

Threat actors target people based on the types of communications they are accustomed to receiving. For instance, we noted surges in attacks targeting HR and Sales & Marketing professionals with recruitment scams; for HR, it was fake job seekers, and for Sales & Marketing, it was fraudulent job offers.

The table below shows the highest and lowest performing job functions based on Success, Miss, and Failure rates, sorted by highest Success rate to lowest.

Phishing Training Performance by Job Role

Department	Success rate %	Miss rate %	Fail rate %
Legal	73%	25%	2.4%
Finance	72%	25%	2.4%
Information technology	70%	28%	2.3%
Customer relationship	68%	30%	2.9%
Software engineering	67%	31%	2.3%
Human resources	66%	31%	2.8%
Business development	65%	32%	3.0%
Marketing	65%	33%	2.7%
Information security	64%	32%	3.8%
Communications	63%	34%	3.2%
Sales	63%	34%	3.2%
Other	67%	31%	2.8%

Trends by department

- **Legal and Communications have the highest and lowest respective success rates.** As expected, legal, finance, and IT departments are high reporters while comms, sales, and marketing are lower performers.
- **Communications and business development have the highest failure rates,** with communications' failure rate being 40% higher than Finance.
- **Direct correlation between job functions' success and miss rates.** Comms, sales, business development and marketing tend to have more spam and email to go through than other departments, which could contribute the poor performance.
- **As with the finance industry in general being historically highly targeted by attackers,** the finance department is attractive to criminals due to its access to money. Thus, they can receive added security training

to protect the bank vault, with stronger security incentives and processes. It’s great news that finance department professionals are amongst the best at reporting and not clicking.

> *"I always take into account the type of workpeople do when I’m designing a security awareness curriculum. For instance, frontline workers in healthcare and retail need practical training. They are very busy, and constantly switching between bursts of computer work and human contact.They need short, relevant training content that mimics and addresses the attacks and issues they’re facing."*
>
> – **Maxime Cartier**, Head of Human Risk at Hoxhunt; formerHead of Security Culture & Competence for H&M Group

Security training performance by country

Training performance varies upon employees' location. Countries contain different business and cultural norms, and therefore certain training approaches or types of phishing attacks may thus perform better or worse.

The table below shows the highest and lowest performing countries based on Success, Miss, and Failure rates, sorted by highest Success rate to lowest.

Phishing Training Performance by Country

Country	Success Ranking	Success rate %	Failure Ranking	Failure rate %
Latvia	1	73%	2	2.0%
Switzerland	4	70%	19	2.7%
Finland	5	66%	3	2.1%
Germany	7	65%	16	2.6%
Denmark	8	65%	26	3.0%
Austria	11	64%	10	2.4%
United Kingdom	14	62%	49	3.7%
Netherlands	17	60%	18	2.7%
Belgium	20	59%	23	3.0%
Japan	21	59%	14	2.6%
Canada	28	57%	51	3.7%
Sweden	22	59%	20	2.9%
Italy	25	58%	46	3.5%
Australia	27	57%	37	3.2%
Singapore	30	55%	27	3.1%
Spain	32	54%	44	3.4%
United States	39	52%	24	3.1%
France	45	51%	50	3.7%
South Korea	48	50%	58	4.1%
Norway	52	49%	42	3.3%
China	73	36%	56	3.9%

> *"When leading cybersecurity awareness programs for globally distributed teams and companies, understanding the differences in behaviours between units (country, department, subsidiary etc.) of an organization is key. Once I have this data, I tend to start where the engagement is the lowest (ie. where I see the highest miss rate), and connect with local colleagues to understand how cultural factors and local environments can affect their attitudes and behaviours, and how we can together find solution to improve engagement. A one-size-fits-all approach fits none, so we need to meet people where they're at."*

> – **Maxime Cartier,** Head of Human Risk at Hoxhunt; former Head of Security Culture & Competence for H&M Group

Security training performance by continent

Similarly, the table below shows the highest and lowest performing continents based on Success, Miss, and Failure rates, sorted by highest Success rate to lowest.



> *“I lived and worked as a CISO in China and my strong assumption is that the culture of ‘losing face’ drives inaction, as seen with the high miss rate. When the miss rate is high, people will not learn. Hence the fail rate is also higher with the cultures where reporting is not instinctual. This cultural norm is not good or bad, but bears keeping in mind when designing an awareness training program with cultural targeting.”*
>
> – **Petri Kuivala**, CISO Advisor to Hoxhunt & Former CISO of Nokia and NXP

Security training performance by phishing theme

Social engineers target people, so training should, too. The variance in the effectiveness of different types of phishing attacks reminds us that a cookie cutter approach to training is not optimal.

Training can be tailored to take into account that click rates vary by industry on different themes.

The table below shows the highest and lowest performing phishing themes based on Success rate, Miss rate, and Failure rate, sorted by Failure rate.



Phishing type glossary

Phishing Theme	Description
Invoice scam	Fraudulent invoice demanding action be taken on a payment.
Authority impersonation	Impersonated authorities include organizations like tax office, healthcare, parking lot company, bank, known brands, etc. It also includes work-related invoice scams.

Personal	Only applicable to the receiver. Uses sender-familiar language and mentions items specific to the receiver.
Sensitive information gathering	Attempts to steal sensitive data via phishing lures like "register here," "update info here," etc.
Temporal attacks	Phishing emails that are only valid at a certain time of the year, e.g. summer, holiday, Black Friday, Christmas, Easter, etc.
Dangerous files	Phishing email containing fake or real attachment, or file share.
IT Admin (inter org)	Phishing email issued from the company's IT department internally.
Inter org communications	Work-related phishing email spoofing the company but not necessarily the IT department. It can come from e.g. your co-worker, CEO, HR manager.
Email environment	Email client-specific phishing email spoofing Outlook or Gmail.
Online services	Phishing email that resembles a real service (logo, brand, colors). Can be a fake brand.
Packet delivery notifications	Classic phishing emails spoofing services like UPS, USPS, DHL, and local carriers.

Conclusion

While the stats and trends around the phishing landscape typically paint an uncertain future, this report offers clarity and hope.

The threat of AI is growing, but organizations still have time to equip employees with the skills and tools to defend themselves. Multiple award-winning programs such as those at AES and Qualcomm have done so, and are reaping the benefits in measurable resilience.

Regardless of employee industry, background, or location, cyber performance *can* be improved. It's a question of focusing on behavior and human risk rather than compliance and awareness.

We challenge the world's phishing training programs to boldly go where no security awareness training tool has gone before: to the center of the security stack.

The importance of connecting threat detection from the training to the real world context can't be overstated.

Human cyber risk can be equated with real threat detection, as a threat report reduces risk more than any other action.

The faster it is submitted and responded to, the less damage the social engineering attack will cause.

The correlation between behavior-based training participation and phishing risk further validates findings by Hoxhunt that engagement is the key to unlocking resilience.

Inactive employees aren't learning or reinforcing secure behaviors, so misses are more likely to become phishes.

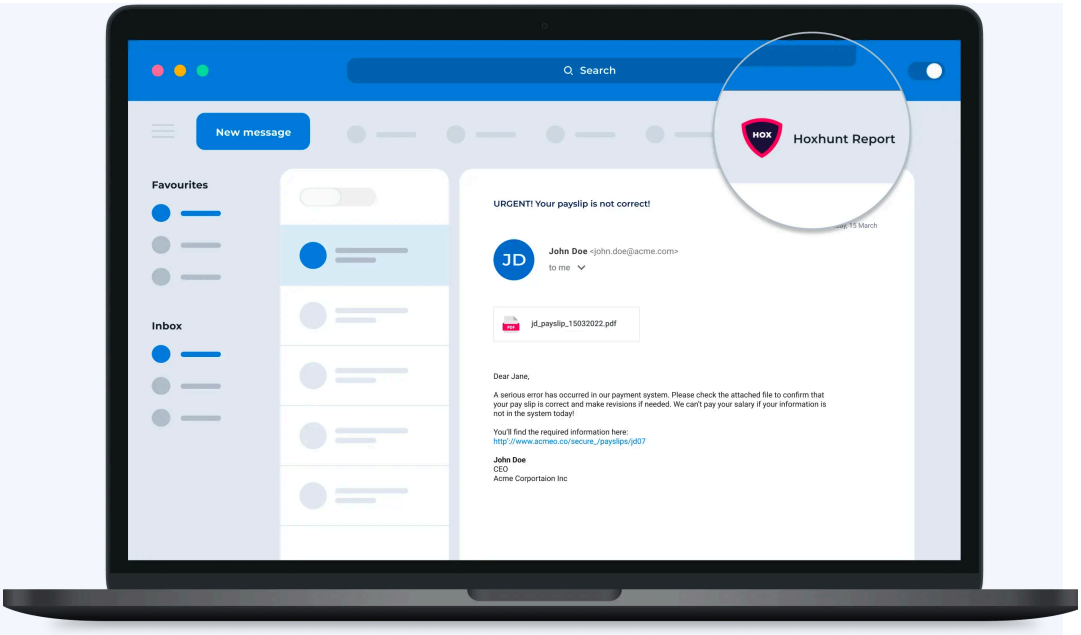
The variations between the different user cohorts' phishing outcomes underscore the need for tailored training and targeted interventions. Everyone can be manipulated by social engineers or trained by security awareness managers in discrete ways.

Knowledge is power. By knowing our people, we have the power to become more secure.

> *"I'm so confident in our staff now with Hoxhunt that if people ask me how many cybersecurity officers I've got, I say '2000.' I know that everybody is going to be reporting threats and doing their job. We're flipping that human layer from being the biggest weakness to the biggest strength."*
>
> – **Mark Sedman**, Global Head of Cybersecurity, WaterAid

Report methodology & key terms

This report is based on data collected from **50 million** Hoxhunt phishing simulations, and millions of real reported malicious emails, sent to **2.5 million users** in **125 countries.**



This report is based on millions of employees reporting suspicious emails using the native Hoxhunt button within email clients like Outlook, Gmail, and more.

To effectively explore this report, you'll need to be familiar with the following terms:

- **Success rate**: Correctly reporting a phishing simulation
- **Miss rate**: Neglecting to report or click a phishing simulation
- **Real cyber threat detection**: Reporting a real phishing email
- **Failure rate**: Clicking a phishing simulation link
- **Dwell time**: Time between receiving and reporting a phishing email
- **Onboarded**: Enrolled in the Hoxhunt program

Hoxhunt: Bridging the gap between training and real threat detection

In addition to simulated threat reporting, Hoxhunt reframes security awareness, behavior, and culture programs around simulated and real threat detection metrics. This is a landmark departure from the old-school Security Awareness Training (SAT) model's simplistic dependency on simulated phishing link click rates.

With Hoxhunt, the amount of real threats reported also grows steadily over time, showing the correlation of training having real-world impact.

Understanding your people, and your approach to security training's impact on them, starts with measuring the cyber behaviors you want to improve.

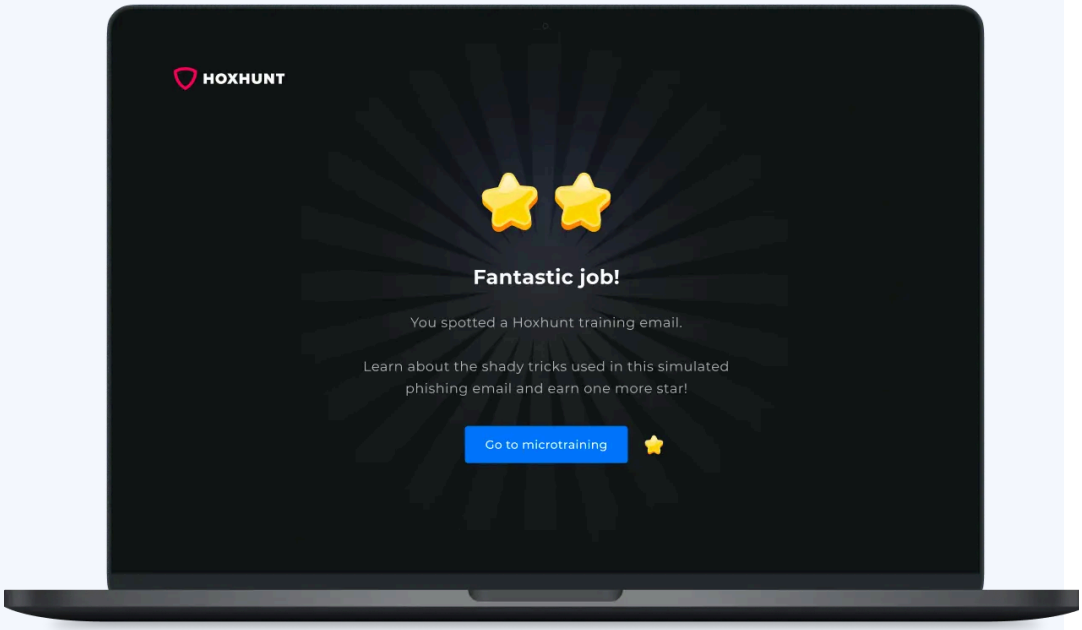
Phishing doesn't stop at training, so neither can the metrics.

The ideal outcome of a phishing attack is that it gets reported so SOC response can remove it from the system.

Thus the most effective behavior to monitor is threat reporting.

Hoxhunt's gamified phishing training platform uses an adaptive learning model to create personalized learning journeys for individuals.

People practice recognizing and reporting phishing simulations until resilience becomes a reflex.



Hoxhunt rewards employees for reporting phishing simulations and real threats alike.

Then, Hoxhunt is designed to extend and connect training to measurable real threat detection outcomes.

People report potential threats the same way that they are taught to in training. Hoxhunt uses AI to categorize reported real threats in real-time.

In-the-moment feedback and gamified rewards are provided to users when they report a real suspicious email, which reinforces that behavior.

All of this becomes a critical part of security behavior and culture programs, according to Gartner:

> *“At the heart of Hoxhunt’s success lies its ability to innovate and adapt its solutions to meet the evolving demands of cybersecurity. The company’s platform integrates gamification, behavior-driven interventions, and adaptive learning to create a training experience that is not only effective but also engaging andsustainable.”*
>
> **– Claudio Stahnke, Frost & Sullivan "Competitive Strategy Recognition" for Hoxhunt, The Human Risk Management Industry, Excellence in Best Practices**

Hoxhunt provides capabilities that go beyond the traditional SAT model, including some or all of:

- AI-enabled adaptive learning
- Automated training operations + threat data orchestration
- Behavioral science-driven curriculum design
- Game mechanics
- Reward-based, personalized learning journeys
- Real threat detection monitoring, with in-the-moment feedback and micro-training
- Measurements of dwell time