



PHISHING TRENDS REPORT 2026



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 interventions. These stats and trends help security awareness leaders deliver risk-relevant training, while CISOs can prioritize defensive measures against the top emerging threats.

Trends revealed in 2026 include a 14X end-of-year surge in AI-generated phishing attacks; new malicious attachments, SVG files, and calendar invites; mobile & 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 will improve their cyber performance and protect organizations against even the most sophisticated social engineering attacks.

Written by **Eliot Baker**

Designed by **Anete Bogulko**

Threat & data analysis and editing by: **Maxime Cartier,**
Petri Kuivala, David Badanes, Jon Gellin

©HOXHUNT 2026

Contents

04 Executive summary: A Phishmas Anti-Miracle

07 Key Trends for 2026 in 5 Infographics

12 PART I: Threat Landscape Trends

13 AI Phishing

24 Recruitment
Scams

20 Callback Phishing

25 .ics Malicious
Calendar Invites

21 Most-impersonated
Entities & Domains

30 PART II: Phishing Training Performance Statistics

35 Methodology & Key Terms

48 Conclusion

Executive Summary: A Phishmas Anti-Miracle

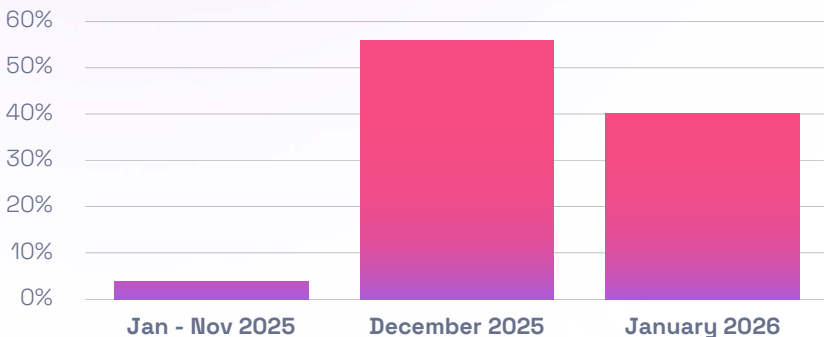
One might call the cyber threat forecast for the first 11 months of 2025, “Cloudy with a chance of Skynet.” Contrary to headlines and hyped-up marketing campaigns, Hoxhunt analysis revealed that under 5% of attacks on our 4 million users each month were AI-generated—until Christmas, that is.

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, which soared from 4% to 56% of all reported attacks across the Hoxhunt global threat detection network 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.

Winter holiday spike in AI-generated phish

↓ % reported threats



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're 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 comms 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 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 will show the latest advances in the threat landscape, and prove that good training will tilt the advantage in favor of us 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 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

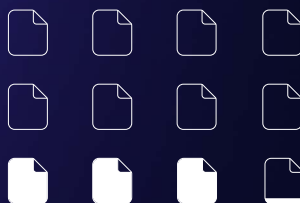
After holding steady at 1%-4% of all reported threats AI-generated phishing emails surged to 56% in December 2025 and dipped to 40% in January 2026.

CALLBACK PHISHING EMERGES

Callback phishing manipulates users to call a phone number and converse with a human or agentic social engineer, rather than click or download a malicious link or attachment that might have otherwise been picked up by a filtering solution.

A large white '500%' is displayed against a dark blue background. A white fishing hook with a line is positioned as if it has just caught the percentage symbol.

500% increase in callback phishing campaigns in Q4 2025
([VIPRE Security Group](#))



26.6% were classified as invoice-themed, impersonating e.g. McAfee, eBay and Zelle (Hoxhunt)



43% of BEC attacks contain callback phishing lure
(LevelBlue, formerly AT&T Cybersecurity)



27.1% of all callback phishing emails were financial service impersonations, e.g. PayPal, Venmo, Bank of America (Hoxhunt)

DESKTOP VS. MOBILE

3X danger



Desktop

6%

Click rate

94%

Report rate



Mobile

19%

Click rate

81%

Report rate

The phishing simulation **failure rate on mobile is 19%, over 3x that of desktop at 6%**. The gap widens after work hours, when users are more tired and distracted, and email activity shifts more to mobile.

Users are over 3x more likely to click a malicious link and 13% points less likely to report a phish on mobile than desktop.



We know that due to UI differences and psychological factors, spotting and reporting a malicious message on mobile is harder than on desktop. We should deploy targeted interventions to mobile-first employees to account for this extra risk.”

Maxime Cartier, VP of Human Risk, Hoxhunt

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.

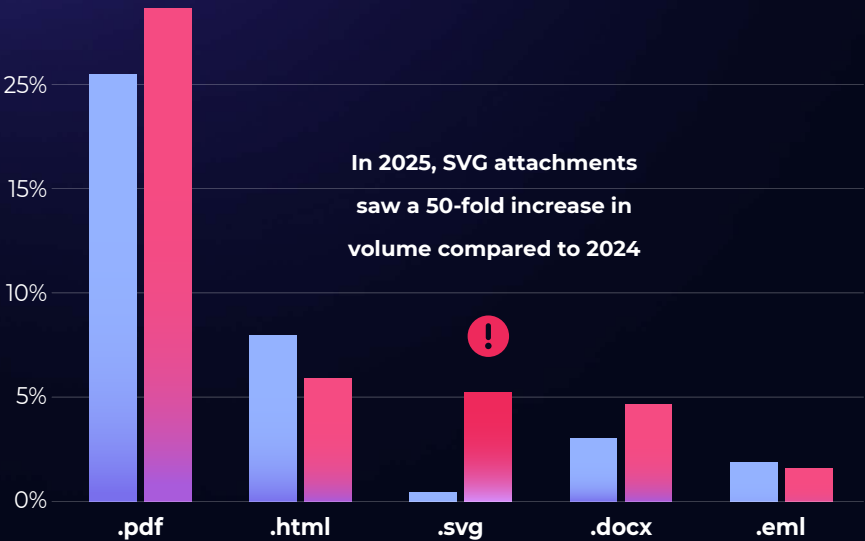


SVG files 50X surge in 2025



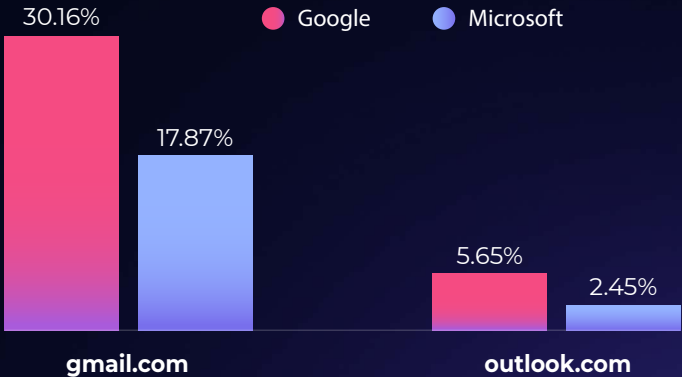
Malicious **QR codes declined** to under 2% of attacks in email bodies, but **re-surged hidden inside attachments**, e.g. PDFs

Attachment Types by Popularity in 2024 vs. 2025



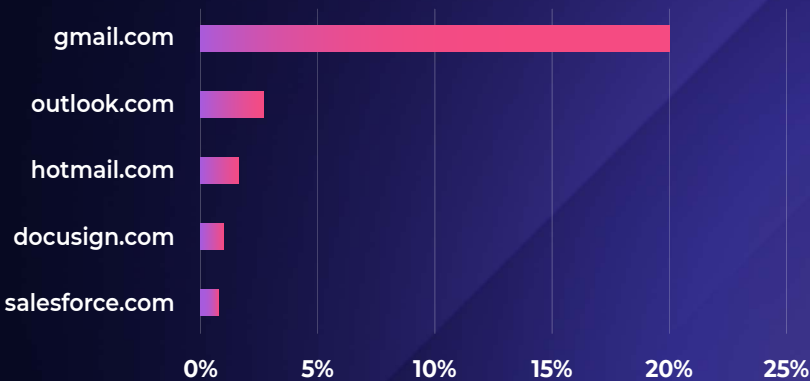
MALICIOUS EMAIL DOMAINS AND DELIVERY

Sender Domain Percentages out of all Malicious Emails



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

Top 5 Malicious Sender Domains in 2025 (occurrence %)



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

Q1 THREAT LANDSCAPE TRENDS

AI Phishing

Phishing is a multi-billion-dollar industry that is driven by an organized service model. Malicious actors opt for 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 that contained 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 deluge, and continue to 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 saw traditional phishing campaigns become more polished over 2025 with good grammar and slick graphics, aligning with the increasing availability and quality of generative AI tools. The landscape has shifted towards these polished lures while the older templates are still in use, as detailed in the Hoxhunt [Cyber Threat Intelligence report](#).

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.



**14X SURGE IN
AI-GENERATED
PHISHING
ATTACKS IN
DECEMBER,
2025.”**



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 both in email bodies and on landing pages. This means the analysis doesn't capture more backend uses of generative AI like 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; generic section markers like "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 had similar elements, including:

- Highlighted box 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 related to and emphasizing the following word.

“📞 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.

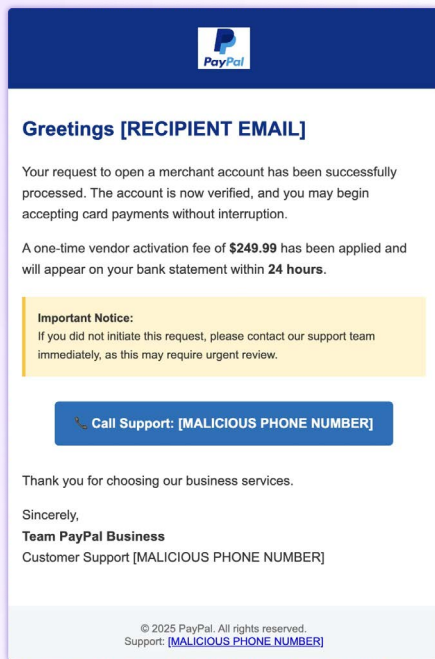


Figure 1, Example of an AI-assisted phishing campaign impersonating PayPal.

Most common themes, techniques and CTAs

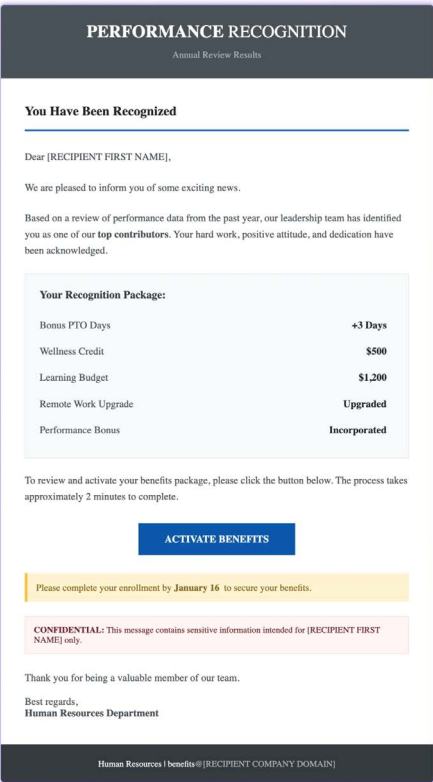
Deeper analysis of the likely AI-assisted phishing campaigns from November and December revealed the most common themes, techniques and calls to action used in the emails.

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, like free phones, car emergency kits or airline rewards.

13.1% impersonated financial service providers, like 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, and 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 sophisticated timing and targeting of attacks.

Techniques

We found that 43.1% of the analyzed emails use links, 11% use attachments and, most notably, 20.3% use open redirects to mask the malicious link from both the human recipient and spam filters. 4.9% of the emails included a malicious phone number, indicating callback phishing campaigns (Figure 1).

Figure 2. HR impersonation with AI-assisted elements.

The most commonly exploited emotion was urgency, for example claiming 24-hour deadlines for taking action (Figure 1, PayPal attack). Commonly exploited emotions also included greed and reward-seeking, present for example in lures about increased benefits and recognition for performance from management (Figure 2, HR impersonation).

Calls to action

The most commonly observed CTAs in the emails were clicking a malicious link, followed by opening malicious attachments and replying to pretext messages.

In other words, the CTAs were conventional, but 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 by the work of a super group of cybercrime gangs: Scattered Spider, LAPSUS\$, and ShinyHunters, who formed an alliance called “The COM” in 2025. They specialize in highly targeted spear phishing campaigns equipped with deepfake voice and video capabilities for access, followed by payloads of malware/ransomware.

Examples of their work include the MGM casino breach, the Jaguar/Land Rover breach, and high-profile breaches of Salesforce, as well as many airline, retail, and financial companies.

But these types of attacks aren't indicative of the AI-powered mass phishing campaigns that typically hit your employees—yet. The Coms' techniques require human social engineers to make phone calls and target SSO accounts such as Okta in order to gain access to systems.

But just as we waited for AI-generated emails to ascend, we are monitoring 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 not very good yet. These error-prone auto-personalized phishing templates use placeholders for target details (much like a spam marketing email sent to a large contact list), and when the replacement breaks, the leftover text, typically in English, reveals how these campaigns are built in English before translation.

Whereas in a spam email, where the leftover placeholders might just read the recipient's email address or a blank space, these malicious AI email templates contain leftover texts like “##victimdomain##” (we're not joking). This unsubtle placeholder exposes the attacker's intent and wave giant red flags to even the untrained eye.

In 2025, we've seen no decline in placeholders artifacts, suggesting GenAI phishing has yet to master personalization. That is likely to change.

Callback Phishing

Callback phishing refers to phishing emails that feature a fake alert (such as an invoice, subscription renewal, or security warning) that urge the recipient to call a malicious phone number. Unlike malicious links or attachments, phone numbers do not trigger filtering solutions, so more callback phish can bypass technical protections.

During the call, the attacker uses social engineering to trick the recipient into sharing credentials, installing malicious software, or making fraudulent payments.

- 500% increase in callback phishing campaigns in Q4 2025 ([VIPRE Security Group](#))
- 43% of BEC attacks contain a callback phishing lure ([LevelBlue, former AT&T Cybersecurity](#))

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

Themes

The most commonly observed theme within the dataset was **financial service impersonation**, including brands like 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 commonly observed theme was **invoice phishing**, with specific lures including **fake subscription renewals** (false notices about expiring subscriptions or fake order confirmations) and **unpaid invoices**. Impersonated brands included McAfee, eBay and Zelle.

27.1% of all callback phishing emails were classified as financial service impersonations, and 26.6% were classified as invoice-themed. Other themes included human resources impersonations and security alerts about, for example, suspicious logins and account verification alerts.

Most-Impersonated Entities & Domains

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

- 01 **Microsoft**
- 02 **Human resources**
- 03 **Docusign**

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.” Docusign has introduced a new service where you can verify these emails and other potential Docusign impersonation by sending them to verify@docusign.com.

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.

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 the popularity of gmail with attackers: gmail accounts are free & easy to create, and it's Google's sole free consumer option versus Microsoft's multiple domains (Outlook, Hotmail, Live) and their regional variants.

	 Microsoft	
% 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 often used campaign-specific domains created primarily for the 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. Discrepancies between confirmed malicious emails in Google and Microsoft environments may be due to different

spam filtering solutions, environment-specific phishing campaigns, and differences in users' training tenure and reporting skills. Beside the "Big 2" domains, malicious emails originate from other free email services, compromised accounts, and mis-used third-party services.

Beyond the top domains, emails originate from diverse sources, including other free webmail (e.g., hotmail.com, iCloud), compromised accounts, and misused third-party services.

Recruitment Scams

Hoxhunt found that recruitment scams have emerged as a top new threat, with targets primarily being employees in marketing departments. We've seen campaigns impersonating e.g. Google, Coca Cola, and Meta target organizations' marketers and social-media administrators with job listing lures.

The recipients have been selected via open source intelligence on social media. They receive a personalized phishing message that leads to a landing page impersonating Calendly, where they are prompted to authenticate using Facebook.

The goal is to get the recipient to sign up for the interview slot using a Browser-in-the-Browser (BitB) credential harvester that displays a fake Facebook login window. If credentials are entered, adversaries can access either personal Facebook accounts or organizations' official accounts.

Opportunity at Meta – Let's Connect

Selby Jennings

Dear Admin Page [RECIPIENT COMPANY],

We would like to share information about an open position at Meta that may be suitable for you. The position offers the flexibility of remote work and involves working on innovative projects that can support your professional growth.

If you're interested, please feel free to choose a convenient time for a discussion via this link: [MALICIOUS LINK]

Thank you for your attention. We look forward to connecting with you.

Best regards,
Emily Durham
Talent Coordination

Recruitment scams surged in 2025

.ics Malicious Calendar Invites: 4x more Dangerous

Hoxhunt monitored a jump in .ics Calendar invite phishing attacks. Hoxhunt created calendar phishing simulations quickly after a late 2025 surge was reported.

The results were concerning: failure rates were 4-6 times higher, at 24%, than the global baseline failure rate.

Attackers send phishing emails including .ics files, which are a standard format for calendar invites in e.g. Outlook. An example is seen below (.ics Figure 1). Many email environments, including

Outlook, automatically interpret these files as events and quietly add them to the user's calendar as soon as the message hits their inbox. In .ics Figure 2 below, you can see the newly added fake event among the user's other calendar items.

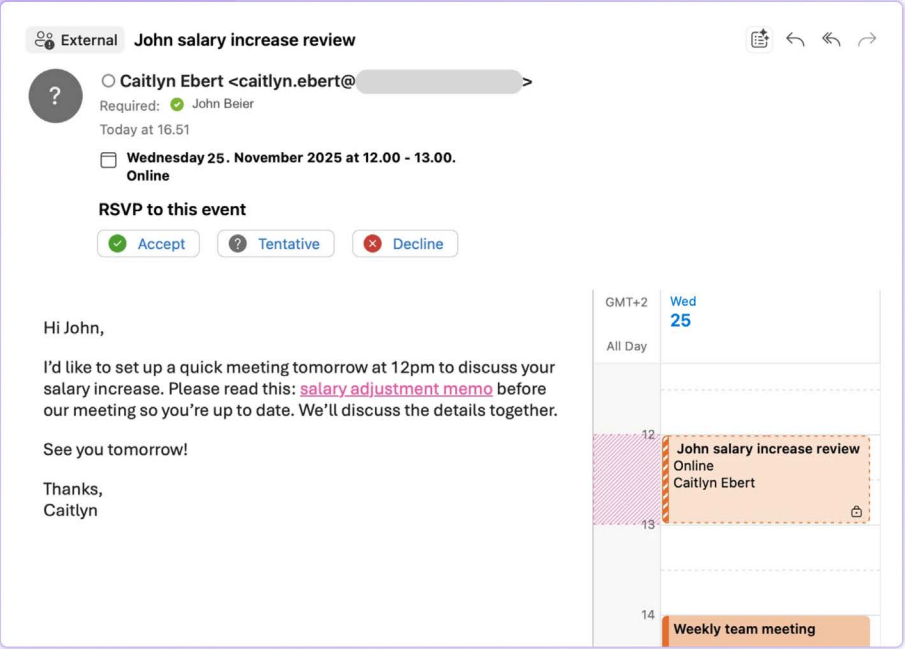


Figure 1: An example of what a calendar invite phishing email with a malicious link can look like

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

You see a new meeting on your calendar - naturally, you'll want to find out the details. These invites often look legitimate, but the links to join meetings and the attachments are malicious.

Sometimes, reporting a suspicious meeting invite does not remove the event from the calendar. Most security tools, including reporting buttons, focus on emails, not calendar objects.

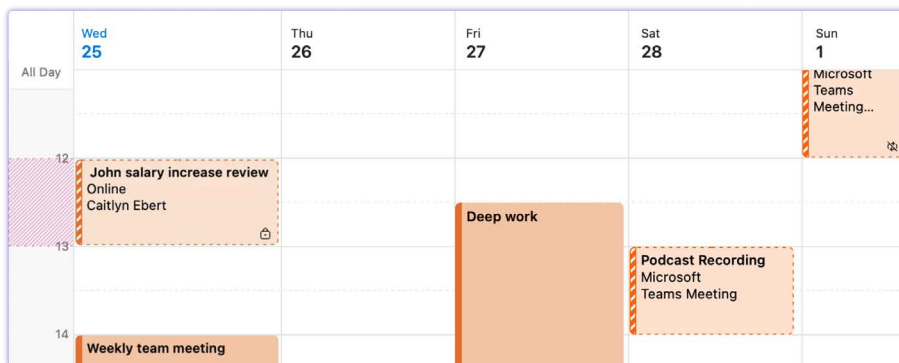


Figure 2: Outlook automatically places new events tentatively among the user's other scheduled items in their calendar. User may naturally click to view the full details where the complete agenda and the malicious link are exposed.

Malicious calendar invites double the attacker's chances with one phishing email: even after reporting the email invite, a user might forget about calendar event. Even after doing the right thing in the email inbox, a user might later be tempted to click the event in their calendar. Hours or even days later, the user might notice the calendar item and think "Oh, what was this meeting again?" Left untouched, the calendar event might trigger popup reminders as well. This is why the calendar item should be deleted separately.

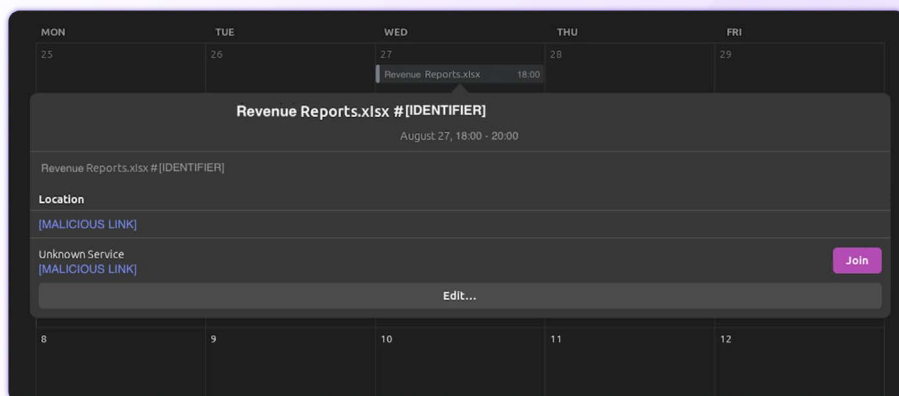
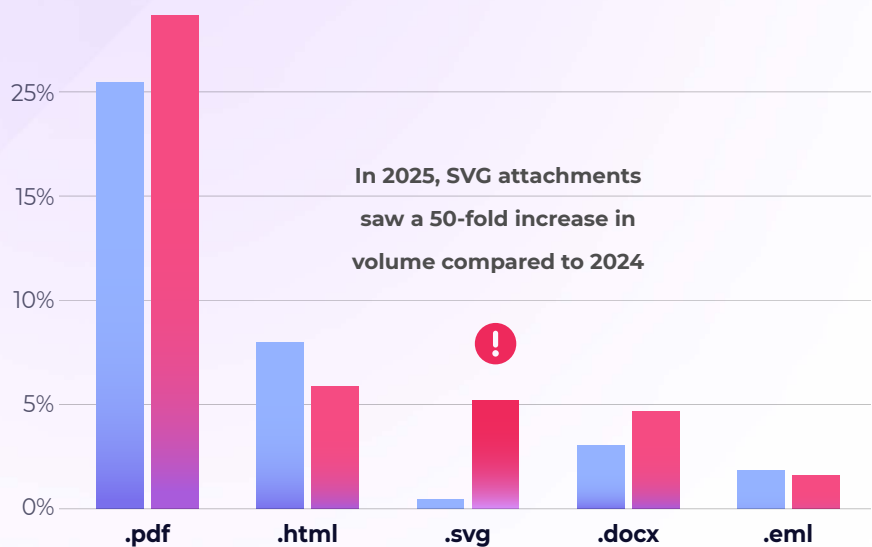


Figure 3: The event gets auto-added to the user's calendar. Attackers sometimes hide malicious links in the 'Location' field of the invite, as this real example shows.

Attachment Types

In 2025, **PDF attachments** remained the top file type used in malicious **attachment**, accounting for 23.7% in the first half of the year. PDF attachments included [fake invoices](#) with fraudulent payment details and fake Europol letters, and some contained links or additional attachments leading to payloads, often credential harvesters. It is probable that PDFs' ability to bypass filters and appear trustworthy contributed to their fairly stable share from 2024.

Attachment Types by Popularity in 2025 vs. 2024



HTML attachments ranked second at 5.6%, down from 10% in 2024. SVG attachments ranked third at 5.0%, marking a significant increase from near-negligible share in 2024.

In 2025, **malicious SVG files exploded with a 50-fold increase in volume compared to 2024**. SVGs appear as harmless graphic files and bypass many anti-spam email tools, making them an attractive technique to attackers. As of September 2025, [Microsoft has stopped displaying inline SVG images](#) to mitigate increasing misuse like cross-site scripting(XSS) attacks. SVG attachments continue to be supported.

Microsoft Word documents were fourth at 4.4%, while EML attachments ranked fifth at 1.4% in 2025. Other 2025 attachments ranged from image files (e.g. fake invoices) to executable files. However, because phishing emails reported to Hoxhunt have always already bypassed filters, executable files which are often blocked by security filters, do not make up a significant proportion of the data set.

2022 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 the 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 your employees to report, and for those reports to be as automated as possible in your workflow in order to help block offending emails and links.”

A founding principle of the Hoxhunt security behavior change model is that a threat report is the ideal outcome of a social engineering attack, and thus reporting is the key behavior to focus upon in a training program. It's encouraging to see that these principles are becoming widely held by the industry, as evidenced by

similar sentiments expressed in the Verizon DBIR 2025.

Behavior-based cyber training engagement unlocks peak cyber performance, and reveals critical insights for human risk management. Exponentially fewer data points are available with an unengaged employee population. Especially when the

SAT



BEHAVIOR
CHANGE

SAT: 4000 data points, confined to a small cohort

Behavior Change: 180,000 data points, representing a statistically significant cohort

featured SAT metric is phishing simulation failure rate alone.

In a hypothetical 10,000-person company, an SAT tool that produces a 10% engagement rate with 4 simulations per year, compared to a security behavior change program (SBCP) with a 50% engagement rate on 36 simulations per year, breaks down to: 4,000 data points in quarterly SAT | 180,000 data points in SBCP.

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 in 2024 and 2025 calculated a global benchmark for users who reported a phishing simulation at around 20%. The participants in, and conditions of, that benchmark test aren't clear, but the 20% reporting rate is encouraging, and 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 real threat reporting: Most programs neglect threat reporting and most users lack the knowledge, skills, and tools to report suspicious messages.

6x_↑

6x rise in simulated threat reporting, from 10 to 60%

3x_↓

3x drop in failure rates



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.



39s

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.

METHODOLOGY & KEY TERMS

This report is based on data collected from over 50 million phishing simulations and millions of real malicious emails, sent to over 4 million users in 125 countries.

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



Success rate

Correctly reporting a phishing simulation.



Failure rate

Clicking a phishing simulation link.



Miss rate

Neglecting to report or click a phishing simulation.



Dwell time

Time between receiving and reporting a phishing email.



Real cyber threat detection

Reporting a real phishing email.



Onboarded

Enrolled in Hoxhunt, and interacted with at least one simulation

Training Performance Improvements Over Time

The standard, pre-Hoxhunt SAT performance baseline is 10% Success, 20% Failure, and 70% Miss rates. 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.

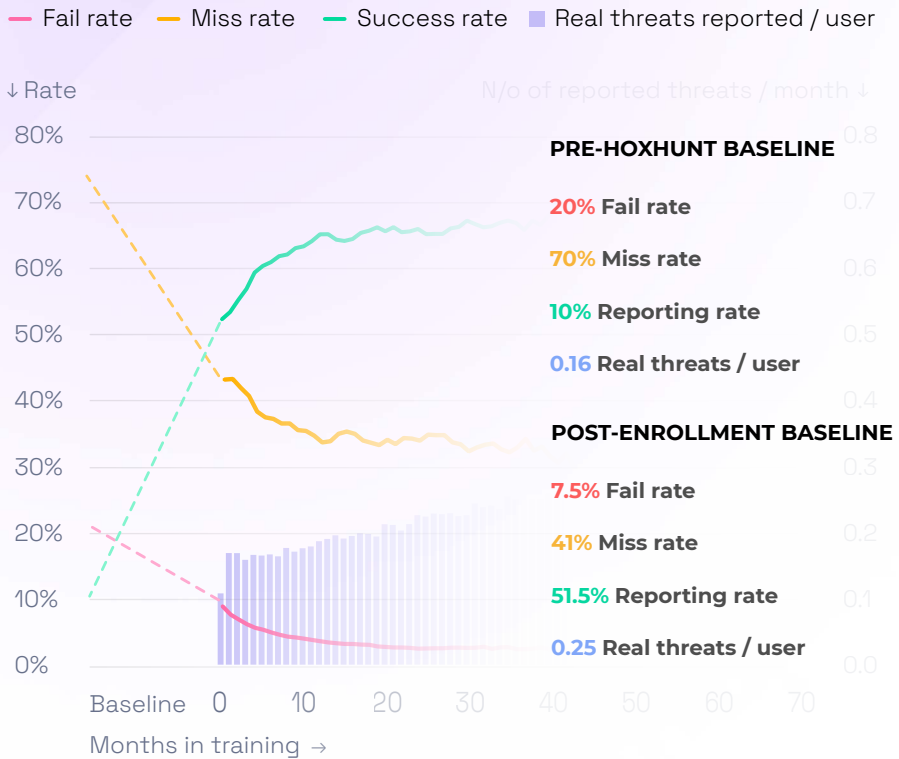
The blue histogram charts real threats detected, which is typically negligent or not tracked before organizations switch to Hoxhunt.

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.

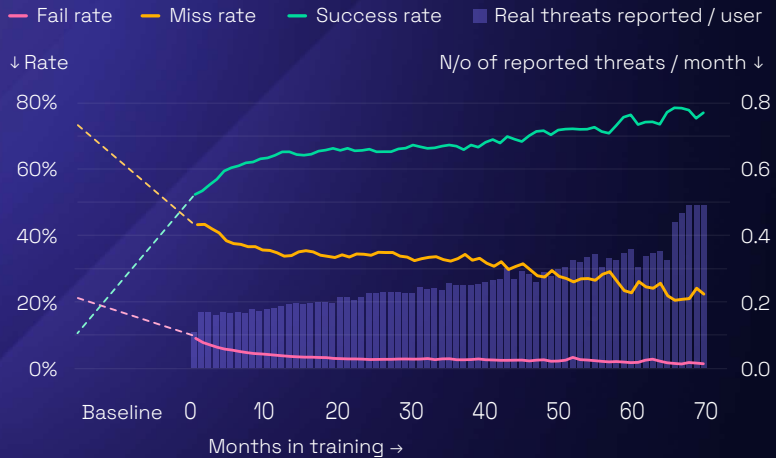
During onboarding, users are given a simple tool embedded in their email client to report phishing simulations. They learn how to use that tool while learning how to spot phishing attacks in gamified micro-trainings, along with communication from the security awareness manager.

Security Behavior Change Improvement



GLOBAL BEHAVIORAL IMPROVEMENT

Security Behavior Change Improvement



Note the blue histogram. It charts the rise in real threat reports / user, per year as a function of time and practice in training.

0 MONTHS IN TRAINING

20% Fail rate

70% Miss rate

10% Reporting rate

0.16 Real threats / user

1 MONTH IN TRAINING

7.5% Fail rate

41.0% Miss rate

51.5% Reporting rate

0.25 Real threats / user

3 MONTHS IN TRAINING

6.0% Fail rate

38.7% Miss rate

55.3% Reporting rate

0.24 Real threats / user

6 MONTHS IN TRAINING

4.8% Fail rate

35.5% Miss rate

59.7% Reporting rate

0.25 Real threats / user

1 YEAR IN TRAINING

3.4% Fail rate

32.3% Miss rate

64.3% Reporting rate

0.28 Real threats / user

2 YEARS IN TRAINING

2.3% Fail rate

32.5% Miss rate

65.2% Reporting rate

0.34 Real threats / user

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 feature, which rewards real threat reports with realtime feedback 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:

- | | |
|-----------------------------|------------------------------|
| → 0 Months in training: 13% | → 6 Months in training: 50% |
| → 1 Month in training: 26% | → 12 Months in training: 64% |
| → 2 Months in training: 34% | → 24 Months in training: 71% |

The parallel rise in simulated and real threat reporting shows a powerful correlation between training performance and real-world threat detection impact as 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.

Success and Failure Rate Improvement by Industry

Success 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.

Fail 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
- Note: with Hoxhunt adaptive training model, difficulty level of simulations increases over time

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, construction	48%	64%	67%
Oil & energy	57%	68%	70%
Pharma & healthcare	52%	60%	62%
Retail	40%	58%	61%
Global Success rate	47%	63%	67%

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%

Cyber Performance by Country

Note that these performance figures from this data set are for onboarded users after one year of training. This explains why their performance rates are so favorable overall; but it also shows how even after a year's worth of good training, performance can vary significantly between geographies and their respective technological environments and societal and business cultures.

Country	Reporting Rank	Reporting %	Miss Rank	Miss %	Fail Rank	Fail %
 Baltics	1	69%	2	29%	4	1.95%
 Switzerland	2	69%	1	28.1%	27	2.90%
 Finland	4	65.4%	4	32.8%	2	1.80%
 Austria	5	64.8%	5	33%	9	2.13%
 Germany	9	63.5%	11	34.1%	16	2.35%
 Denmark	10	62.9%	10	33.9%	40	3.20%
 Luxembourg	11	62.9%	13	35.2%	5	1.94%
 Netherlands	13	61.4%	15	36.3%	14	2.27%
 Poland	14	61.4%	14	36.3%	15	2.31%
 Belgium	16	60.5%	16	36.3%	39	3.20%
 UK	17	60.1%	17	36.6%	45	3.27%
 Ireland	22	58.1%	22	38.7%	44	3.25%

 Sweden	23	57.4%	24	39.9%	23	2.72%
 Italy	26	56.8%	27	40.2%	29	2.99%
 Spain	28	56.6%	31	40.4%	32	3.05%
 Canada	29	56.3%	30	40.3%	48	3.39%
 Australia	31	55.6%	32	40.7%	55	3.66%
 Japan	32	55.4%	33	41.3%	46	3.30%
 Singapore	34	54.5%	34	42.3%	41	3.23%
 South Korea	36	54%	35	42.3%	58	3.73%
 Portugal	38	53.6%	38	43.5%	28	2.93%
 United States	40	52.5%	40	44.5%	30	3.04%
 Hong Kong	42	51.8%	42	44.8%	51	3.44%
 Mexico	45	51.1%	46	45.6%	42	3.24%
 France	47	50.6%	45	45.5%	59	3.96%
 Israel	48	50.5%	49	46.3%	37	3.19%
 Brazil	51	49.1%	55	47.8%	34	3.11%
 Norway	56	47.5%	61	49.8%	12	2.68%
 Vietnam	62	45.1%	63	51.9%	31	2.98%
 India	63	44.3%	65	52.2%	52	3.52%
 Thailand	67	42.6%	67	53%	68	4.42%
 China	72	36.5%	74	59.8%	57	3.72%

Cyber Performance by Industry

Similarly, there are significant differences between cyber performance by industry after one year of training. This is important because threat actors target different industries specifically because click rates are higher, such as in Healthcare and education.

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

Trends by Department

- **Legal and Sales & 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.

Phishing Training Performance by Job Role

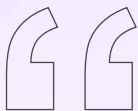
Department	Success rate %	Miss rate %	Fail rate %
Legal	73%	25%	2.4%
Finance	72%	25%	2.4%
Information technology	70%	28%	2.3%
Customer relationship	68%	30%	2.9%
Software engineering	67%	31%	2.3%
Human resources	66%	31%	2.8%
Business development	65%	32%	3.0%
Marketing	65%	33%	2.7%
Information security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

Conclusion

Hoxhunt has refrained from joining the chorus of little shepherd boys crying “Wolf!” about an AI social engineering apocalypse. The game is changing, but deepfake attacks from an agentic AI army aren’t here yet. And even once they’re here, the evidence shows that good training will protect people from even the most realistic attacks.

AI been a game-changer for phishing as well as for security training. Today, you can automate personalized training at scale, and achieve rates of engagement and behavior change once thought impossible.

The real trick is unifying, tracking and acting on threats



Human threat intelligence is a weapon. AI lets you transform employees into a network of threat detection sensors that plug into the security stack to augment the SOC and accelerate incident response.”

MIKA AALTO

CO-FOUNDER & CEO OF HOXHUNT

and behaviors in the simulated and real threat environments.

For the second year in a row, Hoxhunt threat data will be included in the prestigious [Verizon DBIR](#). **According to the 2025 Verizon DBIR, the human element is present in 60% of breaches, and roughly one in five (21%) social engineering incidents in 2025 exhibited linguistic or stylistic markers consistent with AI generation.**

AI-enabled phishing and pretexting campaigns increased by 34% year-over-year, primarily through personalization enabled by LLMs.

It's clear that the threat of AI is growing. In 2025, Hoxhunt showed that our AI spear phishing agents became more effective than elite red teams at getting users to click; it's likely that similar agents will eventually be deployed by malicious actors. Spear phishing will then become the new normal.

But we can fight AI with AI. Hoxhunt has built an agentic reasoning engine and Spear Phishing Agents that auto-curate and personalize training to the individual to optimally build cyber skills and defend against attacks.

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

Organizations still have time to equip employees with the skills and tools to defend themselves against even the latest generation of attacks. In just 3 months with an adaptive training program, you will see measurable improvement; and by 6 months you might see security cultural transformation.

After adopting a security behavior change program over a 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 86%.

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

Human cyber risk can be equated with real threat

detection, because a threat report reduces risk more than any other outcome in a social engineering attack.

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

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

