

EXCLUSIVE REPORT

Phishing Trends Report (Updated for 2025)

Get actionable insights from 2.5 million user clicks on over 50 million phishing simulations, and even more real attacks. This report includes the industry's first 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.



Introduction

The 2025 Phishing Trends Report provides the first reference point for the global incidence of real malicious clicks and the phishing attacks *that bypass email filters*. This information fills a critical gap in the cybersecurity literature.

Here, we drill into the human layer of phishing data beneath the email filters to help answer: “Who’s clicking on what?”

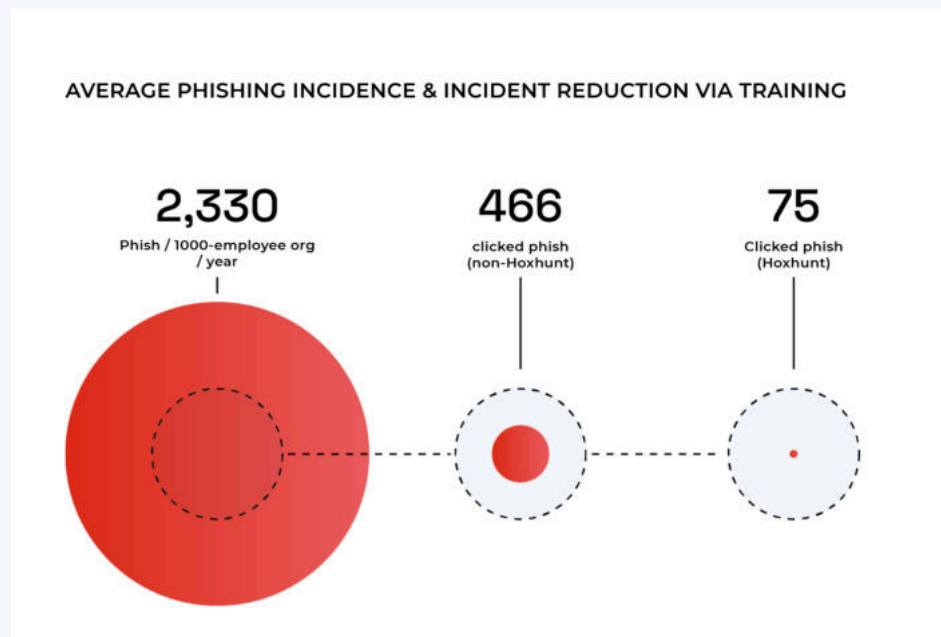
According to the [2024 Verizon DBIR](#), the human element is contained in 68% of breaches. Of those, the [Comcast Business Cybersecurity Threat Report](#) says 80-95% are initiated by a phishing attack, and the total volume of phishing attacks has skyrocketed by 4,151% since the advent of ChatGPT in 2022, [according to SlashNext](#).

At an estimated \$4.88M per phishing breach ([IBM Cost of a Data Breach Report 2024](#)), social engineers are making billions by being better at making people click than we are at understanding what makes them tick.

As phishing continuously reaches new levels, effective phishing protections and cyber security training models must do the same.

The good news is that phishing risk can be measurably reduced *when phishing training is based on behavior*.

Employees can be trained to recognize and report social engineering attacks with a 6x improvement in 6 months, and **reduce the number of phishing incidents per organization by 86%**.



This report reveals an escalation in phishing attacks that evade email filters and land in inboxes, be they AI-enabled or otherwise. The results are categorized by: AI vs. non-AI; threat type; targeting organizational vs. personal assets; and by **departments, locations, and industries**.

Over 50 million data points were collected from the real and simulated threat reports of over 2.5 million threat hunters from around the world.

Connecting phishing simulation results to real threat detection outcomes unfolds new dimensions of analysis, insights, and targeted interventions.

These phishing statistics and insights can help SAMs break through engagement plateaus with their training programs, and give CISOs a map to securing the human element.

The biggest human cyber-risk is neglecting your humans. By leaving them unattended, you leave yourself exposed to, and uninformed of, the greatest risk factor in cybersecurity: social engineering.

Key Phishing Statistics For 2025

Key phishing stats 2025

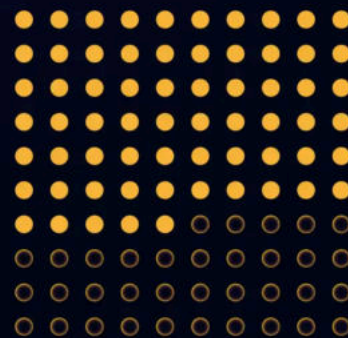


2,330
Total phish bypass filters per 1000 person org



65% Attacks target organizations

35% attacks target individuals



90%

Malicious attachments lead to further social engineering



85%

Fewer malicious clicks with Hoxhunt

0.7% – 4.7%

Reported phish written by AI

Top 3 most spoofed entities:

01  Microsoft

02  docusign



Part I: Phishing Trends & Statistics

Macro trends help illuminate the impact of the Hoxhunt data in filling in critical knowledge gaps around the phishing landscape.

"In the near future, AI will power significantly more phishing attacks—everything from text-based impersonations to deepfake communications will become cheaper, more convincing, and more popular with threat actors." – Mika Aalto, co-Founder and CEO, Hoxhunt

Phishing attacks 2025

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 practices / gullibility
- 26% Lack of cybersecurity training
- 14% Malicious websites

Phish bypassing email filters is rising, but slowed in 2024

Lets' now turn our attention to the data layer beneath the email filters and behind the breaches.

To identify changes in the volume of phish that bypass email filters, and malicious clicks, Hoxhunt isolated threat reporting rates in users who regularly report malicious emails. Their threat reporting rates serve as a constant. Fluctuations in those rates reflect changes in the number of threats bypassing email filters.

The average real threat reporting rates by users who have participated in training for more than one year increased by 28% in 2022, and by another 13% in 2023, before leveling off in 2024 with a 3% increase.

The 2022 surge might be linked to the advent of ChatGPT and the rise of blackhat generative AI that year. The subsequent years where growth leveled off might indicate that email filters have adapted and got better at identifying AI phishing campaigns.

In other words, fewer AI attacks fooled filters in 2024.



AI being used to amplify phishing attacks

Phishing is a multi-billion-dollar industry driven by an organized service model and very cheap tools. Malicious actors opt for phishing-as-a-service tools that yield the greatest ROI, with the lowest risk of getting caught.

As such, highly targeted, AI-enabled spear phishing attacks are on the rise. These attacks may for example automatically scrape open source intelligence from the web and incorporate advanced capabilities like deepfake video and voice calls of executives to redirect an invoice payment or gain access to sensitive data.

Anyone, anywhere, can appear to be anyone else, anywhere else.

However, AI-powered mass phishing campaigns have not yet entirely disrupted the cybercrime ecosystem. Hoxhunt analyzed 386,000 malicious phishing emails that landed in employee inboxes during 2024 to see how many were written by AI, and including emails that were uncertain, found that only 0.7-4.7% phishing emails were written by AI.



Of 386,000 malicious phishing emails analyzed, only 0.7% - 4.7% were crafted by AI.

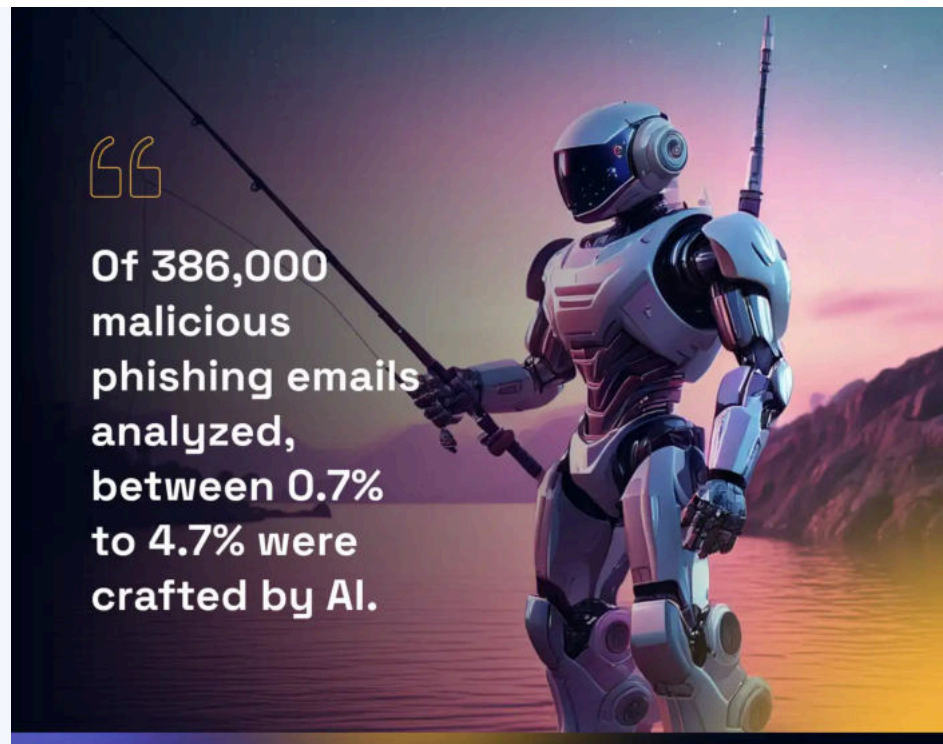
For now, it appears that the cheap, well-established phishing kits that have long been on the darkweb remain most popular. However, as AI continues to develop rapidly and as AI-powered phishing kits become more popular and accessible, this trend could change drastically by next year.

That happened with QR phishing attacks in the fall of 2023, when Hoxhunt reported a 20X surge in QR phishing attacks, which had been negligible just 6 months before.

Still, the larger school of AI-generated phish is innumerable, and they're constantly evading email filters more effectively.

"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."

– Pory Åvist, Co-Founder and CTO, Hoxhunt



“

Of 386,000
malicious
phishing emails
analyzed,
between 0.7%
to 4.7% were
crafted by AI.

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.

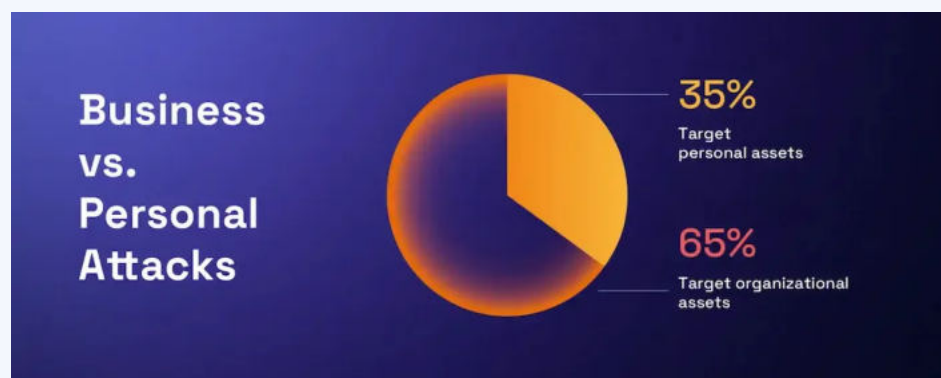
As for **Docusign impersonations**, the recipient is often asked to review & sign documents. Sometimes cyber attackers give no details about the “document”, and other times they may claim that it is coming from a company administrator. They might include words like “termination.”

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

Over the last six months of 2024, 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

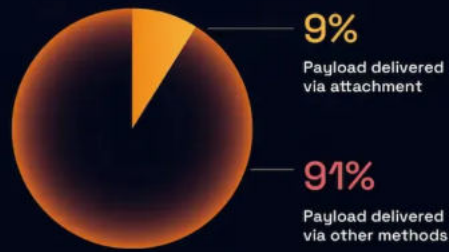
According to the 2024 Verizon DBIR, 94% of malware is delivered through email attachments. Malicious messages with attachments may contain a malware payload in the initial attachment, or a credential harvester or, more likely, lead users to the next step in a scam, where the ultimate payload might for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

Payload via attachment or other methods



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

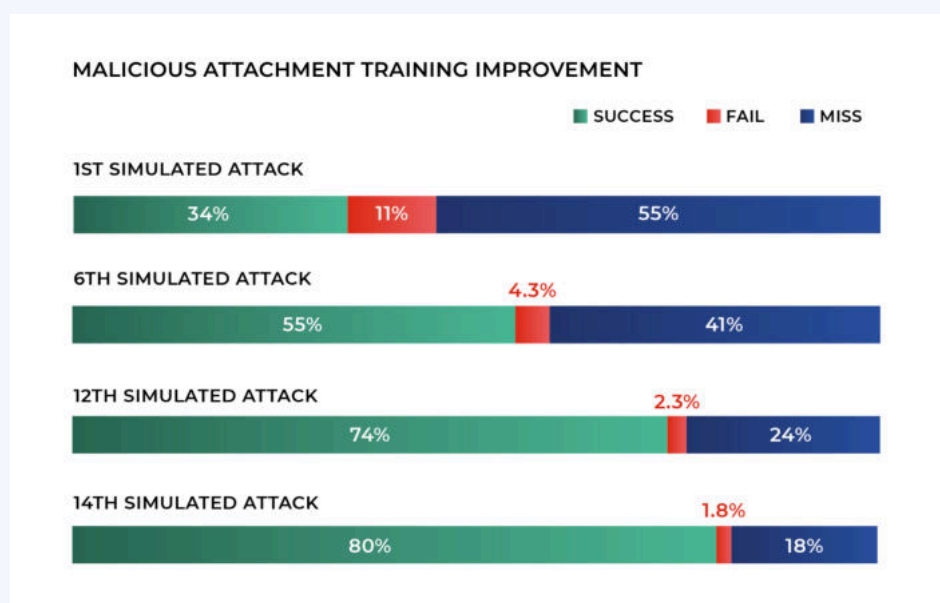
Attachments arouse curiosity, and to the untrained email user, it can be hard to resist seeing what's inside.

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.

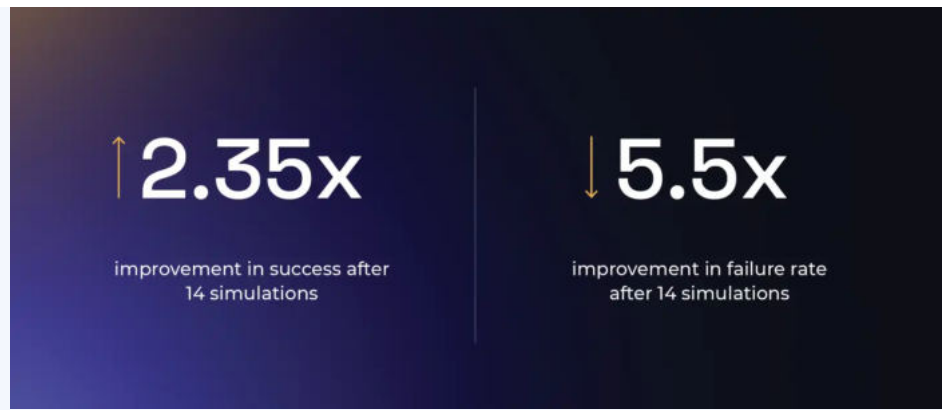
Before training, only 34% of users successfully report these phishing simulations, while an alarming 11% fail by opening the attachment or clicking a malicious link.

Failure rates are sliced by 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%.

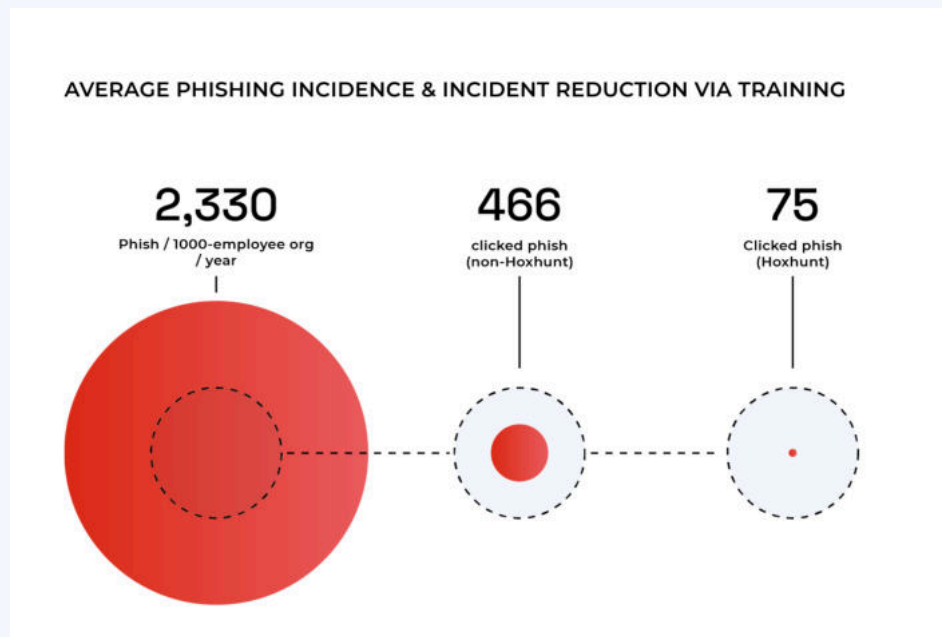
The global averages for general success and failure after 12 months of training is 67% and 3% respectively.



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.

Real Phishing Incidence

On average, employees in a 1,000-person company will face roughly 2,330 phishing attacks per year that bypass their technical layers. Of those attacks, in companies with standard SAT training, 466 phishing will be clicked per year. Accordingly, a 10,000-employee enterprise would have 23,300 phish in the system and 4660 clicks, and so on.



These clicks can be deemed “malicious clicks” or “phishing incidents.” Not all incidents rise to the level of breaches as not all phishing attacks target organizations; and not all clicks immediately open access to sensitive corporate information.

The number of clicks on these phishing links and attachments will be determined by the cyber skill level of the user base. A standard security awareness training tool’s 20% failure rate translates to 466 phishing incidents / year / 1000-person org, or 4660 incidents / year / 10000-person org.

It's a different picture with a security behavior change and adaptive phishing platform like Hoxhunt. With global failure rates of 3.2% for Hoxhunt users after 12 months of training, the per-1000-org total number of phishing incidents are whittled down by a factor of 6, from 466 to 74.6.

This translates to an 86% drop in phishing incidents with Hoxhunt compared to a standard, quarterly SAT tool.

It's important to note that phishing incidence and incidents vary by industry and by corporate security maturity. Highly targeted and highly security- mature industries like finance, for instance, may have added technical layers that reduce the number of phish that reach employees.

Most importantly, numbers will vary by employees' level of training and cyber skill.

A high level of simulated phishing reporting and a low level of phishing simulation failure directly translates to fewer cyber incidents.

Phishing incidence by industry

Calculating how many phish are in the actual email environment is possible via human threat intelligence. The number of real reported malicious emails represents only a percentage of the total, as many phish are missed and some are clicked on.

Rank	Industry	Malicious Threats reported / user / year	Total phish / 1K org	Breaches / 1K org (Hoxhunt)	Breaches / 1000 (Hoxhunt)	% Reduction
—	Global Average	1.40	2330	466	74.56	86%
1	Media Production	2.91	4610	922	138.00	85%
2	Government	2.08	3010	602	93.31	85%
3	Manufacturing & Construction	1.65	2540	508	81.28	84%
4	Financial Services	1.41	1990	398	45.77	89%
5	Oil & Energy	1.28	1820	364	47.32	87%

By harmonizing data on real and simulated phishing reports, we can triangulate:

- How many attacks are actually getting through filters
- What industries are most under attack
- What industries are most vulnerable to attack
- How many phishing breaches there likely are per organization

The Hoxhunt platform tracks and unifies phishing reporting data in simulated and real-world contexts. This report's global cohort of over 2.5 million users boasts an over-60% threat-reporting engagement rate and fail about about 3.2% of phishing simulations. The rest are called "misses." Hoxhunt users reported 1.4 malicious emails per year, per person on average in 2024. Some users report over 7 phish per year, while others report none. According to Cofense, the top 5 most-targeted industries by phishing, as per their email gateway data, are:

1. Finance and Insurance
2. Manufacturing
3. Mining, quarrying, oil & gas extraction
4. Healthcare and social assistance
5. Retail trade

Hoxhunt data tracks with these findings to a degree. The notable differences are the Healthcare and the Retail industries, which are highly targeted but, according to our data, contain comparatively fewer phish in the email environment. This might be because the proportion of regular computer-using employees in retail and healthcare are few compared to frontline workers, skewing the data.

Phishing incidents and incidence per industry

Rank	Industry	Total phish / 1K org	Phishing Breaches (non-Hoxhunt)	Phishing Breaches (Hoxhunt)	% reduction
1	Media Production	4610	922	138	85%
2	Government	3010	602	93.31	85%
3	Manufacturing & construction	2540	508	81.28	84%
4	Financial Services	1990	398	45.77	89%
5	Oil & Energy	1820	364	47.32	87%
6	Legal, professional & business services	1890	378	64.26	83%
7	Entertainment	1800	360	48.6	87%
8	Logistics and Supply Chain	1800	360	54	85%
9	Pharma & Healthcare	1980	396	73.26	82%
10	IT, software, internet	1680	336	48.72	86%
11	Travel & tourism	1890	378	107.73	72%
12	Utilities	1660	332	58.1	83%
13	Retail	1460	292	40.88	86%

Note: Total threats / user is calculated by dividing the Real Reported Threats / User value by the industry's success rate. This estimate is made possible by high simulated threat reporting rates, which we call success rates, because it lets us know that people report e.g. 60% of all attacks. A global success rate of over 60% lets us estimate that the reported Threats / User / Year value is around 60% of the actual total, yielding the equation:

(REPORTED THREATS) = (SUCCESS RATE)(X), where X=TOTAL THREATS.

Thus: TOTAL THREATS = (REPORTED THREATS) / (SUCCESS RATE)

Part II: Phishing Training Performance Statistics

For the first time, the 2024 Verizon DBIR calculated a global benchmark for phishing simulation reporting rates.

The benchmark? 20%. From their sample audience with varying levels of training, only 1 in 5 people successfully recognize and report a phishing attack when they are sent one.

Is this in line with expectations? Unfortunately yes--Hoxhunt observes an average 7% phishing reporting rate from users who only receive

quarterly security awareness training.

The good news? When these same users enroll in an adaptive phishing training program like Hoxhunt, we see reporting rates spike, reaching an average of 60% after 1 year of training.

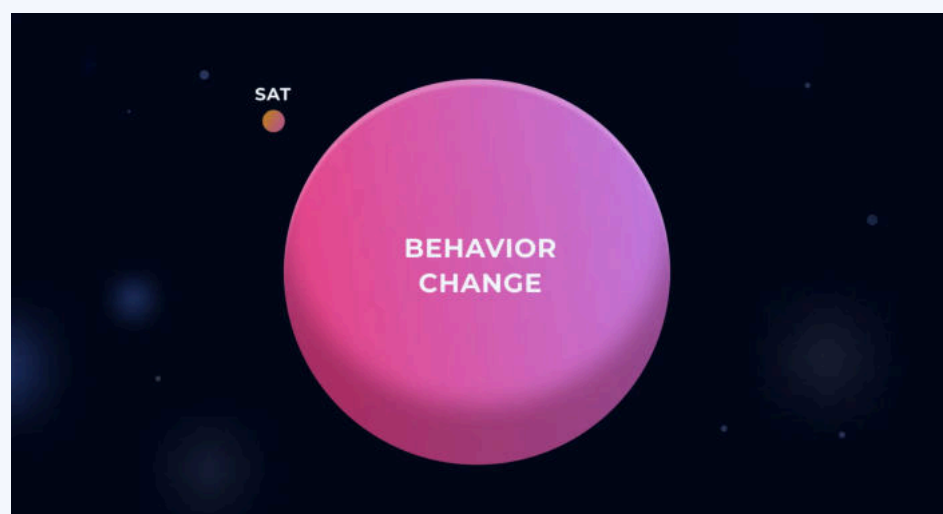
Of course, benchmarks vary across geography, industry, job function, and phishing type.

In this next section, we'll dig into each of these categories, using data collected from 15 million Hoxhunt phishing simulations, and millions of real reported malicious emails, sent to 2.5 million users across 125 countries, between January-December 2024.

More engagement unlocks better understanding of cyber behavior

Exponentially fewer data points are available with an unengaged employee population. Especially when the 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 behavior change program with a 50% engagement rate on 36 simulations per year, breaks down to:



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 7% 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.

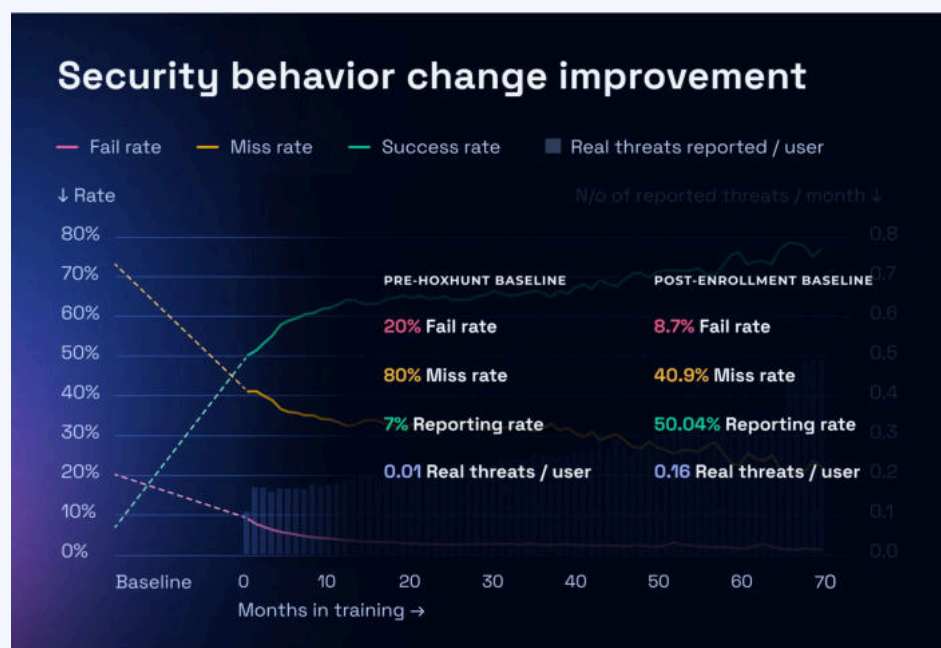
The below graph charts dramatic improvement that is the product of training that includes:

- 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.



Note: the blue histogram represents real threat detection rates. They go up along with simulated threat reporting rates.

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%

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.

"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 AES

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%

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, construction	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.

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; former Head 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.

Security training performance by continent



"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 Training performance by theme

Phishing theme	Success rate %	Miss rate %	Failure rate %
Inter org communications	47%	48%	4.8%
Invoice scam	56%	40%	4.6%
Dangerous files	48%	49%	3.4%
Email environment	35%	62%	3.6%
IT Admin (inter org)	49%	47%	3.5%
Personal	42%	54%	3.3%
Online services	39%	58%	2.7%
Authority impersonation	44%	54%	2.8%
Sensitive information	42%	55%	2.7%
Temporal attacks	38%	59%	3.4%
Packet delivery notifications	21%	76%	2.9%

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.

TABLE OF CONTENTS

Introduction

Key Phishing Statistics For 2025

Part I: Phishing Trends & Statistics

AI being used to amplify phishing attacks

Impersonation campaigns leverage trusted brands

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

personal

Malicious attachment campaigns

Real Phishing Incidence

Phishing incidence by industry

Part II: Phishing Training Performance Statistics

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

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.

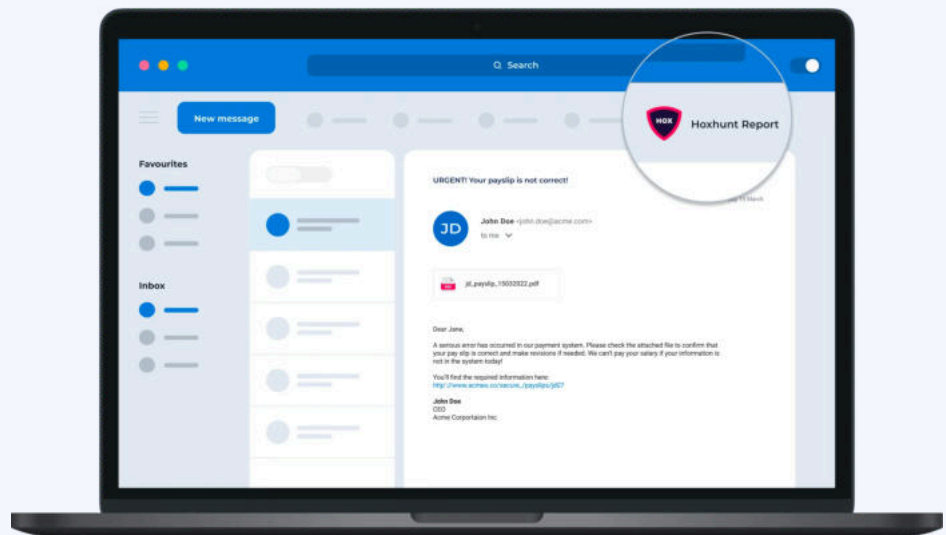
Knowledge is power. By knowing our people, we have the power to become more secure.

"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

ABOUT THE AUTHOR



Eliot Baker
Director of Content Marketing, Hoxhunt



Maxime Cartier
Head of Human Risk, Hoxhunt



SHARE THIS GUIDE



- **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.

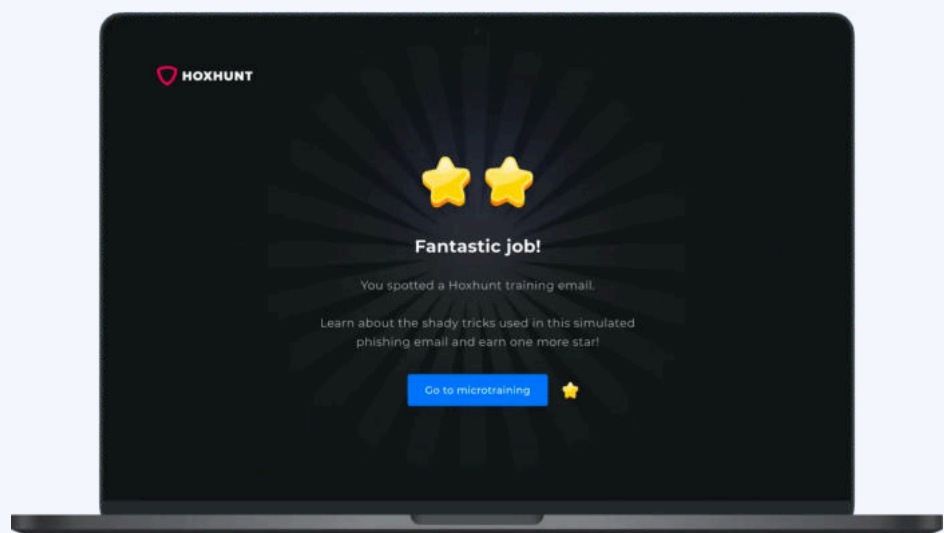
Phishing doesn't stop at training, so neither can the metrics.

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 and sustainable.”

– 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

Get started with Hoxhunt

If your organization isn't quite up to benchmark, or you'd just like to improve your organization's resilience through better security training, learn how Hoxhunt can make the difference.