HOXHUNT

# Behavioral Cybersecurity Statistics

EBOOK | 2022

# Table of contents

Security professionals will tell you there are three parts to security: people, processes, and technology. But people are the ones who write and employ processes. People are the ones who create and use technology. It shouldn't be surprising to learn, then, that people are the cause of nearly 95 percent of all cybersecurity incidents, according to a recent Verizon Data Breach Report. I would go further and say that people are the cause of 100 percent of cybersecurity breaches. These statistics have led many security practitioners to want to write off people as the weakest link in security. I would argue that people are the only link in security. And if there were a way to improve human security, even by just a small amount, say 20 percent to 30 percent, the outlook for the cybersecurity world would be radically changed."

**– Award-winning CISO, George Finney, Bestselling author of Well Aware: Master the Nine Cybersecurity habits to Protect Your Future; pg. 4**

# Glossary

**Hoxhunt training:** Phishing simulation training geared for behavior change in which 12 - 36 phishing simulations per year are automatically customized to employee skill level and profile, and emailed at sporadic frequency.

**Phishing attack:** An email containing malicious links or attachments laced with malware that compromise one's computer or provide access to the whole network upon clicking or downloading; the email has been crafted by cybercriminals who use social engineering to manipulate people into providing sensitive information, security credentials, or funds for criminal purposes.

**Phishing simulation:** An email based on a real phishing attack created by Hoxhunt and sent to employees as practice on spotting and reporting real phishing attacks.

**Success:** User successfully reported a phishing simulation sent by Hoxhunt by hitting the Hoxhunt reporting button plug-in.

**Success rate:** The ratio of phishing simulations that were successfully reported, against phishing simulations that were either neglected (known as a "Miss") or failed (simulated malicious link was clicked).

**Failure:** User clicked or downloaded a simulated malicious link or attachment in a Hoxhunt phishing simulation.

**Failure rate:** The ratio of phishing simulations failed against those that were otherwise successfully reported or those that were missed.

**Miss:** User neither clicks nor reports a phishing simulation

**Miss rate:** The ratio between phishing simulations that were missed, against those that were either failed or successfully reported.

**Real threat report:** Non-simulated emails that were reported using the Hoxhunt reporting plug-in, including real phishing attacks, spam, or other types of emails.

**Behavioral cybersecurity:** A Hoxhunt term, pending trademark, that describes the study of people and how they interact with email as a distinct behavioral science that can be measured and managed for better cybersecurity outcomes.

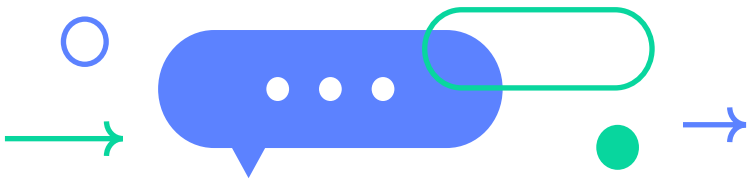
**Behavioral cybersecurity entrainment:** Training methodology designed to ingrain threat reporting and security-positive behavior as an instinctive habit.

Verizon Media believes the simulations and training offered by most security education teams do not mimic real life situations, do not parallel the behaviors that lead to breaches, and are not measured against real attacks the organization receives. This is why it is important to progress from the traditional security awareness model to that of using *behavioral science* to change the habits that lead to attack path breaking actions.”

– Verizon DBIR 2021

# Key takeaways

## Misleading metrics



**Fail rate alone is a misleading metric.** Without simulated + real threat reporting metrics, phishing simulation fail rate is empty. It fails to accurately:

- Capture organizational resilience
- Predict real threat reporting
- Reflect employees' cyber self-defense skills

**Success rate rules.** The frequency with which people report phishing simulations is the best:

- Indicator of individual security skill
- Predictor of phishing breaches
- Metric to convey risk

**Fail rate becomes meaningful** when placed within the larger context of phishing simulations that have been reported, missed, and failed, as well as real threats that have been reported.

**Reporting threats** – real and simulated – is the key to behavior change and skill acquisition

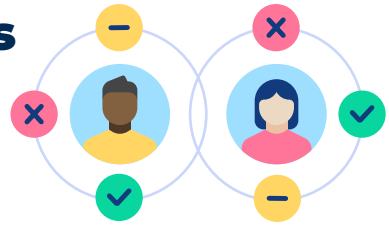
**Measuring true risk** of a phishing breach can be achieved with:

- Success + Failure + Miss + Real threat reports
- Training engagement of over half the organization
- Frequent phishing simulations (12-36 per year)
- Adaptive learning technology; simulations get harder as the training and user skill levels progress

**Measuring and rewarding Success** ingrains good reporting behavior. High success rates are linked to high real threat reporting rates.

**Misses matter.** The number of phishing simulations that employees miss strongly predict how likely they are to report or fall for real phishing attacks. Misses are bad.

# Who you are predicts how you'll behave



Training programs must factor in who employees are and be able to individualize content to fit their strengths and weaknesses.

**Cybersecurity performance varies significantly depending on:**

- Geography
- Job role
- Industry

**Countries with the highest real threat reporting rates** – Switzerland and Denmark – report threats 10 times more frequently than the lowest-reporting countries, China and Romania.

**IT** had the highest Success rate (63%); **Sales** had the lowest Success rate (54.1%).

**The Public Policy** category had the lowest phishing simulation failure rate, 1.2 %, and the highest success rate, 74%. Comparatively worse are **the Dairy industry's** failure rate of 7.7%, and the Construction industry's 47.5% Success rate.

# Good security training works

When trained correctly, employees improve cybersecurity skills and report more real phishing threats. With the Hoxhunt phishing training:

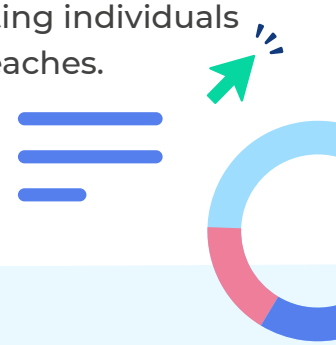
- Organizational phishing simulation **fail rates dropped** from 14% to 4% globally
- **Success rates** – with Success measured as the reporting of a simulated phishing attack- – jumped from near-zero to between 52% - 74% of simulations based on industry
- **Real threat reporting rate** improved by nearly 70% from training baseline
- **Real threat reporting accuracy** continuously improved from near-zero to 60%
- **Engagement rate soared** to 88.75% of employees onboarded to the Hoxhunt training

BEHAVIORAL CYBERSECURITY STATISTICS

# Overview

# Theft by a thousand clicks

Email-originated cyber attacks account for roughly 90% of all data breaches, which in total exacted a $6 trillion toll on the global economy in 2021 at a clip of over $14 million-and-climbing per company per successful phishing attack, according to reports by the Ponemon Institute and Cybersecurity Ventures. Collectively, those little clicks would add up to the GDP of the third largest nation in the world behind the US and China. Understanding employee behavior in relation to cybersecurity as well as effective behavior change methodology is a critical step towards protecting individuals and organizations from phishing attacks and data breaches.



This inaugural Behavioral Cybersecurity Report by Hoxhunt analyzed email data of 1.6 million Hoxhunt participants and their 24.7 million simulations. The results of this analysis indicate that user email behavior can vary significantly depending on their industry, type of job, and geographical location. More importantly, user behavior, skill and progress over time indicates robust improvement. Global phishing simulation failure rates and missed simulations clearly decline, while rates of skill acquisition, threat reporting, and phishing simulation success increase.

Employees and their mailboxes constitute the greatest cybersecurity risk factor for enterprises and all other organizations. 2021 saw record-setting venture capital and PE activity in the cybersecurity space. But investment into security awareness solutions lagged behind technical solutions, as has effective innovation in security awareness models. Traditionally, improving employee cybersecurity awareness has been seen as

**We have analysed:**

USERS:
**1.6 MILLION**

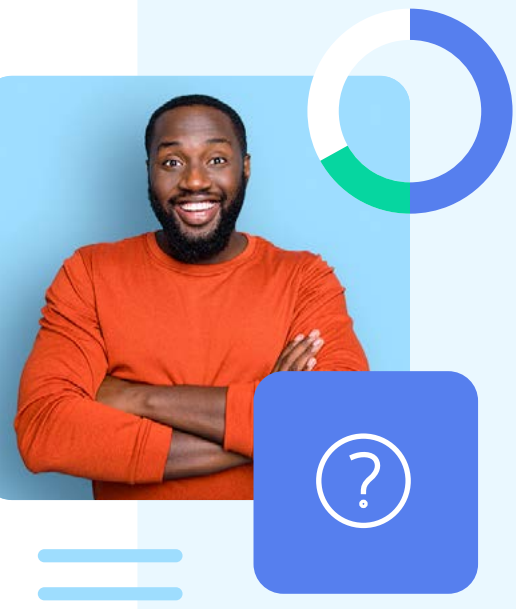
SIMULATIONS:
**24.7 MILLION**

COUNTRIES:
**100+**

a lost cause in terms of actually reducing risk. Awareness has thus been relegated to a compliance-based approach, which is more check-a-box than actual risk reduction. But with next-gen training solutions, which combine advanced technology with a people-centric approach, a truly risk-based approach can and will offer high ROI in terms of risk reduction.

The results section of this report will show how a global sample of 1.6 million Hoxhunt users performed with millions of highly realistic phishing simulations of varying difficulty over time. Users are segmented by their geography, industry, and job role. Their behavior is segmented by their failure rates, success rates, and missed email rates. There are many intriguing findings that bear further inquiry as we seek to understand why users behave the way they do with emails. But, more importantly: so what?

## Does awareness training actually work?



**YES.** Our data shows that user behavior can, with certainty, be changed at population levels to significantly reduce risk of email-originated data breaches for organizations. Awareness training delivered in the right way is effective. It starts with people. By understanding users and their behavior, we can better protect them and their organizations with training that demonstrably:

- **Changes behavior**
- **Produce positive outcomes**
- **Reduces risk of data breaches**
- **Builds long-term cybersecurity skills**

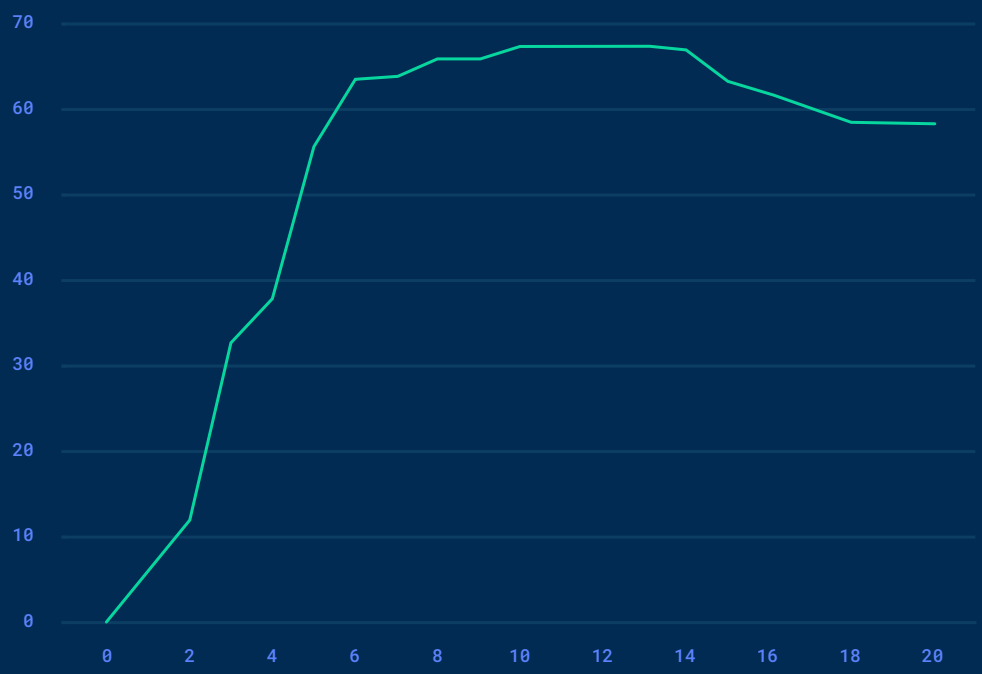
# Behavioral cybersecurity

Managing behavior begins with measuring it. Ingraining threat reporting as an instinctive behavior simultaneously measures the cybersecurity skill of the workforce while conditioning security-positive behavior.

When a malicious email lands in the inbox, the ideal outcome is an immediate threat report. This removes the threat from the system and demonstrates the user's ability to identify a malicious email and act appropriately. Reporting threats, both real and simulated phishing emails, gives security teams invaluable insight into their organization's risk and the nature of the attacks on their system. Rewarding those successful reports with, as for example in the Hoxhunt methodology, a gold star along a gamified journey gives users incentive to spot and report the next phishing attack.

**Malicious actors target people with social engineering. Phishing solutions should, too. We submit "behavioral cybersecurity" is the white hat answer to social engineering. Grounded in behavioral science and propelled by phishing simulations that ingrain threat reporting as a reflex, the Hoxhunt training results demonstrate that online behavior can be measured, managed, and indeed improved.**

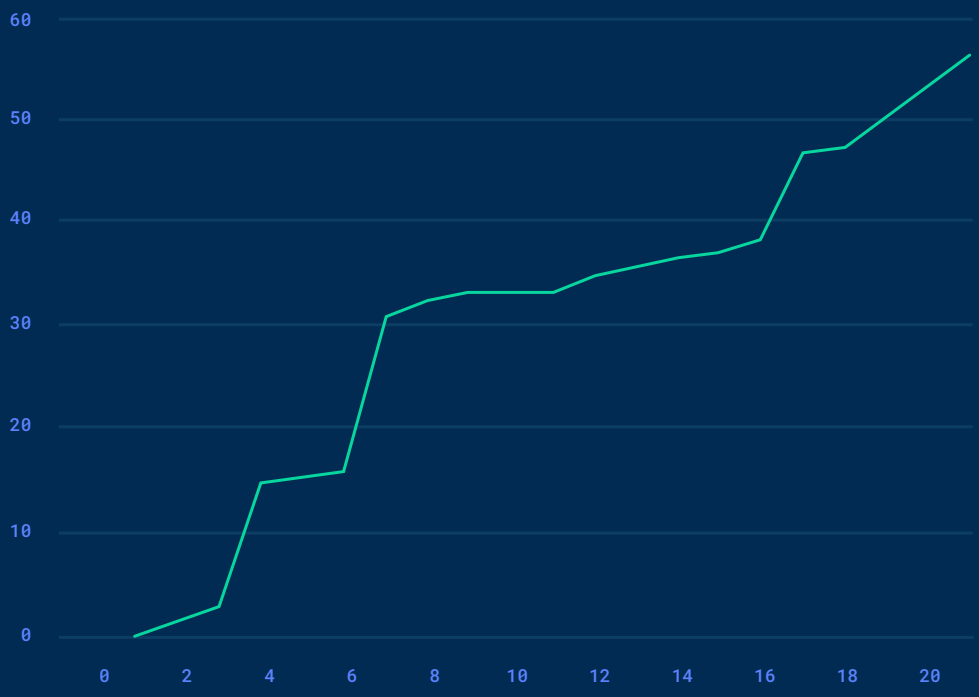
1. REAL THREAT REPORTING RATE, RELATIVE IMPROVEMENT PERCENTAGE FROM HOXHUNT TRAINING BASELINE




Employees learn to report real threats with the Hoxhunt training. After 6-10 Hoxhunt phishing simulations, cybersecurity behavior undergoes dramatic and sustained improvement. The dramatic rise in real threat reporting rates indicates that cybersecurity skill can be acquired and will be actively used on an ongoing basis with proper training based on threat reporting behavior.

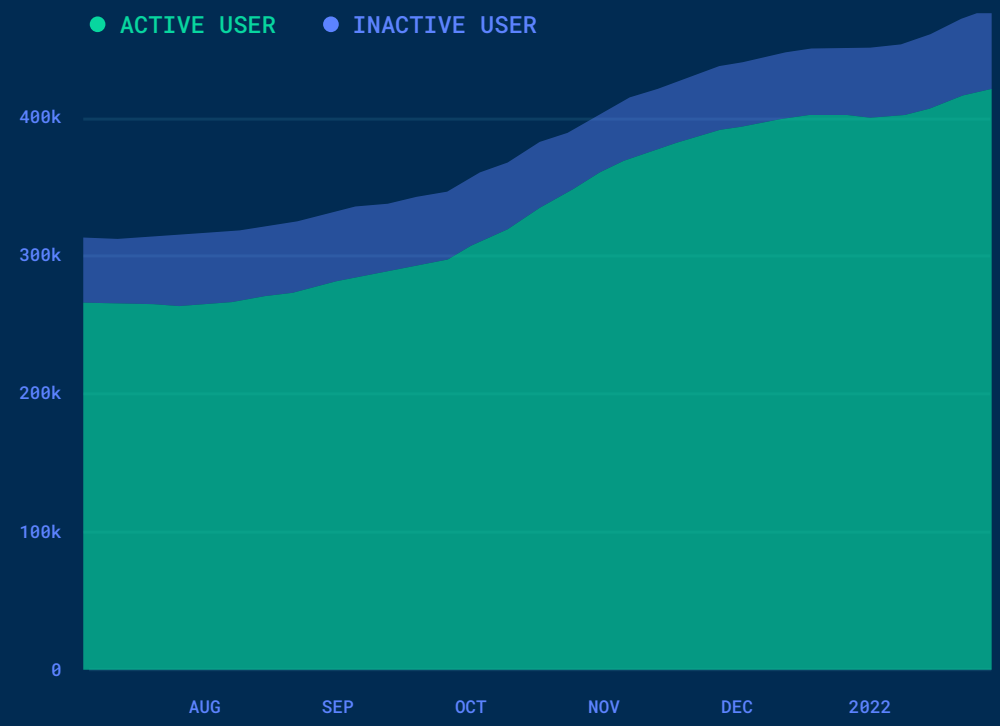
**Reporting real threats is the goal of a phishing training program. Email cybersecurity is a behavior based on habits. Good habits can be ingrained with good practice.**

## 2. REAL THREAT REPORTING ACCURACY, RELATIVE IMPROVEMENT PERCENTAGE FROM HOXHUNT TRAINING BASELINE




Real threat reporting accuracy—the skill to recognize and report a real phish—improves with the Hoxhunt training, too. The proportion of real phish reported vs. spam and other emails continuously rises with the Hoxhunt training. Phishing attacks are increasingly sophisticated, so employees must be able to continuously improve their skill.

**The continuous improvement at recognizing and reporting real phish translates to the elimination of thousands of real threats from corporate systems.**




➔ To better control for confounding variables, this sample includes users who were onboarded into the training program and who did not leave their company or job function during the observation period. 88.75% of users who began training in January stayed engaged through February 2022.

Our data indicates significant improvement can be achieved on threat reporting activity and accuracy with the Hoxhunt cyber-security awareness training program, which integrates the threat reporting into the training.

Ongoing user engagement is crucial. It ensures new knowledge is being acquired and existing knowledge is retained. Globally, 88.75% of users who began training with Hoxhunt in January, stayed engaged into 2022 even though the number of simulations ran into the dozens. This is usually administered as a voluntary training program but engagement rates approach those of mandatory programs.

User engagement is positively correlated with rising skill level. High skill level is correlated with high success rates and low failure rates and low missed-email-threat rates. This report will later show the relationship between user skill level (as defined by shield ranking) and user behavior.


Here, we can see how failure rate, the industry standard metric for awareness, declines significantly from the baseline. While we propose that success rate – hitting the threat reporting button – is a better metric, the decline in global user failure rate with Hoxhunt training is significant.

This report illuminates the interplay between user behavior and cybersecurity: how people's backgrounds influence their email behavior.

**User engagement is positively correlated with rising skill level. High skill level is correlated with high success rates and low failure rates and low missed-email-threat rates.**

# Some key findings on user background and cybersecurity behavior include:

**Measuring success AND failure is important**

While phishing simulation failure rates are the most traditionally valued metric for tracking an awareness training program's progress, success rate provides a fuller picture of user behavior because it demonstrates their actual skill at recognizing and responding to a suspicious email.

**Industry matters**

The wide top-to-bottom distribution of user performance between industries reveals the need for training interventions targeted to those challenged cohorts.

**Geography matters**

Given the state of globally distributed workforces, contractors, and outsourced agencies, it's important to know that certain regions are more likely to click on a dangerous link than others in order to implement an appropriate training program to suit those regions' needs.

**Job Role matters**

The wide top-to-bottom distribution of user performance between job functions reveals the need for training interventions targeted towards specific departments.

**Threat reporting appears seasonal**

Certain months saw clear drops and upticks in threat reports – where users reported a suspcious email to their IT department – across industries, job functions, and regions.

**Training type matters**

While recent research out of Switzerland indicated that some industry-standard awareness training methods are ineffective and even harmful, we have robust data showing dramatic organizational decreases in phishing simulation fail rates that are sustained throughout months and years of training. These results appear sustainable, with baseline failure rates dropping from over 17% to 2-6% and holding across organizations of all industries and sizes, even with phishing simulations that increase in difficulty level.

MALICIOUS ACTORS TARGET PEOPLE. THE FUTURE OF CYBERSECURITY HINGES UPON SOLUTIONS THAT DO AS WELL.

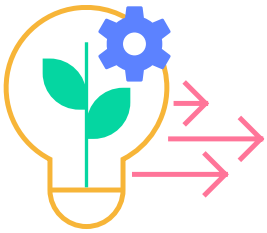
# Background

# Misalignment between dynamic cybercrime landscape and outdated awareness training models benefits cybercriminals

The evolving threat landscape is in a state of constant acceleration. Industry-standard awareness training models have been rendered obsolete.

**Costs of phishing have increased year over year since 2015**

**Cybersecurity VC/PE investment up**



**Security Awareness Innovation stays stagnant**

**The volume and costs of data breaches continue to shatter records. While cybersecurity investments have reached new heights, security awareness training innovation has lagged behind and has not adapted to effectively decrease the click rates of malicious emails and to lower the overall risk level.**

# Standard training methodology is obsolete

Traditionally, cybersecurity awareness training programs have taken a tough love, compliance-based approach. Protecting people from clicking the wrong thing in an email--and thereby opening a Thanos-sized portal to a data breach apocalypse--meant punishing them into compliance. Phishing awareness training models have thus been designed to check a compliance box and humiliate employees with booby prizes like rubber chickens, punish failure with extra training, sentence them to phishing prison, or even terminate them for failing a phishing attack simulation. The guiding success metric for such programs have been fail rates of phishing simulations, which are often delivered infrequently and with dry, stale content in a cookie-cutter format.

But phishing attack breaches continue to rise. That's mainly because the traditional approach is fundamentally misguided.

Traditional training is not just a culture killer but, as indicated by Verizon's 2021 Data Breach Investigation Report, it also obscures an organization's true risk of a breach: "Additionally, real phishing may be even more compelling than simulations. In a sample of 1,148 people who received real and simulated phishes, none of them clicked the simulated phish, but 2.5% clicked the real phishing email." – DBIR 2021

The DBIR continued: "Verizon Media believes the simulations and training offered by most security education teams do not mimic real life situations, do not parallel the behaviors that lead to breaches, and are not measured against real attacks the organization receives. This is why it is important to progress from the traditional security awareness model to that of using behavioral science to change the habits that lead to attack path breaking actions."

A Jan. 2021 Forrester report, "How To Manage The Human Risk in Cybersecurity," stressed a hearts-and-minds approach to cybersecurity. In addition to creating a positive experience around cybersecurity training, the Forrester report emphasized behavior change over awareness. Too often, the authors said, security programs dwell on passing awareness tests at the cost of achieving real risk-reducing awareness and behaviors. "Traditional approaches to security communication are limited to perfunctory one-off training sessions that fail to take customers, regulators, and other external stakeholders into account and rarely effect long-term behavioral change," states the report.

In fact, some training solutions based on established industry-standard methodologies (for example, quarterly phishing simulations with contextual training following failure, and no reward or even measurement for success) might actually increase

the risk of phishing breaches, as reported in 2022 Swiss research by Laine, Kostiainen and Capkun.

In their 15-month study of the phishing simulation results of 14,000 employees in a large multi-national corporation, the authors noted that the surprising outcome of elevated data breach risk following a traditional awareness training needed to be investigated further.

“This perhaps surprising result requires a careful interpretation. What our experiment showed is that this particular way of delivering voluntary training does not work. Instead, such training method may cause unexpected and negative side effects, such as increased susceptibility to phishing. This finding is significant, because the tested phishing training delivery method is a common industry practice... and the training material ... was designed by a specialized company according to known guidelines and best practices from previous work .... It would be interesting to study whether other possible ways to deliver contextual training (e.g., ones where interaction with the provided training material is enforced) would work better. Our study did not test the effectiveness of mandatory training.”

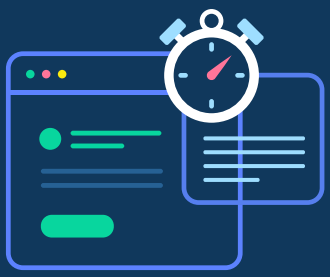
As a cybersecurity training platform built on reporting simulated phishing emails, Hoxhunt contains millions of data points on users' dangerous email behavior. The data helps uncover how and why people interact with attack emails based on who and where they are, and what they do for a living.

**“As the last year has taught us, just one bad click can have catastrophic consequences given today’s highly interconnected online environments.“**

# Methodology

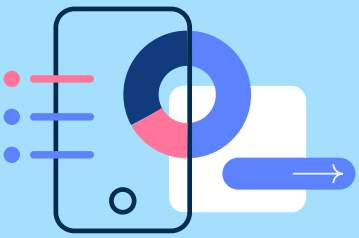
**Positive reinforcement:**
Measures success and failure

**Adaptive training:**
Adjusts difficulty level of simulations to skill level of user



**Microtraining:**
Short, enjoyable experiences

**Instant feedback:**
Connects threat feed to awareness training



**Gamification:**
Motivates long-term skill-building and engagement with rewards for success

Not all awareness training solutions are alike. There are key differences in elements of the training such as:

- goals (risk-based vs. compliance-based)
- style (didactic vs. interactive)
- tone (positive vs. punitive)
- difficulty, quality, relevance (dynamic vs. static; customized vs. cookie-cutter)
- content type (videos vs. simulations),
- volume (once a quarter vs. ongoing),
- cadence (scheduled vs. sporadic)

This is important because differences between awareness program designs and implementations significantly influence results on learning and behavior change. As the previously-referenced research by Laine et al. indicated, some traditional awareness trainings are actually detrimental to the objective of lowering risk of phishing breaches.

Results in this paper, however, show significant improvement in user performance over time in training in terms of:

- Lower failure rates
- Lower missed rates
- Higher success rates

The design and user experience of Hoxhunt cybersecurity awareness training is thus fundamentally relevant. Hoxhunt is designed for maximum long-term engagement, earning user participation with gamified content targeted towards risk-based (not compliance-based) training and behavior change.

Hoxhunt is a gamified phishing training platform. It leverages AI and machine learning models to automatically customize learning paths to individuals' needs and skill levels as they progress over time. Phishing simulations are based on up-to-date, real-world attacks and sent to employees at varied intervals; between 12-36 threat simulations are sent per year.

### Threat reporting is key. So is measuring success + failure.

Users participate in the training by reporting all suspicious emails via the Hoxhunt reporting button, which is integrated into their corporate email client. The training is built around threat reporting behavior, which differs from most training programs that focus on failure rates, which consider a missed phishing simulation as a successful outcome. But threat reporting serves dual functions of revealing true risk while actively modifying behavior.

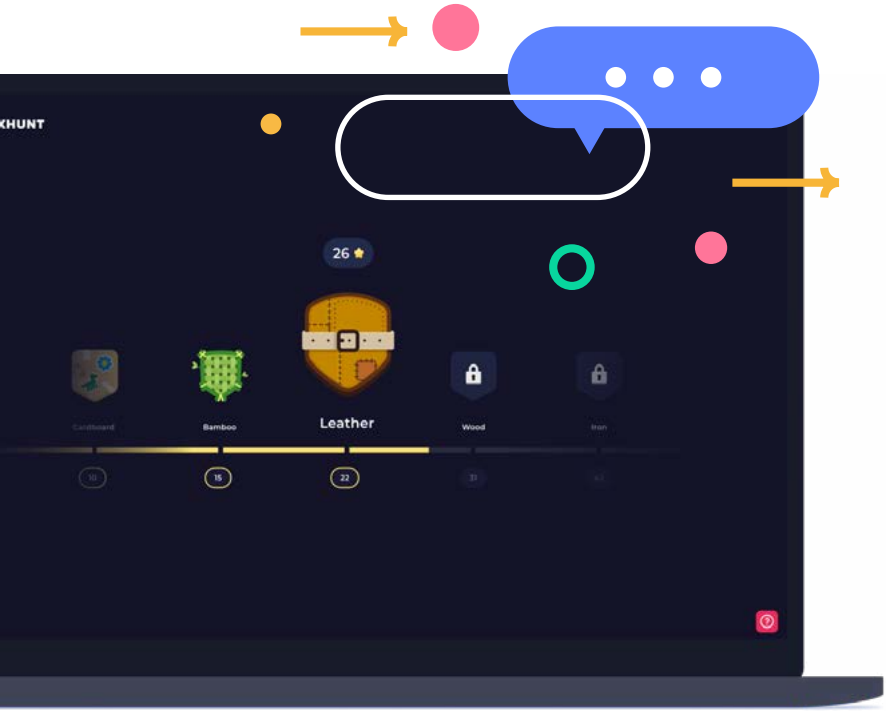
**"Hoxhunt is designed for maximum long-term engagement, earning user participation with gamified content targeted towards risk-based (not compliance-based) training and behavior change."**

Threat reporting is an activity that replaces a bad behavior (clicking a malicious link) with a good behavior (clicking the report button). The gamified platform provides rewards and/or lessons following both success and failure with a simulated phishing email. Clicking the report button promises a small hit of dopamine, which entrains desirable email behavior.

Hoxhunt actually values success rates (reporting a simulated phishing threat) more highly than failure rates (clicking on a simulated phishing link). This is a crucial difference. High success rates and low failure rates are correlated, but not perfectly. The gap between successfully reported phishing simulations and failed simulations is called “missed” emails. Misses equate to unknown user behavior, skill level and organizational risk. Hoxhunt training aims to give the highest true risk value possible for cybersecurity leaders and their teams. The discussion section will go further into the value and concept of true risk vs. measured risk, but ultimately there must be a high reporting rate in order to actually measure and manage true risk at the organizational level.

## Adaptive training

Phishing simulation difficulty levels (classified on a scale of 1-4) are adapted to user skill levels as they fluctuate over time. Simulations are delivered at varied intervals of up to 36 simulations per year. The gamified aspect of the Hoxhunt training encourages users to continue reporting phishing simulations and real threats with in-game rewards and dashboards that keep track of the employee’s skill progress through the Hoxhunt Shields. The more someone reports threat simulations successfully, the more difficult the simulations will become and the higher their skill level becomes. As shown in a later graph, engagement rates do improve over time and hold steady despite elevations in difficulty level. This is in keeping with known gamification practices, in which users must be challenged at the sweet spot of difficulty level in order to encourage skills acquisition but not discourage them with too difficult a task.



“

**HOXHUNT GIVES SOMEONE A BUTTON AND MAKES IT SO EASY TO REPORT A THREAT THAT IT BECOMES INGRAINED AS AN INSTINCTIVE BEHAVIOR. THE BUTTON IS KEY TO BEHAVIOR CHANGE, AND THAT’S WHAT I WAS LOOKING FOR: SOMETHING THAT WOULD ACTUALLY GET PEOPLE TO PARTICIPATE FREQUENTLY ENOUGH THAT THE LESSONS WOULD STICK AND THEIR BEHAVIOR WOULD CHANGE.”**

**– Lisa Kubicki, Director, Trust & Security Training & Awareness At Docusign**

# This report examines employee interactions with phishing simulations in terms of:

**Success / success rate:**
User successfully reported a simulated phishing email with the Hoxhunt threat reporting button

**Missed / miss rate:**
User did not react to a phishing email

**Failure / failure rate:**
User clicked on a malicious link, entered credentials on a malicious site, or tried to download an attachment in a simulated phishing email

**Report / reporting rate:**
User reported a simulated threat, spam or non-malicious email, or a real non-simulated threat that bypassed email filters

# Countries:

- Argentina
- Australia
- Austria
- Bangladesh
- Belarus
- Belgium
- Brazil
- Bulgaria
- Cambodia
- Canada
- Chile
- China
- Colombia
- Costa Rica
- Croatia
- Czech Republic
- Denmark
- Dominican Republic
- Egypt
- El Salvador
- Estonia
- Finland
- France
- Germany
- Greece
- Hong Kong
- Hungary
- India
- Indonesia
- Ireland
- Israel
- Italy
- Jamaica
- Japan
- Kenya
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malaysia
- Mexico
- Morocco
- Myanmar
- Netherlands
- New Zealand
- Norway
- Pakistan
- Peru
- Philippines
- Poland
- Portugal
- Qatar
- Romania
- Russia
- Saudi Arabia
- Serbia
- Singapore
- Slovakia
- Slovenia
- South Africa
- South Korea
- Spain
- Sweden
- Switzerland
- Taiwan
- Thailand
- Trinidad and Tobago
- Turkey
- Ukraine
- United Arab Emirates
- United Kingdom
- United States
- Uruguay
- Vietnam

# Job roles:

SALES

MARKETING

COMMUNICATIONS

FINANCE

HR

IT

SOFTWARE DEVELOPMENT

CUSTOMER RELATIONS

BUSINESS DEVELOPMENT

**There are clear and sometimes surprising differences in email behavior between users based on their geography, industry, and job role. Behavior change solutions must take those differences into account.**

# Industries:

| | |
|---|---|
| Accounting | Information Technology and Services |
| Airlines/Aviation | Insurance |
| Automotive | Legal Services |
| Banking | Logistics and Supply Chain |
| Biotechnology | Machinery |
| Chemicals | Manufacturing |
| Civil Engineering | Maritime |
| Computer Hardware | Mechanical or Industrial Engineering |
| Computer Software | Media Production |
| Construction | Mining & Metals |
| Consumer Goods | Oil & Energy |
| Dairy | Packaging and Containers |
| E-Learning | Pharmaceuticals |
| Electrical/Electronic Manufacturing | Public Policy |
| Energy/Utilities & Waste Treatment | Publishing |
| Engineering | Real Estate |
| Entertainment | Retail |
| Financial Services | Security and Investigations |
| Food & Beverages | Semiconductors |
| Food Production | Telecommunications |
| Gambling & Casinos | Transportation/Trucking/Railroad |
| Government Administration | Utilities |
| Hospital & Health Care | Wholesale |

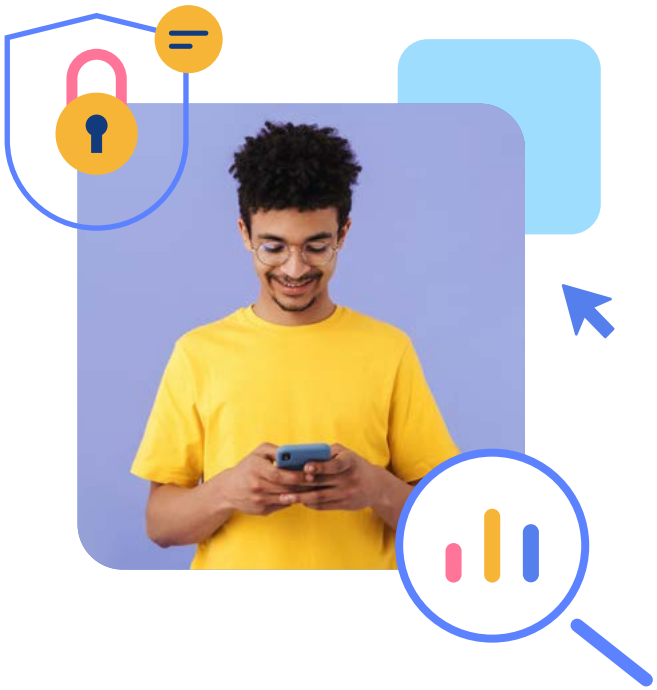
# Results

# Measuring success matters.

The differences in worst and best simulation performance appear more accurate when characterized by high success rates for good performance and low success rates for bad performance, as opposed to high and low failure rates for bad and good performance. Cohorts with the highest fail rates do not necessarily possess the lowest success rates, and vice-versa. This finding supports the hypothesis that counting success is important for identifying the true level of skill and true risk posture of a cohort; and that success must therefore be counted. Misses cannot be assumed to be equivalent to success (or to failure).

In the discussion section, we expand on the power of focusing on threat reporting and success. By measuring user behavior based on success and threat reporting, you actually influence it towards better outcomes. This is likely due to replacement behavior theory, in which a bad behavior (clicking a phish) is replaced with a good behavior (hitting the report button).

Overall, there are clear discrepancies between user behavior based on their geographical and professional backgrounds. Also, threat reporting might have a seasonality component.



**“By measuring user behavior based on success and threat reporting, you actually influence it towards better outcomes.“**

# Results – Performance by Department

Hoxhunt conducted an analysis by Department (see more on page 29), and found a few interesting key takeaways. The breakdown of failure, success, and miss rate reveals that more missed phishing simulations translates to higher risk of a phishing breach. The Customer relationship (CR) department (see page 29) had the lowest fail rate, which would appear to make make CR a lower risk employee group by traditional standards. However, CR had the second-lowest success rate, which would place CR in the high-risk employee group. This discrepancy is due to the department's high miss rate, where CR was second-worst. The un-known risk represented by misses translated to poor email behavior.

**Lowest miss rate**

1. IT **32.9%**
2. Software development **33.7%**
3. Business Development **33.9%%**

**Highest miss rate**

1. Sales **40.5%**
2. Customer relationship **39.1%**
3. HR **37.0%**

**Lowest fail rate**

1. Customer relationship **4.0%**
2. IT **4.1%**
3. Finance **4.1%**

**Highest fail rate**

1. Sales **5.3%**
2. Business Development **4.9%**
3. Marketing **4.9%**

**Highest success rate**

1. IT **63.0%**
2. Software development **62.1%**
3. Business Development **61.9%**

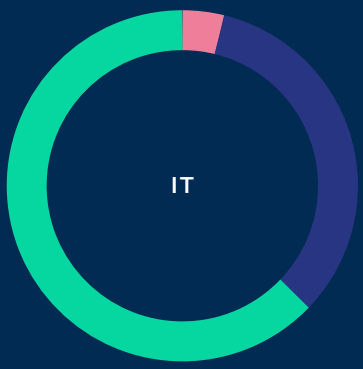
**Lowest success rate**

1. Sales **54.1%**
2. Customer relationship **56.9%**
3. HR **57.6%**

**High miss rate correlates to poor performance; sales had the worst performance across the board.**

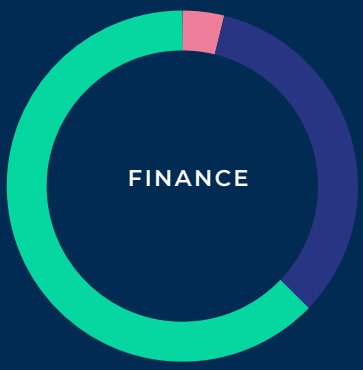
# Performance by department - full breakdown

HIGHEST SUCCESS RATE




- Success rate **63%**
- Fail rate **4.1%**
- Miss rate **32.9%**


- Success rate **62.1%**
- Fail rate **4.2%**
- Miss rate **33.7%**

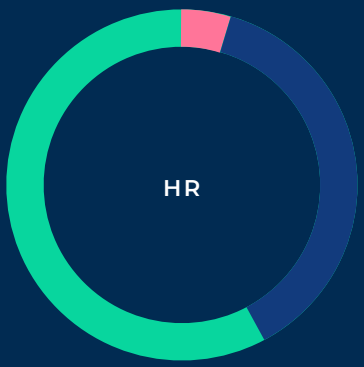



- Success rate **61.9%**
- Fail rate **4.1%**
- Miss rate **34.0%**

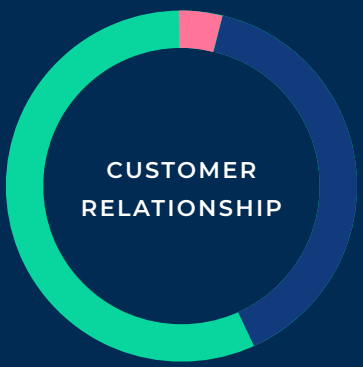

- Success rate **61.2%**
- Fail rate **4.9%**
- Miss rate **33.9%**


- Success rate **60.0%**
- Fail rate **4.5%**
- Miss rate **35.6%**

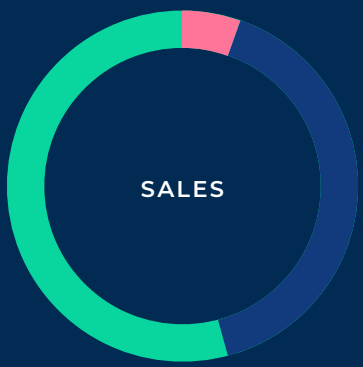

- Success rate **59.1%**
- Fail rate **4.9%**
- Miss rate **36.0%**




- Success rate **57.6%**
- Fail rate **4.7%**
- Miss rate **33.7%**




- Success rate **56.9%**
- Fail rate **4.0%**
- Miss rate **39.1%**



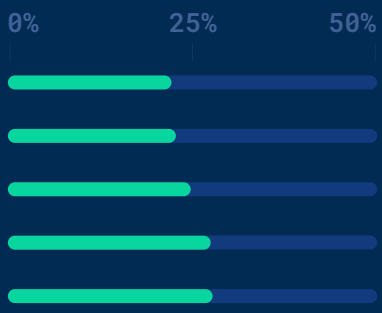

- Success rate **54.1%**
- Fail rate **5.3%**
- Miss rate **40.5%**

# Results – Performance by Industry

Hoxhunt analyzed performance by industry and found that performance variation was higher between different industries than in any other cohort.  There could be multiple reasons for this variation. Email habits and the nature of computer work are likely different between industries. Further research into users' profiles will help reveal whether personal characteristics such as age, gender, culture and language play a role. But the high variation in success and fail rates between industries would indicate some industries, like construction, are at a higher risk of getting phished than others.

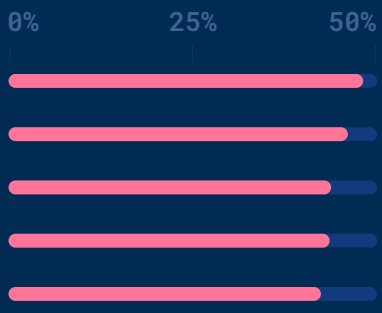
# Miss rate

## Lowest miss rate



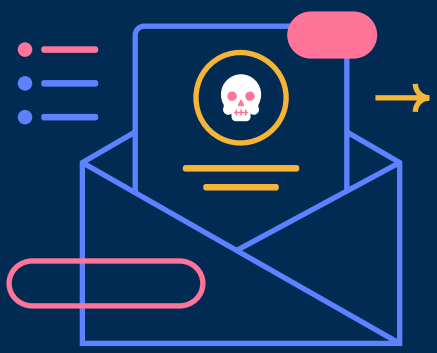

1. Pharmaceutical **22.2%**
2. Entertainment **22.8%**
3. Public Policy **24.8%**
4. Mechanical/Industrial Engineering **27.5%**
5. Biotech **27.6%**

## Highest miss rate



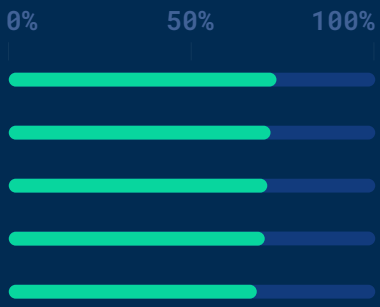

1. Security and investigation **48.7%**
2. Construction **46.6%**
3. Electronic manufacturing **44.3%**
4. Real Estate **44.1%**
5. Gambling & Casinos **42.9%**

There is a more than **2x differentiation** between industries that don't report phishing simulations and those that do.



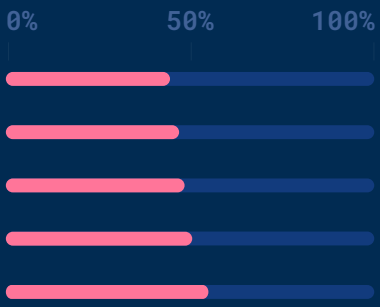
# Success rates

**Highest success rate**




1. Public Policy **74.0%**
2. Pharma **72.2%**
3. Entertainment **71.3%**
4. Mechanical/industrial engineering **70.6%**
5. Banking **68.4%**

**Lowest success rate**

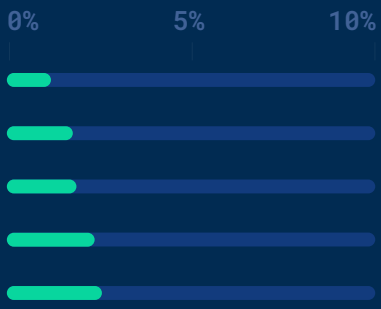



1. Security and Investigations **45.0%**
2. Construction **47.5%**
3. Real Estate **49.0%**
4. Electrical / Electronic Manufacturing **51.1%**
5. Gambling & Casinos **52.6%**

**High relationship between miss rate and performance. Missing phishing simulations equates to bad outcomes.**

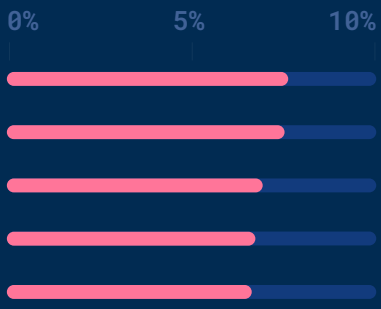
# Failure rates

**Lowest failure rate**




1. Public Policy **1.2%**
2. Maritime **1.8%**
3. Mechanical/industrial engineering **1.9%**
4. Banking **2.4%**
5. Computer Hardware **2.6%**

**Highest failure rate**




1. Dairy **7.7%**
2. Publishing **7.6%**
3. Automotive **7.0%**
4. Real Estate **6.8%**
5. Semiconductors **6.7%**

**Fail rates are many times higher in certain industries than others.** Fail rates do not correlate with success rates as closely as expected.

# Results – Performance by Country

Geography appears to play a role in cybersecurity user behavior. Note that the phishing simulations and overall training is localized to specific languages, but language may still play a role.

# Fail rate by country


**Lowest fail rate**

1. Croatia **2.3%**
2. Hungary **3.3%**
3. Austria **3.4%**
4. Poland **3.4%**
5. Finland **3.7**

**Highest fail rate**

1. Saudi Arabia **8.1%**
2. Taiwan **7.7%**
3. India **7.2%**
4. South Africa **6.7%**
5. New Zealand **6.6%**

**High variation between fail rates of best/ worst performers indicates geography plays a significant role in phishing breach risk. Multinational companies might be able to lower risk by putting in extra effort at strengthening skills of lower performers.**

# Success rate by country


**Highest success rate**

1. Hungary **70.9%**
2. Austria: **66.7%**
3. Switzerland **65.9%**
4. Denmark: **65.1%**
5. Czech Republic **64.7%**

**Lowest success rate**

1. China **29.0%**
2. Saudi Arabia **32.9%**
3. Peru **36.5%**
4. Myanmar **37.5%**
5. Brazil **37.6%**

**Success rates varied significantly between top and low performers. Success and fail rates by country do not match perfectly, but European countries appeared to perform best.**

# Miss rate by country


**Lowest miss rate**

1. Hungary **25.8 %**
2. Austria **29.8%**
3. Switzerland **30.1%**
4. Denmark **30.3%**
5. Germany **32 %**

**Highest miss rate**

1. China **64.4%**
2. Peru **58.6%**
3. Qatar **57.5%**
4. Myanmar **57.3%**
5. Saudi Arabia **57.0%**

**High miss rates are strongly correlated with negative outcomes: low success rates and high fail rates.**

# United States performance

SUCCESS RATE

**55.6%**

FAIL RATE

**5.5%**

MISS RATE

**38.9%**

# Other Key Performers

### Canada

- Fail rate: **4.8%**
- Miss rate: **33.5%**
- Success rate: **61.6%**

### United Kingdom

- Fail rate: **5.1%**
- Miss rate: **34.1%**
- Success rate: **60.8%**

### Norway

- Fail rate: **4.5%**
- Miss rate: **33.0%**
- Success rate: **62.5%**

### Denmark

- Fail rate: **4.6%**
- Miss rate: **30.3%**
- Success rate: **65.1%**

### Finland

- Fail rate: **3.7%**
- Miss rate: **33.3%**
- Success rate: **63.0%**

### Sweden

- Fail rate: **5.2%**
- Miss rate: **37.4%**
- Success rate: **57.4%**

# Other Key Performers

**Switzerland**

- Fail rate: **4.0%**
- Miss rate: **30.1%**
- Success rate: **65.9%**

**Belgium**

- Fail rate: **5.1%**
- Miss rate: **37.7%**
- Success rate: **57.2%**

**Spain**

- Fail rate: **5.3%**
- Miss rate: **43.8%**
- Success rate: **50.9%**

**Austria**

- Fail rate: **3.4%**
- Miss rate: **29.8%**
- Success rate: **66.7%**

**Germany**

- Fail rate: **4.1%**
- Miss rate: **32.0%**
- Success rate: **63.9%**

**France**

- Fail rate: **5.2%**
- Miss rate: **43.1%**
- Success rate: **51.7%**

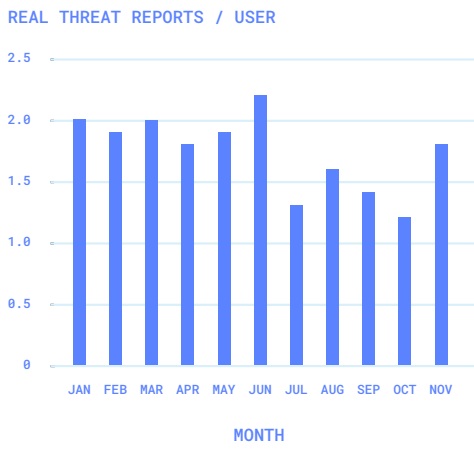
**Netherlands:**

- Fail rate: **4.1%**
- Miss rate: **33.4%**
- Success rate: **62.4%**

**Denmark, Finland and Germany have the highest success rate.**

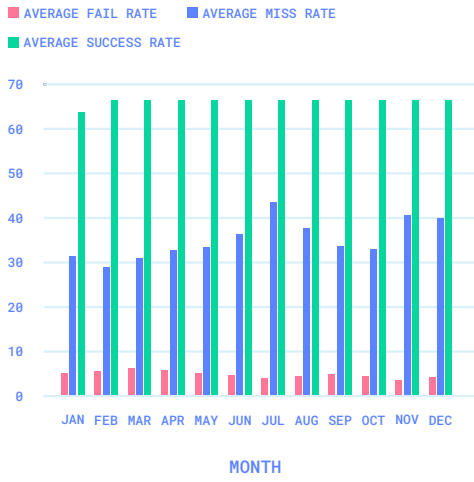
# Seasonality of threat reporting

Monthly threat reports per user globally showed a high point in June, followed by a summer drop and then steady rise through November. The summer drop could likely be due to less work email use by employees due to vacation. The upticks in January, March, and the high point in June bears further investigation.




### Monthly changes in rates of failure, misses, and success

This graph indicates that while failure rates have some fluctuation and are on a downward trend with the training program, there are more pronounced seasonal fluctuations with miss rates and success rates. The spike in misses in June and July could be attributed to summer vacations. But what's interesting in these fluctuations is that success and miss rates appear tethered, as lower miss rates coincide with higher success rates; this would indicate that the training is working and participation results in more accurate threat reporting skills.




**"The upticks in January, March, and the high point in June bears further investigation."**

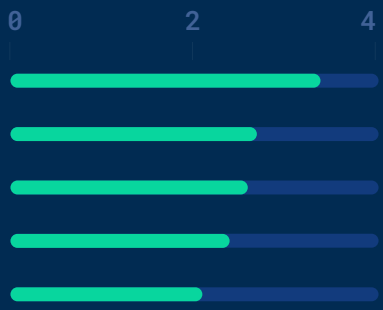
# Results – Threat reports by Industry

There is significant variance between industries in levels of threat reporting and threat reporting accuracy. This is important as threat reporting is crucial for determining individual skill level and organizational risk posture. Also important is that threat reporting is not rendered less effective when higher levels of spam are reported along with higher levels of real threats. Phishing attacks today are so sophisticated that threat reporting should be an instinctive behavior, and threat reports should be made when there is any question at all about an email or notification.

# Real threat reporting by industry: Monthly threats-per-user

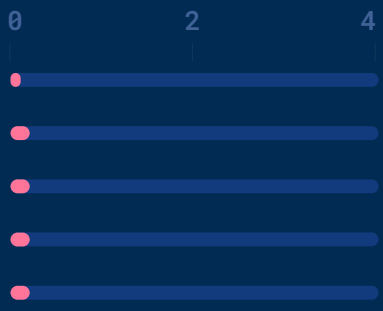
**Best threat reporting**

1. Biotechnology **3.4**
2. Automotive **2.7**
3. Computer Hardware **2.6**
4. Information Technology and Services **2.4**
5. Insurance **2.1%**




**Lowest threat reporting**

1. Food & Bev **0.1**
2. Consumer Goods **0.2**
3. Dairy **0.2**
4. Financial Services **0.2**
5. Hospitals **0.2**

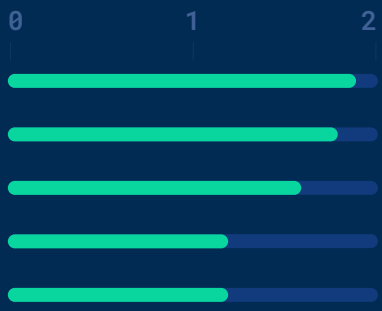



**The low threat reporting by Financial Services is surprising, considering the performance of other high-computer-and-email-use industries. Further inquiry into the way computers are used between industries would be helpful to understand the stark differences between industries. The high-threat-reporting industries tend to do most of their work on computers, and email use is core to their job function.**

# Accurately reported phish per-user, per month

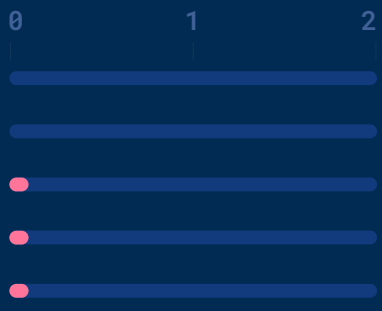
**Highest accuracy**

1. Insurance **1.9**
2. Automotive **1.8**
3. Biotechnology **1.6**
4. Civil Engineering **1.2**
5. Packaging and Containers **1.2**




**Lowest accuracy**

1. Utilities **0.0**
2. Food & Beverages **0.0**
3. Consumer Goods **0.1**
4. Dairy **0.1**
5. Financial Services **0.1**

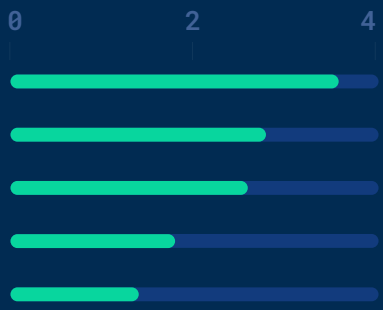



**Accuracy signifies skill. High and low accuracy is linked to total threat reporting. Those who report more, appear to be, or to become, more skilled.**

# Spam misreported as real threats per-user, per month

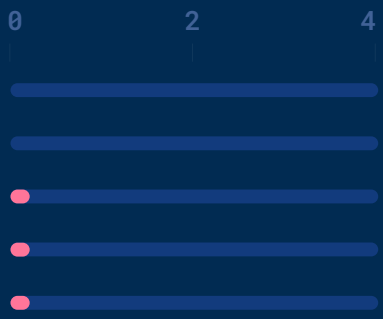
**Best spam reporting**

1. Biotechnology **1.8**
2. Computer Hardware **1.4**
3. Information Technology and Services **1.3**
4. Automotive **0.9**
5. Packaging and Containers **0.7**




**Lowest spam reporting**

1. Utilities **0.0**
2. Food & Beverages **0.0**
3. Telecommunications **0.1**
4. Consumer Goods **0.1**
5. Dairy **0.1**




**Misreporting spam as a threat is not a bad thing. It's better to be safe than sorry. The best-performing industries also misreport spam at higher levels.**

# Results – Threat reports by Country

Geography appears to play a role in cybersecurity user behavior. Note that the phishing simulations and overall training is localized to specific languages, but language may still play a role.

# Real monthly threat reporting by country

AVERAGE NUMBER OF THREAT REPORTS PER USER


**Best threat reporting**

1. Switzerland **2.2**
2. Denmark **2.0**
3. United Arab Emirates **2.0**
4. United Kingdom **1.5**
5. Australia **1.4**

**Worst threat reporting**

1. China **0.2**
2. Romania **0.2**
3. Brazil **0.3**
4. Greece **0.3**
5. Hungary **0.3**

**10X**

The best performing countries report 10 times more threats per user

# Accurately reported phish per-user, per month


**Most reported phish**

1. Switzerland **1.7**
2. United Arab Emirates **1.4**
3. Denmark **1.3**
4. South Africa **0.9**
5. United Kingdom **0.9**

**Least reported phish**

1. China **0.1**
2. Luxembourg **0.1**
3. Pakistan **0.1**
4. Romania **0.2**
5. Brazil **0.2**

**1.7**

**Total threat reporting is associated with accuracy and skill level.**

# Most/least spam reported per user


**Most reported spam**

1. Denmark **0.7**
2. United Arab Emirates **0.6**
3. United Kingdom **0.6**
4. Australia **0.6**
5. Switzerland, Canada, Austria, Turkey, Mexico: **0.5**

**Least reported spam**

1. Ireland **0.1**
2. Philippines **0.1**
3. Taiwan **0.1**
4. Romania **0.1**
5. Brazil and 12 others **0.1**

**0.7**

**Misreporting spam is not a dangerous behavior. Denmark is consistently a top-5 performing country.**

# United States performance

THREAT REPORTS / USER

**0.9**

REPORTED REAL PHISH / USER

**0.5**

REPORTED SPAM / USER

**0.4**

IN A GLOBAL ENTERPRISE, EACH COUNTRY'S THREAT REPORTING IS VITAL TO THE SECURITY OF ALL COUNTRIES WITHIN THE NETWORK. THE MORE FREQUENTLY PEOPLE REPORT THREATS, THE GREATER THEIR SKILL BECOMES, AND THE MORE THREATS ARE REMOVED FROM THE SYSTEM.

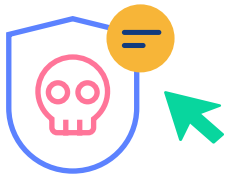
# Discussion

# Several key points emerge in this report.

**Email behavior** differs between users based on geographical background, job function, and their industries.

**Measuring success**, based on threat reporting, likely entrains threat reporting as a replacement behavior to clicking a malicious email

**High success rates** are of greater value to determining user risk and skill level than low failure rates



**Threat reporting** is key to behavior change and skill acquisition

**High success rates** are associated with low miss rates: missed phishing simulations are more correlated with failure than success

**The most important findings in this report are that user behavior and skill level can indeed be changed and improved based on the Hoxhunt security awareness training methodology.**

There are several findings that bear further inquiry. It's important to better understand the root causes of variance in threat reporting behavior and skill level between geographies, industries, and job functions, in order to design a curriculum (or perhaps security controls) that would help close those performance gaps.

Engagement is crucial to understanding and conditioning user behavior. The KPIs in traditional training methodologies typically start and stop at failure rate. This report provides, to our knowledge, the most convincing data supporting the efficacy of threat reporting as foundational to behavior change in an awareness training program.

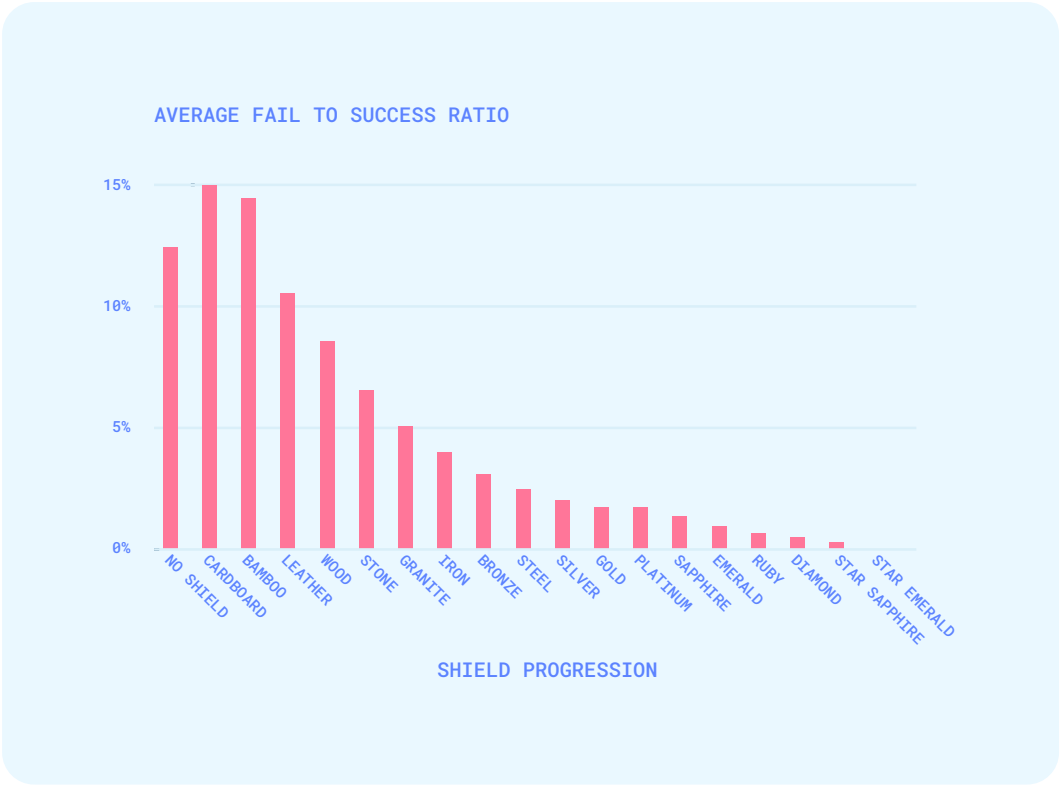
**This report provides, to our knowledge, the most robust data supporting:**

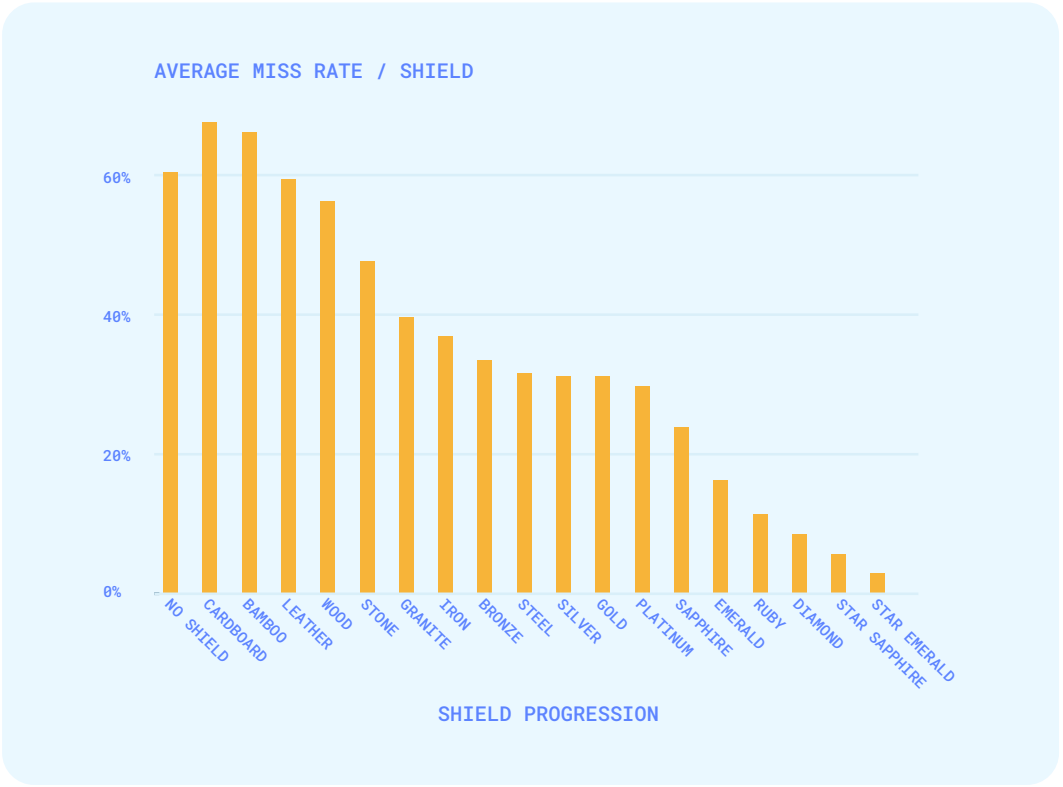
- the efficacy of threat reporting as foundational to behavior change in an awareness training program
- the use of success rate (as measured by threat reporting) rather than failure rate alone, as a valuable metric for measuring skill level, performance, progress, and organizational risk posture
- the conclusion that misses cannot be assumed to be equivalent to success from a cybersecurity behavior perspective

Moreover, when a single user reports a single threat, it can be removed from the system before harming other users. Threat reporting is a crucial metric and central to behavior change and risk reduction.
Also important is the factor of rewarding success and tracking skill level in training. Hoxhunt does this by rewarding employees with stars, achievements, and shields for successfully reporting phishing simulations along a gamified user journey. We believe this gamified system of rewards for good behavior improves skill, which is highly correlated with the positive outcomes of low fail rates, low miss rates, and high success rates.

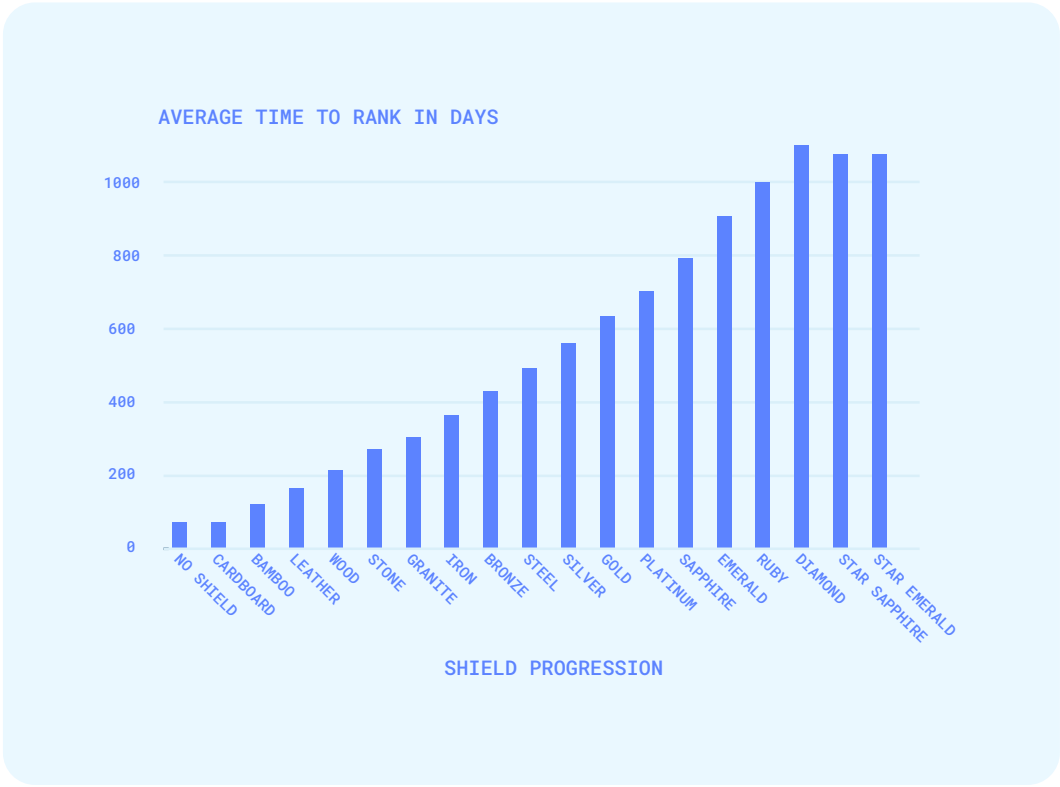
Crucially, the time it requires for individual users to elevate skill follows predictable patterns. And, given the high level of engagement maintained throughout the Hoxhunt training, that skill level can translate to an organizational skill level and risk posture.

**"This report provides, to our knowledge, the most convincing data supporting the efficacy of threat reporting as foundational to behavior change in an awareness training program."**


AVERAGE FAIL TO SUCCESS RATIO
15%
10%
5%
0%
NO SHIELD
CARDBOARD
BAMBOO
LEATHER
WOOD
STONE
GRANITE
IRON
BRONZE
STEEL
SILVER
GOLD
PLATINUM
SAPPHIRE
EMERALD
RUBY
DIAMOND
STAR SAPPHIRE
STAR EMERALD
SHIELD PROGRESSION


AVERAGE MISS RATE / SHIELD
60%
40%
20%
0%
NO SHIELD
CARDBOARD
BAMBOO
LEATHER
WOOD
STONE
GRANITE
IRON
BRONZE
STEEL
SILVER
GOLD
PLATINUM
SAPPHIRE
EMERALD
RUBY
DIAMOND
STAR SAPPHIRE
STAR EMERALD
SHIELD PROGRESSION


SUCCESS RATE
80%
60%
40%
20%
0%
NO SHIELD
CARDBOARD
BAMBOO
LEATHER
WOOD
STONE
GRANITE
IRON
BRONZE
STEEL
SILVER
GOLD
PLATINUM
SAPPHIRE
EMERALD
RUBY
DIAMOND
STAR SAPPHIRE
STAR EMERALD
SHIELD PROGRESSION


AVERAGE TIME TO RANK IN DAYS
1000
800
600
400
200
0
NO SHIELD
CARDBOARD
BAMBOO
LEATHER
WOOD
STONE
GRANITE
IRON
BRONZE
STEEL
SILVER
GOLD
PLATINUM
SAPPHIRE
EMERALD
RUBY
DIAMOND
STAR SAPPHIRE
STAR EMERALD
SHIELD PROGRESSION

# CONCLUSION

Because behavior can be changed, employees must be reconsidered as the first line of defense in a cybersecurity system. At present, the people layer is considered the greatest weakness and virtually unsolvable. As recent research has shown, this has been due in part to rapid advancement of social engineering beyond the capabilities of old-school security awareness methodology, which can actually be detrimental to lowering risk. But new technologies can be combined with a more human touch to deliver behavior replacement training that people like and which actually works.

Malicious actors target people with social engineering tricks and tactics. Solutions must also target people. Built around threat reporting and propelled by measuring success + failure, we propose a new approach we call behavioral cybersecurity entrainment. With every push of a button, individuals and their organizations become smarter, more resilient, and more cyber-secure.

**With every push of a button, individuals and their organizations become smarter, more resilient, and more cyber-secure.**

HOXHUNT

# Interested in learning more about Hoxhunt?

If you have a question feel free to contact marketing@hoxhunt.com.

HOXHUNT.COM