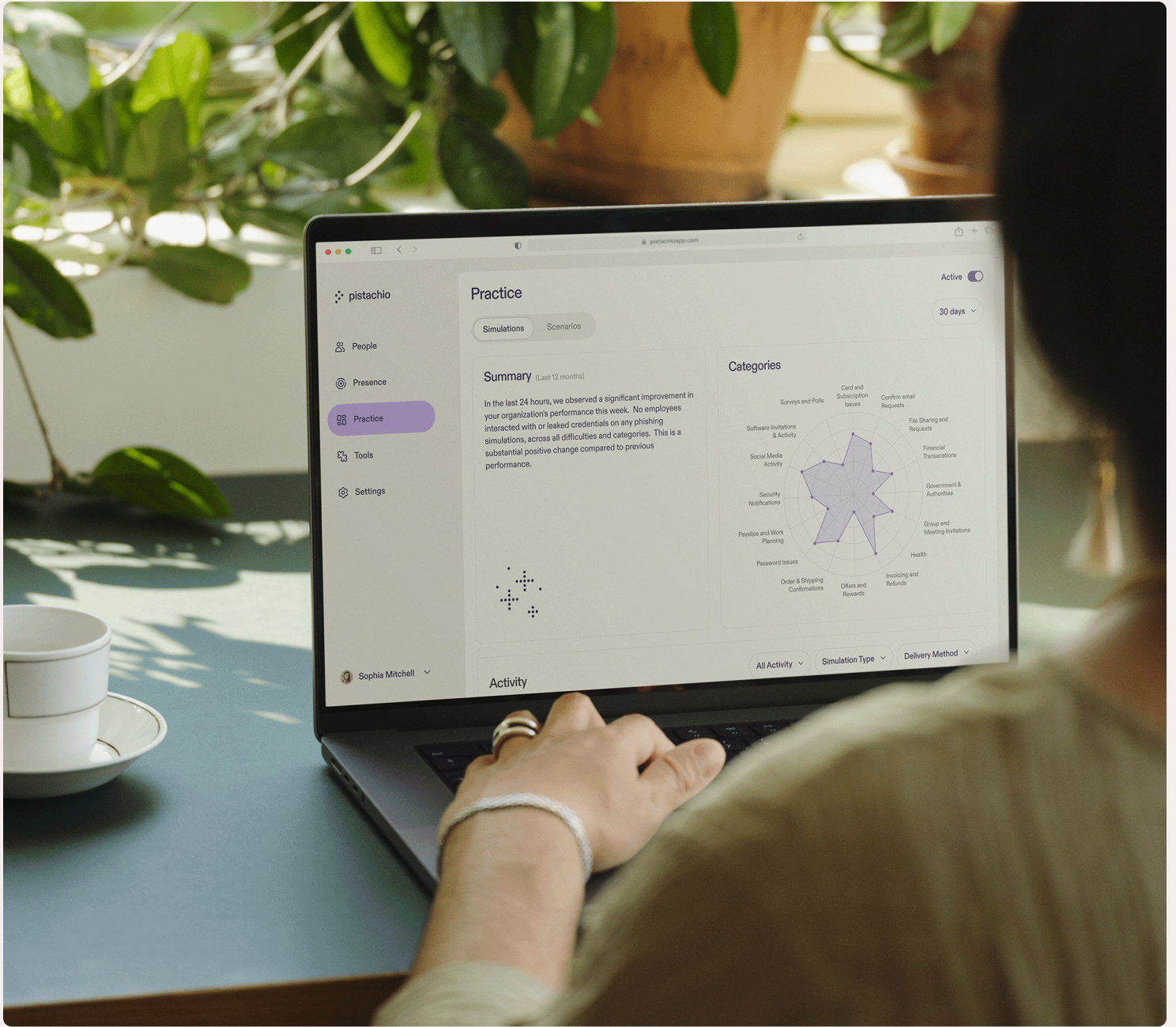




The Phishing Behaviour Report 2026

Why progress can't be measured by click rate alone.

Contents

Executive Summary	04
Introduction: 12-Month Journey	06
The Data	07
Section 1: How Phishing Behaviour Changes Across the Journey	12
Section 2: How Your Sector Compares	17
Section 3: Where the Biggest Risks Sit Inside the Organisation	21
Section 4: What Your Business Is Up Against	26
Conclusion: From Measuring Click Rates to Building Resilience	29
Methodology	32

23 Years

of IT admin time saved.

In 12 months, 2,473,158 simulations were sent from the Pistachio platform to 1,288 organisations.
Sending these manually would have taken 206,097 hours of IT admin time.
That is more than 23 years, around the clock.

Executive Summary

This report examines a year of phishing behaviour across 648 organisations with a complete 12-month record.

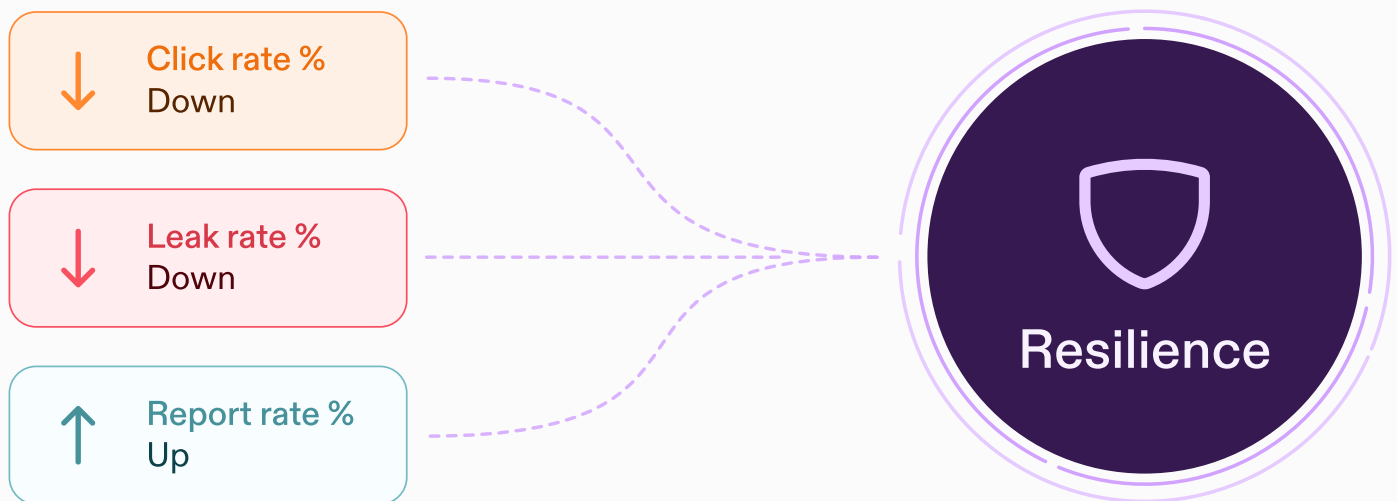
Based on 123,692 users it analyses:

- How people respond to simulations at every stage of a 12-month programme
- Where risk concentrates by sector and department
- What the results say about how phishing resilience should be measured



One key finding stands out:

Click rate, the metric most phishing programmes are judged on, is only part of the picture. A strong indicator of improvement needs to go beyond click rate, and should look at how click, leak and report behaviours change together over time.



Five findings that challenge conventional security awareness programmes

1

More users report than click on their first simulation, but 1.57% still leak credentials.

There is a baseline of security awareness, but in an organisation of 500, that still means up to eight people could hand over their login details to a convincing attack.

2

Click rates peak at six months, when users are tested hardest.

It looks like regression, but the 6-month stage contains more simulations and the highest share of Hard tests. The increase reveals risk that simpler tests don't expose.

3

Technical teams are not automatically low risk.

Over a year, 30.27% of Tech Development users and 28.53% of IT users clicked at least once. Knowledge does not guarantee behaviour.

4

The same test produces very different results across teams.

With a similar difficulty mix across all 18 departments, cumulative click rates ranged from 26.35% in Design to 41.31% in Construction. A one-size-fits-all approach cannot account for that variation.

5

Click rate is only part of the picture.

Resilience means fewer clicks, fewer credential leaks and more reports. By 12 months, users reported suspicious emails nearly twice as often as they clicked them, showing that effective programmes build vigilance, not just fewer clicks.

**Simulation scoring**

Each Pistachio simulation is scored 1 to 10 and grouped into Easy (1 to 3), Medium (4 to 7) and Hard (8 to 10).

Introduction:

12-Month Journey

Across 354,962 phishing simulations, the results follow a consistent pattern: click and leak rates rise through the first six months of a programme, then decline and settle.

That mid-point peak is what an effective programme looks like: simulations at their hardest and most frequent, surfacing risk that was already there. Section 1 shows this in detail.

Most phishing programmes are judged on one question: did the click rate go down? This report makes the case that it is the wrong metric to look at in isolation. Simulations that remain static may produce falling click rates without necessarily improving resilience. A falling click rate can hide a workforce that has simply learned to recognise the templates.



A phishing simulation programme has one objective:
a workforce that responds well when a real attack arrives.

The organisations showing the strongest signs of resilience in this dataset are not necessarily those with the lowest click rates. They combine improving click and leak rates with consistently strong reporting behaviour.



Report rate

Report rate measures the proportion of users who actively flagged a suspicious email using the reporting mechanism available to them.

This report covers how behaviour changes across the 12-month journey, which sectors and departments carry the most risk, and what the data says about designing a programme that builds resilience rather than familiarity.



Resilience

Throughout this report, resilience refers to a workforce that is increasingly likely to recognise, report and avoid phishing attempts over time.

The Data

Scale and scope:

- Analysis cohort: the 648 organisations (of 1,288 active) with a full 12-month window, covering 123,692 users. Every finding in this report comes from this cohort.
- Journey analysis (Section 1) draws on 354,962 simulations across the 3, 6, 9 and 12-month stages.
- Sector and department benchmarks (Sections 2 and 3) draw on every simulation sent by the cohort during the analysis year.



123,692 users

What happened when 123,692 users received their first simulation:

Click rate

4.14%

Leak rate

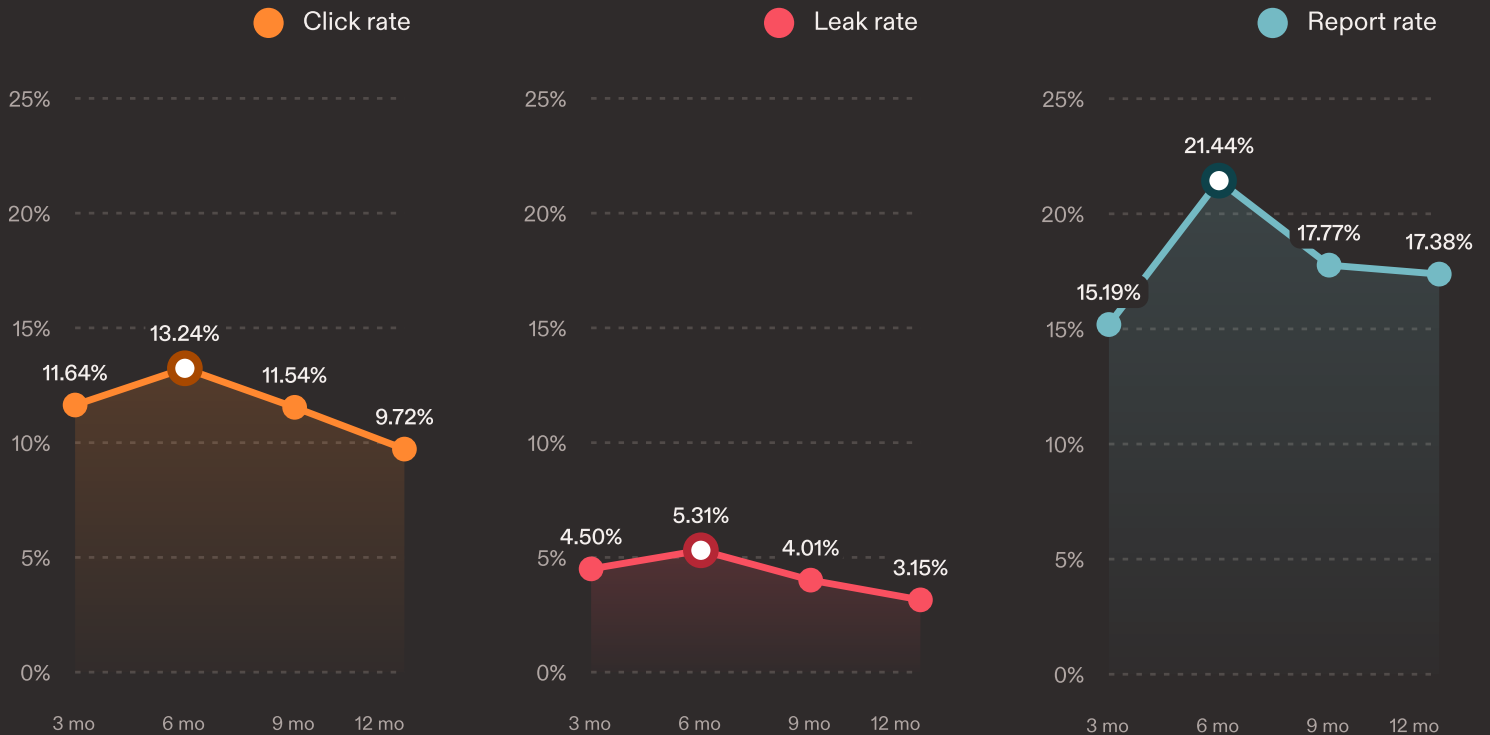
1.57%

Report rate

7.68%

The Journey Series

The journey series tracks the comparison cohort at each stage of the Pistachio journey. Stage sample sizes are shown in Section 1.



All three behaviours peak at the 6-month stage. Reporting declines least: the report-to-click ratio rises from 1.3 at the 3-month stage to 1.8 at the 12-month stage, meaning reports outnumber clicks nearly two to one by the end of the first year .

Sector and Department Extremes

Cumulative 12-month rates: the proportion of users who performed each action at least once across the year. Sector figures cover the whole cohort; department figures cover the 96,802 users tagged into the 16 named departments. Sample sizes are shown in the tables in Sections 2 and 3.

Click rate	By Department		By Sector	
	26.35%	41.31%	24.42%	45.74%
	Design	Construction	Healthcare & Life Sciences	Construction & Real Estate
	Lowest	Highest	Lowest	Highest

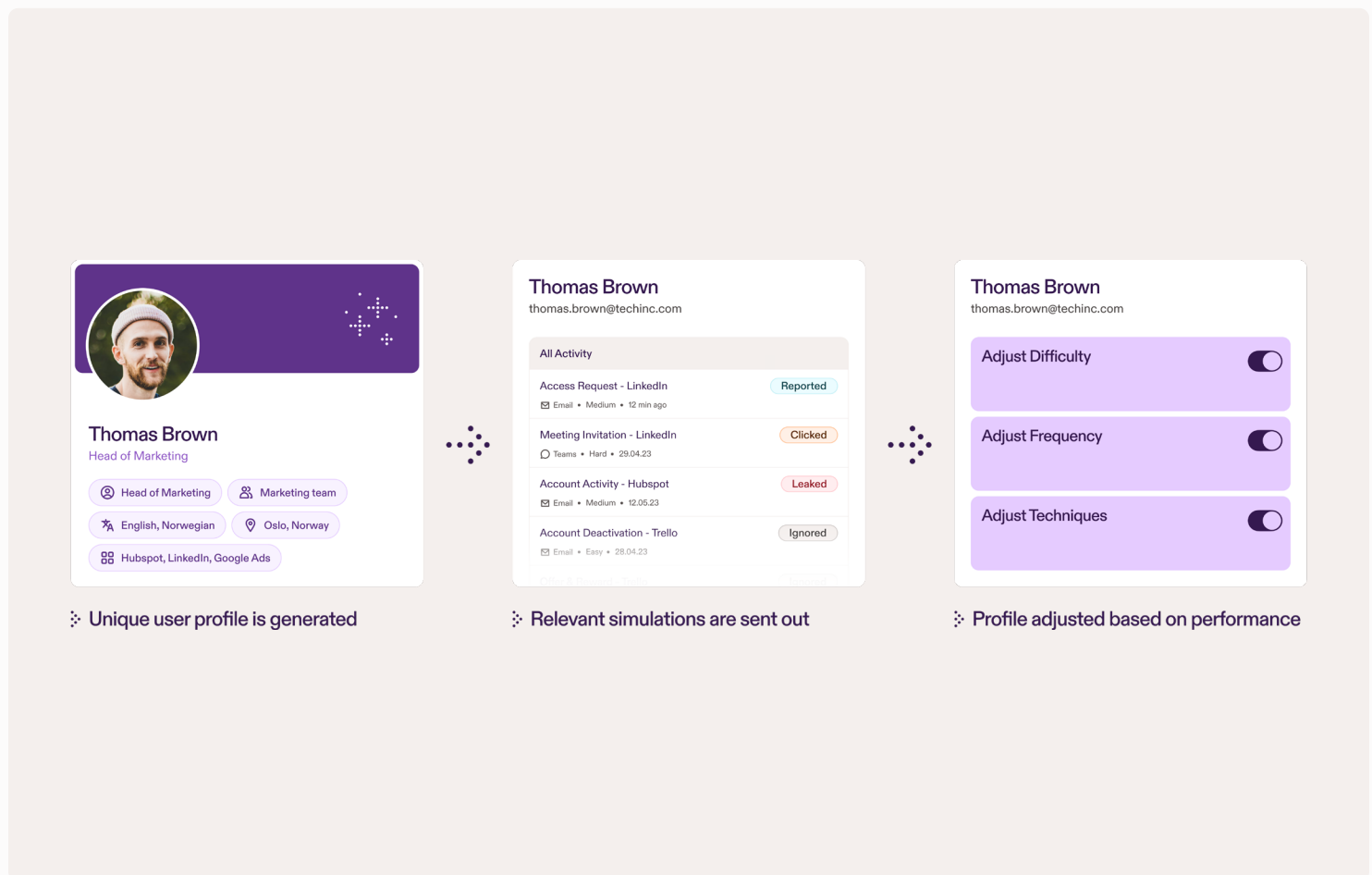
Leak rate	By Department		By Sector	
	9.62%	16.47%	8.56%	18.83%
	Data Analysis	Construction	Financial Services	Construction & Real Estate
	Lowest	Highest	Lowest	Highest

Report rate	By Department		By Sector	
	13.17%	36.45%	15.31%	33.11%
	Health	Data Analysis	Transportation & Logistics	Financial Services
	Lowest	Highest	Lowest	Highest

How Pistachio approaches security awareness training

Pistachio simulations are designed to reflect the real-world threats employees are likely to face, not generic templates that experienced users learn to recognise.

Difficulty adapts over time based on how each user responds. Users who are struggling receive simulations calibrated to build confidence. As performance improves, difficulty increases to match it. The goal is continuous resilience: a workforce that becomes harder to compromise over time and develops the reflex to report suspicious emails, not just a 0% click rate.



How rates are measured

Every rate in this report is a per-user figure: the proportion of users who performed each action at least once. The difference between sections is the time window. Journey-stage rates in Section 1 measure behaviour within each stage, comparing organisations at different stages of their journey. Sector and department rates in Sections 2 and 3 measure behaviour across the full analysis year.



Section 1:

How Phishing Behaviour Changes Across the Journey

How to read this section:

Journey stages are anchored to each organisation's own start date, not calendar months. Each stage covers the organisations whose journey reached that point during the analysis window, so later stages include more organisations and the groups overlap but are not identical. This is a comparison of organisations at different journey stages, not the same users tracked over time. Stage populations do not sum to the cohort total: organisations can appear at more than one stage, longer-tenured cohort organisations appear at none, and users join and leave organisations during the window.

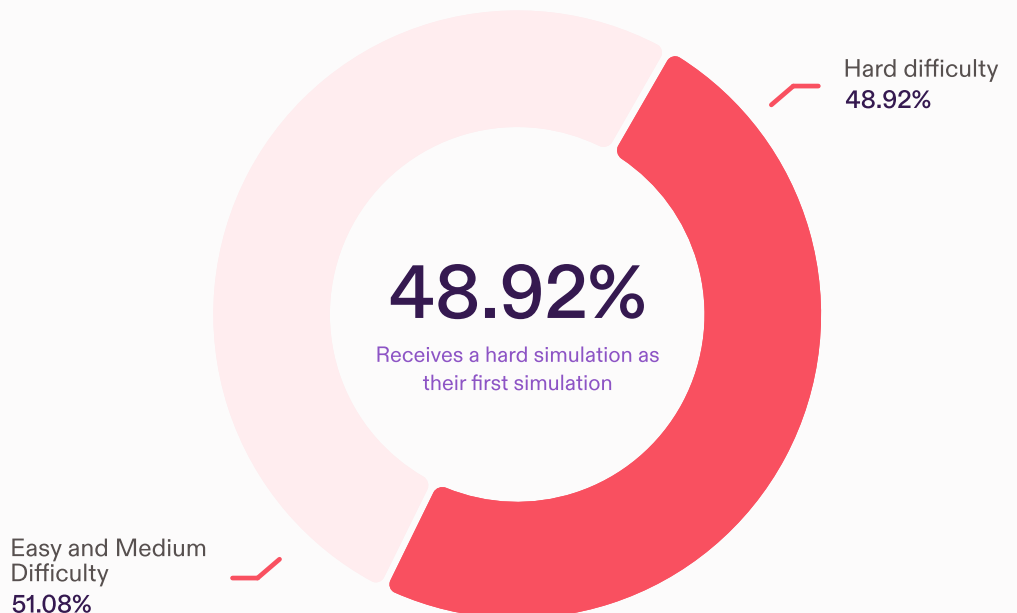
Stage rates are per user: the proportion of users who clicked, leaked, or reported at least once during that stage.

The Baseline

Where users start

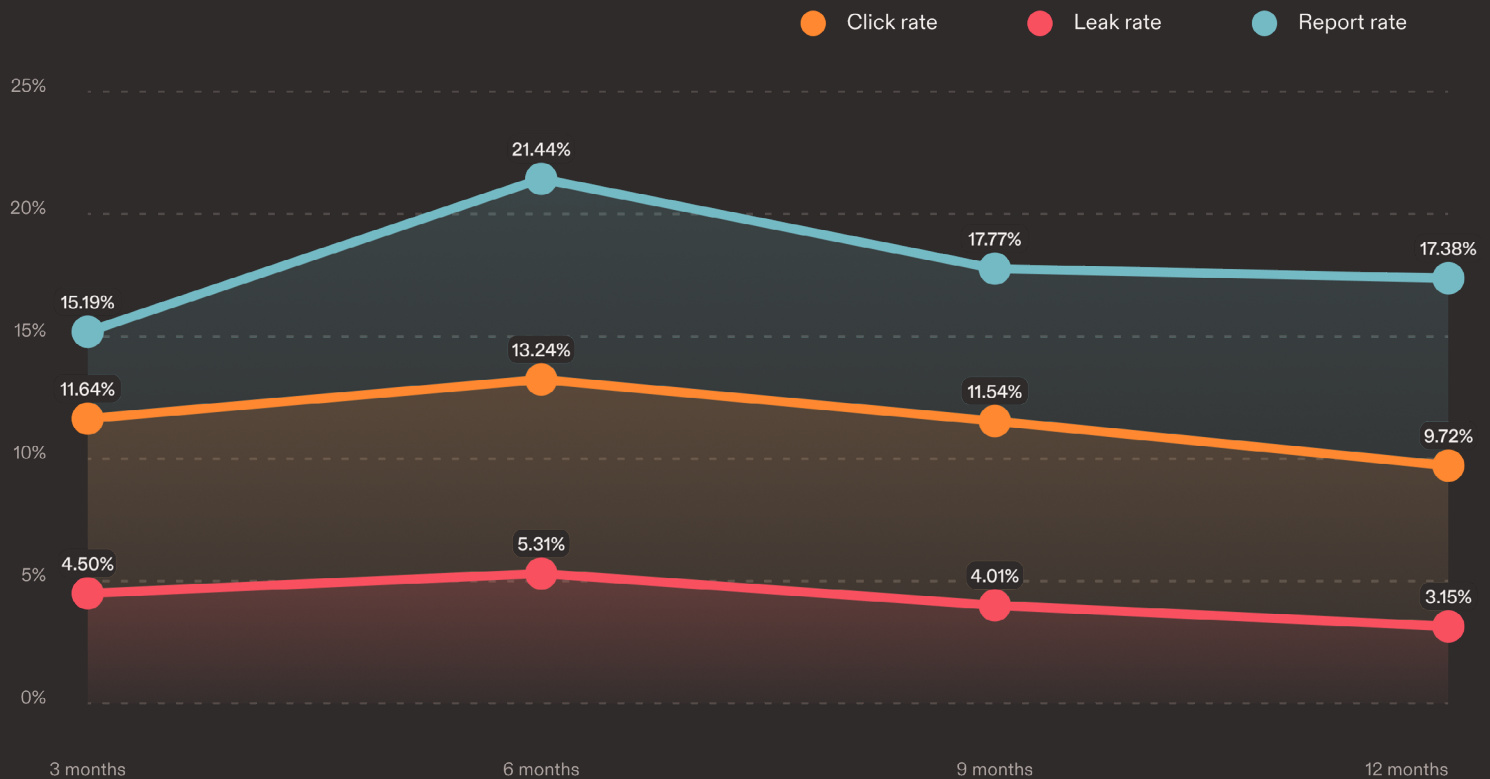
- Across all 123,692 cohort users, the very first simulation: click rate 4.14%, leak rate 1.57%, report rate 7.68%
- 48.92% of users received a Hard simulation as their first exposure
- The report rate exceeds the click rate before any simulation programme has taken effect

First-simulation rates are one test per user, so they are not comparable to the journey-stage rates below, where users receive multiple simulations per stage. This is the report's day-one snapshot, not the start of the trend line.



The Journey Curve

The journey analysis draws on 354,962 simulations across the four stages below.



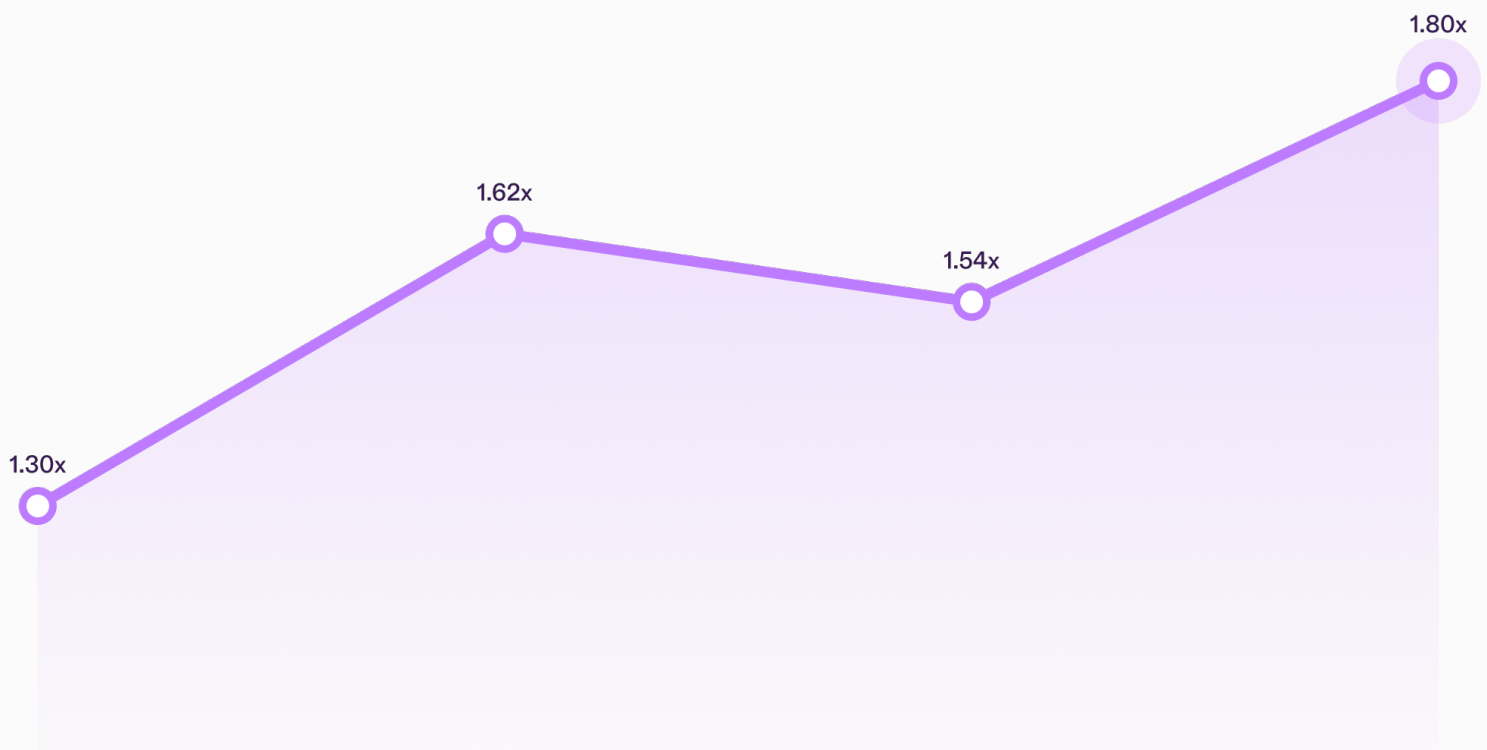
- All three behaviours peak at the 6-month stage and decline through the 9-month and 12-month stages.
- The 6-month stage is when users are tested most: 3.5 simulations per user, versus 2.6 at 3 months and 2.8 at 12 months, with the Hard share at its ceiling of 50.4%. More testing catches more users at least once.
- After the 6-month stage the difficulty mix holds constant at roughly 50% Hard, so the decline from the peak happens against a consistent testing environment, not an easier one.

The Reporting Reflex

From the peak to the 12-month stage, clicking declines faster than reporting. Clicks fall by 27% and leaks by 41%, while reports fall by only 19%. **The report-to-click ratio rises from 1.3 at the 3-month stage to 1.8 at the 12-month stage (1.62 at 6 months, 1.54 at 9 months).** Because the ratio compares two behaviours within the same stage, among the same users receiving the same simulations, it is unaffected by how many simulations each user received.

Vigilance gains ground

The balance shifts towards vigilance. That shift is what resilience looks like in the data.



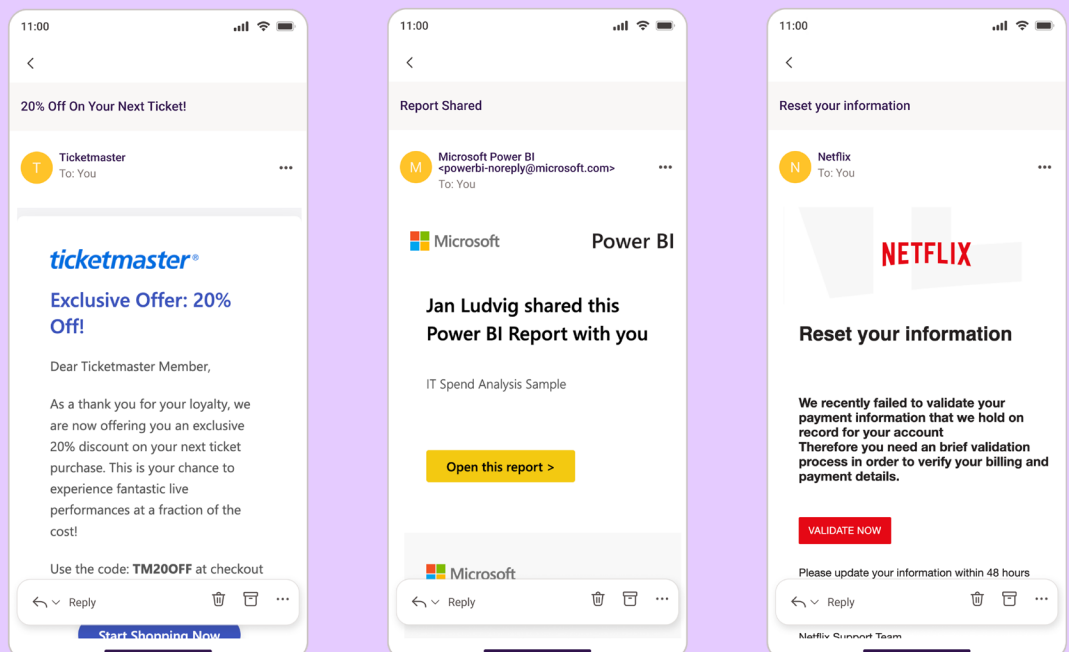
What This Means for Your Programme

A falling click rate against static, repeated simulations tells you users have learned the templates, not that they are harder to phish. In this dataset the decline from the 6-month peak happens against a difficulty mix holding at roughly 50% Hard, which is what makes it meaningful. A workforce that consistently reports suspicious emails gives the security team earlier visibility into potential attacks, making users an active part of the organisation's detection capability.

In practice:

- Ask: what difficulty mix produced this click rate? If your simulations haven't changed but clicks are falling, you have familiarity, not resilience. If difficulty has increased (more Hard simulations) and clicks are falling, you have resilience building.
- Compare your 6-month results to your 12-month results. If clicks fall while Hard difficulty stays constant at roughly 50%, resilience is building. If they're flat or rising, your simulations may have become predictable to your users.
- Calculate your report-to-click ratio at 3, 6, 9, and 12 months. If the ratio is rising (meaning fewer clicks relative to reports over time), vigilance is building. If it's flat, your users are avoiding clicks but not reporting. Shift investment toward making reporting effortless and rewarding.

Examples of difficult simulations:





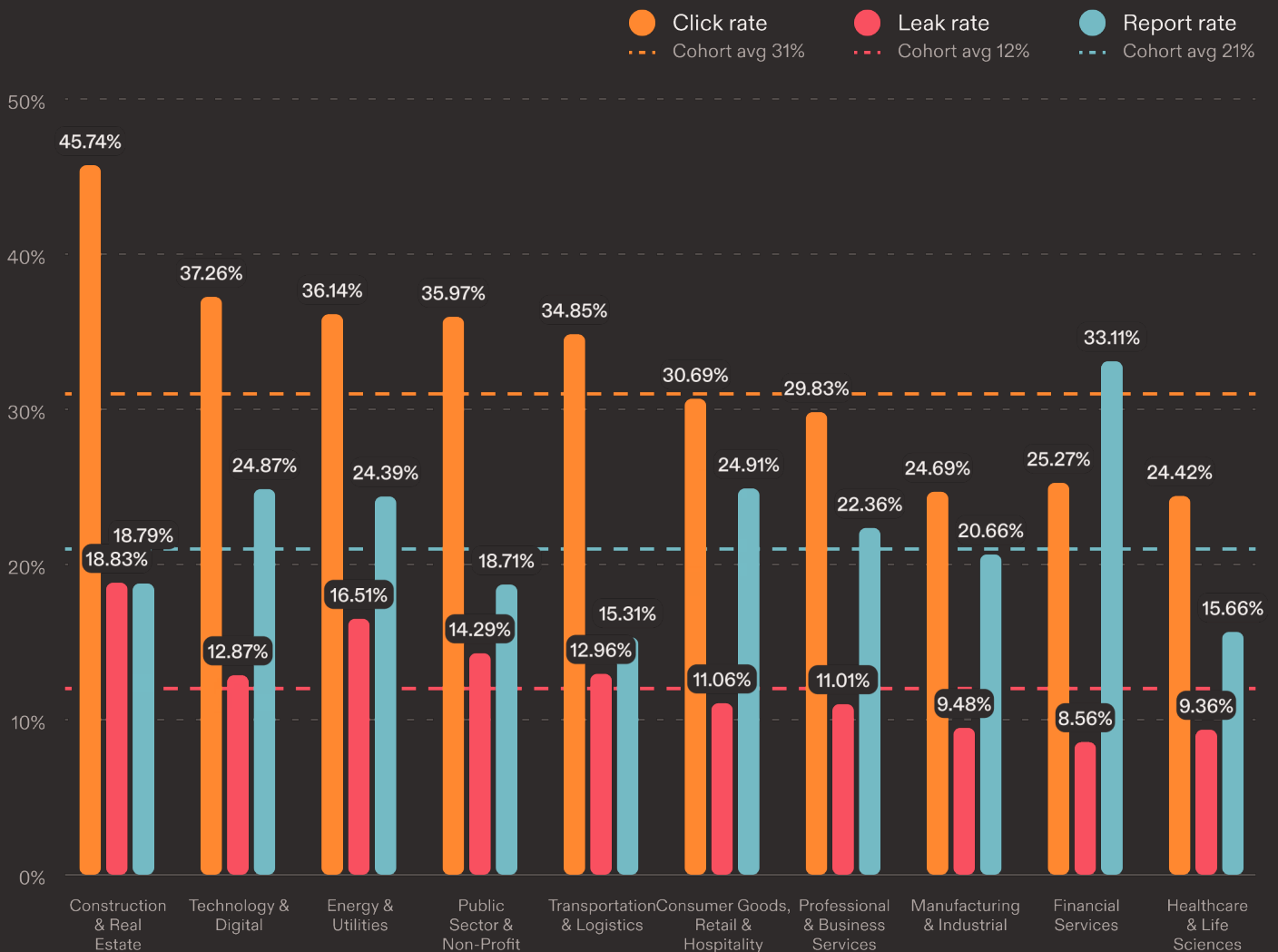
Section 2:

How Your Sector Compares

How to read this section:

These are cumulative 12-month rates: the proportion of users in each sector who performed each action at least once across the analysis year. A sector with an 18% leak rate does not have an 18% leak rate on any given simulation: it means 18% of users in that sector submitted credentials at least once during the year.

Sector Risk Comparison



⚙️ Across the whole cohort, the user-weighted averages are:
click rate 31%, leak rate 12%, report rate 21%.

Read your sector against these. On click and leak rates, lower than average is better; on report rate, higher is better.

Key insight:

Financial Services: Low click/leak rate + high report rate = **Goal State**

Highest risk

Construction and Real Estate performs worst across every metric in the dataset: the highest click rate at 45.74% and the highest leak rate at 18.83%, both well above the cohort average, with a report rate below it.

Technology and Digital and Energy and Utilities are the aware-but-exposed cases: click and leak rates above average, but report rates above average too. These users get caught often and flag often. Energy also carries the highest leak rate of any above-threshold vertical at 16.51%, so when its users click they are more likely to submit credentials.

Public Sector and Transportation and Logistics are the concern: above average on click and leak, below average on reporting. Risk is accumulating without a vigilance reflex to counter it. Transportation has the lowest report rate of any above-threshold sector at 15.31%.

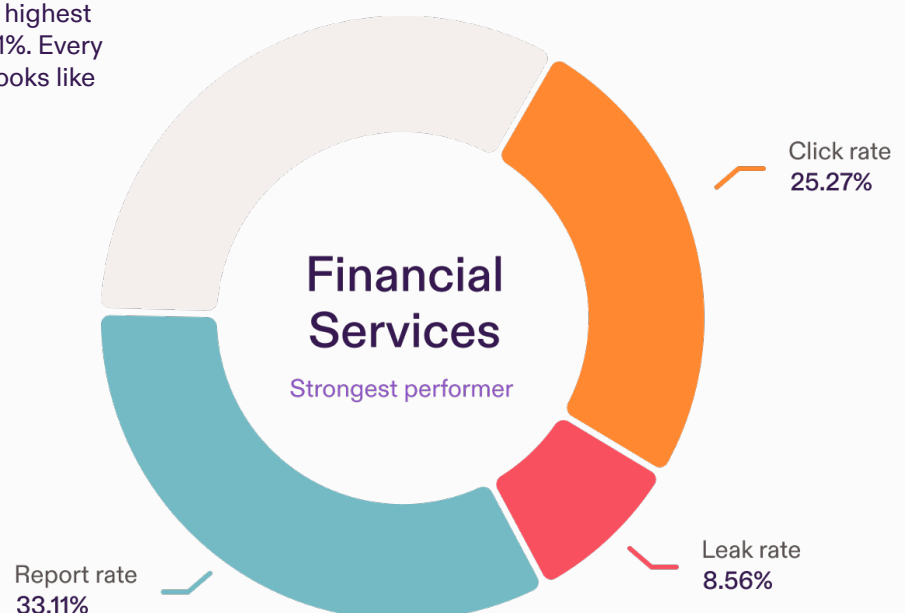
Mid-range

Consumer Goods and Professional and Business Services sit close to the cohort average on click and leak and comfortably above it on reporting. Solid, unremarkable profiles.

Manufacturing and Healthcare share a quieter risk. Both have low click and leak rates, the lowest two click rates of any sector, which looks reassuring. But both report below the cohort average, Manufacturing at 20.66% and Healthcare at just 15.66%. A low click rate with a low report rate is not a workforce beating attacks. This may indicate a workforce that is less likely to recognise or report suspicious emails when they encounter them. Manufacturing is the mild version of this; Healthcare is the sharp one.

Strongest performers

Financial Services is the only sector below average on both click and leak while sitting well above average on reporting. The lowest click rate, the lowest leak rate, and the highest report rate of any above-threshold vertical, at 33.11%. Every measure points the same way. This is what good looks like across all three behaviours at once.

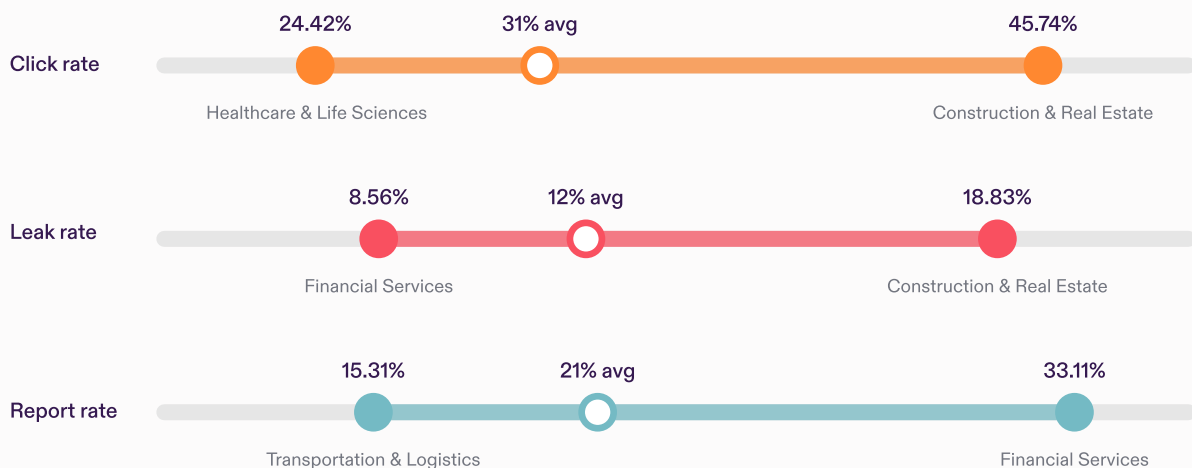


What This Means for Your Programme

The gap between the best and worst performing sectors on report rate is 18 percentage points. Financial Services reports at 33.11%; Transportation and Logistics at 15.31%. Every sector carries a different problem: Construction and Real Estate has a credential exposure problem, Energy and Utilities a credential submission problem the click rate alone does not reveal, and Healthcare looks safe on click rate but is not. A single uniform programme is unlikely to address these equally.

In practice:

- Benchmark all three rates against your sector average (31% click, 12% leak, 21% report). If your click rate beats the sector but your report rate trails it, you're solving the wrong problem. You have reporting visibility gaps. Prioritize building reporting culture.
- Understand your leak-to-click ratio. If more than 4 in 10 users who click also submit credentials, focus training on the moment between clicking and entering credentials.
- If click rate is below average but report rate is also below average, you have a recognition problem. Run a batch of highly convincing simulations and measure: are users ignoring them (not recognizing) or seeing them but not reporting (not confident)? Train accordingly, either on 'what to look for' or 'report first, ask questions later.'





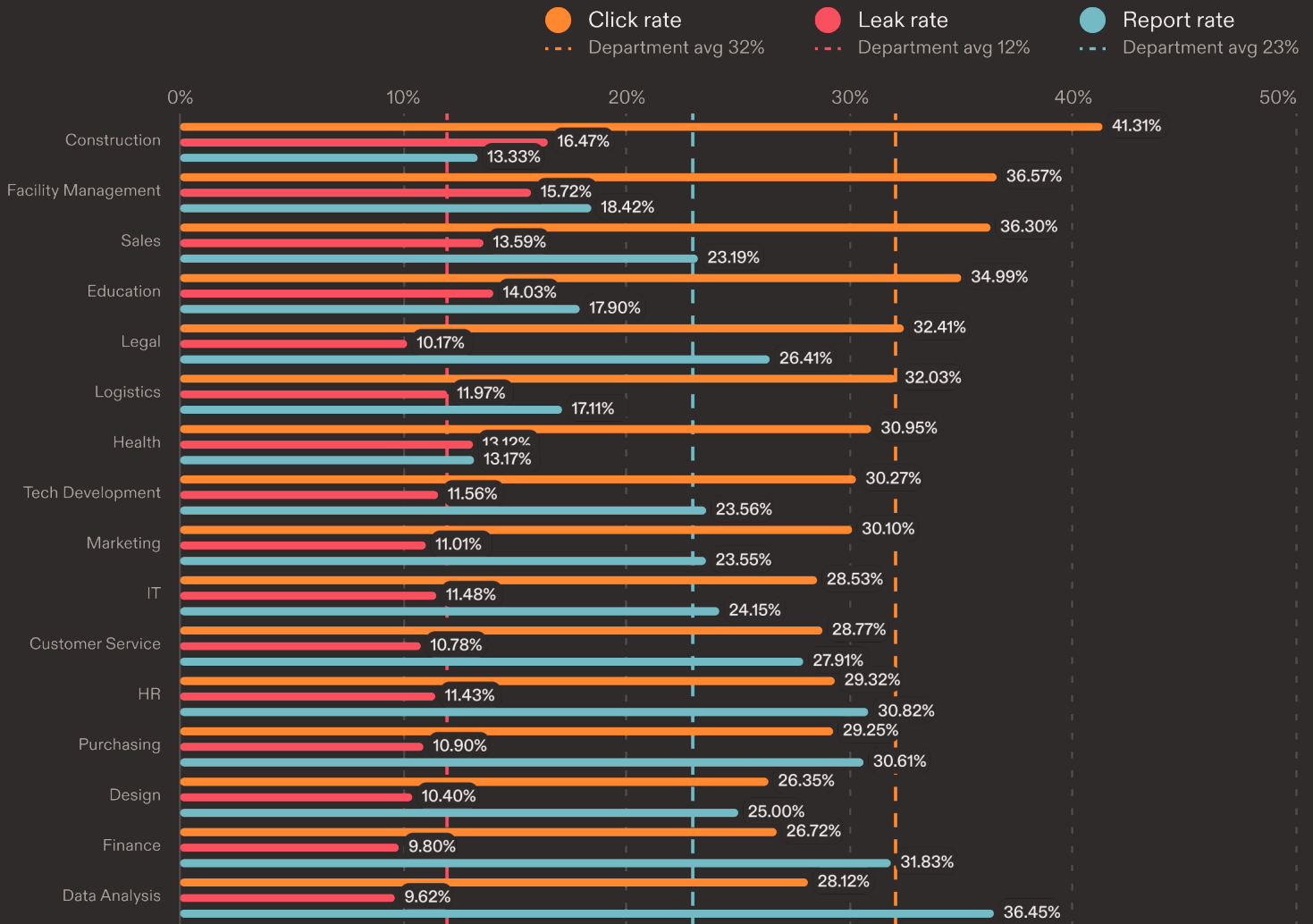
Section 3:

Where the Biggest Risks Sit Inside the Organisation

How to read this section:

These are cumulative 12-month rates: the proportion of users in each department who performed each action at least once across the analysis year. Of the 123,692 cohort users, 96,802 could be tagged into the 16 named departments below; the remainder sit in an unclassified Other category or could not be tagged from their job title.

Department Risk Comparison



Across the tagged departments, the user-weighted averages are:

click rate 32%, leak rate 12%, report rate 23%. Read each department against these.

On click and leak rates, lower than average is better; on report rate, higher is better.

Risk profiles:

High risk:

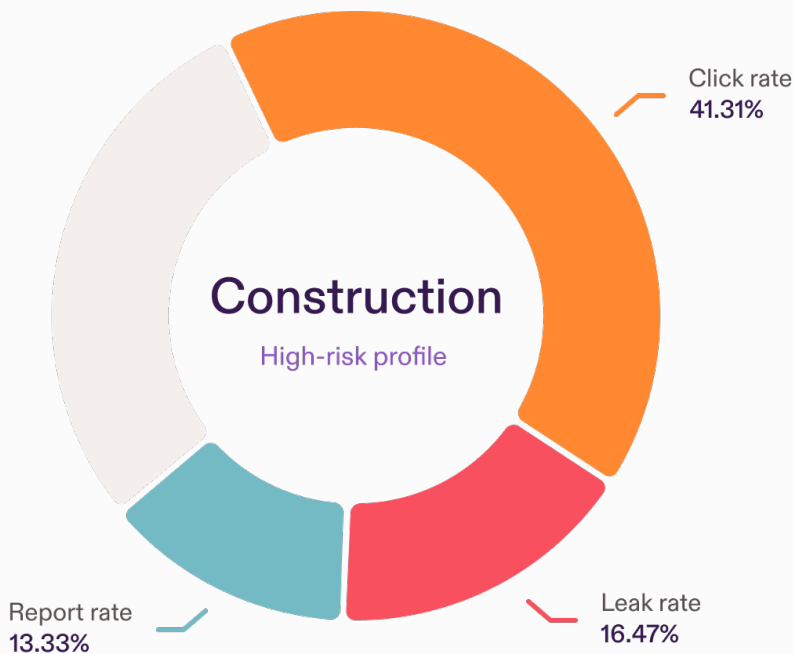
Construction isolated with highest click/leak

Quiet danger:

Health - low click, low report (untested)

Best-in-class:

Finance/Data Analysis



The high-risk operational profile

Construction and Facility Management have the highest click and leak rates in the dataset, and Construction has the second-lowest report rate of any department.

Sales has a similar click rate but a much higher report rate at 23.19%, above the department average. The vigilance reflex is developing despite high exposure. Logistics is the opposite: an above-average click rate paired with a below-average report rate of 17.11%, so its exposure is not being offset by reporting.

Health is the outlier. The click rate is lower, but the report rate, at 13.17%, is the lowest of any department: fewer than one in seven Health users flagged a suspicious email all year. A low click rate with minimal reporting suggests awareness may not be translating into reporting behaviour.

The learning but-not-applying profile

This group reports well, at or above the department average, but still clicks more than you would expect from teams that should be security-aware. IT and Tech Development are the clearest cases: the departments most likely to have had security training through multiple channels, yet over a year 30.27% of Tech Development users and 28.53% of IT users clicked at least once.

Training teaches people what to look for. Simulations train them to act on it. The gap between knowing and doing is measurable here.

The mid-table profile

Moderate click and leak rates. Report rates above the dataset average.

HR and Purchasing report at above 30% despite below-average click rates. HR is a documented spear-phishing target, with recruiters and hiring managers "often considered to be the weak point in an organization by attackers" (Arctic Wolf Labs), while APWG data shows Finance and Payroll functions increasingly hit by BEC and payroll-diversion campaigns.

The strongest-performing profile

Finance and Data Analysis have the lowest leak rates and the highest report rates in the dataset. Data Analysis has the highest report rate overall at 36.45%.

Difficulty is distributed equally

- Hard simulations account for 44% to 52% of sends across all 16 departments
- No department receives a systematically easier or harder mix; the differences in this section reflect genuine behavioural variation

What This Means for Your Programme

Your organisation does not have one phishing risk profile. It has several. Operational departments need difficulty calibrated to where they are; technical departments need repeated pressure, not more information; and departments with low click rates are not automatically low risk.

In practice:

- Segment your programme metrics by department. If your organisation-wide click rate is 30% but Construction is 41% and Finance is 27%, an organisation-wide programme underserves Construction. Assign more frequent simulations or calibrated difficulty to high-risk departments, lighter touches to Finance.
- Include IT and Tech Development in your programme at the same frequency and difficulty as other departments. They have lower click rates than operational teams, but 28 to 30% still clicked at least once. They need the same testing discipline, not a lighter load.
- If a department has low clicks and low report rates together, they're untested, not safe. Send them a batch of highly convincing simulations and track the report rate. If reports don't rise, you have a recognition or confidence problem. Deploy targeted 'what to look for' training before ramping up testing.
- For high-risk departments (Construction, Facility Management): send reinforcement content between simulations. Include tips on common lures, success stories, and micro-training on specific threats. Measure whether reinforcement without additional simulations reduces click rates. This builds habit without fatigue.

Section 4:

What Your Business Is Up Against

Data insights:

For most phishing attacks targeting SMB and mid-market organisations, credential submission is the event that creates a breach opportunity. A user who clicks but does not submit credentials has significantly reduced the risk. The leak rate is therefore the metric most directly tied to real-world breach potential.

Across most departments and sectors in this dataset, the leak rate runs at roughly 35 to 40% of the click rate. For every user who clicks, approximately one in three also submits credentials. Energy and Utilities is the outlier. Its leak-to-click ratio is the highest in the dataset: approximately 46% of users who click also submit credentials, compared to a sector average of 35 to 38%.

Energy and Utilities users are not just clicking more than average. When they click, they are significantly more likely to hand over credentials. For a sector where credential access to operational systems carries serious consequences, the click rate alone understates the actual exposure.

The report rate matters too. A reported simulation gives the security team intelligence they can act on. The same is true of a real attack, once an employee reports a suspicious email, most tools enable you to purge any identical emails from all mailboxes.

What The External Data Tells Us

The simulation data shows how users behave. The external threat data shows what businesses are up against.

- **~60% of breaches** involve a human element. Error, manipulation or misuse means people remain central to how breaches happen, a figure that has held steady year on year. (Verizon, 2025 Data Breach Investigations Report).
- **88% of SMB breaches** involve ransomware, with a **median payment of \$115,000**. Small and medium businesses are disproportionately hit, and the cost of giving in stays substantial even as demands fall. (Verizon, 2025 Data Breach Investigations Report).
- The median time to click a phishing link is **21 seconds**, and just **28 seconds** more to hand over credentials, so a user can be compromised in under a minute. That speed leaves security teams almost no window to react. (Verizon, 2025 Data Breach Investigations Report).
- AI-written phishing has **doubled in two years**. Synthetically generated text in malicious emails has doubled over the past two years as attackers adopt generative AI to craft more convincing lures. (Verizon, 2025 Data Breach Investigations Report).
- **\$6.3 billion** was moved through business email compromise scams in 2024. BEC and wire-transfer fraud targeting finance functions continue to rise, with a median loss of around **\$50,000 per incident**. (Verizon DBIR 2025, citing FBI IC3).
- **QR-code phishing** is a fast-growing evasion tactic. Attackers increasingly embed QR codes to slip past email filters and push users onto malicious sites from a second device. (Cofense, Annual State of Email Security Report).
- A large-scale RCT found **no meaningful link** between completing annual awareness training and phishing resilience. (Ho et al., IEEE Symposium on Security & Privacy "Oakland" 2025 — University of Chicago and UC San Diego)

What This Means for Your Programme

Email is still the dominant phishing vector, but it is no longer the only one. Attacks are more convincing, arriving faster, and targeting specific departments rather than entire organisations. A programme that only tests email, at a uniform difficulty, across every department the same way, is not keeping pace.

In practice:

- Audit your simulation channels. Are you testing only email? Review other comms channels, such as Teams or Slack. Measure click rates on each channel separately and prioritize the channels where your users are most vulnerable.
- Track your leak rate separately. If 30% click but only 10% leak, your gap is the stopping point. Users are clicking but catching themselves before submitting. Focus training on that moment. If 30% click and 15% leak, credential submission is the bigger risk. Train on recognizing phishing at the ask moment.
- Audit your reporting workflow. Can users report in one click? Do they get confirmation within 24 hours? If not, redesign it. Then measure: does ease of reporting correlate with rising report rates? Track reporting time. If it's above 5 minutes, friction is suppressing reports.

Microsoft Teams: Invite to a group

Ignored

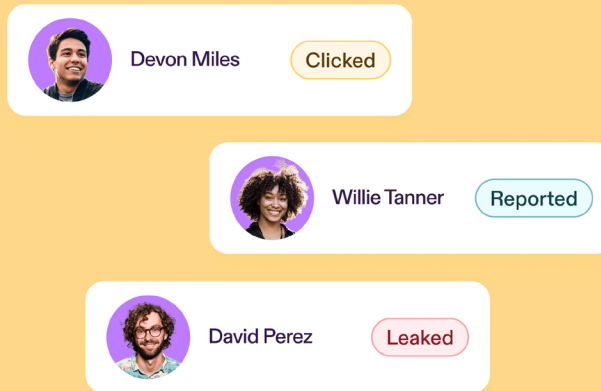
Aug 05 at 08:16

Ignored

Aug 06 at 11:44

Reported

Aug 07 at 15:21



Conclusion:

From Measuring Click Rates to Building Resilience

Most phishing simulation programmes measure click rates, report the numbers to the board annually, and assume lower numbers mean lower risk. The data in this report shows why that is not enough.

Continuity over events

The journey takes 12 months and does not move in a straight line. Organisations at the 6-month stage look worse on paper than those just starting. Organisations that stop there, or measure at the wrong point, never see the stage that follows.

Adaptive difficulty over uniform testing

A programme that sends the same simulations to every user risks building familiarity rather than sustained vigilance. In this dataset, organisations at the 12-month stage show markedly lower click and leak rates than those at the 6-month stage, while roughly half of all simulations remain Hard. That pattern is consistent with what calibrated testing is designed to produce: performance improving against difficulty that does not relent.

Challenge over familiarity

Sending more simulations is not the same as running a better programme. A generic phishing email that every user recognises tells you little about how users will respond to a convincing attack. The organisations that show the strongest outcomes in this dataset are being tested with simulations that reflect the real threats their employees are likely to face: convincing, personalised and calibrated to the individual user.

That is a different product to a library of generic templates sent on a schedule. Volume is easy to measure. Whether a simulation would challenge someone is the harder, more important question.

Report rate as well as click rate

Although click rate is the metric most programmes track, report rate is the one that most directly reduces real-world risk. In this dataset the report-to-click ratio rises from 1.3 to 1.8 across the journey: the balance shifting decisively towards vigilance.



Manage outcomes, not just metrics

The programmes that move from good to genuinely effective tend to share one characteristic: someone treats the report rate and the leak rate as outcomes to manage, not just metrics to monitor.

Organisations do not become resilient because fewer people click. They become resilient because more people recognise attacks, report them quickly and avoid giving away credentials. Those are the behaviours worth measuring.



John

Phishing Reported



Danielle

Phishing Reported



Devon

Phishing Reported



Laura

Phishing Reported



James

Phishing Reported



Patrick

Phishing Reported



Isabelle

Phishing Reported

What to do next:

Five Questions for Your Next Programme Review

The findings in this report reduce to five questions. If you can answer all five, your programme is measuring resilience. If you cannot, you now know where to look.

1

What difficulty mix is your click rate measured against?

A falling rate against static simulations is familiarity, not progress.

2

Is your report rate rising faster than your click rate is falling?

In this dataset, that ratio, not the click rate, is what separates the strongest performers.

3

How many of your users report a suspicious email?

A deleted email is invisible. A reported one is a warning your team can act on.

4

Which of your departments are quiet?

Low clicks with low reports means untested, not safe.

5

What happens in your organisation after someone clicks?

One in three clickers submit credentials. The gap between the click and the submission is where training either works or does not.

Methodology



Why these findings are not just a Pistachio effect

The findings in this report are observational rather than causal. The report does not claim Pistachio caused these outcomes. It analyses how phishing behaviour changes across a large cohort of organisations using adaptive simulations, and what those patterns imply for how resilience should be measured. Where interpretation goes beyond the data, it is framed as such.

- Cohort and scope:**
- Analysis window: 1 June 2025 to 31 May 2026.
 - Headline volume figures (2.47 million simulations, hours saved) cover all 1,288 organisations active in the window.
 - All analytical findings come from the 12-month cohort: 648 organisations that started with Pistachio on or before 1 June 2025 and remained active through 31 May 2026, covering 123,692 users. Organisations that joined partway through the year are excluded because they do not have a full year of data. No organisation was excluded for any other reason.
 - The cohort includes organisations at every stage of platform maturity: some joined shortly before the window, others have been customers for years.

Journey stages: (Section 1)

- Stages are anchored to each organisation's own start date, not calendar months. The journey-stage analysis uses the subset of cohort organisations whose relevant stage fell within the window, which is why stage sample sizes (64 to 240 organisations) are smaller than the full cohort. Stage populations overlap and do not sum to the cohort total: organisations can appear at more than one stage, longer-tenured organisations appear at none, and users join and leave organisations during the window.
- Stage rates are per user: the proportion of users who clicked, leaked, or reported at least once during that stage.
- The baseline stage (organisations in their first two months) covers 530 users across 11 organisations and is excluded from headline findings for sample size, consistent with the 15-organisation threshold applied to industry verticals. Its figures (click 6.23%, leak 1.89%, report 7.74%) are available on request.
- The journey analysis compares organisations at different stages rather than tracking the same organisations over time. A longitudinal analysis following individual organisation trajectories is planned for a future edition.
- The report-to-click ratio compares report rate to click rate within the same stage. Because both behaviours are measured among the same users receiving the same simulations, the ratio is unaffected by variation in simulations per user across stages.

Cumulative rates: (Sections 2 and 3)

- Sector and department rates are cumulative 12-month per-user figures: the proportion of users who performed each action at least once across the analysis year, covering all 648 cohort organisations regardless of platform maturity.
- Clicks, leaks and reports are tracked as separate events: a click is a user following a simulation link; a leak is a user submitting credentials after clicking; a report is a user actively flagging the simulation.
- Department data: AI-processed role tags applied to user records based on job titles and Active Directory labels. Of 123,692 cohort users, 96,802 are tagged into the 16 named departments, 17,600 carry an unclassified Other tag, and roughly 9,300 without a recognisable job title are excluded. Department rates represent tagged users within each category, not the full cohort.
- Industry data sourced from HubSpot company records matched to Pistachio organisation IDs. Two verticals fall below the 15-organisation threshold: Agriculture and Natural Resources (11 organisations), Media Entertainment and Creative (12 organisations); findings are directional only.
- Department sample sizes vary significantly; differences between departments with smaller user populations should be treated as indicative rather than definitive.

Difficulty & other definitions:

- Each simulation is scored 1 to 10 and grouped into Easy (1 to 3), Medium (4 to 7) and Hard (8 to 10). Hard simulations rise from 46.7% of sends at the 3-month stage to 50.4% at the 6-month stage, then hold at roughly 50% for the rest of the journey.
- Flat or rising click rates during a period of difficulty escalation are consistent with resilience building, not stagnation. Performance should always be read alongside the difficulty mix it was measured against.
- Time-saved calculation: total simulations multiplied by 5 minutes, divided by 60.
- The associations described in this report are observational. The data does not establish causation.

References

[Verizon, 2025 Data Breach Investigations Report \(full report\)](#)

[Verizon, 2025 DBIR — Executive Summary \(PDF\)](#)

[FBI Internet Crime Complaint Center \(IC3\), 2024 Annual Report \(PDF\)](#)

[Cofense, Annual State of Email Security Report](#)

[Ho et al., "Understanding the Efficacy of Phishing Training in Practice," IEEE Symposium on Security & Privacy \("Oakland"\) 2025 — University of Chicago and UC San Diego](#)

[SHRM \(May 2025\), citing Arctic Wolf Labs](#)

[APWG Phishing Activity Trends Report, Q1 2026](#)

About Pistachio:

Pistachio is a cybersecurity company building human risk management tools for small business and mid-market organisations. Founded in 2023 and headquartered in Oslo, with offices in London and Valencia, Pistachio automates security awareness training and insider threat detection, adapting to each employee's role and behaviour.

Trusted by over 1,000 organisations globally and backed by exclusive partnerships across key markets, Pistachio is on a mission to make enterprise-grade cyber resilience accessible to everyone.

