FORTRA

2025 Phishing Simulation Benchmark Report

Benchmark Findings

June 2026

Foreword

Fifteen years ago, phishing was relatively simple. Attackers copied legitimate login pages, hosted them on compromised websites or look-alike domains, then blasted spoofed emails to large numbers of victims in hopes of harvesting usernames and passwords. In response, major banks, payment providers, and webmail companies developed DMARC, a standard designed to prevent exact-domain email spoofing when properly implemented.

Attackers adapted quickly. Rather than spoofing legitimate domains directly, they began using free webmail accounts and newly registered look-alike domains, relying on display names and visually similar addresses to deceive users.

Browsers introduced real-time warnings for known phishing sites, but these protections were inherently reactive. Early victims of a new phishing campaign still had little protection before a site was identified and blocklisted. Email security vendors responded with URL rewriting and time-of-click analysis, while enterprises deployed secure web gateways to better protect corporate users.

Phishing operators adapted again. QR code phishing campaigns proved especially effective because they moved victims away from hardened corporate devices and onto personal smartphones, where enterprise security controls were often absent or significantly weaker.

The widespread adoption of multi-factor authentication (MFA) was expected to dramatically reduce phishing risk. Instead, attackers evolved their techniques yet again.

Some groups focused on SIM-swapping attacks, convincing mobile carriers to transfer a victim's phone number to a device under attacker control. Once credentials were stolen, intercepted SMS codes provided the final step needed to access accounts.

Others relied on social engineering. In one common scenario, attackers first obtained a victim's username and password, then triggered an MFA challenge on the legitimate service. The victim would receive an automated phone call claiming to be from their bank and warning of suspicious activity. The caller would then ask the victim to enter the recently received verification code, unknowingly handing the attacker the MFA token in real time.

More technically sophisticated methods soon followed. Adversary-in-the-middle phishing frameworks began proxying entire login sessions, relaying keystrokes, session data, and authentication challenges directly to legitimate services. These attacks proved particularly effective against corporate environments with customized login portals because victims saw the exact authentication flow they expected. Other groups shifted focus toward session hijacking, token theft, and device-level compromise, bypassing traditional credential theft altogether.

Perhaps the most significant development, however, has been the rise of Phishing-as-a-Service (PaaS). These platforms provide pre-built phishing templates, resilient delivery infrastructure, and modern phishing kits capable of bypassing MFA through a variety of established techniques. As a result, sophisticated phishing operations no longer require deep technical expertise. Many can now be launched with minimal skill, low cost, and only a few clicks.

The modern phishing ecosystem is no longer defined by isolated scams, but by rapidly evolving criminal platforms that continuously adapt to defensive improvements. The trends explored in this paper demonstrate how phishing has matured into a scalable, service-driven industry. Considering this maturation, it's imperative we focus on educating the human component of this equation. Mitigating human risk through awareness is a key factor on securing companies' ecosystems.

John Wilson
Sr. Threat Research Fellow, Fortra

2025 Phishing Simulation Benchmark Report

Benchmark statistics and response-rate patterns

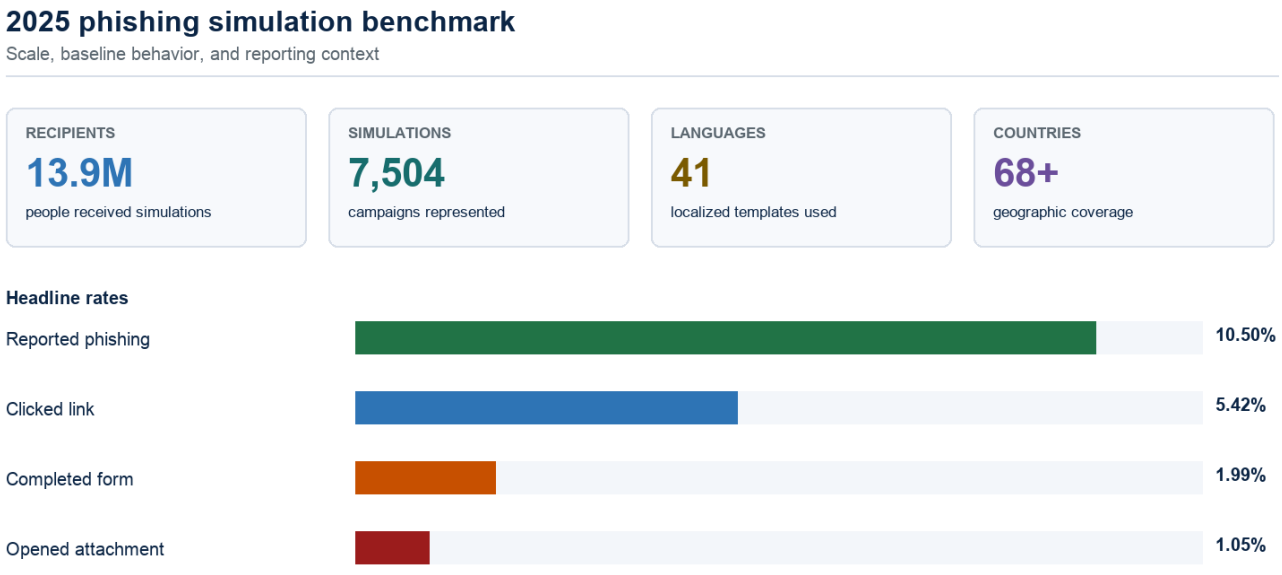

Figure 1. Overall benchmark scale and headline response rates.

These numbers set the stage for the rest of this report, reflecting 14M simulation recipients across more than 7500 campaigns. At this scale, we can clearly establish the significance of metrics presented in the remainder of this report.

Understanding the benchmarks

A 10.5% reporting rate is not something to be celebrated. This means that 9/10 phishing attempts are not reported. One cannot overlook the value that reporting phishing emails provides to internal security teams. A single report may be the difference in determining whether a phishing campaign is successful or not. This one statistic alone should be enough to prove that more education is required. This report will break down the geographic locations, languages, organization sizes, and industries where that education is most required.

It is easy to assume that a 5.42% click rate or a 1.99% password submission rate is reasonable because they are low. Translating those seemingly small percentages into raw numbers reveals the magnitude of the threat. More than 750,000 individuals clicked on phishing simulations and more than 250,000 individuals provided their passwords.

1. Geographic Risk Patterns

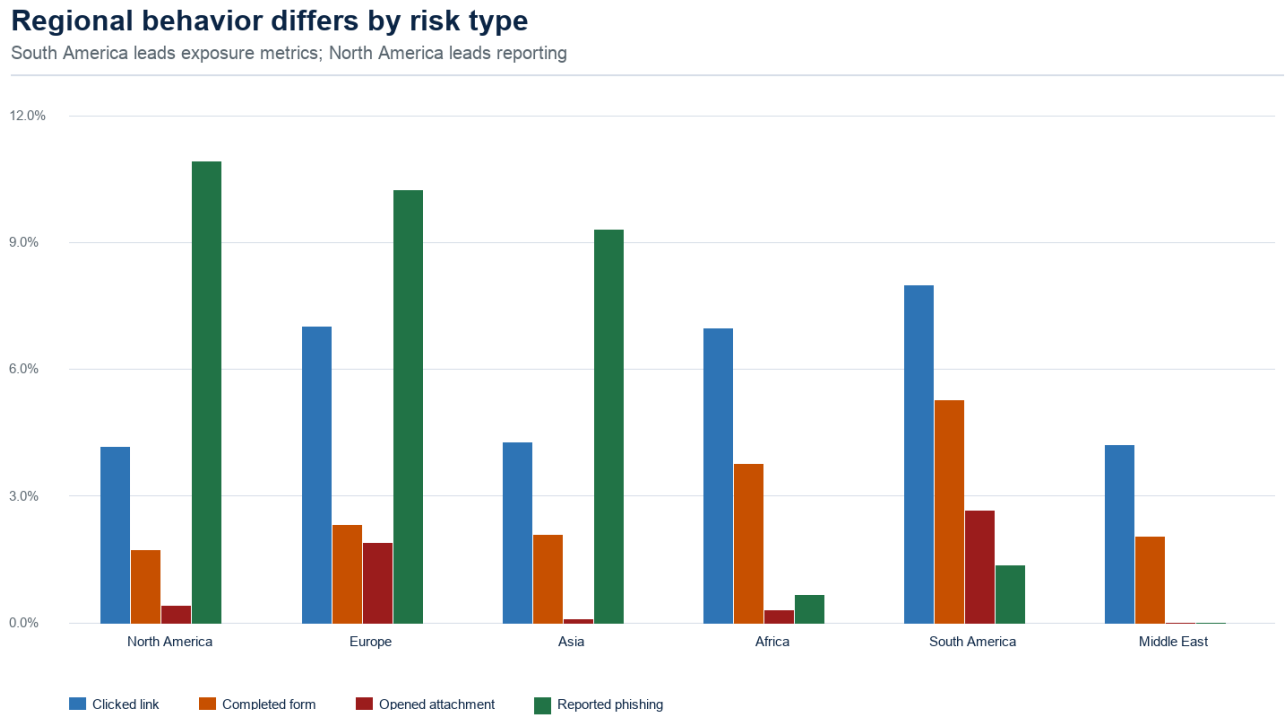

Figure 2. Regional comparison of click, form-completion, attachment-open, and reporting rates. See Appendix I - table 1

Regional data provides interesting insight into users' behaviors across geographies during phishing simulations.

There is a significant distinction between North America, Europe, and Aisia versus Africa, South America, and the Middle East. Particularly, the latter regions have extremely poor reporting rates comparatively, with the Middle East having the worst phish reporting rate of all six regions. However, the Middle East has the lowest credential leakage rate, i.e., form completion. North America comes in with the best reporting rates followed closely by Europe and Asia. Europe shows a similar rate of form completion and opening attachments. South America shows a very interesting pattern whereby rates (based on this ordering of the data) decrease from left to right with clicked links having the highest rate, followed by form completion, then opening attachments, and finally reporting having its lowest rate of all four.

In all cases, each region had higher form completion rates than opening attachments. Opening malicious attachments can have very detrimental effects on an organization's infrastructure due to the potential of a virus or ransomware outbreak. However, one can argue that users submitting credentials such as usernames and passwords via form completion is just as detrimental.

Core Insights

This data suggests that more effort is needed, regardless of region, in training users to identify potentially malicious attachments and credential harvesting attacks.

2. Language-Level Performance

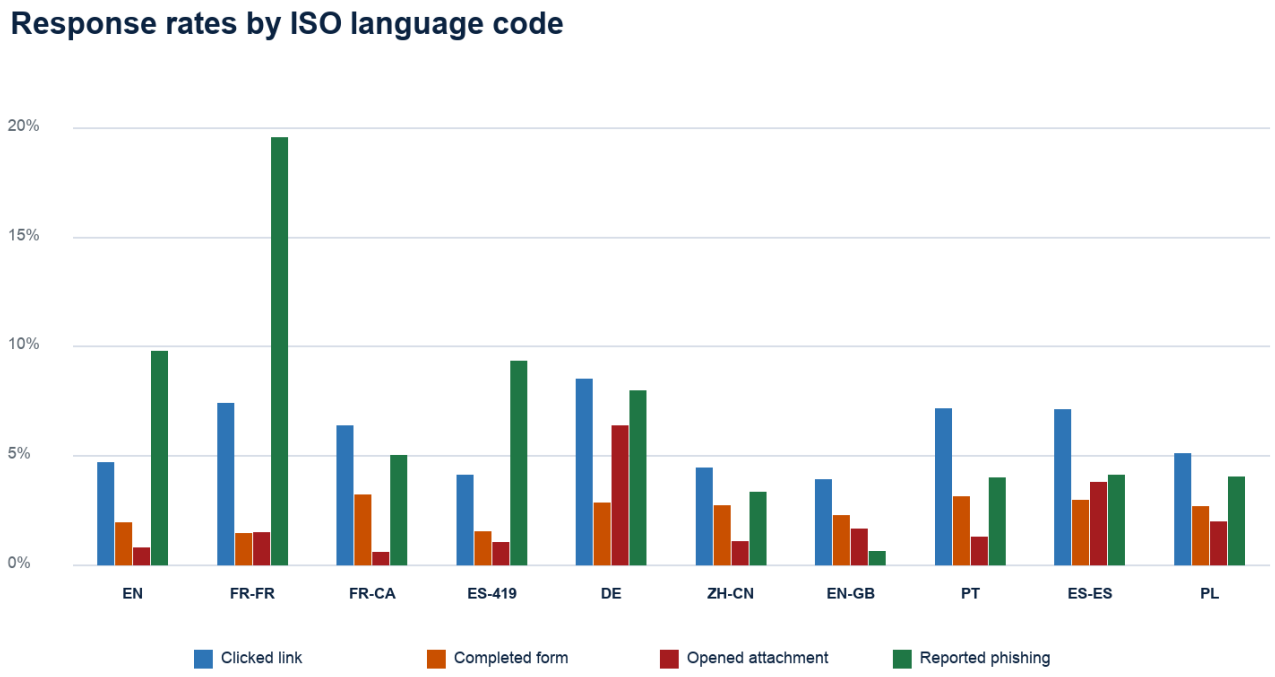

Figure 3. Response rates for the ten largest ISO language-code cohorts by active recipients. See Appendix I - table 2

Language-level performance data shows a different trend from geographic risk data.

There are only three out of ten language groups with higher reporting rates than clicked links, completed forms, and opening attachment rates. Conversely, three out of six showed the same trend in the geographic data. EN-GB shows the same pattern as South America from the geographic data, with click rates higher than all other rates, followed by form completion, then opening attachments, and finally reporting as the weakest rate for EN-GB. FR-FR has the highest reporting rate, which is approximately twice that of second place reporting rate in the data – English. FR-FR has an almost equal rate of form completion and opening attachments, like the Europe trend in the geographic data from Figure 2.

Of interest is a comparison of FR-FR to FR-CA rates. The trends are different. FR-CA has a lower reporting rate than click rates, opposite of FR-FR. FR-CA has a lower attachment opening rate compared to form submissions, once again, different than FR-FR. Trend differences between ES-419 versus ES-ES are also interesting like the French comparisons. ES-419 has a better reporting rate than ES-ES. Both have higher click rates than form submission and opening attachments, but this is true for all languages in Figure 3.

Core Insights

This data suggests that users on average are more susceptible to falling victim to form submission based phishing attacks than email attachment phishing. The data also indicates that click rates are on average more common than phish reporting across most languages within this cohort.

3. Company Size Patterns

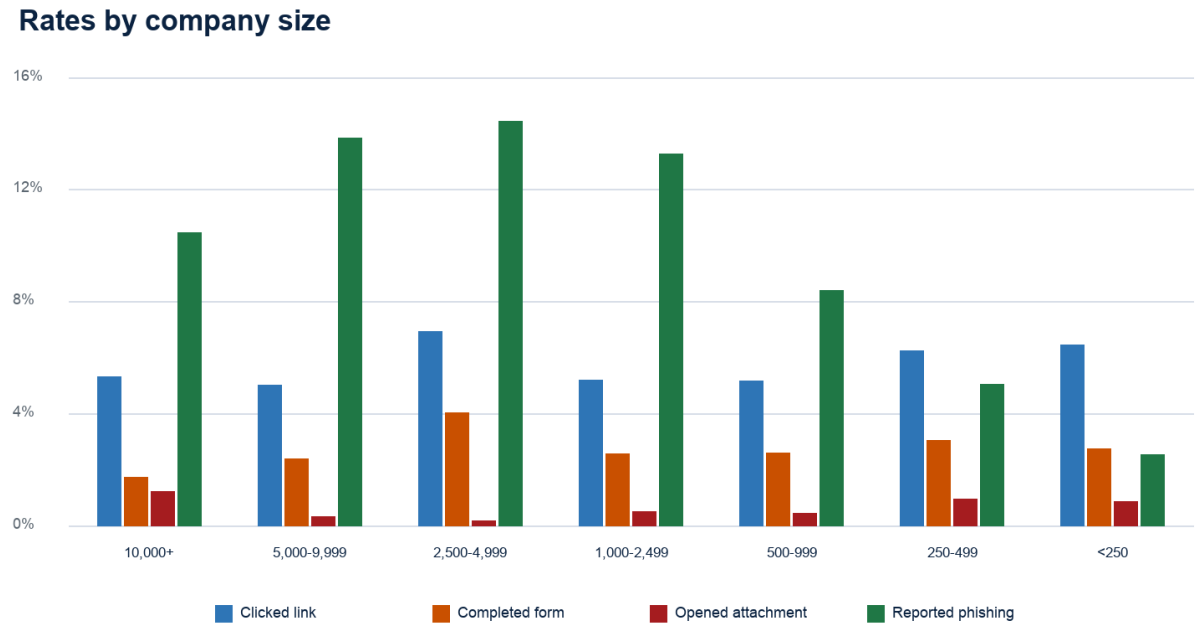

Figure 4. Click, form-completion, attachment-open, and reporting rates by company size. See Appendix I - table 3

When examining phishing simulation numbers by company size, several conclusions are clear.

According to Innovation, Science and Economic Development Canada, businesses are defined as follows[1]:

Micro-Enterprise	1 – 4 Employees
Small Business	5 – 99 Employees
Medium-Sized Business	100 – 499 Employees
Large Business	500 or more Employees

While companies with 2,500 – 4,999 employees are an outlier, the highest risk businesses appear to be small and medium businesses. Not only do they have higher click rates and password submission rates, but they also have the lowest reporting rates. The reporting disparity between our larger companies and our smaller companies potentially speaks to resourcing. According to Training Magazine's 2025 Training Industry Report[2], training budgets vary greatly with organizational size:

Small Companies	100 – 999 Employees	**$333,305**
Midsize	1000 – 9,999 Employees	$1,628,415
Large	10,000 or more Employees	$11,698,715

An interesting note here is that the largest businesses, with 10,000+ employees, are the most likely to open attachments in phishing emails. Have those employees been trained to more freely open attachments due to the nature of their work?

[1] https://ised-isde.canada.ca/site/sme-research-statistics/en/key-small-business-statistics/key-small-business-statistics-2025
[2] https://trainingmag.com/2025-training-industry-report/

4. Industry Patterns

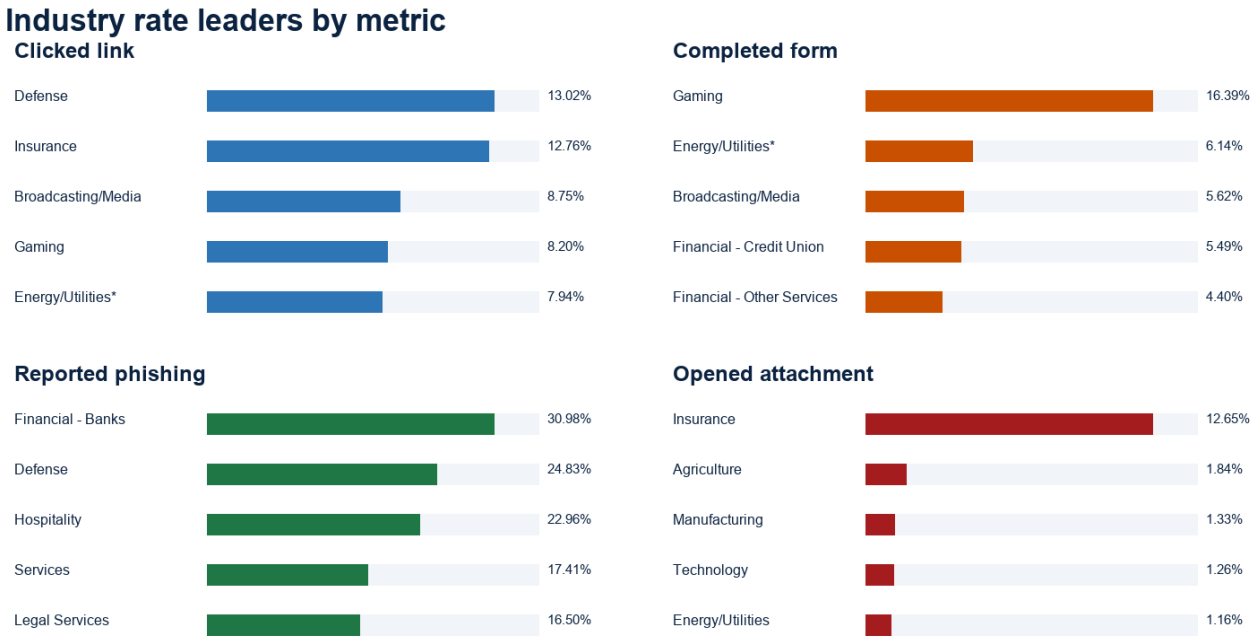

Figure 5. Industry leaders by click, form-completion, reporting, and attachment-open rates. See Appendix I - table 4

The data presented here provides a beacon of hope in one way, and a loss of faith in another. On the hopeful side, nearly 31% of bank employees and 25% of defense employees reported phishing. That is significantly higher than the 10.5% average across all industries and is significant given the importance of those industries.

Sobering stats come from the gaming and insurance industries. More than 16% of gaming industry employees were willing to enter their passwords on phishing pages. That number is almost as alarming as the more than 12% of insurance industry employees who open attachments.

Core Insights

While click rates are concerning, the potential consequences of entering your password or opening an attachment are significantly more severe. It is imperative that employees pay attention to these threats. The industries mentioned above would do well to review training and controls for any hope of improvement next year.

Key Takeaways

2025 Phishing Simulation Benchmark Report

What the benchmark suggests for security awareness priorities

Benchmark results should drive targeted action, not annual scorekeeping.

The strongest value of the report is not a single global rate; it is the pattern of where users report, click, complete forms, and open attachments across segments.

1

Reporting gap remains central

A 10.5% reporting rate is useful, but most simulated phishing still goes unreported.

2

Risk varies by segment

Geography, language, company size, and industry each reveal different weak points.

3

Focus beyond clicks

Form completion and attachment opens are higher-risk behaviors than clicks alone.

4

Smaller orgs need support

Lower reporting rates point to resource and training gaps.

5

Tune strategy with data

Use benchmark patterns to prioritize targeted awareness, controls, and role-specific coaching.

Appendix I – Raw Data

1. Geographic Risk Patterns

Region	Click	Form	Attach	Report
North America	4.16%	1.71%	0.39%	10.91%
Europe	7.00%	2.31%	1.89%	10.22%
Asia	4.25%	2.08%	0.07%	9.30%
Africa	6.95%	3.74%	0.28%	0.65%
South America	7.98%	5.27%	2.65%	1.35%
Middle East	4.20%	2.03%	0.00%	0.00%

2. Language-Level Performance

Language code	Recipients	Share	Click	Form	Attach	Report
EN	7.66M	55.03%	4.66%	1.91%	0.75%	9.75%
FR-FR	2.51M	18.06%	7.37%	1.42%	1.45%	19.55%
FR-CA	1.25M	9.01%	6.36%	3.17%	0.56%	4.98%
ES-419	957.5K	6.88%	4.09%	1.52%	1.02%	9.30%
DE	214.7K	1.54%	8.51%	2.80%	6.36%	7.95%
ZH-CN	198.8K	1.43%	4.44%	2.70%	1.06%	3.30%

3. Company Size Patterns

Company size	Click	Form	Attach	Report
10,000+	5.32%	1.73%	1.22%	10.45%
5,000-9,999	5.00%	2.39%	0.30%	13.82%
2,500-4,999	6.92%	4.02%	0.15%	14.42%
1,000-2,499	5.18%	2.55%	0.50%	13.26%
500-999	5.16%	2.60%	0.42%	8.38%
250-499	6.24%	3.05%	0.93%	5.05%
<250	6.44%	2.75%	0.84%	2.53%

4. Industry Patterns

Industry	Click	Form	Attach	Report
Defense	13.02%	3.65%	0.00%	24.83%
Insurance	12.76%	2.02%	12.65%	0.43%
Financial - Banks	5.21%	0.37%	0.22%	30.98%
Hospitality	2.99%	0.34%	0.00%	22.96%
Services	3.84%	1.47%	0.08%	17.41%
Legal Services	3.94%	1.70%	0.12%	16.50%
Broadcasting/Media	8.75%	5.62%	0.15%	0.00%
Gaming	8.20%	16.39%	0.00%	0.00%