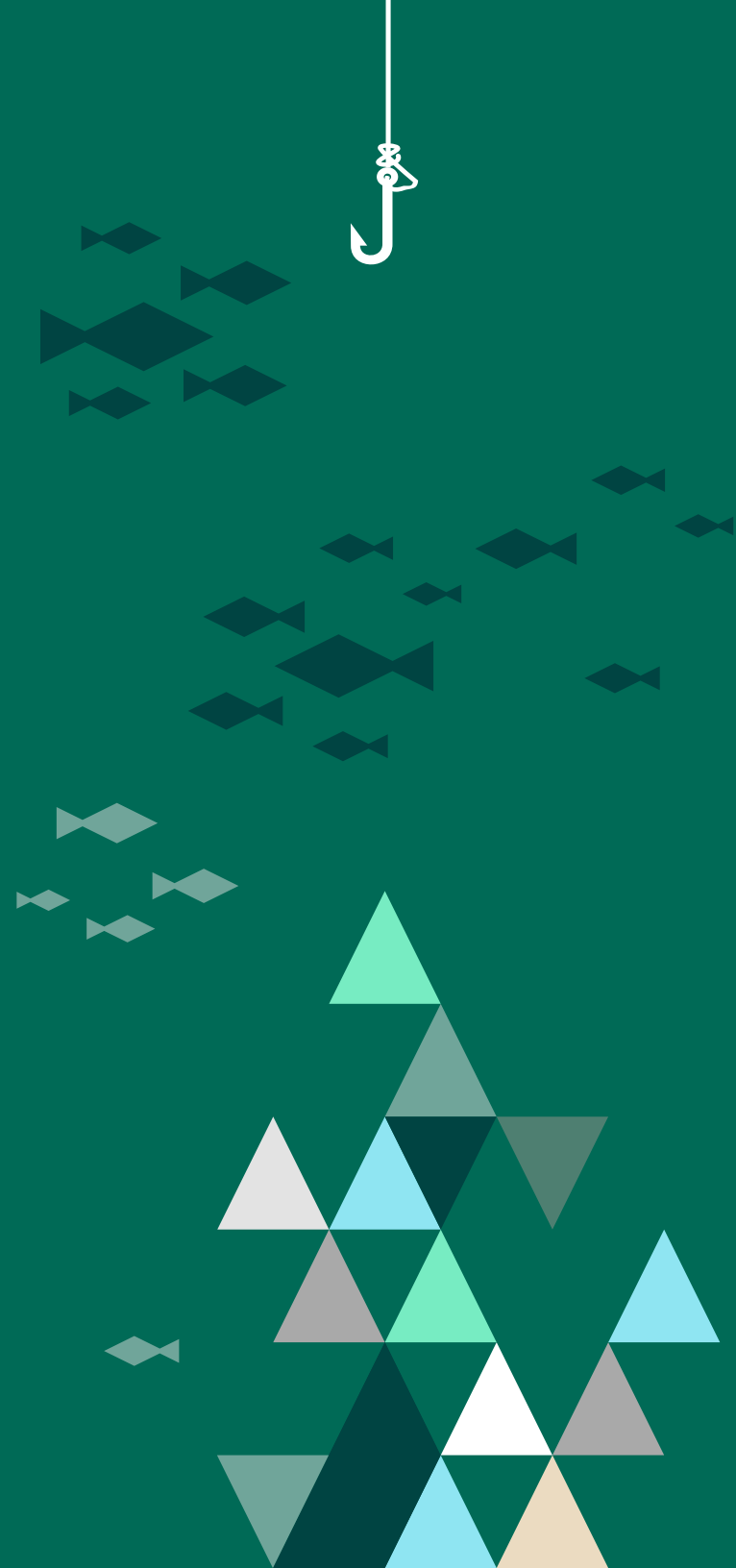


FORTRA™

GONE  
PHISHING  
TOURNAMENT®

# Phishing Benchmark Global Report 2023

Co-sponsored by



## Foreword

Digital transformation is accelerating faster than ever, particularly when it comes to AI technology. Tools like ChatGPT have enjoyed widespread adoption, but their ubiquity has also meant cyber attacks have grown more sophisticated and harder to detect. This reality is especially true of phishing attacks, which regularly target millions of end users with messages and offers that are incredibly convincing.

Now more than ever, organizations must strengthen their defenses against these types of scams and the negative consequences of a data breach by mitigating the human risk element. Doing so involves deploying training that empowers employees and third-party affiliates to consistently spot and report potentially malicious activity.

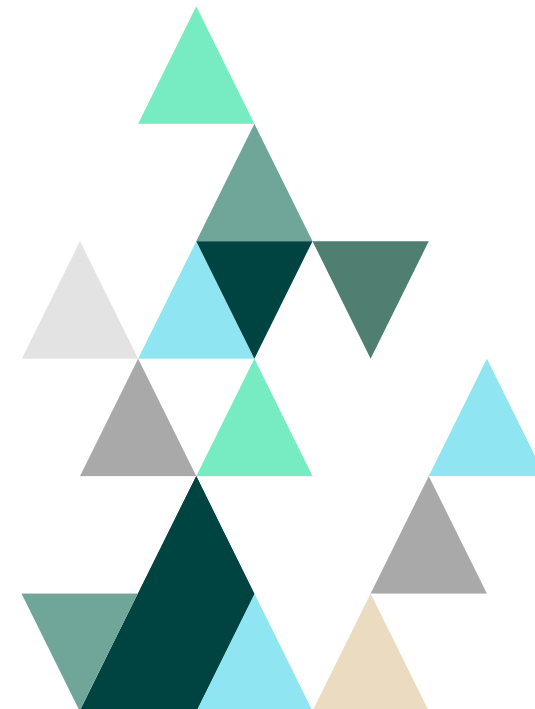
A crucial component of effective phishing training are simulations that provide vital hands-on experience. It's one of the reasons why the National Cybersecurity Alliance supports the Gone Phishing Tournament. This annual event is a terrific resource for organizations looking to assess overall cyber knowledge, gauge areas for improvements, and reinforce key phishing awareness best practices.

By using this report to prioritize the human element in cyber security, your organization is showcasing a commitment to safeguarding sensitive information against increasingly complex online threats. Whatever the next digital transformation chapter brings, your end users will be equipped to handle what hackers may send their way.

**Lisa Plaggemier**  
**Executive Director at the National Cybersecurity Alliance**



**NATIONAL  
CYBERSECURITY  
ALLIANCE**



## TABLE OF CONTENTS

<b>Security Awareness &amp; Phishing Training: An “AI For an Eye” Reality?</b>	<b>4</b>	<b>Results</b>	<b>14</b>
<b>What is the Gone Phishing Tournament?</b>	<b>5</b>	Overall	15
<b>The 2023 Gone Phishing Tournament Methodology</b>	<b>5</b>	Data breakdown by industry: which sector fared best?	16
About the 2023 simulation	6	Data breakdown by number of employees: when does size matter?	20
2023 simulation languages	7	Data breakdown by region: does location make a difference?	22
2023 participating organizations overview	8	<b>The Secret to Launching Effective Phishing Simulation Training</b>	<b>24</b>
<b>Summary of Findings</b>	<b>9</b>	Maximizing results with risk-based phishing training campaigns	24
<b>Phishing Simulations: A Pillar of Strong Cyber Security Awareness</b>	<b>10</b>	How to launch effective phishing simulations	26
<b>How Phishing Impacts All Organizations</b>	<b>12</b>	<b>CISO Recommendations for Employees</b>	<b>27</b>
		<b>CISO Recommendations for Security Leaders</b>	<b>28</b>
		Changing unsafe online behaviors is easier than ever	29
		<b>About Terranova Security</b>	<b>30</b>

## Security Awareness and Phishing Training: An “AI For an Eye” Reality?

AI’s technological versatility has significantly streamlined productivity in various sectors. Organizations are able to accomplish tasks quicker and with greater accuracy, not to mention scale operations by leaps and bounds.

However, those same digital advancements have increased the frequency, sophistication, and complexity of cyber attacks that leverage phishing tactics to compromise sensitive information. Recent data<sup>1</sup> shows that 85% of security professionals attribute the rise in cyber incidents to bad actors using generative AI as part of their scams.

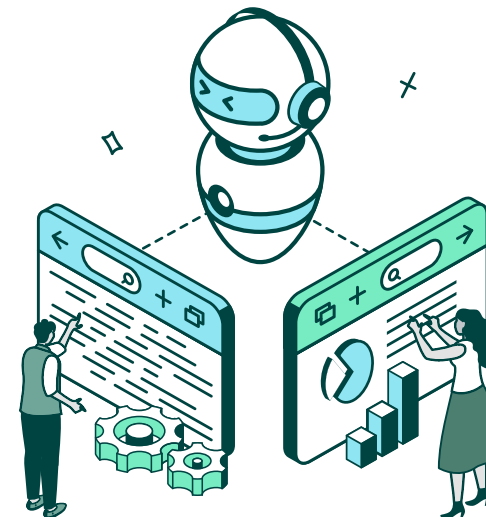
Take content generation, for example. Generative AI tools like ChatGPT, based on large language models, can be misused to create convincing phishing emails and landing page content, blurring the line between legitimate and fraudulent communications. The same issue extends to smishing and vishing, malicious code injection, website spoofing, voice and video cloning, and much more.

In the face of all these concerning developments, the inciting incident for many data breaches remains the same: human error. Even with better technological safeguards at the average organization’s disposal, hackers are enriching themselves more than ever before.

The reason is simple—phishing links don’t click themselves. Human beings, however well-intentioned, do.

To truly secure your confidential data, cyber security awareness and phishing training must strive to go beyond minimum compliance standards. Cyber security best practices must be a top priority across an organization’s entire business ecosystem, from executive leadership on down. They need to be an integral part of your cultural fabric.

Globally, individuals don’t want to leave information vulnerable to cyber criminals. They want to do the right thing, which includes learning more about phishing tactics. By allowing everyone to learn in a safe, hands-on environment, mitigating risk through behavior change becomes an attainable reality for any organization.



<sup>1</sup>Source: <https://www.securitymagazine.com/articles/99832-study-finds-increase-in-cybersecurity-attacks-fueled-by-generative-ai>

## What is the Gone Phishing Tournament?

The Gone Phishing Tournament™ (GPT) is a free annual cyber security training event that helps organizations strengthen their security awareness training programs with accurate phishing benchmarking data.

The insights generated by this benchmarking data empower security and risk management leaders to:

- ▶ **Better understand their high-risk vulnerabilities**
- ▶ **Compare phishing performance to their peers**
- ▶ **Set realistic objectives for user behaviors**
- ▶ **Establish stronger, data-driven security awareness goals**
- ▶ **Support the need for ongoing awareness activities**

When organizations can accomplish all this and more, they also maximize their cyber security awareness return on investment and minimize the confidential data left vulnerable by human risk.



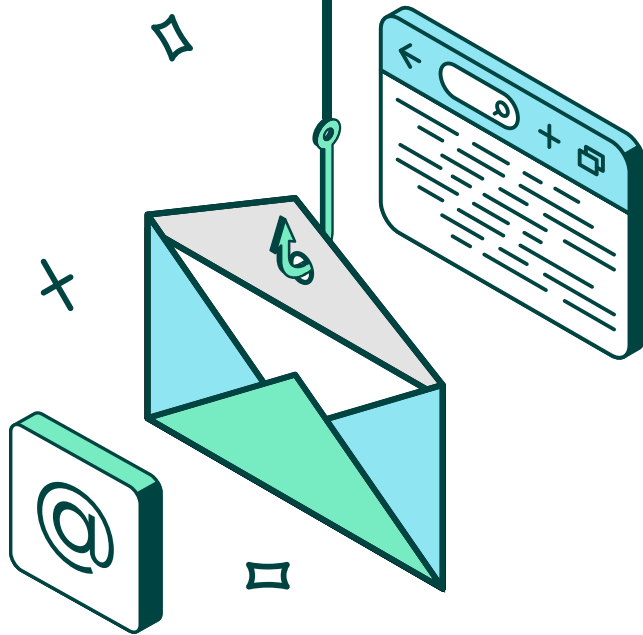
## The GPT Methodology

Every year, the GPT welcomes organizations from various regions and industries around the world. The event is open to all, with 2023 participants including both existing Fortra's Terranova Security customers and parties with no prior relationship with the company.

This global phishing simulation measures employee behaviors with realistic phishing tactics they may encounter in their day-to-day activities. Unlike other phishing simulation events, the GPT does not evaluate performance across different scenarios throughout a calendar year. GPT participants all receive the same phishing simulation during the predetermined event timeframe.

As a result, click rates and related benchmarking data are based on the same simulated phishing threat, offering security leaders with a true apples-to-apples performance overview.

The results for each cohort (industry, size, and region) are weighted averages based on the number of users in each segment, not the number of participating organizations.



## About the 2023 simulation

As in previous years, Terranova Security worked with Microsoft to create the GPT phishing simulation email and webpage templates. The simulation emulated a common cyber tactic: a fake password expiration notification aimed at stealing user credentials.

The email and webpage spoofed the look of emails end users can receive related to business account security. However, there was a critical twist: The phishing simulation email prompted recipients to keep the same password associated with their account instead of resetting it, which goes against cyber security best practices. As in real-world attacks, the simulation used manipulative techniques preying on the human desire to keep using the same password and avoid resetting it.

The scenario measured several user behaviors, such as clicking on a link in the body of a phishing email and entering business account credentials into a phishing webpage form. Participants who submitted their password during the simulation were directed to a feedback page that provided just-in-time training on the red flags they missed in the email and webpage. No actual passwords were collected during the event.

The 2023 GPT took place from October 9th to 27th. Throughout the process, Terranova Security operated using its existing data security controls on its Security Awareness Platform. After the tournament, Terranova Security executed the data analysis stage of the event. All participant data was anonymized, and all personal information used during that process was deleted after completion.

This process ensured end-to-end data privacy and security for all participating organizations.



# 31 Languages



## 2023 simulation languages

To provide an inclusive experience, the 2023 GPT template was made available in more languages than in previous years (31 in total), including:

- |                                      |                              |
|--------------------------------------|------------------------------|
| <b>Arabic</b>                        | <b>Korean</b>                |
| <b>Chinese (Hong Kong) Cantonese</b> | <b>Polish</b>                |
| <b>Chinese (PRC*) Mandarin</b>       | <b>Portuguese (Brazil)</b>   |
| <b>Czech</b>                         | <b>Portuguese (Portugal)</b> |
| <b>Dutch</b>                         | <b>Romanian</b>              |
| <b>English</b>                       | <b>Russian</b>               |
| <b>English UK</b>                    | <b>Slovak</b>                |
| <b>French (Canada)</b>               | <b>Slovenian</b>             |
| <b>French (France)</b>               | <b>Spanish</b>               |
| <b>German</b>                        | <b>Spanish (Spain)</b>       |
| <b>Greek</b>                         | <b>Swedish</b>               |
| <b>Hebrew</b>                        | <b>Thai</b>                  |
| <b>Hungarian</b>                     | <b>Turkish</b>               |
| <b>Indonesian</b>                    | <b>Ukrainian</b>             |
| <b>Italian</b>                       | <b>Vietnamese</b>            |
| <b>Japanese</b>                      |                              |
- 

## 2023 participating organizations overview

For the second consecutive year, Terranova Security enjoyed a record-setting GPT.

In 2023, nearly 300 organizations participated in this year's event, making it one of the largest phishing simulation events of its kind. We also saw a 10% year-over-year increase in the number of participating end users, with over 1.37 million receiving the event's phishing simulation email.

In total, end users from 142 different countries participated in the 2023 edition of the event. The increased demand to partake in this global phishing simulation underscores how vital cyber security and phishing awareness are worldwide in the face of ever-increasing prevalence of real-world threats.





## Summary of Findings

The 2023 GPT results revealed many end users are still prone to leaving sensitive information vulnerable to cyber attacks, even if the email comes from an unknown sender.

10.4%<sup>2</sup> of all phishing simulation email recipients clicked the message’s phishing link. This click rate represents a 3.4 percentage point increase compared to the previous year’s metric results<sup>3</sup>. Globally, 6.5% of all recipients submitted their passwords in the form embedded in the malicious webpage, a 3.5 percentage point increase compared to 2023.

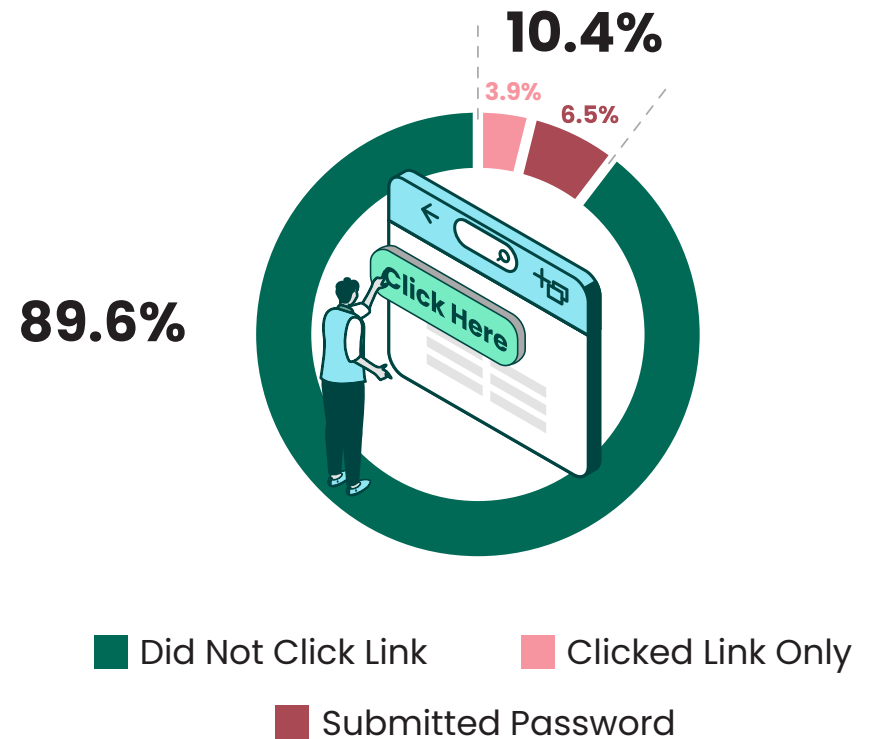
More shocking was the ratio of simulation clickers to password submissions. Overall, 6 out of every 10 end users who clicked on the phishing email links failed to recognize the phishing website and submitted their password.

Amplify this reality by tens of millions of targeted end users, and there are still opportunities for organizations of all sizes to better inform employees and third-party vendors on detecting phishing email messages. With new AI-based tools at their disposal, bad actors can set up attacks where browsers or security providers may not inform end users of potential risks.

Technical safeguards, including firewalls and email security measures, cannot guarantee information security, especially at the enterprise level. As a result, everyone must have the knowledge and reflexes required to detect and report incoming phishing threats consistently.

Otherwise, confidential data is at a high risk of being exposed to criminals.

## All users actions



<sup>2</sup> The averages in this summary section are calculated based on the total number of participating users. To calculate this average, Terranova Security grouped all participating users and clickers together, treating it as one simulation.

<sup>3</sup> The 2023 simulation template used a different context but targeted the same behaviors with its tactics.


## Phishing Simulations: A Pillar of Strong Cyber Security Awareness

The theoretical side of security awareness, while important, is far from the only crucial aspect of a successful training program.

Practical, hands-on exercises like phishing simulations help end users understand common threat tactics and acquire the know-how necessary to pinpoint possible attacks. That expertise can mean the difference between avoiding or succumbing to a data breach and all the repercussions it can leave in its wake.


### Phishing simulations like the one used during this year's GPT can answer questions like:

- ▶ Who are the high-risk employees and roles within my organization?
- ▶ Which roles have the most inherent risk factors, such as access to sensitive information and the volume of emails received?
- ▶ How is security awareness training performance contributing to overall risk reduction?



**Remember:  
Phishing links  
require human  
interaction  
to work**

**Once deployed and assessed, phishing simulation data delivers actionable information that empowers decision-makers to:**



Mitigating risk involves more than deploying a by-the-numbers security awareness training course or initiative. It requires deep integration with your organization's existing culture, ensuring every team member makes security best practices a top priority.

**1**

**Reduce human risk levels**  
considerably

**2**

**Change end use behaviors**  
by lessening the automatic trust response

**3**

**Minimize costs**  
associated with cyber security and attacks

**4**

**Measure vulnerability**  
at the individual and organizational level

**5**

**Provide targeted training**  
and just-in-time feedback to employees

**6**

**Improve user reporting**  
and responses to phishing attempts

**7**

**Create a cyber-aware culture**  
that proactively secures data



## How Phishing Impacts All Organizations

Successful phishing attacks can inflict financial harm on all types of organizations, regardless of their industry, region, or customer base. The run-off effects can also do irreparable harm to relationships with investors and affiliates, as well as a brand's reputation in a global marketplace.

The consequences of phishing attacks only continue to grow. In their 2023 Internet Crime Report<sup>4</sup>, the FBI's Internet Crime Complaint Center (IC3) received over 800,000 cyber incident complaints, with estimated total losses topping \$10 billion. Despite this, according to the 2023 Cyber Culture Report<sup>5</sup>, 52% of employees still say their job has nothing to do with cyber security.

The negative impacts can be widespread if an organization does not implement an optimal security awareness training program that includes immersive, gamified eLearning modules. These qualities promote knowledge retention, course completion, and other crucial training success vectors.

<sup>4</sup> Source: [https://www.ic3.gov/Media/PDF/AnnualReport/2022\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf)

<sup>5</sup> Source: <https://terranosecurity.com/from-data-protection-to-cyber-culture>



**Results**



FORTRA™

**GONE  
PHISHING  
TOURNAMENT®**

**The following sections of this report examine overall benchmarks and trends extracted from the 2023 GPT results<sup>6</sup>.**

**You'll get a complete breakdown of the event's data by industry, organization size, and region.**

**Working with Microsoft to create a real-world simulation experience, this report provides a true phishing behavior benchmarking opportunity for organizations worldwide.**

<sup>6</sup>The overall, industry, size and regional averages are based on total end-user click rates to ensure equal data weighting.

## Overall

In total, 10.4% of all phishing simulation email recipients who participated in the 2023 GPT clicked the phishing link. Strictly from a data point of view, this click rate represents a 3.4 percentage point increase compared to the previous year's event<sup>7</sup>.

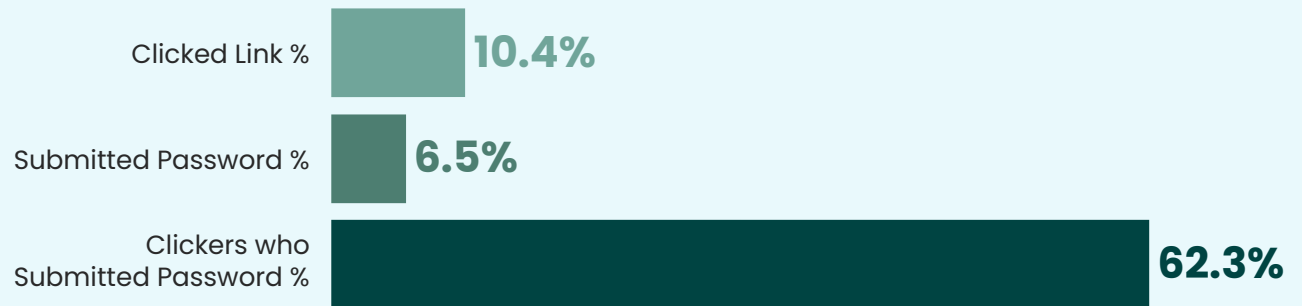
6.5% of all simulation email recipients submitted their password in the form embedded in the malicious webpage, a meaningful 3.5 percentage point increase compared to the 2023 results. Most concerning for security leaders may be the ratio of clickers to password submitters—6 out of every 10 end users who clicked on the simulation email link ended up compromising their credentials.

**To put these numbers into perspective, had this been an actual phishing attack, cyber criminals could have collected close to 90,000 passwords that secure business accounts.**

**Once obtained, this data could've been used for Account Takeovers (ATO), Business Email Compromise (BEC), credential stuffing attacks and many other nefarious purposes.**



## Global Data



<sup>7</sup>The 2023 simulation template used a different context but targeted the same behaviors with its tactics.

## Data breakdown by industry: which sector fared best?

When comparing click rates based on an organization’s industry<sup>8</sup>, there are many additional variables at play. Internal standards, data privacy and compliance requirements, and other specifics will differ from organization to organization, even if they operate in the same marketplace.

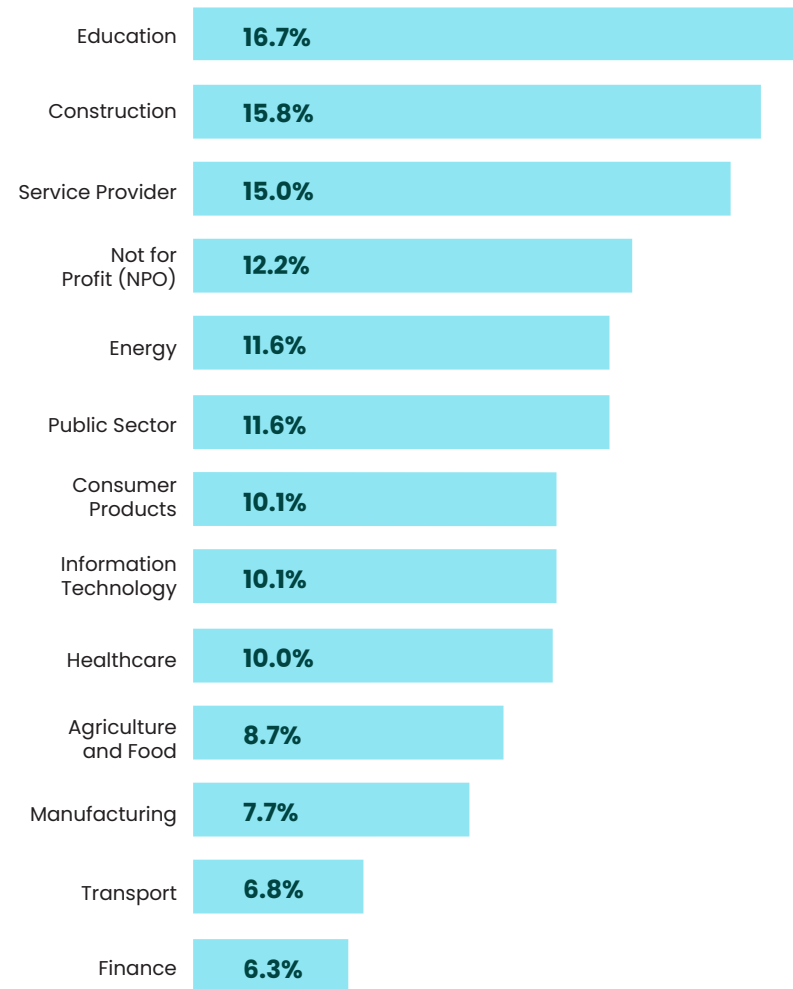
To account for this, results in this category are based on a weighted average<sup>9</sup>. As the scenario used for the 2023 GPT simulation is generic, a variance in click rates, even for organizations in the same sector, is to be expected.

The Finance sector posted the lowest click rate (6.3%) across all industries for the second consecutive year. The Transport sector (6.8%) finished with the second-best click rate, followed by the Manufacturing sector (7.7%).

<sup>8</sup>To obtain results by industry, and size, Terranova Security calculated the average based on the number of participating users in each grouping. This was done to ensure organizations in a specific sector or size segment were weighted based on the number of users when calculating the average.

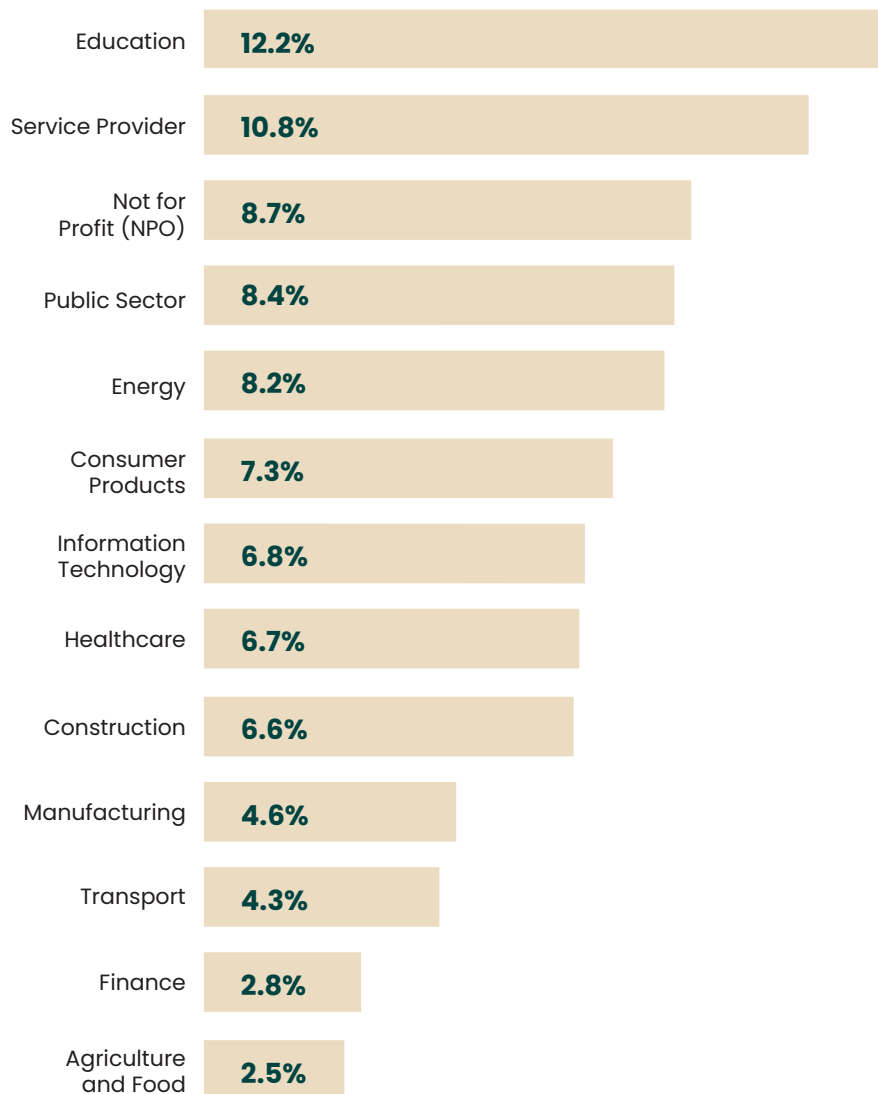
<sup>9</sup>Note on the weighted standard deviation included in this report (page 19): A lower number indicates that the results for all participants in a specific cohort are close to each other. Most sectors have what is considered a higher weighted standard deviation which indicates that click rates vary greatly across members of each cohort.

## Clicked link by industry (%)





## Submitted password by industry (%)



Conversely, the Education sector saw both the highest click and password submission rates, totaling 16.7% and 12.2%, respectively. Other industries that saw click rates 50% or more above the event’s average were the Construction (15.8%) and Service Provider (15%) sectors.

The minimum and maximum values (page 19) are the lowest and highest values among participants in each sector. In 11 of the 13 sectors, there was at least one organization that had click rates higher than 25%.

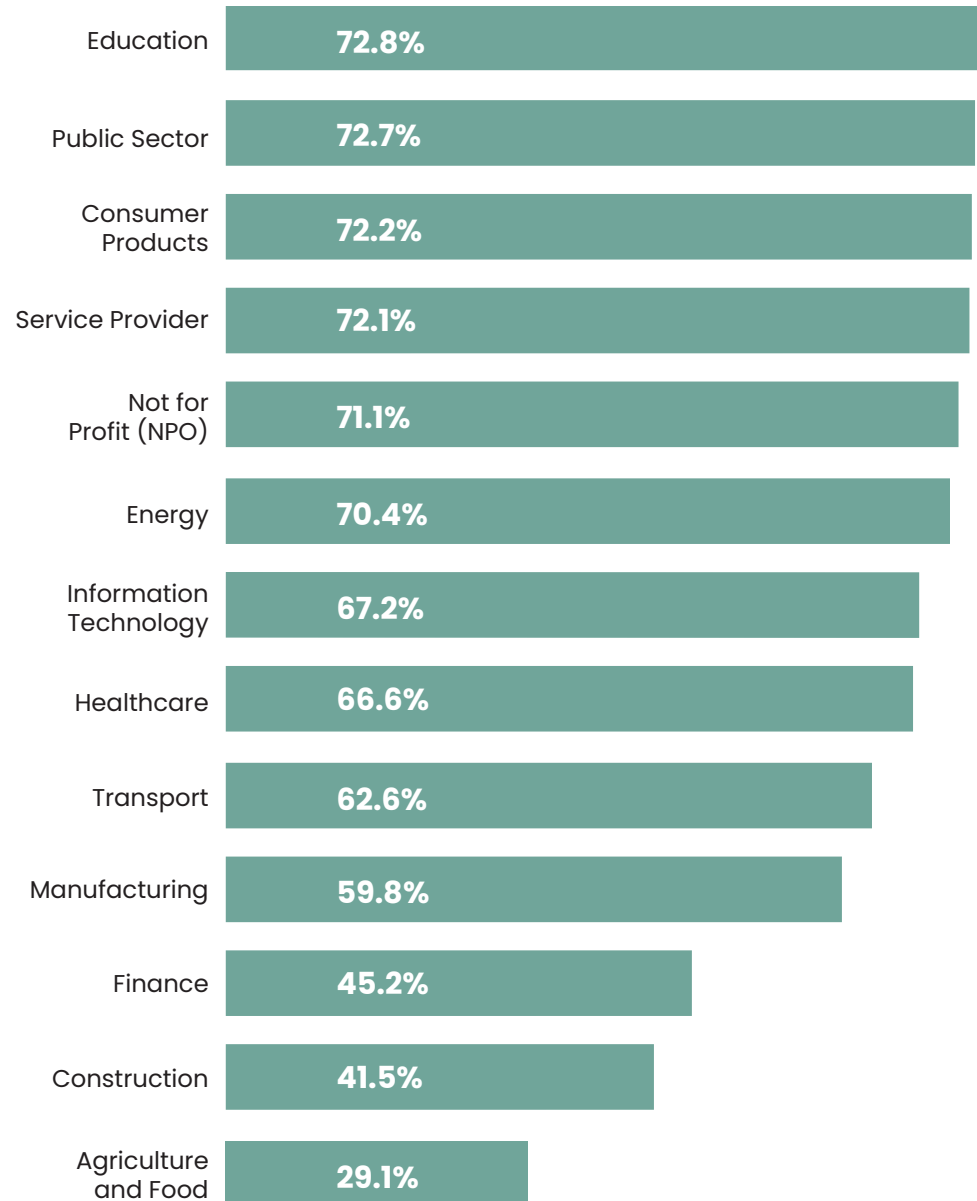
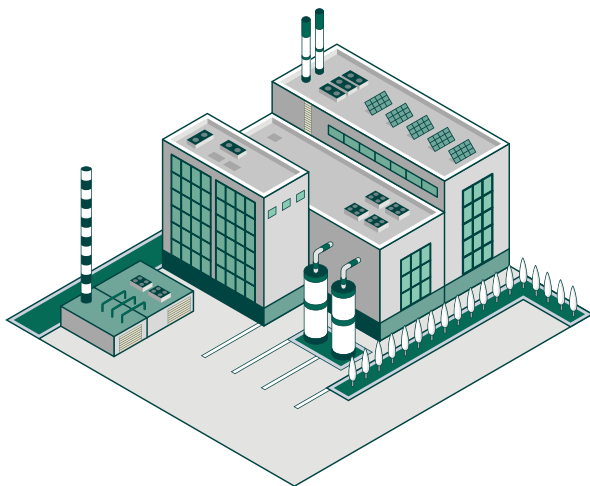
When it comes to password submission rates, Finance and the Agriculture & Food sectors posted the lowest totals, with 2.8% and 2.5%, respectively. The Transport sector came in third-lowest in this category with a 4.3% password submission rate among their end users.



## Clickers who submitted password by industry (%)

The ratio of phishing simulation clickers to password submitters can be seen as a silver lining for participating organizations with higher-than-expected click rates. The lower the figure, the less likely end users were to unquestioningly trust the simulation web page’s validity and submit their credentials.

In that regard, Agriculture & Food was the only participating industry to keep that ratio under 30% during the 2023 GPT. Finance (45.2%) and Construction (41.5%) also performed well, considering the overall average in this category. On the other end of the spectrum, six industries posted a click-to-submission ratio above 70%, with Education topping that list at 72.8%.



The following chart indicates the standard deviation value per industry. The lower the number, the closer to each other the results were for all participants in a specific cohort. The 2023 GPT results indicate that most sectors have what is considered a higher weighted standard, meaning their click rates vary greatly across all participating organizations in that category.

These results showcase a continued disparity between security awareness norms by industry, as well as how common certain activities are in end

users' daily activities. Depending on their role, certain professionals may be more aware of potential red flags in a password-related request like the one featured in this simulation. Consequently, the suspicious activity may be easier to pinpoint and report.

Regardless of industry, it's clear that even the best-performing sectors can still be susceptible to phishing emails that prey on busy schedules and the automatic trust response.

Industry	Minimum of Clicked Link %	Weighted Average of Clicked Link%	Maximum of Clicked Link %	Weighted Standard Deviation	Minimum of Clicked Link% (Not Zero)
Agriculture and Food	0.0%	8.7%	16.1%	0.75	7.7%
Construction	0.0%	15.8%	27.2%	6.13	14.0%
Consumer Products	0.8%	10.1%	19.3%	5.33	0.8%
Education	1.2%	16.7%	37.5%	8.86	1.2%
Energy	2.9%	11.6%	36.2%	4.89	2.9%
Finance	0.9%	6.3%	35.4%	5.85	0.9%
Healthcare	2.8%	10.0%	26.8%	6.09	3.5%
Information Technology	0.0%	10.1%	33.3%	4.3	2.2%
Manufacturing	0.0%	7.7%	34.6%	3.76	2.3%
Not for Profit (NPO)	0.3%	12.2%	27.8%	7.64	0.3%
Public Sector	0.0%	11.6%	28.0%	5.82	0.3%
Service Provider	0.0%	15.0%	22.6%	8.63	2.3%
Transport	0.0%	6.8%	40.8%	4.61	1.0%

**KEY TAKEAWAY:** Even the most security-aware individuals can miss phishing red flags if they're scanning a message quickly. Ensure everyone takes the time to read and react to every incoming email appropriately.

## Data breakdown by number of employees: when does size matter?

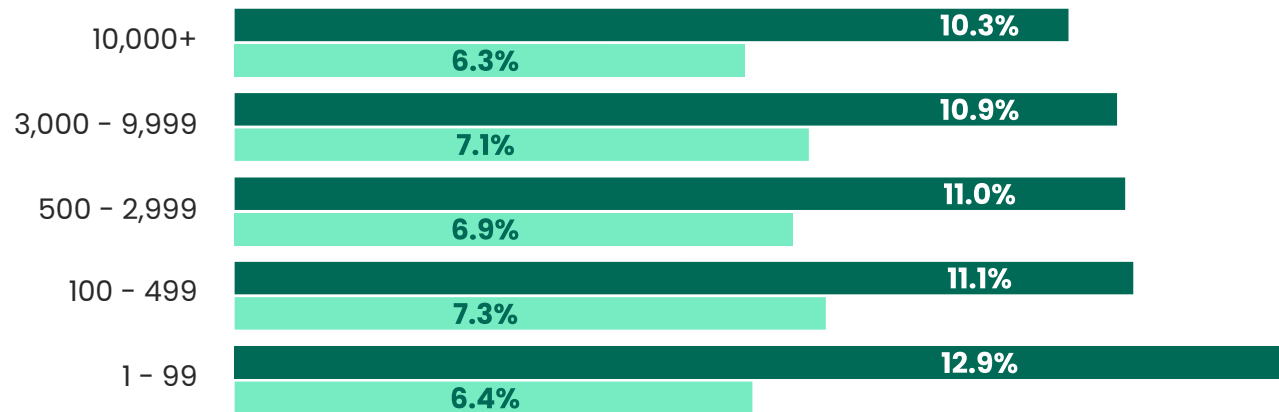
Organization size is always a double-edged sword with regard to security awareness initiatives. More internal resources, including budget and staff devoted to the cause, sound advantageous. However, with many organizations adopting remote or hybrid workplace protocols, it's the "how" related to security awareness implementation that matters most.

You can see that narrative unfold in the GPT results segmented by organization size. During the 2023 event, organizations with an employee count between 1 and 99 posted the highest click rate (12.9%), outpacing organizations with larger headcounts and, presumably, resource allocation.

### Results by organization size (%)

■ Clicked Link %

■ Submitted Password %

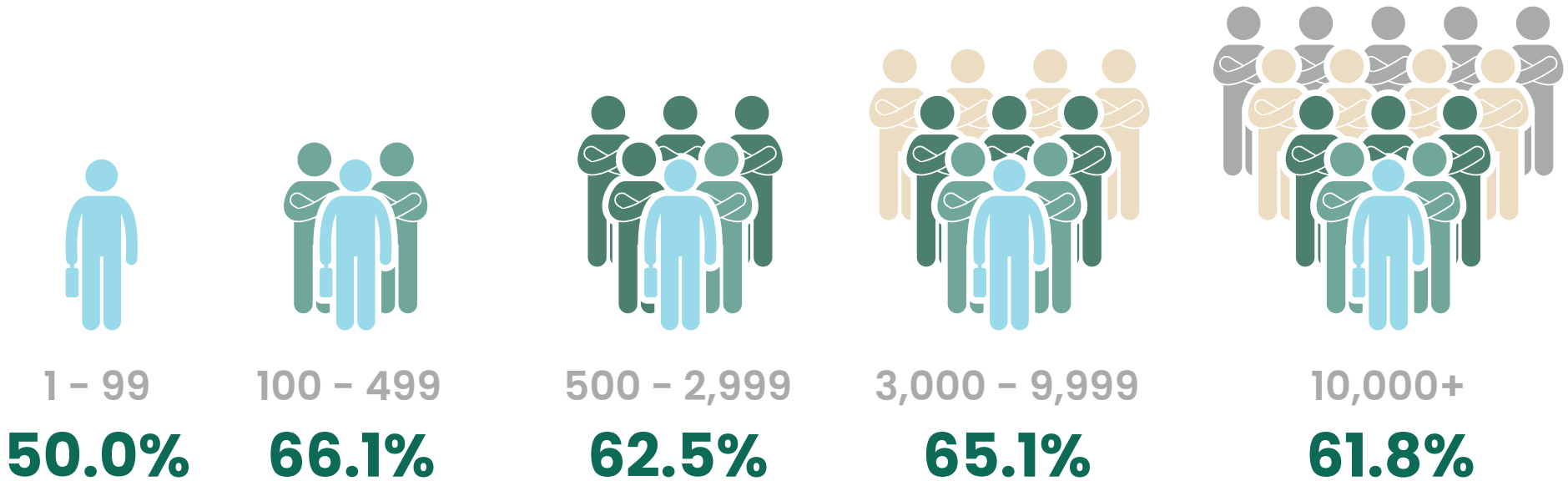


This data paints a different picture compared to the 2023 results, where organization with employee counts over 10,000 posted the highest click rate. Organizations with less than 100 end users actually finished with the lowest click rate in 2023.

Interestingly, the same trend didn't carry over to password submission rates in 2023. Organizations with an employee count between 100 and 499 had the highest overall password submission rate at 7.3%. The same size segment also finished with the highest click-to-submission ratio (66.1%). Participants with an employee count under 100 were the only ones who kept that ratio at or under 50%.

These results prove there is no one-size-fits-all solution for security awareness. The existing culture, as well as leadership's willingness to make cyber security awareness a top priority versus a low-stakes compliance consideration, can often dictate how engaging and effective awareness programs end up being at the corporate level.

## Clickers who submitted password by organization size (%)



Cyber criminals also don't treat all organizations the same way from a threat targeting perspective, either. They may look at smaller organizations and see "quick win" potential, as investment in cyber security and awareness components may be a less urgent action item. On the other hand, larger organizations are often seen as primary targets due to the massive payout potential.

At the enterprise level, universal security awareness availability for end users does not automatically strengthen data protection. Larger organizations often struggle to reach all employees with awareness activities and increase course participation and completion rates. They also have to account for more frequent and complicated employee onboarding requirement, particularly if it's a remote-first setup.

**KEY TAKEAWAY:** Understand your organization's high-risk areas and unique needs before building a security awareness strategy or program.

## Data breakdown by region: does location make a difference?

Regionality can significantly influence an organization’s cyber security operations, both from an operational and customer base point of view.

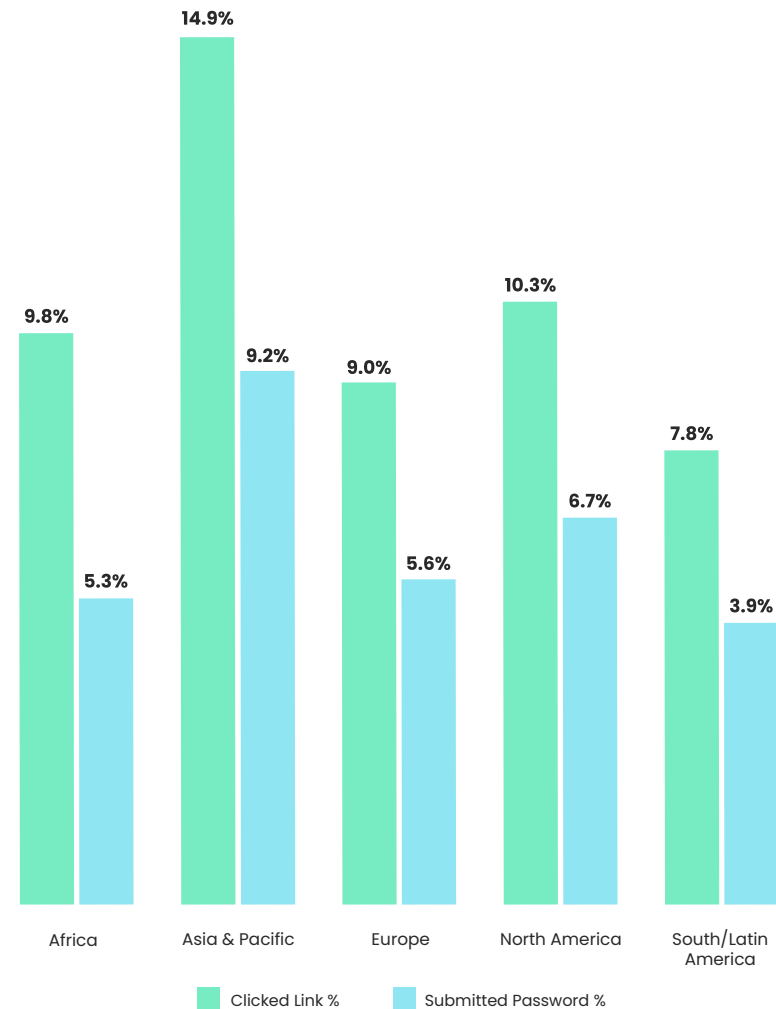
Data privacy regulations are getting increasingly more stringent worldwide and, like GDPR, dictate how an organization collects, stores, and manipulates consumer data. Couple those realities with the increasing number of distributed workforces adapting information security policies for that new normal, and it’s clear that IT departments have far more to consider than they did even a few years ago.

Of the five regions represented in the 2023 GPT<sup>10</sup>, South/Latin America performed the best. This region posted a click rate of 7.8% and a password submission rate of only 3.9%, both the lowest in their respective categories. Meanwhile, the Asia & Pacific region performed the worst in both categories, with a click rate of 14.9% and a password submission rate of 9.2%.

North America’s GPT click rate total slotted in below the global average at 10.3%. However, the region posted an above-average password submission rate of 6.7%. This dichotomy demonstrates that performance in one area, such as click rate, doesn’t always tell the entire story regarding security awareness maturity.

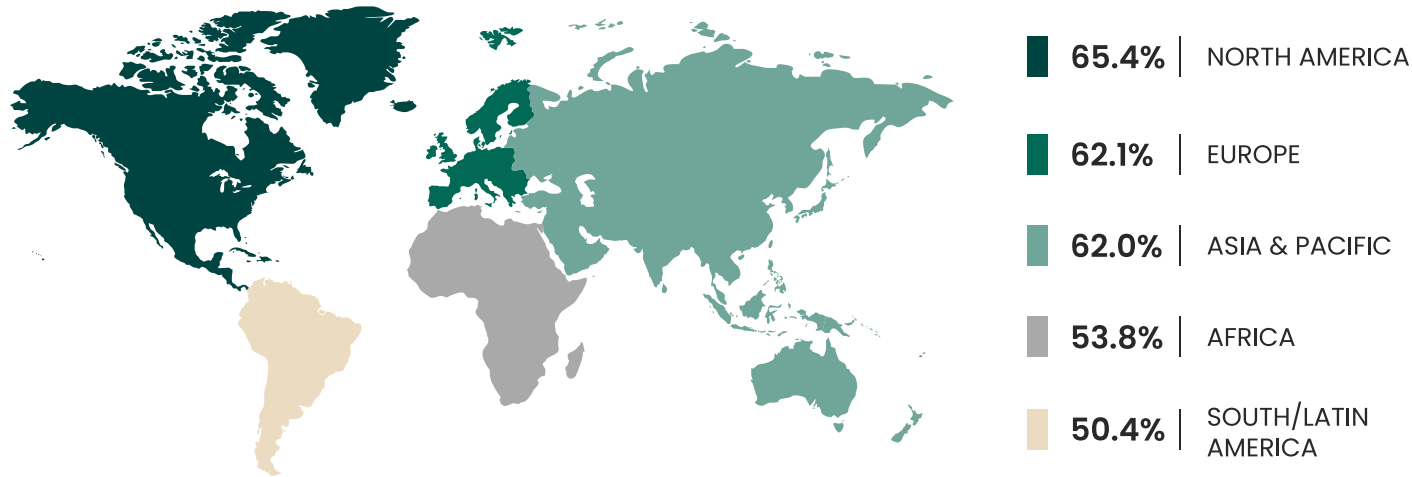
Comparatively, European participants finished in the middle of the pack, scoring a click rate of 9%, just below the global average. End users in Europe submitted their passwords at a rate of 5.6%, nearly two whole percentage points higher than the strongest performers, South/Latin America.

## Results by region (%)



<sup>10</sup> Regional results were calculated based on the location of participating users. To calculate this average, all participating users and clickers were grouped by region based on their country.

## Clickers who submitted password by region (%)



North America posted the highest click-to-password-submission ratio, topping 65%. South/Latin America (50.4%) and Africa (53.8%) were the only two regions to finish with ratios under the 2023 GPT average in this category.

One of the constants in phishing attacks that target end users in multiple regions is preying on a sense of familiarity. Cyber threats evolve to look and sound as close to common messages professionals may encounter in an ordinary workday as possible.

By blending into crowded inboxes effectively, many phishing emails can easily go undetected.

This tactic is one of the many reasons why investing in security awareness training that evolves alongside the threat landscape is critical. Training courses and practical exercises like phishing simulations must be continuously updated to reflect current realities. Otherwise, end users may not have the most up-to-date intel on how cyber criminals may try and steal their data.

**KEY TAKEAWAY:** Choose a security awareness training platform that’s continually updating existing content and releasing new modules that accurately reflect new cyber crime trends.

## The Secret to Launching Effective Phishing Simulation Training

While security service providers do their best to inform end users on malicious sites or potential risk, security experts have seen an overreliance on those technical safeguards in recent years. As a result, end users may not do enough due diligence on a case-by-case basis.

Effective phishing simulation training is one of the best ways to ensure end users are well-prepared to exercise proper judgment when detecting and reporting phishing messages and sites. Automatically trusting a website or link because their browser isn't warning them of malicious activity is a prime example of unsafe online behavior that can be "unlearned" with the help of security awareness training.

That said, the individual training components must feed focused cyber security goals designed to mitigate risk and grow a security-aware culture. When security leaders leverage data-driven insights from initiatives like the GPT, they're better positioned to determine high-risk end users or roles and address those weaknesses with appropriate training measures.

From reducing click rates to maximizing training course completion rates, it all starts with the right data.

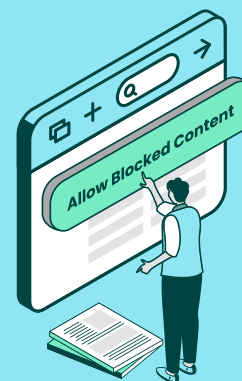
## Maximizing results with risk-based phishing training campaigns

With the right data, security leaders must establish a security awareness strategy supported by a proven framework for lasting behavior change. Setting the foundation for a defined end-user learning path ensures your awareness training campaigns target the correct user habits most often leveraged by hackers.

## Terranova Security experts advise clients on the following seven common behaviors that hackers will routinely target during a cyber attack

### THREATS

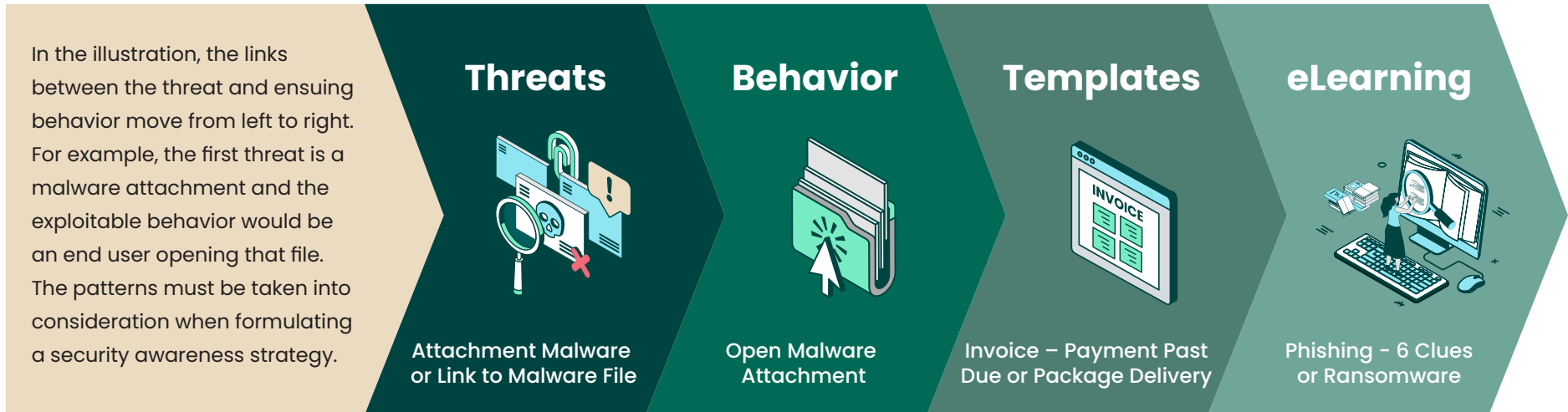
- Attachment Malware
- Link to Malware File
- Link in Attachment
- Drive-By URL
- Credential Harvesting
- Business Email Compromise



### BEHAVIORS

- Open Malware Attachment
- Clicking on a Link or Button
- Giving Out UID/PW
- Giving Out Employee PII
- Giving Out Corporate Financial Info
- Giving Out Personal PII
- Giving Out Personal Financial Info





**Once the action plan is ready to go, Terranova Security encourages the use of:**

- ▶ **A baseline simulation to clarify your organization’s starting point knowledge-wise**
- ▶ **Communication tools to promote the training program and underscore its importance**
- ▶ **Gamification techniques that keep participants engaged with training initiatives.**

The phishing simulations you choose to launch as part of a security awareness program will, in part, influence the resulting click rate. If end users never click on simulation links, your chosen phishing templates may not be challenging them. Effective practical exercises must prioritize quality over quantity.

# How to launch effective phishing simulations

To educate users and change key behaviors cyber criminals can look to exploit, follow these guidelines.



1

Target the right user behaviors by delving into your existing cyber security data and pinpointing unsafe behavior patterns or actions

2

Create phishing simulations that address those weaknesses and leverage up-to-date scenarios that end users may encounter

3

Collect real-time phishing simulation data to facilitate the assessment, maintenance, and growth of a security-aware culture

4

Track and monitor user progress to determine user-specific risk ratings and overall security awareness effectiveness

5

Deploy just-in-time training modules to give users the instant feedback they need should they fail a phishing simulation

6

Utilize customizable training campaigns based on the data you collect to tailor every aspect of the process and drive goal attainment

7

Choose a scalable, inclusive solution with multilingual, accessible training content that helps cater eLearning to a diverse employee base

## CISO Recommendations for Employees

To avoid having confidential data compromised by phishing threats like the one depicted in the 2023 GPT, Terranova Security CISOs recommend all employees and third-party vendors keep top-of-mind when faced with a suspicious message.

**1**

**Confirm the sender's email domain** to ensure legitimacy (e.g., check for misspellings like an extra "n" in amazonn.com).

**2**

**Scrutinize the email's content** for urgent language that pressures immediate action. Be skeptical of too-good-to-be-true offers.

**3**

**Never email personal or financial information** in response to unsolicited or suspicious emails.

**4**

**Exercise caution with email links**—hover to preview the URL and assess the sender's reliability.

**5**

**Double-check the URL and site security** before inputting data on a website to avoid scams.





## CISO Recommendations for Security Leaders

To boost security awareness participation and take steps to instill a security-first culture within your organizations, Terranova Security CISOs recommend doing the following.

1

**Use data to set and pursue realistic goals**, like reducing employee click rate on suspicious emails by 5% in a year.

2

**Implement only the highest quality training content**, including interactive and gamified elements, to keep users engaged.

3

**Develop ongoing training programs** that regularly provide new materials to keep security awareness sharp.

4

**Regularly assess and refine your strategy** based on performance metrics to enhance user experience.

5

**Foster a company-wide culture of security awareness**, emphasizing that data protection is everyone's responsibility, not just IT's.



## Changing unsafe online behaviors is easier than ever.

Mitigate the human risk factor and strengthen your cyber security practices across your entire organization with Fortra's Terranova Security, a trusted leader security awareness and phishing training.

[Get a Personalized Demo](#)

## About Terranova Security

Fortra's Terranova Security makes it easy to build risk-based campaigns that feature the industry's highest-quality training content and real-world phishing simulations. As a result, any employee can better understand phishing, social engineering, data privacy, compliance, and other critical best practices. All our security awareness training options are crafted with customer goals in mind. Every content asset and phishing simulation template is constructed to support an organization's cyber security objectives and strengthen its long-term information security.

Terranova Security is proud to be part of Fortra's comprehensive cyber security portfolio. Fortra simplifies today's complex cyber security landscape by bringing complementary products together to solve problems in innovative ways. With the help of powerful protection from Terranova Security and others, Fortra is your relentless ally, here for you every step of the way throughout your cyber security journey.



# FORTRA™

## **About Fortra**

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at [fortra.com](https://fortra.com).