GONE PHISHING TOURNAMENT™

2020 Phishing Benchmark Global Report

Co-sponsored by

TERRANOVA SECURITY

Microsoft

Anyone working in cyber security, technology, or business leadership roles knows that the stakes around safeguarding confidential data have never been higher. Many organizations are shifting how they work, with remote work and other considerations lessening the impact of your average technical safety nets. Now more than ever, your employees need to know how to detect and avoid phishing scams.

For organizations looking to see how their security awareness training efforts measure up versus their peers, the Terranova Security Phishing Benchmark Global Report, which draws on the results from the most recent Gone Phishing Tournament, is a great starting point.

Microsoft was proud to co-sponsor the 2020 edition of the Gone Phishing Tournament and collaborate with its leadership team on the phishing template used during the event. As a group, we wanted to deliver a scenario that was current and ingrained in the everyday lives of end users worldwide and leveraged real-time Microsoft phishing email data to raise the bar with regards to security awareness training quality.

Microsoft is also grateful to count Terranova Security as our global security awareness partner of choice that ensures we bring the best training possible to customers around the world. The data and insight in this report can help any organization, regardless of size, industry, or geographic location, reinforce its human firewall and, through accurate benchmarking, get a real picture of how to grow your security awareness training initiatives effectively.

By empowering your people via data-driven phishing awareness, your data will be much better protected.

Microsoft

BRANDON KOELLER

Principal Program Manager Lead - Office 365 Security

TABLE OF CONTENTS

Phishing: A More Complex Threat Than Ever

2020 was a year of seismic shifts for organizations everywhere. A global pandemic and accelerated digital transformation paved the way for more remote workforces and a "new normal" that's anything but. Those shifts also led to an overall increase in information security risk levels as cyber criminals worldwide took advantage of this widespread volatility with targeted phishing attacks.

Cyber criminals know that many people are adjusting to a new working environment, namely a home office, making users more susceptible to carefully crafted phishing emails, calls and text messages or other cyber attacks. Cyber criminals leverage the fear and uncertainty created by this global event to trick users and compromise systems and information.

From January to March 2020 alone, the number of blocked suspicious messages targeting remote workers rose an astounding 30,000% (no, that is not a typo). The number of COVID-19-related spear phishing attacks also increased by 667%. According to Microsoft, of the millions of targeted phishing email messages we see and track each day, roughly 60,000 include COVID-19 related malicious attachments or malicious URLs.

The average cost of a data has hit $137,000, raising organizations' stakes everywhere. After all, it usually starts with a phish. It only takes one user to be victimized by a malicious email, webpage, or download to potentially compromise vast amounts of confidential data.

The first step in effective phishing and security awareness training programs is knowing where you stand. To establish accurate benchmarks based on real-world phishing threats, Terranova Security launched the second edition of the Gone Phishing Tournament.

What is the Gone Phishing Tournament™?

The annual cyber security event collects representative data about phishing awareness and helps generate powerful insights used by security and risk management leaders to better understand their organization's phishing vulnerabilities. It also serves as the starting point for their respective security awareness journeys and can help establish more concrete goals.

This edition of the Gone Phishing Tournament also benefited from Terranova Security's partnership with Microsoft. The phishing simulation was a collaboration between the two organizations and leveraged Microsoft's real-time intel to ensure the accurate portrayal of a phishing simulation users can encounter in their daily lives.

SO, HOW DOES YOUR CLICK RATE STACK UP?

Summary of Findings

The second edition of the Gone Phishing Tournament took place over 11 days in October 2020. It highlighted the consequences of a lack of phishing awareness.

The 2020 Gone Phishing Tournament revealed that nearly 20% of employees are still quick to click on phishing email links—even if their organization already had either a security awareness or phishing-related training program in place. The results were concerning, considering the Tournament took place during National Cyber Security Awareness Month, where learning and communication activities around phishing and related topics tend to be heightened.

19.8% of all recipients clicked the phishing link

13.4% of the recipients submitted their credentials on the phishing website

Also, most organizations that perform a phishing simulation for the first time observe a 20% to 30% click rate and a 10% to 15% data submission rate in web forms. On average, 50% of clickers submit data on a web form. Most of the Tournament participants already had a phishing simulation program in place and should theoretically not have such high click rates.

Once those individuals clicked, the majority continued down a slippery slope.

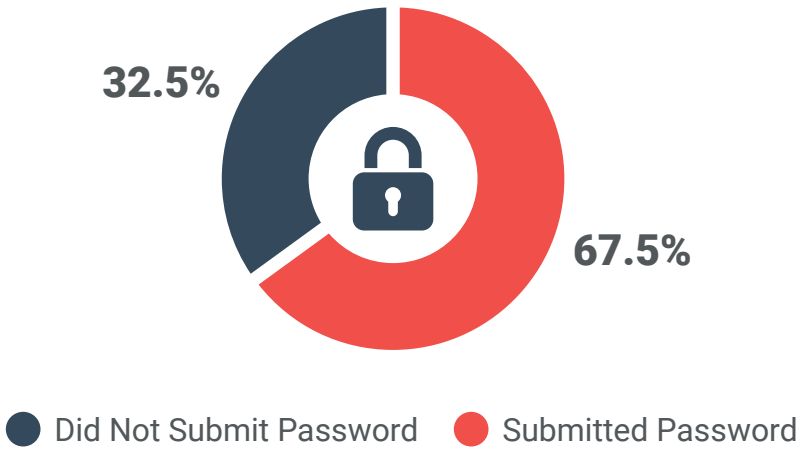
More than 67% (figure 1) of clickers entered their credentials on the simulation's phishing webpage, which means that, overall, 13.4% (figure 2) of the Tournament's participants submitted their password.

These figures are all up substantially from the 2019 Gone Phishing Tournament, where only 11% clicked on the phishing email link and just 2% submitted their credentials.

These findings highlight why it is critical to establish, maintain, and optimize an effective security awareness training program and support it with real-world phishing simulations. One informs and strengthens the other, resulting in a much more well-rounded learning experience and a much stronger cyber-secure organizational culture.

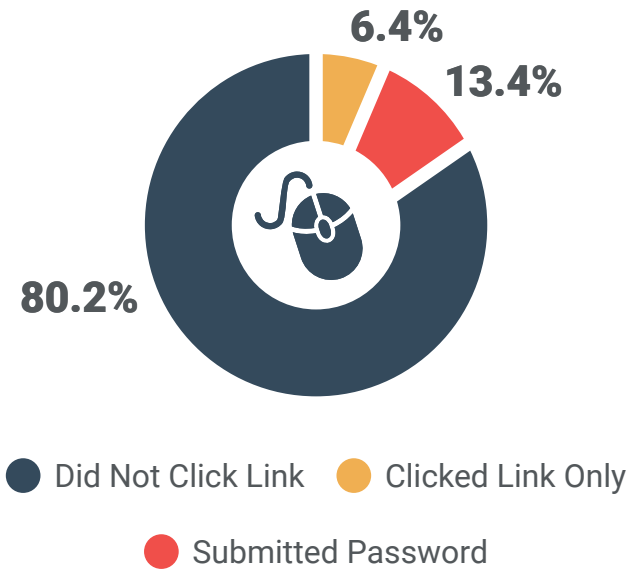
ACTIONS ON PHISHING WEBSITE

Figure 1



ALL USERS ACTIONS

Figure 2



The emergence of more remote and remote-hybrid workforces also underscores the importance of understanding, detecting, and avoiding the most recent phishing threats. Technical infrastructure means less and less as end users adopt a flexible work style that may involve using a personal device to access a business document, cloud storage, server, or email account.

Terranova Security is committed to giving all organizations the knowledge they need to safeguard against the latest, most complex cyber threats. That's why, even if they've never participated in a previous Gone Phishing Tournament, they can access our free phishing simulation. This way, they benefit from seeing how their click rates measure up against others in their industry, of a similar organization size, or in the same geographic region.

How Phishing Attacks Impact All Organizations

A successful phishing scam can bring instant financial harm to any business, as well as their investors and partners. It can also inflict severe long-term reputational harm, which damages any citizens' trust, especially for their local government or health institution.

From SMBs to the largest multinational corporations, universities, hospitals and government agencies, phishing attacks can have a devastating impact on an organization's well-being.

Remote work brings to the forefront several security concerns that may not have been previously addressed. When working remotely, the possibility of data leakage to unauthorized individuals increases, due at least in part to users adopting lax security practices. Another aspect to consider is how quickly organizations have had to deploy a remote workforce, which puts best practice communication under a more intense microscope.

Phishing continued to be a concern for many, as it is the number one attack targeting users. Remaining operational and productive, with minimal disruption and overhead, was the priority as organizations did not have the time or money to properly educate a remote workforce.

Many consumers, investors, third-party vendors, and so on want to avoid associating with any organization that has been a victim of a phishing attack. In a world where data is more valued than ever, failure to protect confidential information can permanently taint an organization's public image, especially if it fails to shore up its security awareness training initiatives.

In their 2019 Internet Crime Report, the FBI's Internet Crime Complaint Center (IC3) received nearly 1,300 phishing-related complaints every day and reported billions of dollars in losses for both individual and business victims. According to IC3, CEO fraud (a type of phishing) alone is worth $26 billion total so far.

The impacts of a successful phishing attack are far-reaching, particularly with workforces becoming more distributed. Cyber security best practices around how you access, share, store, and modify all data types become more complex. Add increased personal device usage to that mix, and you have an infinite number of opportunities cyber criminals can pounce on.

Importance of Phishing Simulations

The radical changes brought on by the coronavirus pandemic has fundamentally changed the way businesses are approaching cyber security. As more and more people work outside the safe digital confines of offices, the need to focus on the human element of data protection is more important than ever before.

When organizations put people first in their information security processes, it gives everyone the knowledge, tools, confidence, and support needed to avoid the latest phishing threats. Unfortunately, the click rates and credential sharing numbers from this year's Tournament show many organizations are still lagging in this area.

Regardless of how airtight any technical barriers may seem, it's an organization's end users who provide the most important line of defense against cyber threats. So, when you expose employees to real-world learning scenarios via phishing simulations, they are tested in a safe environment, and you empower them to make correct decisions in real-life down the line.

Since it only takes one misstep to open one or several doors for cyber criminals to gain access to sensitive individual or organizational information, consistent vigilance is crucial. To successfully detect and avoid phishing threats, user vigilance must be supported and empowered by up-to-date, dynamic phishing simulations.

Leveraging phishing simulations in security awareness training initiatives allows organizations to:

1. Reduce risk levels by a considerable margin
2. Increase organizational awareness of the latest scams
3. Minimize the costs associated with being victimized by a phishing attack
4. Accurately measure individual and organizational vulnerability levels
5. Lessen the automatic trust response by changing user behavior
6. Provide employees with targeted feedback and just-in-time training
7. Improve user reporting and responses to phishing attempts
8. Assign specific role-based phishing training for enhanced relevancy
9. Protect confidential data, both personal and organizational
10. Create a cyber-secure culture made up of cyber heroes

On their own, firewalls, software updates, patches, and security software are not sufficient phishing protection in a world full of phishing scams. If you do not address the human risk element in the equation, you will never arrive at a cyber-secure culture.

The Gone Phishing Tournament Methodology

Each year, the Tournament is open to all security leaders. Participating organizations from the 2020 event included both existing Terranova Security customers and parties who had no prior relationship with the security awareness training leader.

The goal of this yearly global phishing simulation is to measure and evaluate employee detection rates for realistic phishing threats they may encounter in their everyday lives.

However, unlike other yearly security awareness training benchmarking reports, the Gone Phishing Tournament results represent data that offers a more accurate performance comparison for all participants.

Instead of gauging performance across a wide variety of phishing scenarios, each introducing its own contextual variables to the mix, the Gone Phishing Tournament leverages the same phishing simulation for the event's duration.

This consistency means that click rates and credential input data are strictly apples-to-apples. Every user sees the same email and phishing webpage, during the same timeframe, and in their native language.

This section of the report offers a detailed breakdown of the 2020 Gone Phishing Tournament's methodology, information on the simulation itself, and an overview of both the participants and the global event strategy.

About the simulation template

This year's email and web page templates were supplied by Microsoft and reflected a real-world scenario that any user, especially those working remotely, may encounter. The scenario included in the template was selected by the Terranova Security leadership team. It measured several end user phishing behaviors, including clicking on a suspicious email link and submitting data —in this case, login credentials —using a webpage form.

The template's difficulty level was also increased when compared to the previous year's simulation. It was rated medium-high for complexity by Terranova Security's in-house experts based on the number of phishing indicators and how difficult it was to spot various warning signs.

The email and webpage were personalized using the recipient's email address, contained no spelling errors and featured an authentic look. All these are tactics that any cyber criminal can apply in their phishing attacks with little sophistication and effort.

This decision was made to give users a real taste of the ever-evolving nature of current phishing threats affecting professionals across all industries.

To ensure maximal accessibility, readability, and responsiveness, the 2020 Tournament template was supported in 12 languages

- English
- Chinese Traditional (ZH-HK)
- French Canada (FR-CA)
- French France (FR-FR)
- German (DE)
- Italian (IT)
- Japanese (JA)
- Korean (KO)
- Portuguese BR (PT)
- Russian (RU)
- Simplified Chinese (ZH-CN)
- Spanish Spain (ES-ES)

An added lure in the 2020 Gone Phishing Tournament was that the initial phishing email appeared to come from a trusted source, originating from noreply@easysharefolder.com.

The subject line was also explicitly designed to align with relatable remote work email exchanges. The subject line read: "Updated Policy for Remote Workers Has Been Shared with you,"

The email urged recipients to open a document that supposedly contained an updated organizational policy for remote workers. Once clicked, the link redirected them to a phishing landing page spoofed to match Microsoft's branding and asked them to enter the password associated with their work email account.

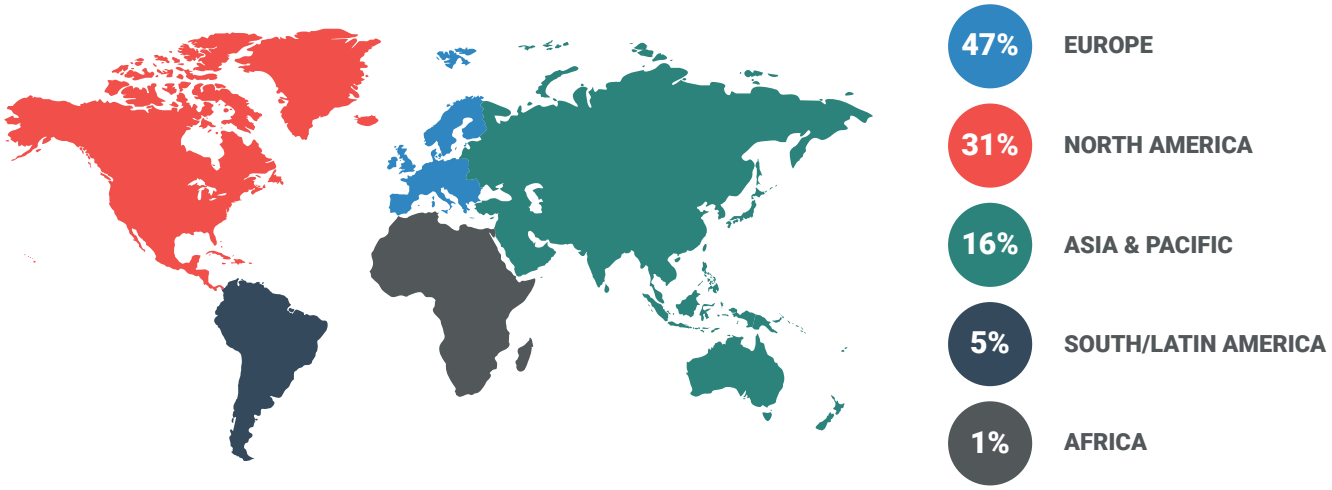
About the participants

The 2020 Gone Phishing Tournament welcomed 57% more participating organizations than the 2019 edition and boasted a 90% increase in participating end users.

The Tournament also benefited from an extended global reach, with users participating in the simulation in 98 different countries (figure 3).

PARTICIPANT REGIONS

Figure 3



Participating organizations came in all sizes and from a wide variety of industries. 28% of organizations who took part in the event were small and midsize businesses (SMBs), consisting of less than 100 employees. 32% were mid-market enterprises, ranging from 100 to 499 employees, while 24% fell in the 500-2999 employee count range. 16% of participating organizations featured 3000 employees or more (figure 4).

SIZE OF ORGANIZATIONS

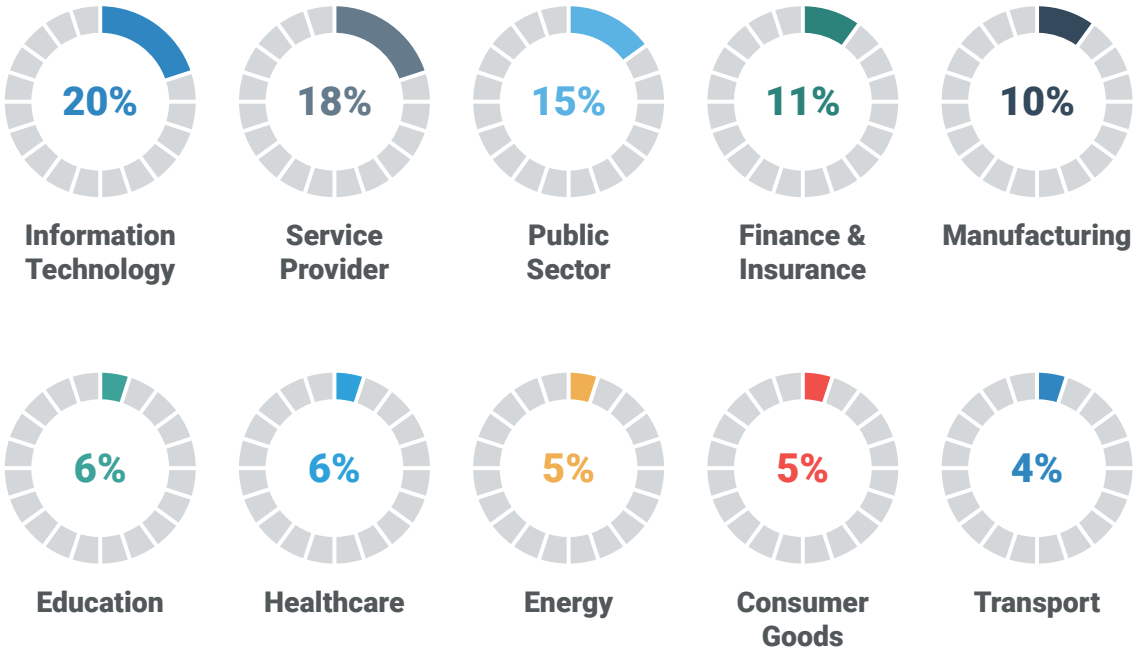
Figure 4

1-99	100-499	500-2999	3000+
28%	**32%**	**24%**	**16%**

Organizations who completed the 2020 Tournament operate in the following sectors (figure 5):

VERTICALS PARTICIPATING

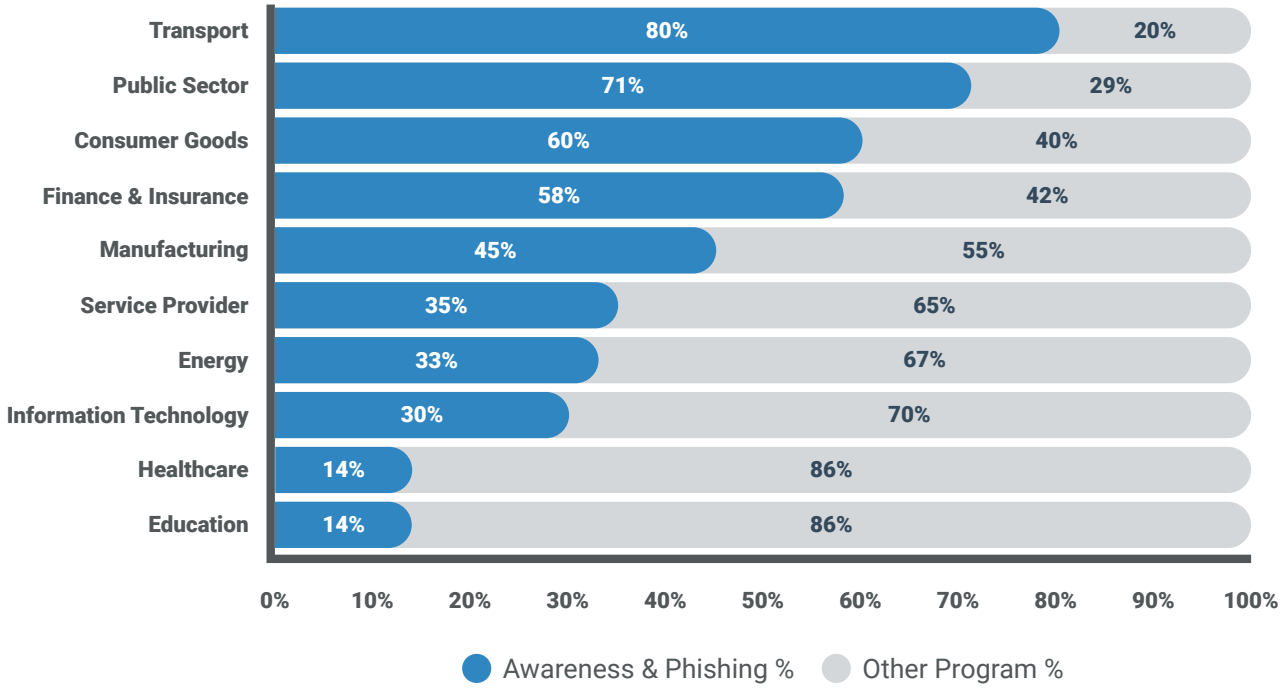
Figure 5



The nature of each organization's existing security awareness program varied considerably by sector. For example, 80% of participating organizations in the Transport category already had a training program that encompassed security awareness educational modules and phishing simulations, which is the ideal combination (figure 6).

PROGRAM TYPE BY VERTICAL

Figure 6

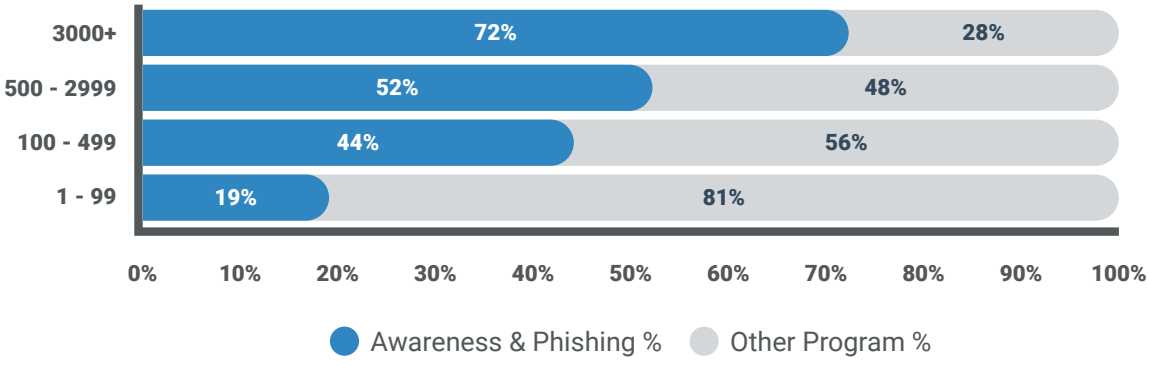


Conversely, sectors like Education and Healthcare lagged farther behind, with only 14% in either category currently deploying both types of initiatives. Surprisingly, only 30% of organizations in the Information Technology category offered that ideal combination to their users.

Existing training programs also became more robust and dynamic as the employee count climbed higher. Only 19% of SMBs said their training program featured both educational security awareness modules and phishing simulations, compared to 72% of organizations with an employee count of at least 3000 (figure 7).

PROGRAM TYPE BY SIZE

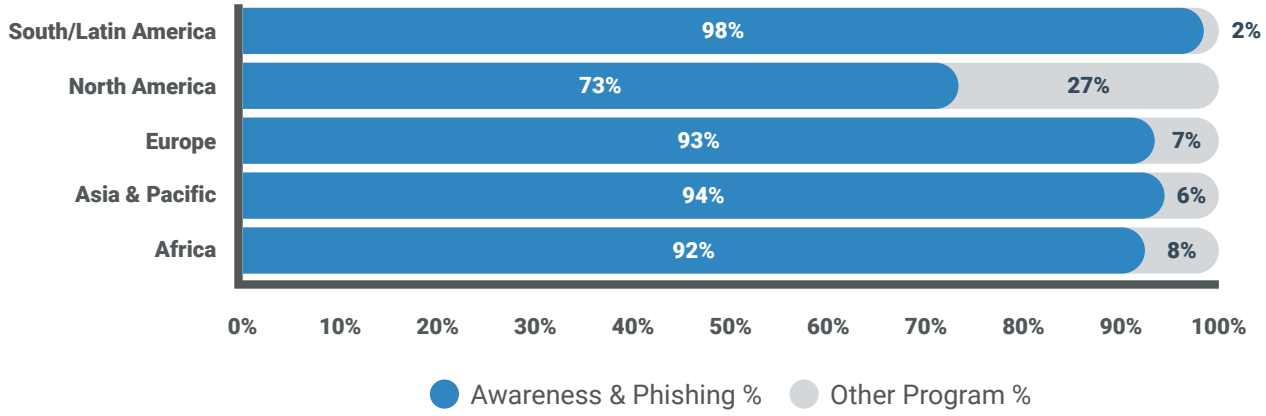
Figure 7



Users of organizations in North America were exposed to awareness and phishing simulation activities at a rate of 73%, a lower rate than organizations in the rest of the world (figure 8).

USER EXPOSURE TO AWARENESS ACTIVITIES

Figure 8



About the strategy

The second edition of the Gone Phishing Tournament took place over 11 consecutive days in October 2020. Throughout the process, Terranova Security adhered to the existing data security controls on its Security Awareness Platform. This distinction meant that no password data was collected if users submitted the form and that, for the duration of the Tournament, the highest level of information security was observed.

If users entered their login information, they were immediately redirected to a phishing simulation feedback page that outlined the warning signs they missed. It also highlighted several essential best practices that should always be observed when faced with a similar phishing attack.

After the simulation was completed, Terranova Security began the data analysis stage. All participant data was anonymized, and, after the analysis was finalized, the data used during that process was deleted, ensuring end-to-end data privacy and security for participating users.

Overall, the Gone Phishing Tournament's success hinges on an organization's ability to compare its click rates against organizations with similar characteristics. You need data that gives you true insight into how your performance measures up to your peers, either size-wise or in the same industry, and answers the question at the event's core: How does my click rate stack up?

This underlying principle, combined with the fact that each user is tested against the same phishing simulation, means organizations get a deeper, more accurate understanding of where they stand when keeping their data safe from cyber criminals.

Gone Phishing Tournament Results

Phishing attacks prey on a person's fundamental tendency to trust others and, in general, tend to click links when they appear in an email or text message. However, as this report demonstrates, even the most harmless-looking phishing links are gateways to malicious criminal activity.

Clicking on the phishing link is just the beginning. Fuelled by Microsoft's real-time phishing email intel, the simulation crafted for this Tournament lured users to a phishing webpage, asking them to input their password. Once obtained, cyber criminals can use those credentials to access confidential data and commit fraudulent acts under the guise of someone else's account.

The increased level of difficulty for this year's template, combined with the human trust element, led to a higher click rate than the 2019 Tournament. Since only one template was sent to all participants, this combination of tactics has a universal effect on users and consistently leads to compromised data.

The 2020 Phishing Benchmark Global Report examines overall results and trends before breaking down the event's data by industry, organization size, and region.

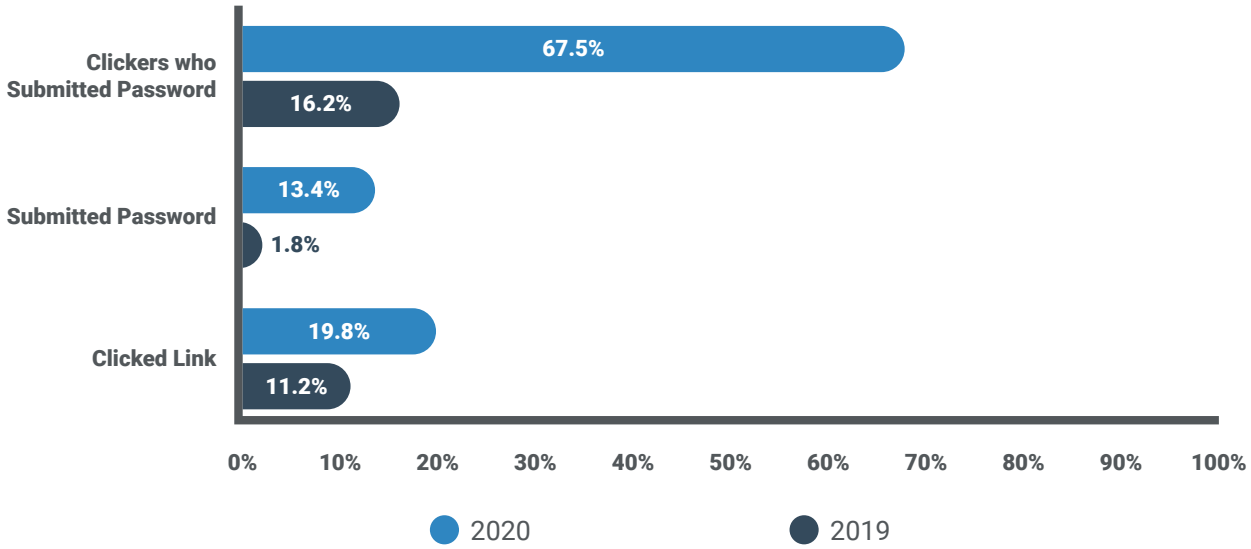
Overall Results

Compared to the 2019 Gone Phishing Tournament, users who participated in the 2020 edition were more apt to click on the link in the simulation's phishing email. As a result, the number of users who submitted their login credentials in the phishing webpage form increased significantly.

Out of all the users who participated in the 2020 Gone Phishing Tournament, 19.8% clicked on the phishing email link, up nearly nine percentage points from the 2019 Tournament. 13.4% of users also submitted sensitive information in the webpage form, up more than 11 percentage points from the previous year's results (figure 9).

COMPARISON BETWEEN 2019 AND 2020

Figure 9



However, perhaps the most concerning trend was the number of clickers who ended up completing the form—a staggering 67.5%. As stated earlier in the report, Terranova Security's security awareness experts cite a 50% click-to-form-completion ratio as a more typical average during phishing simulations.

For added context, consider how these numbers play out in an organization with 1000 employees. Based on these overall results, had this phishing simulation been an actual attack, nearly 200 employees would've clicked on the phishing email link and 134 of those individuals would've had their login information compromised, all during a single phishing incident.

Data Breakdown by Industry: Which Sector Fared the Best?

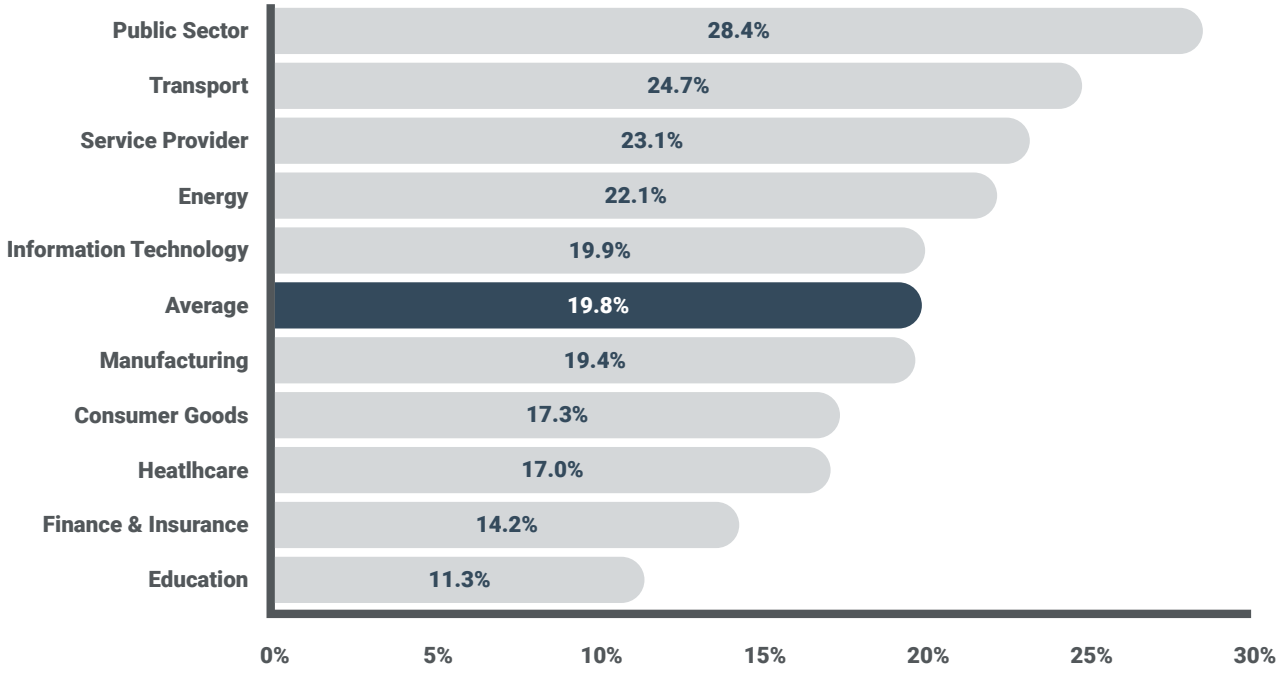
Analyzing the 2020 Gone Phishing Tournament results by industry revealed various challenges that affect organizations in different ways. Since no two sectors are the same, nor are they operating with the same information security standards, an organization must compare their click rates and credential submission rate against similar players.

As illustrated in the graphs below, five industries posted above-average phishing email click rates (figure 10):

- Public Sector
- Transport
- Service Provider
- Energy
- Information Technology

CLICKED LINK BY INDUSTRY (%)

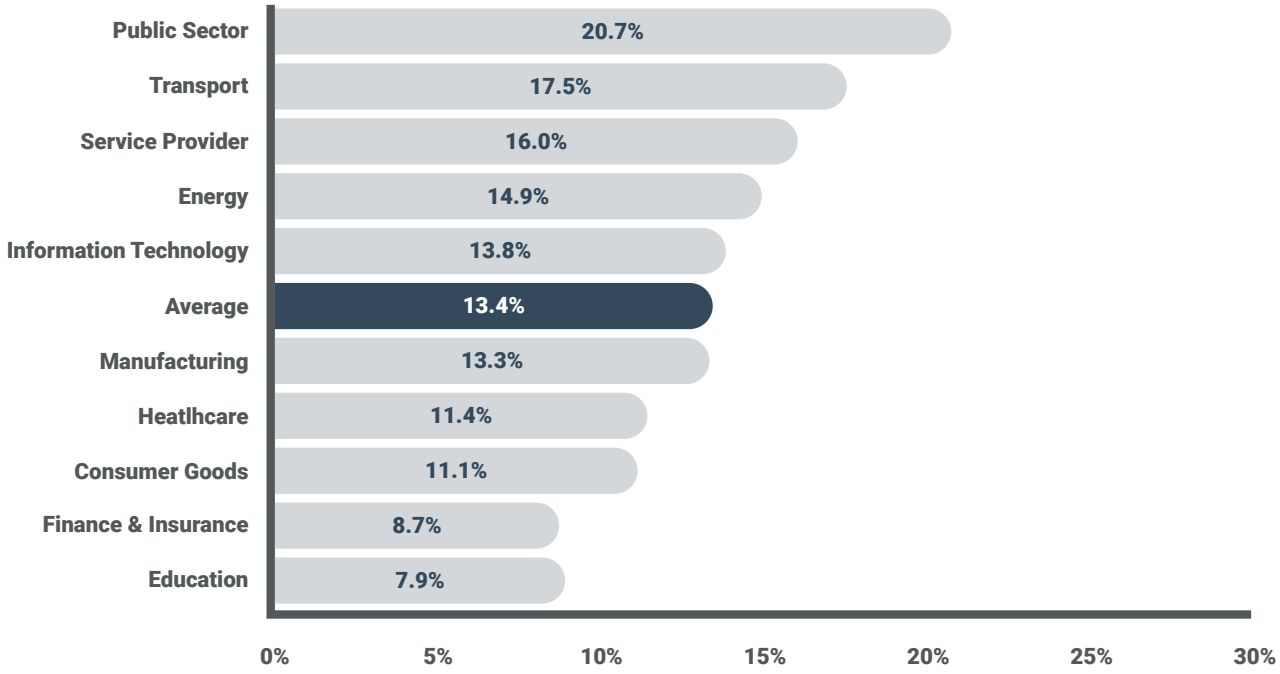
Figure 10



Those five industries also saw form completion rates higher than the Tournament average (figure 11).

SUBMITTED PASSWORD BY INDUSTRY (%)

Figure 11



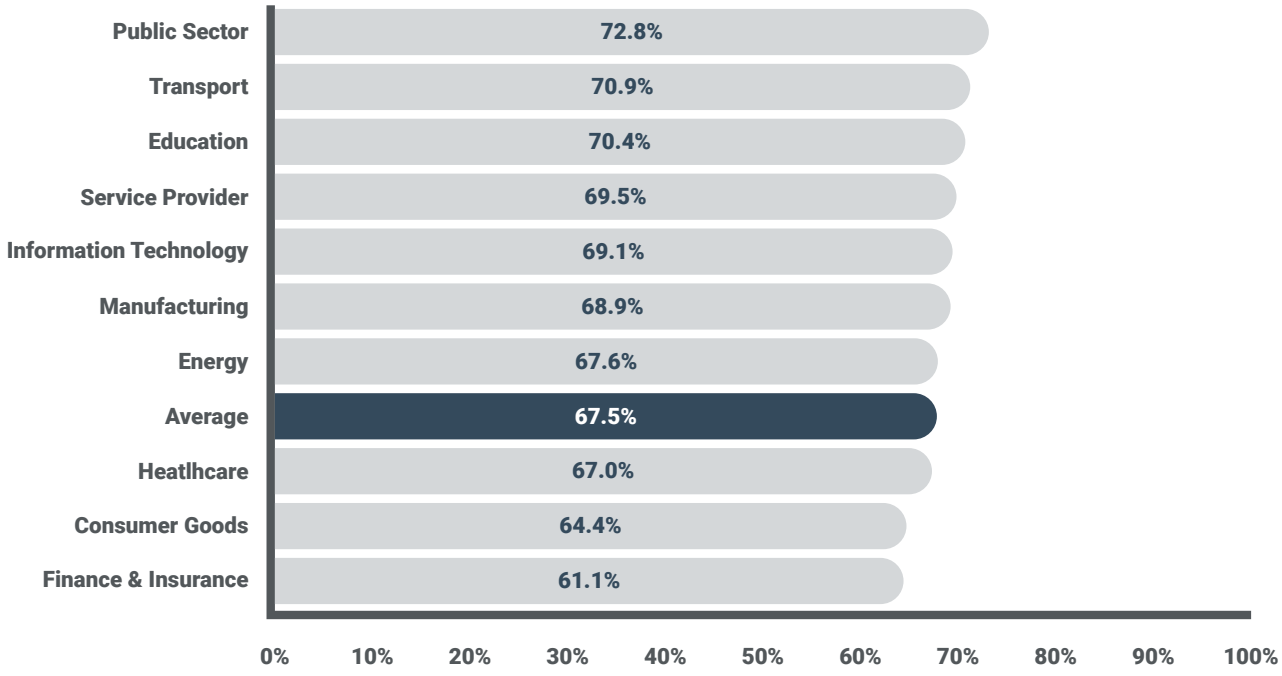
Meanwhile, only two industries posted a click rate lower than 15%: Finance & Insurance and Education. The same two sectors also performed better than other organizations in terms of credential submission, scoring well below the Tournament average at 8.7% and 7.9%, respectively.

Data specifying which industries have the highest number of clickers who also compromised their login credentials provides a fascinating cross-section of modern security awareness training.

Three industry categories—Public Sector, Transport, and Education—all post click-to-submission ratios over 70% (figure 12). Roughly, this distinction means that at least seven out of every ten users who clicked on the phishing email link also ended up compromising sensitive data. The Service Provider, Information Technology, and Manufacturing industries weren't far behind, posting a click-to-submission ratio of 68.9% or higher.

CLICKERS WHO SUBMITTED PASSWORD BY INDUSTRY (%)

Figure 12



As for the best performers in this category, Finance & Insurance came out with the lowest ratio at 61.1%, followed by Consumer Goods at 64.4%. However, those performance ratios still represent a click-to-submission ratio of at least six out of ten people, a figure that isn't likely to impress business leaders and cyber security experts.

The industry breakdown reveals a universal need to ensure that security awareness training programs include phishing simulations that are up to date to reflect the latest threats. In an age of accelerated digital transformation and distributed workforces, employees must identify and safeguard against complex potential attacks like the one reflected in Microsoft's scenario, which reflects a real phishing email.

Otherwise, vast amounts of data may be exposed, affecting organizations' bottom lines across participating industries and beyond.

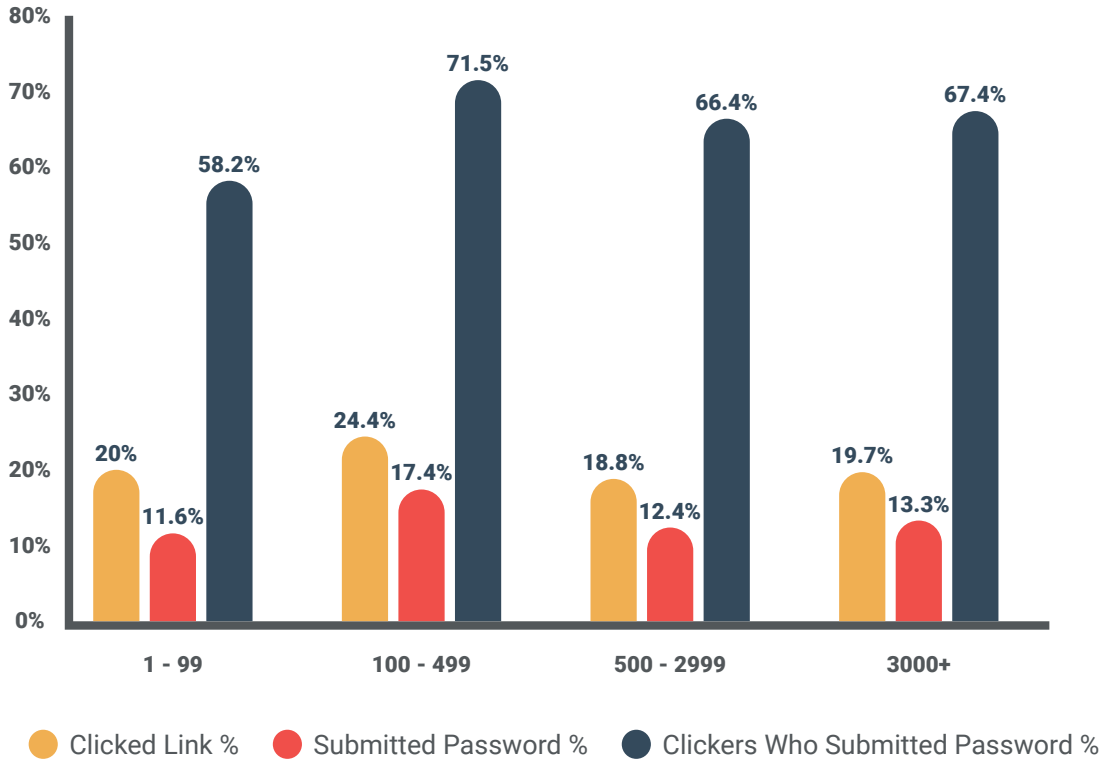
Data Breakdown by Number of Employees: Does Size Matter?

The 2020 Gone Phishing Tournament unearthed a similar truth in response to the age-old question of whether bigger is better. In other words, does the size of an organization (and possibly the resources at its disposal) impact the human aspect of its data protection infrastructure?

If this Tournament's results are any indication, the short answer is not really (figure 13), as the phishing simulation used had a similarly significant impact across all organization size ranges.

RESULTS BY ORGANIZATION SIZE (%)

Figure 13



As seen in the above graphic, SMBs fared the best across all industries. Organizations in this size range posted a 20% click rate (the second-best rate overall), an 11.6% credential submission rate, and a 58.2% click-to-submission ratio. While these numbers aren't stellar, they tell a more optimistic story than those posted by larger organizations.

Out of the remaining three size categories, organizations with an employee count between 500 and 2999 performed the best, with the best click rate of 18.8% and a credential submission rate of 12.4%. However, with a click-to-submission ratio of over 66%, the credential submission rate would've been far more damaging had the simulation been an actual phishing attack.

Breaking down the tournament data by the number of employees underscores the importance of implementing a security awareness training program supported by real-world phishing simulations. Regardless of size, an organization will still suffer relatively devastating consequences if a significant number of its employees have their passwords compromised.

While Terranova Security can't speak to the unique realities of every participating organization, some logical inferences can be made:

- Smaller organizations may not have a dedicated IT department or the internal resources to dedicate the appropriate time and energy to planning and executing a full-fledged security awareness training program with phishing simulations.
- Larger organizations, while possibly better positioned when it comes to staff and other resources, may lack the communication needed across all business units to obtain universal training program buy-in.
- The rising popularity of remote workforces almost certainly means that employees will be interacting and sharing information with external contributors, vendors, and partners more frequently. This reality only makes effective phishing training more critical because of the increased variables that are not within its control.

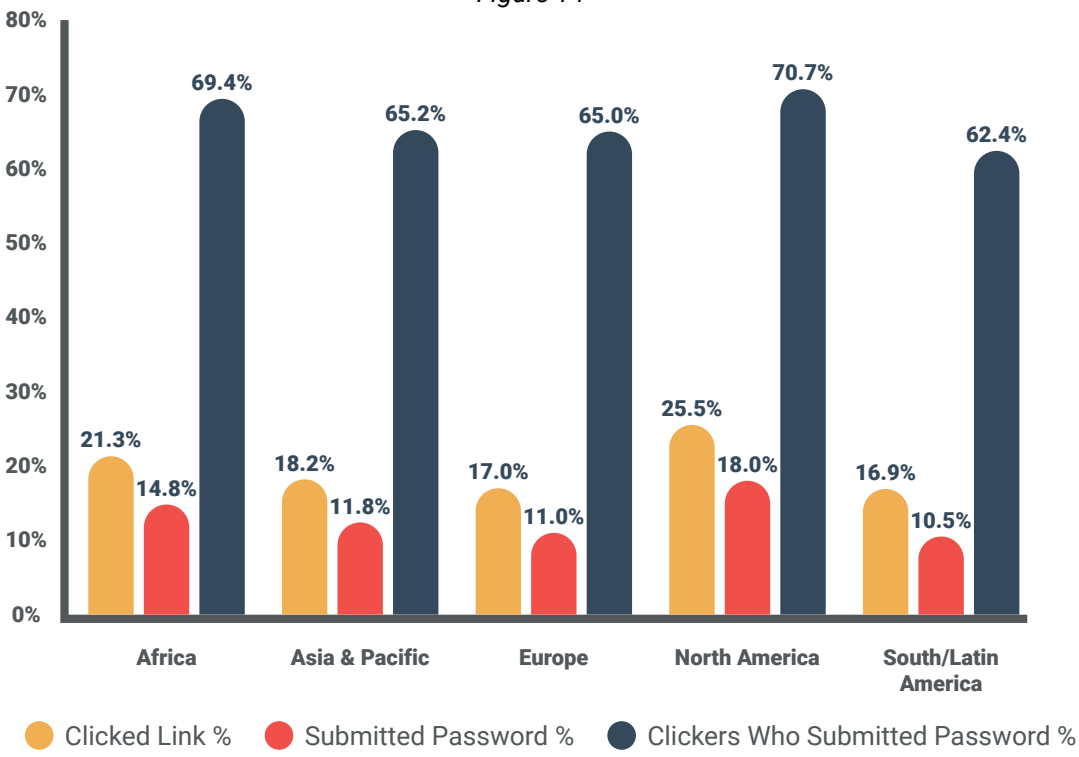
Data Breakdown by Region: Does a User's Location Matter?

The rise in remote work or remote-hybrid workforces has dramatically affected the average organization's cyber security infrastructure. With employees and their work-sanctioned devices no longer chained to an office environment, those organizations and their IT personnel cannot rely on software and VPNs alone to protect their confidential data.

This new reality has only made the need for up-to-date universal phishing training more urgent for 2021 and beyond. The pressing nature of this knowledge gap was reflected in sharp detail in Terranova Security's region-specific Gone Phishing Tournament results (figure 14).

RESULTS BY REGION (%)

Figure 14



North America finished in last place out of five participating regions. More than a quarter of participating users from this region clicked on the phishing email link, and nearly 20% submitted credentials via the web form. These data points translate into roughly 7 out of every 10 clickers exposing sensitive login data.

Conversely, users based in Europe exhibited stronger results, with a 17% click rate and 11% submission rate. Users based in South and Latin America posted the best simulation numbers overall, with rates of 16.9% and 10.5%, respectively.

The high click and submission rates of the phishing simulation Terranova Security designed in collaboration with Microsoft can be attributed to its ripped-from-the-headlines nature of the content as much as its complexity. Appealing directly to remote-based work policies, the scenario preyed on the anxiety and responsibility many professionals may be balancing during their organization's digital transformation.

Phishing threats are always evolving to include fresh ways of enticing or pressuring users into acting, whether that's clicking on a link or downloading a malicious file. As a global leader in both business and information technology, North American organizations in particular must improve these results if they hope to avoid repercussions from targeted cyber attacks down the road.

To successfully safeguard their data from cyber criminals, organizations must also evolve their security awareness training efforts to include data on the latest scams and news items hackers may be leveraging. If those measures aren't taken seriously, it may impact their consumer-facing reputation regarding data processing, privacy, and security.

How to Make Phishing Simulation Training a Priority

Phishing simulations add an extra dimension to the average security awareness training program. Informative, interactive, real-world phishing simulations (as well as just-in-time training content) can educate users on the tactics employed by phishing attacks quickly and effectively.

By offering diverse, inclusive learning opportunities to its employee base, any organization can instantly strengthen its data protection processes in ways that purely technical cyber security tools, like antivirus software or other encryption apps, cannot match.

The Importance of Targeted, Risk-Based Phishing Training Campaigns

When designing a security awareness program, it's essential to establish a framework that creates a defined, effective learning path for the user. To achieve that, Terranova Security has identified the seven behaviors related to the threats every organization must address to strengthen its data protection:

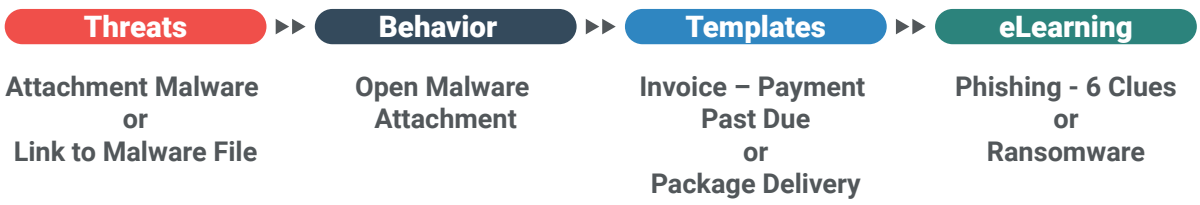
THREATS

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

BEHAVIORS

- Open Malware Attachment
- Clicking on 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

Risk-based Training Example



This illustration depicts the link between the threat, which, in this case, is a malware attachment or link, to the user behavior which may compromise data. Depending on the type of behavior you want to address, you must choose learning modules and real-world phishing simulations that mirror those threats and allow you to accurately measure behavior change.

When launching a security awareness training campaign, Terranova Security recommends using communication tools to encourage participation across all business units. Then, start with a general phishing module that establishes baseline knowledge across an organization.

This is followed by a monthly microlearning module that educates users on a specific risk related to the targeted behavior. After that, the next step is a phishing simulation directly related to the microlearning topic.

To get actionable, data-driven insights on user progress, organizations carry out an average of 4–6 simulations per year, with at least four awareness activities on the phishing threat. Terranova Security recommends targeting a 5% improvement of the overall average click rate after completing 4–6 simulations and continuous awareness initiatives over 12 months.

As scenarios vary in terms of complexity and story, the likelihood of someone clicking will also vary. Your average click rate is the average rate of all simulations completed in a given timeframe, not just the last one. Therefore, it is imperative to train users on detecting a phishing attack from the first step: the phishing email.

7 Easy Steps to Powerful Phishing Simulation Training

Taking a proactive, data-based approach to security awareness training using real-world phishing scenarios doesn't have to be a struggle. To educate users and change key behaviors that lead to data exposure, follow these simple guidelines:

1. **Target the right user behaviors** by delving into your existing cyber security data and pinpointing patterns or specific actions that have led to data breaches
2. **Create phishing simulations** that address those weaknesses and leverage up-to-date scenarios that users may encounter in their daily lives
3. **Collect real-time phishing simulation data** to facilitate the assessment, maintenance, and refinement of your security awareness initiatives
4. **Track and monitor user progress** to determine user knowledge levels and the overall effectiveness of your security awareness training approach
5. **Deploy just-in-time training modules** to give users the instant feedback they need should they fail a phishing simulation
6. **Utilize customizable simulation templates** that enable your organization to tailor every aspect of the training process to help meet your goals
7. **Choose a scalable, inclusive solution** with multilingual, accessible, mobile responsive training content that makes educating diverse, global user base seamless

Enhance Employee Awareness with Phishing Attack Transparency and Support

Even with the most dynamic security awareness training program available, your organization may still fall victim to a successful phishing attack. If an incident occurs, your employees need transparent communication and assurances that the appropriate policies and next steps are in place to prevent a future attack.

To enhance employee phishing awareness through these practices, you must:

- Explain how the phish happened, including the red flags that identify it as a phishing email or another cyber threat.
- Use communication tools like videos, infographics, newsletters, and other shareable content to raise additional phishing awareness and encourage participation in educational initiatives.
- Create an internal cyber hero ambassador group that can support employees when they're suspicious of an unexpected message or download request.
- Continually engage employees on the prevalence of phishing through diverse, interactive communication and learning tools.
- Emphasize the importance of employee transparency in the event of a successful phishing attack, including how their immediate communication with their manager(s) or their IT department, according to the organization's existing policy, can help their team recover quickly.

Next Steps to Ensure Security Awareness Training Success

With remote work and accelerated digital transformation changing the business landscape as we know it, security awareness training and phishing simulations must be a real priority for all organizations.

Holding a one-time lunch-and-learn on phishing threats or doling out intermittent bits of security awareness training is no longer useful. Cyber criminals change their schemes too often to hold the notion that infrequent training initiatives can keep data safe.

Organizations serious about strengthening their phishing defenses must prioritize educating their employees by giving them consistent access to high-quality security awareness content and phishing simulations that are engaging, informative, and fun to navigate.

Organizations must also acknowledge their weak points and take advantage of communication tools such as videos, infographics, email newsletters, and other customizable campaigns to enhance their security awareness efforts and boost organizational buy-in across all business units.

Terranova Security recommends that organizations leverage all opportunities to collect data about employee awareness, click rates, and industry standards. Having this information on-hand allows them to take proactive steps and create real behavior change that puts an end to the automatic trust, click, and response in the wake of an imminent phishing threat.

Above all else, it's crucial to ensure that any security awareness training initiatives and phishing simulations continuously evolve to include learning material about the latest active phishing threats. Only then can an organization's employee base detect and safeguard against phishing attacks with consistency and confidence.

Your Global Security Awareness Training Partner of Choice

Terranova Security is always offering cyber security leaders and end users alike new, industry-leading content that helps employees gain knowledge on key information security topics. If you're looking for the right place to start your security awareness journey, look no further than the Cyber Security Hub!

This free content repository gives all interested parties access to fun, engaging, instantly shareable assets like infographics, comics, videos, in-depth guides, and much more. Plus, Terranova Security's experts are continually updating the Hub so that you can check back regularly for all the latest content editions.

Get started now!

The Cyber Security Hub

Sign up now to access engaging, shareable cyber security awareness content that's available in multiple formats.

ACCESS THE HUB

For more information on the Terranova Security training solution and how it's helping empower tens of millions of users worldwide with high-quality content and robust phishing simulations, visit TerranovaSecurity.com.

About Terranova Security

Founded in 2001, Terranova Security was born out of CEO Lise Lapointe's passion for education, training, and technology. This passion would intersect with the growing need for cyber security awareness and training to help organizations worldwide protect their data and well-being against an ever-increasing number of cyber threats.

In 2003, Terranova Security went to market with its first security awareness solution and, over two decades, has grown into a force to be reckoned with. Today, Terranova Security is a recognized global partner of choice in security awareness and has been recognized in publications like the 2020 Gartner Market Guide for being a representative vendor in Security Awareness Computer-Based Training.

Terranova Security works with organizations to help change behavior and reduce risk by effectively combining education and technology. Education helps individuals actively participate in ongoing professional and societal developments, and technology facilitates a much more meaningful, long-lasting, and fun learning environment. Terranova Security was also named 2020 Information Technology Educator of the Year GOLD WINNER - IT World Awards.

International corporations like Microsoft have partnered with Terranova Security to drive long-term behavioral changes based on targeted, real-world training programs that leverage the industry's highest-quality content. Terranova Security is also working with Microsoft's phishing email data to ensure that users benefit from the most up-to-date training material.

Terranova Security's security awareness solution brings a host of benefits to all customers and partners, including multilingual support for its Security Awareness Platform, intuitive phishing simulations, engaging and shareable communication tools. It also offers an innovative, advisory approach to Managed and Customization Services to ensure that every security awareness initiative conforms to an organization's needs and goals.

Notes

Notes

GONE PHISHING TOURNAMENT™

Co-sponsored by

TERRANOVA SECURITY

Microsoft