TERRANOVA SECURITY

Co-sponsored by

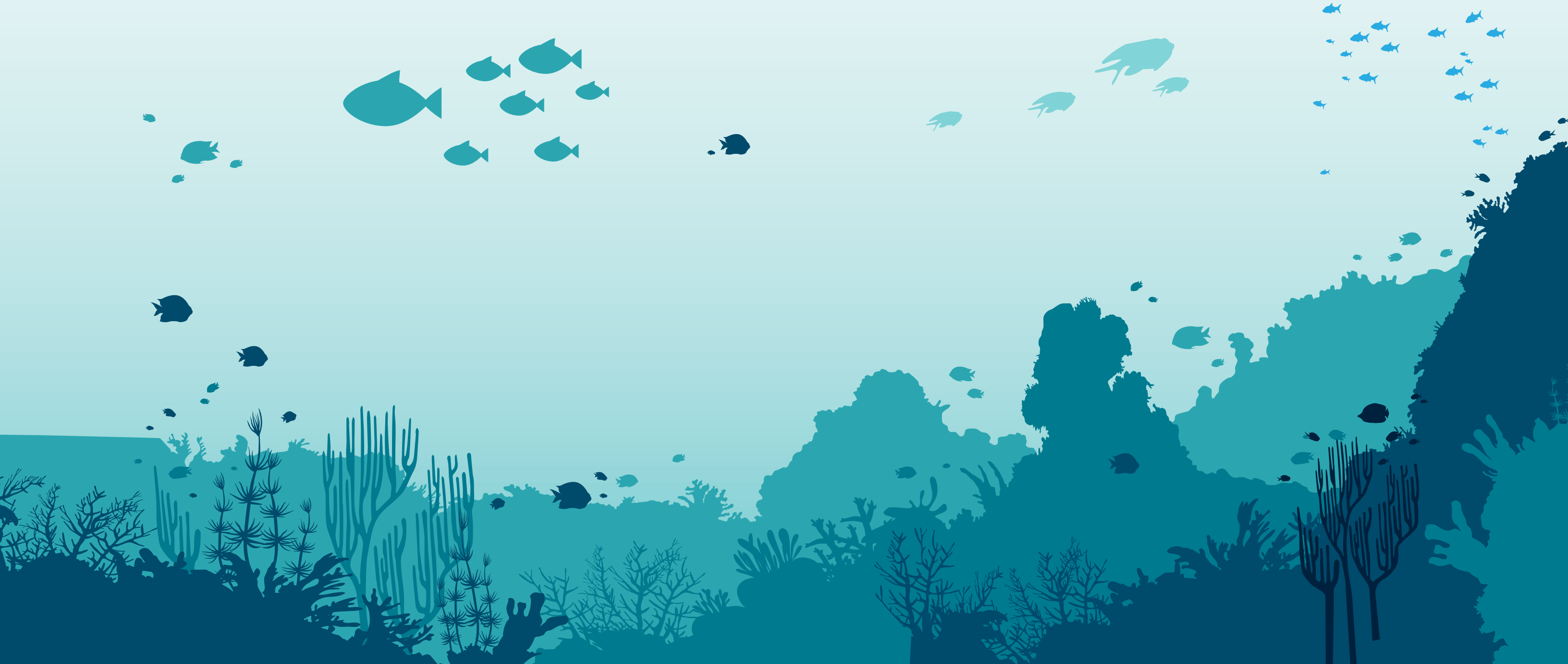
Microsoft

GONE PHISHING TOURNAMENT™

Phishing Benchmark

Global Report

2021



As accelerated digital transformation continues to reshape how organizations around the world collaborate and complete everyday tasks, ensuring the safety of sensitive information has only grown in importance. Threats like phishing, malware, and ransomware have become more ubiquitous in the last year, putting the human element of cyber security under greater strain.

As a result, ensuring that all employees can consistently detect and avoid different cyber threats has never been a more crucial component of strong confidential data protection.

For organizations who want to understand how their security awareness training efforts compare to those of their peers, the Gone Phishing Tournament Benchmark Report is an essential starting point. By providing security and risk management leaders with insights from the 2021 edition of this event, this report can help any organization strengthen its information security efforts in the years to come.

Microsoft was proud to co-sponsor the 2021 Gone Phishing Tournament and work with the Terranova Security leadership team on the phishing template used during the event. The goal was to deliver a phishing scenario relevant to end users' everyday lives while also drawing from real-time Microsoft phishing email data to ensure the highest security awareness training quality.

Microsoft is thankful to count on Terranova Security as our global security awareness partner of choice. Together, we're committed to bringing the industry's best phishing simulation training to customers worldwide, enabling them to grow their awareness initiatives effectively.

By leveraging this report to prioritize the human element in cyber security, your organization is taking important steps to safeguard your most sensitive information against increasingly complex cyber attacks.

BRANDON KOELLER

Principal Program Manager Lead - Office 365 Security

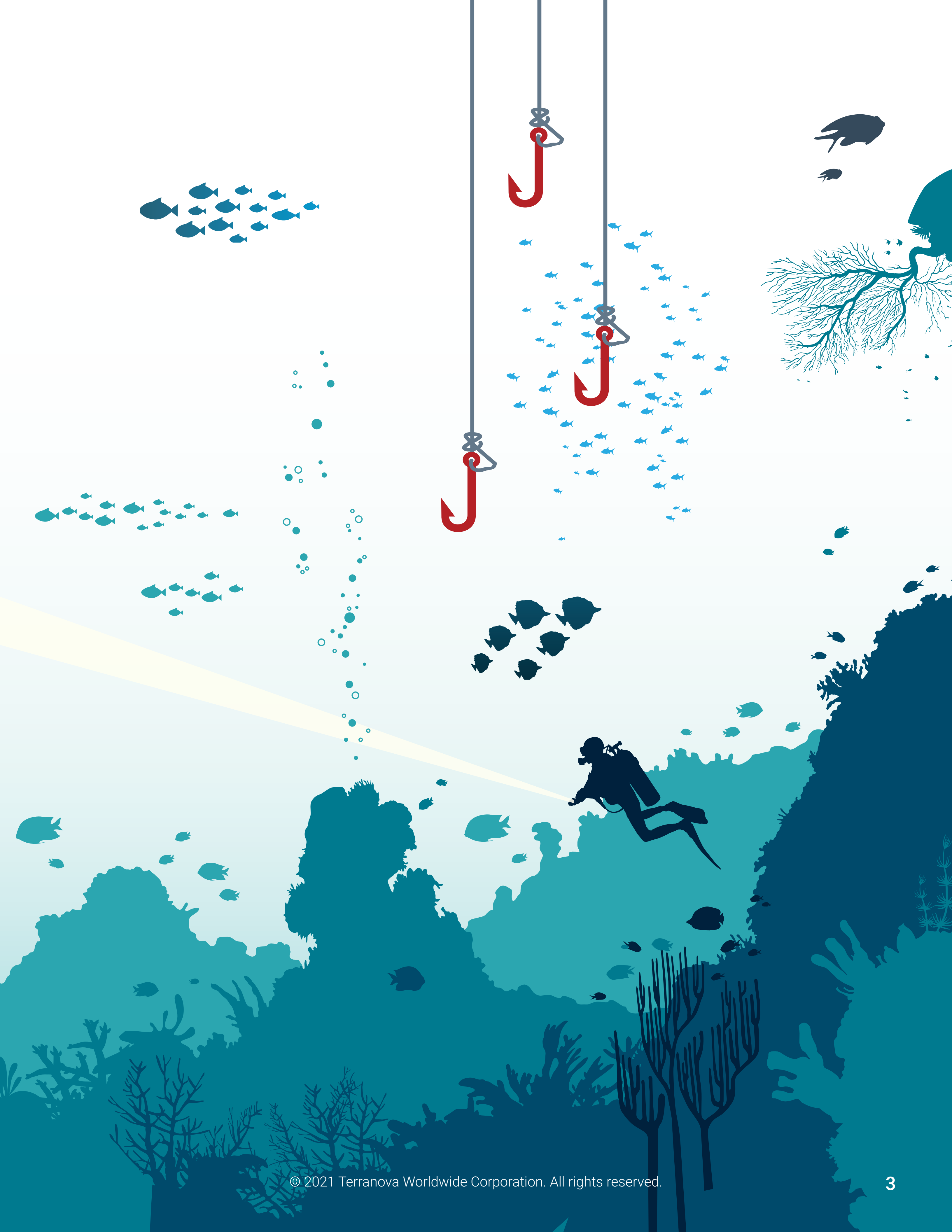


TABLE OF CONTENTS

Ransomware and Malware: Opening the Floodgates

2021 was a year marked by continued digital transformation by organizations worldwide across all industries. The widespread adoption of remote-only or hybrid workplace cultures and technologies that ease collaboration and enhance productivity was a priority for everyone.

However, these positive changes were counterbalanced by organization-wide cyber security awareness levels being tested far more frequently. Data published by the Identity Theft Resource Center (ITRC) revealed that 2021 was a record-setting year for cyber attacks. This reality is especially true of ransomware and malware attacks, which exploded in terms of prevalence and severity.

As per the U.S. Treasury's Financial Crimes Enforcement Network, the average monthly suspicious amount of ransomware transactions totaled over $66 million in 2021. That's roughly $2.2 million per day. Additionally, the total value of reported suspicious activity in the first six months of 2021, $590 million, exceeded the value reported for all of 2020.

These jaw-dropping numbers are only expected to climb in the coming decade, with ransomware-related damage costs alone to exceed $265 billion by 2031. These realities prove, more than ever before, that technological safeguards alone can't prevent ransomware, malware, or any other type of cyber attack from occurring.

To effectively reduce risk and ensure their sensitive information is always protected, organizations must implement and maintain continuous security awareness training that includes real-world phishing simulations for all their employees. If every team member has the knowledge and tools needed to detect and avoid cyber threats, cyber criminals will have a much harder time accessing, exposing, or corrupting confidential data. And, with remote and hybrid workforces firmly established as the new standard, in-depth benchmarking data has never played a more instrumental role in establishing and growing a cyber-aware organizational culture.

What is the Gone Phishing Tournament™?

The Gone Phishing Tournament is a free annual cyber security event that empowers organizations everywhere to strengthen their security awareness training programs with in-depth benchmarking data. The insights generated by this data help security and risk management leaders better understand their organization's phishing vulnerabilities, establish concrete cyber security goals, and maximize their return on investment.

The 2021 edition of the Gone Phishing Tournament once again benefited from the partnership between Terranova Security and Microsoft. The two organizations collaborated on the phishing template used for the phishing simulation, leveraging real-world Microsoft intel to accurately portray the emulated cyber threat.

Summary of Findings

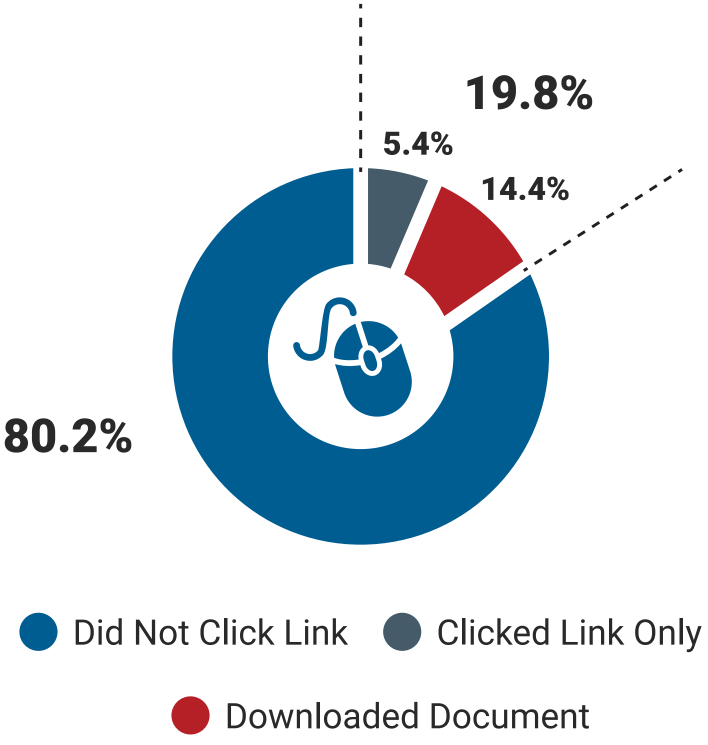
19.8% of all recipients clicked the phishing link

The 2021 Gone Phishing Tournament results revealed that many end users are still prone to clicking on links included in phishing emails and, in the case of this year's template, downloading malicious files.

19.8% of all recipients – or nearly one in every five employees – clicked the simulation message's phishing link. When you consider the Gone Phishing Tournament takes place during Cybersecurity Awareness Month, a time of year when learning opportunities around information security best practices are at their peak, this statistic should raise more than a few eyebrows.

Globally, 14.4% of all recipients failed to recognize the phishing website and clicked the link to download the malicious file, a notable increase from the 2020 event.

ALL USERS ACTIONS

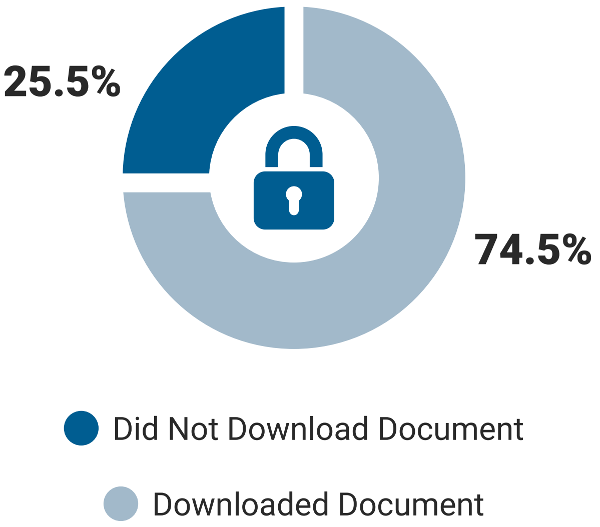


In a real-world scenario, malware would've been installed on the user's device and left their system and sensitive information vulnerable to hackers. Specific to ransomware, the user would've been locked out of their device and unable to access any data until the cyber criminals received payment.

This result means that more than 70% of those who clicked on the phishing link in the initial message also downloaded the malware from the simulation's landing page.

Compared with the previous Gone Phishing Tournament, the number of end users who completed the action on the phishing website increased by nearly three percentage points.

ACTIONS ON PHISHING WEBSITE



These findings underscore why establishing, maintaining, and optimizing an engaging security awareness training program is such an essential part of strong digital asset protection. This year's phishing simulation proves technical infrastructure doesn't guarantee information security from cyber threats. End users must be able to identify potentially malicious messages and act accordingly.

At an organizational level, continuous improvement is a major contributor to sustained cyber threat risk reduction. Repeat clickers must be identified and, over time, receive the support needed to change behaviors that cyber criminals may target. And, since most individuals learn best by doing, this optimization process must include real-world phishing simulations and just-in-time training.

The phishing simulation template also featured a feedback page at the end of the simulation, which gave clickers a rundown of warning signs they missed and best practices they should observe. As a total package, the Gone Phishing Tournament provided an opportunity for participating organizations and their end users to recognize and learn the correct action to take in the face of similar phishing attacks.

How phishing impacts all organizations

Successful phishing attacks can inflict instant financial harm on organizations and their customers, suppliers, investors, and negatively affect the overall brand. In the case of ransomware, repercussions typically involve extended outages, impact on operations and loss of strategic information, and irreparable reputational harm. The latter can severely affect the perception of and trust in any organization.

Phishing threats have only grown in complexity in 2021, thanks to an increased reliance on remote work and corresponding changes in end user habits. As a result, the possibility of accidental data leakage due to unauthorized access to documents or systems, or a lack of overall scrutiny, has increased as well.

In many remote and hybrid work cultures, the clear, consistent communication of cyber security best practices has become crucial for strong data protection strategies. By ensuring employees can detect and avoid phishing attempts, an organization can minimize disruptions to their operations and services, reducing unnecessary costs and maximizing profitability.

The negative impacts can be widespread if an organization doesn't implement a multifaceted security awareness training program that includes phishing simulations as a safe, powerful education tool. Many consumers, investors, third-party vendors, and more may want to avoid associating with any organization that has been a victim of a phishing attack or data breach.

In short, cyber security policies, training opportunities, and the communications strategy around how end users can recognize cyber threats and tactics have never been more critical than they are now. Couple that reality with a growing number of apps and devices being used for productivity every day, and it's clear addressing the human risk factor is the truest way to upscale cyber security practices moving forward.

In their 2020 Internet Crime Report, the FBI's Internet Crime Complaint Center (IC3) received over 241,000 phishing-related complaints, with adjusted losses of over $54 million. Total complaints covering all cyber threats rose by 69% compared to numbers detailed in the 2019 report, with reported losses topping $4.1 billion.

According to the 2021 ENISA Threat Landscape Report, the frequency and complexity of ransomware attacks spiked by more than 150 percentage points in 2020, becoming one of the most dangerous threats organizations face today, regardless of sector.

Importance of phishing simulations in cyber security

The reality is simple: Three billion fraudulent emails are sent out every day as part of phishing schemes aimed at accessing or compromising sensitive information. As unprecedented digital transformation continues to impact many industries worldwide, the need to bolster the human side of cyber security through phishing simulation and awareness training initiatives is top-of-mind for many organizations.

By emphasizing this aspect of its data protection infrastructure, organizations can successfully reduce related risks and minimize the possibility of a data breach. However, these positive outcomes are possible only when the awareness training provided ensures that everyone has the knowledge, tools, confidence, and support to consistently detect and safeguard against the latest phishing threats. As this year's results demonstrate through benchmarking data, many organizations can improve in this area.

Even if the technological barriers an organization uses are among the strongest available, its employees still provide the most crucial line of defense against cyber attacks. Because of this, real-world phishing simulations are a great way to safely test any end users' knowledge (since no sensitive information is compromised in the process) and, over time, empower all team members to make the correct decisions if faced with a similar threat.

To successfully detect and avoid phishing threats, that level of vigilance must be fueled by up-to-date, dynamic phishing simulations. Leveraging this critical training format enables organizations to:

1. Reduce risk levels by a considerable margin
2. Increase organizational awareness of the latest threats
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

Remember

Firewalls, software updates, security patches, and other technology-based safeguards don't offer sufficient protection on their own from phishing and other threats. Cyber criminals have shifted their focus from exploiting technology to the end user. As a result, phishing simulations are indispensable for maximizing your awareness training experience's effectiveness.

Methodology

Each year, the Gone Phishing Tournament is open to all security leaders and their organizations. Those who participated in the 2021 edition of the event included both existing Terranova Security customers and parties who had no prior relationship with the company.

This yearly global phishing simulation aims to measure and evaluate employee behaviors with realistic phishing threats they may encounter in their everyday lives. Unlike other cyber security awareness phishing and benchmarking reports, the corresponding results offer a more accurate, data-driven performance comparison to participating organizations and other readers.

Instead of gauging performance across a wide variety of phishing scenarios, each introducing different 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 related actions are all based on the same simulated phishing threat. Every user sees the same phishing message components, during the same timeframe, and in their native language.

This section of the report offers a detailed breakdown of the 2021 Gone Phishing Tournament methodology, information on the simulation itself, and an overview of the participants and the global event strategy.

About the simulation template

This year's email and webpage templates were supplied by Microsoft and reflected a real-world scenario all end users, particularly those working in a remote or hybrid environment, may encounter in their daily lives. The template's scenario, selected by the Terranova Security leadership team, measured several end user phishing behaviors, including clicking on a link in the body of a phishing email and delivering ransomware in a downloadable file through a phishing webpage.

The template's difficulty level was rated medium-high for complexity by Terranova Security's in-house experts. This rating was based on the number of phishing indicators and how difficult it was to spot various warning signs.

The email and webpage spoofed the Microsoft SharePoint interface for an authentic look and feel. The email message even included instructions on how to download the file, which further enticed the end user to complete the action once they landed on the webpage. These tactics can be leveraged with minimal effort by hackers looking to infect a device with malware.

These decisions were made to give recipients a realistic sample of the increasingly complex nature of current phishing threats affecting professionals across many different industries.

2021 simulation languages

To provide participating organizations with an inclusive, accessible experience, the 2021 Gone Phishing Tournament template was supported in the following languages:

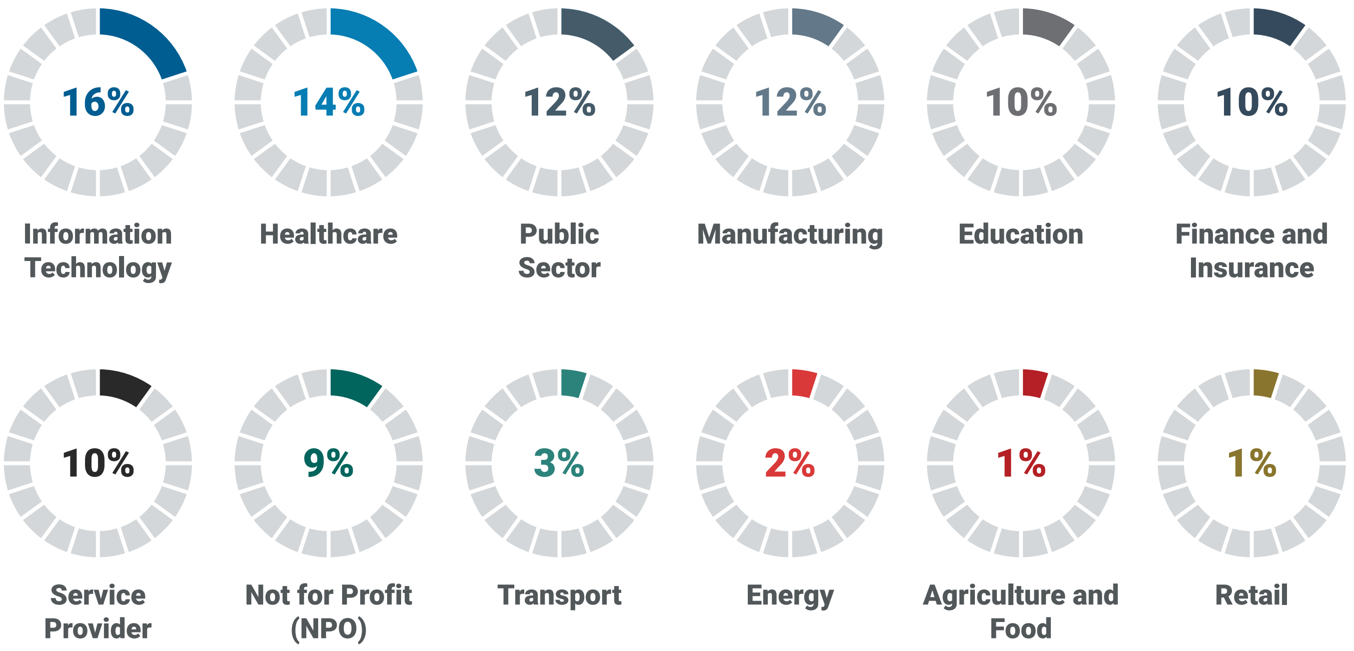
- English
- Chinese (Hong Kong) Cantonese
- Chinese (PRC) Madarin
- French (Canada)
- French (France)
- German
- Greek
- Hungarian
- Hebrew
- Italian
- Japanese
- Korean
- Polish
- Portuguese (Brazil)
- Portuguese (Portugal)
- Spanish (Spain)
- Thai
- Turkish
- Ukrainian
- Vietnamese

2021 participating organizations overview

The 2021 Gone Phishing Tournament saw a significant increase in the participating organizations compared to the 2020 edition. In total, close to 1,000,000 emails were sent to end users over the event's two-week period. Simulation emails were also sent in 20 different languages.

Participating organizations hailed from many different industries:

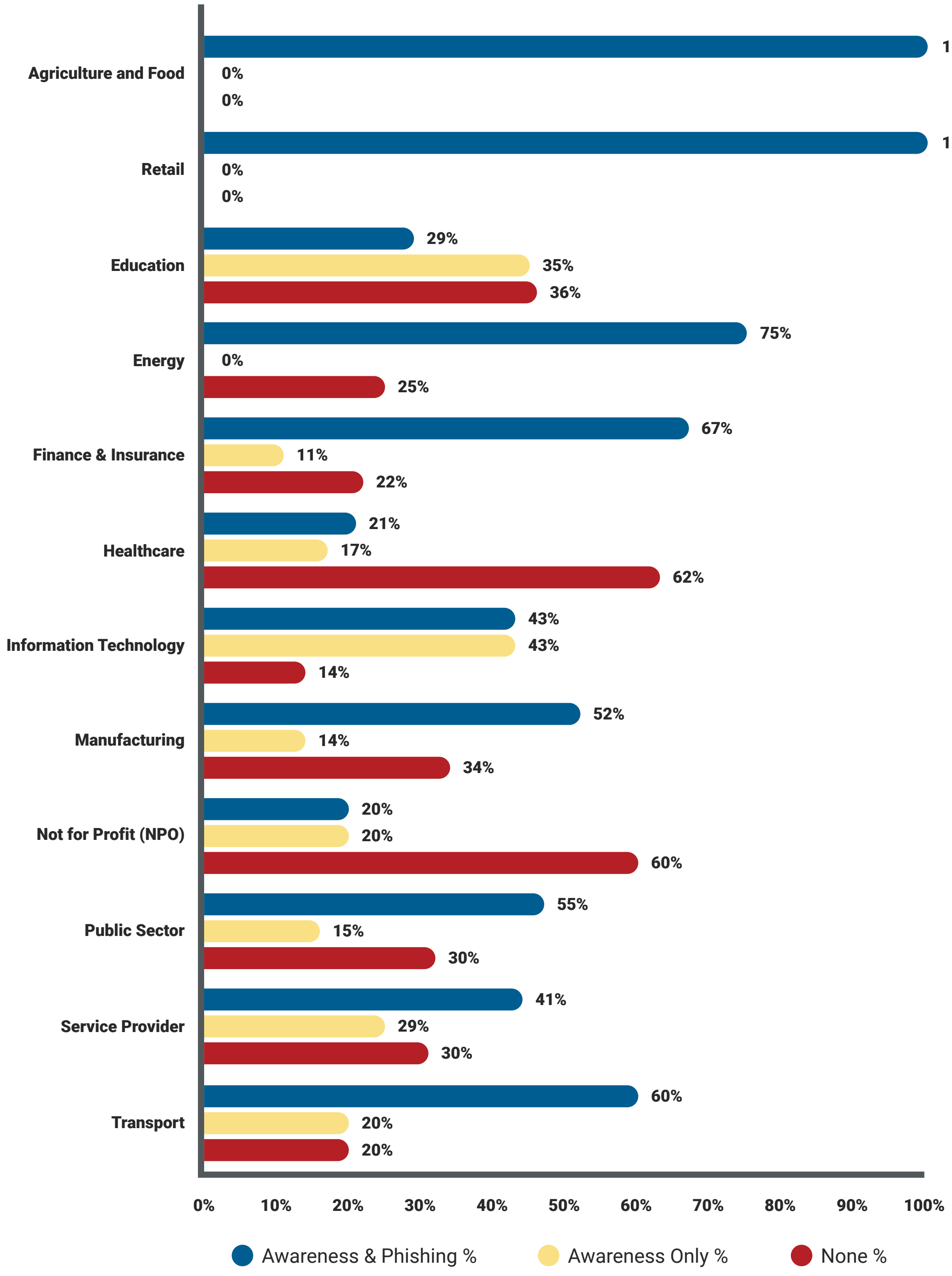
REPRESENTATION BY INDUSTRY



The nature of each organization's existing security awareness training program also varied considerably based on their sector. Consumer Products, Finance and Insurance, and Agriculture and Food led the way in terms of the sectors with the highest number of existing programs that included both security awareness educational modules and phishing simulations, which is the best possible combination.

At the other of the spectrum were the Healthcare, NPO, and Education sectors, with under 30% of organizations in either sector currently deploying both types of awareness initiatives. Overall, 21% of organizations did not deploy phishing simulations as part of their program, and 34% had nothing in place to inform their users.

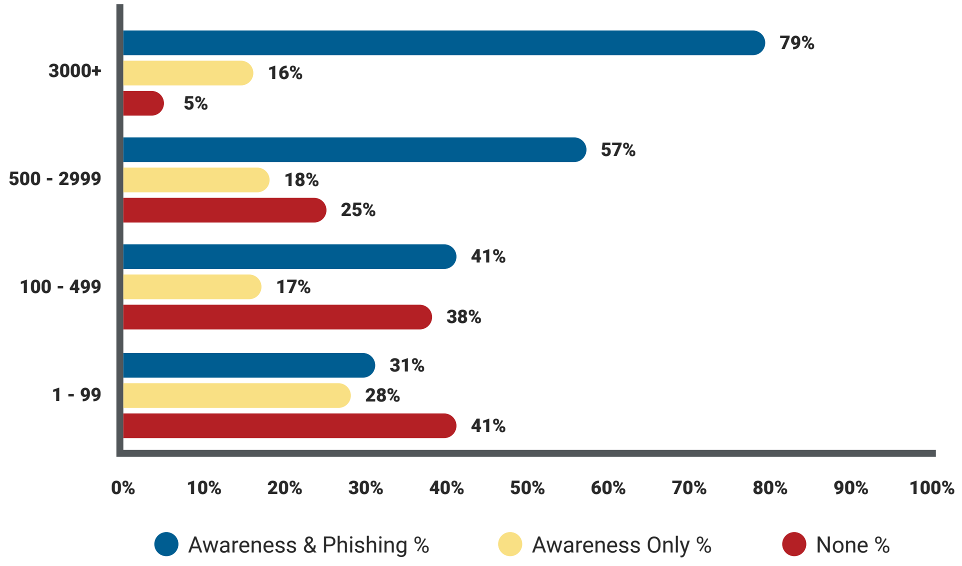
PROGRAM TYPE BY INDUSTRY (%)



Existing security awareness training programs become noticeably more complex, utilizing a diverse collection of content assets and end user initiatives, as the total employee count grew.

31% of participating small businesses said their existing training program featured awareness modules and phishing simulation training. Comparatively, 41% of medium-sized and 57% of large-size organizations reported including both facets in their current program structure. Organizations with 3000+ employees led the charge, with 79% of participants having both awareness and phishing simulations in place at the time of the tournament.

PROGRAM TYPE BY SIZE (%)



2021 simulation strategy

The third edition of the Gone Phishing Tournament took place between the 18th and the 29th of October 2021. Throughout the process, Terranova Security operated using its existing data security controls on its Security Awareness Platform. As a result, the highest possible level of information security was observed for the duration of the event.

If users clicked on the link to download the file, they were immediately redirected to a phishing simulation feedback page that highlighted the warning signs they missed, as well as the best practices they should always observe when faced with a similar scenario.

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

Overall, the success of each installment of the Gone Phishing Tournament hinges on an organization's ability to compare its click rates against its peers. Insights from the event empower security leaders to compare phishing simulation performance against other organizations accurately and determine how their click rate stacks up. They can then use the resulting intel to update their awareness program to keep their data and systems safe from cyber attacks.

Results

Most of the world's cyber attacks take advantage of basic human emotions, such as the willingness to trust another individual or organization, as a means to access, steal or otherwise compromise their sensitive information. In the case of ransomware, most victims must pay a cyber criminal a large sum of cryptocurrency before they can even hope to regain access to their information.

Fueled by Microsoft's real-world phishing email intel, the simulation crafted for the 2021 Gone Phishing Tournament maintained the same level of difficulty as the previous year's template, albeit targeting different end user behavior entirely. Since only one template was sent to all participants, the insights delivered in this report are as universal as they are prevalent, regardless of any technological lines of defense.

The 2021 Phishing Benchmark Global Report examines overall results and trends before breaking down the event's data by industry, organization size, and region.

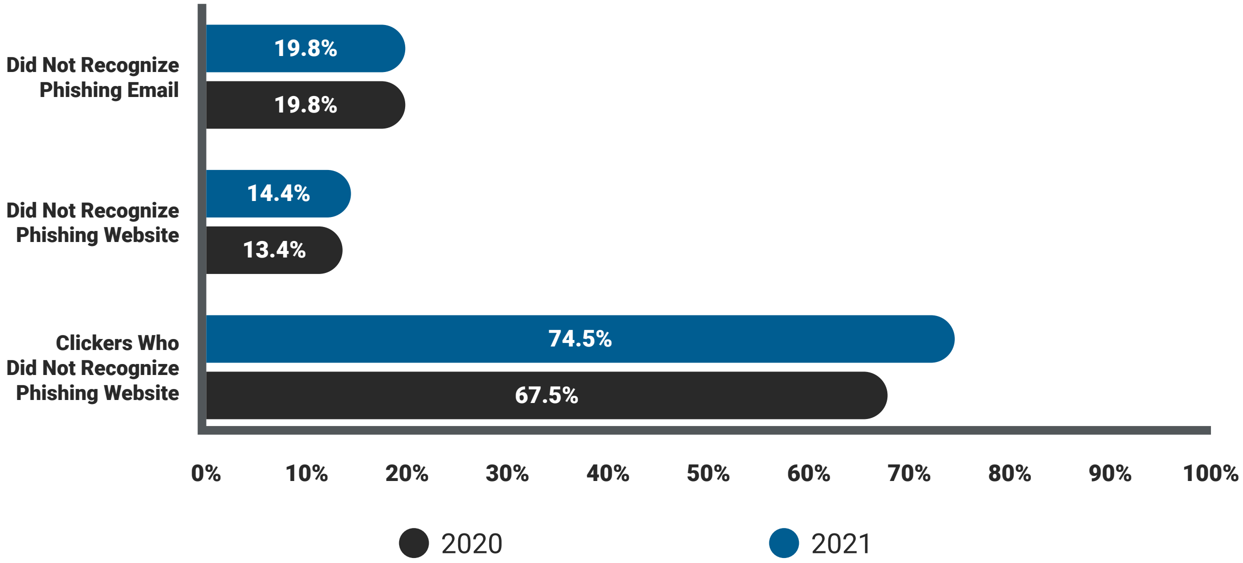
Overall

In total, 19.8% of all end users who participated in the 2021 Gone Phishing Tournament clicked on the link in the phishing email, a rate similar to the 2020 event's results. In addition, 14.4% of all end users failed to recognize the simulation's webpage as unsafe and clicked on the malicious file download link.

These truths mean that the number of initial clickers who ended up downloading the phishing simulation's webpage file exceeded 70%, representing an increase of nearly three percentage points from the previous year. Terranova Security in-house experts cite a 50% ratio as a more typical average during phishing simulations.

To bring those numbers into sharper focus, the event's results dictate that if a similar cyber attack would've been perpetrated against an organization with 1000 employees, just under 200 of them would've clicked on the initial phishing link, and more than 140 would've downloaded the malware file.

COMPARISON BETWEEN 2020 AND 2021



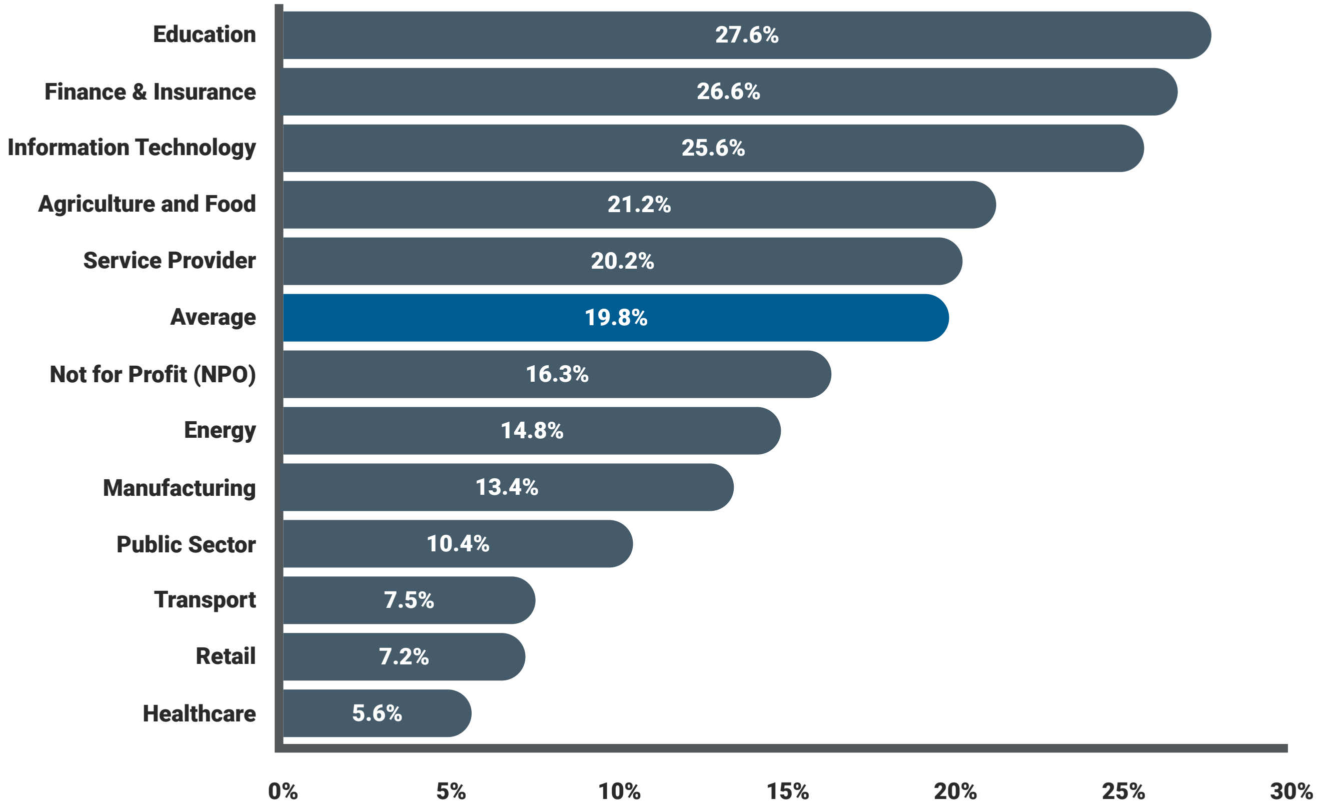
Data breakdown by industry: which sector fared best?

When measuring click rates between organizations based on their industry, it's important to recognize that no two are exactly the same in terms of individual starting points. Varying levels of security standards, compliance requirements, and so on means organizations need to compare their click rate against those from parties with similar realities.

In all, the following sectors posted phishing email click rates that were higher than the event's average:

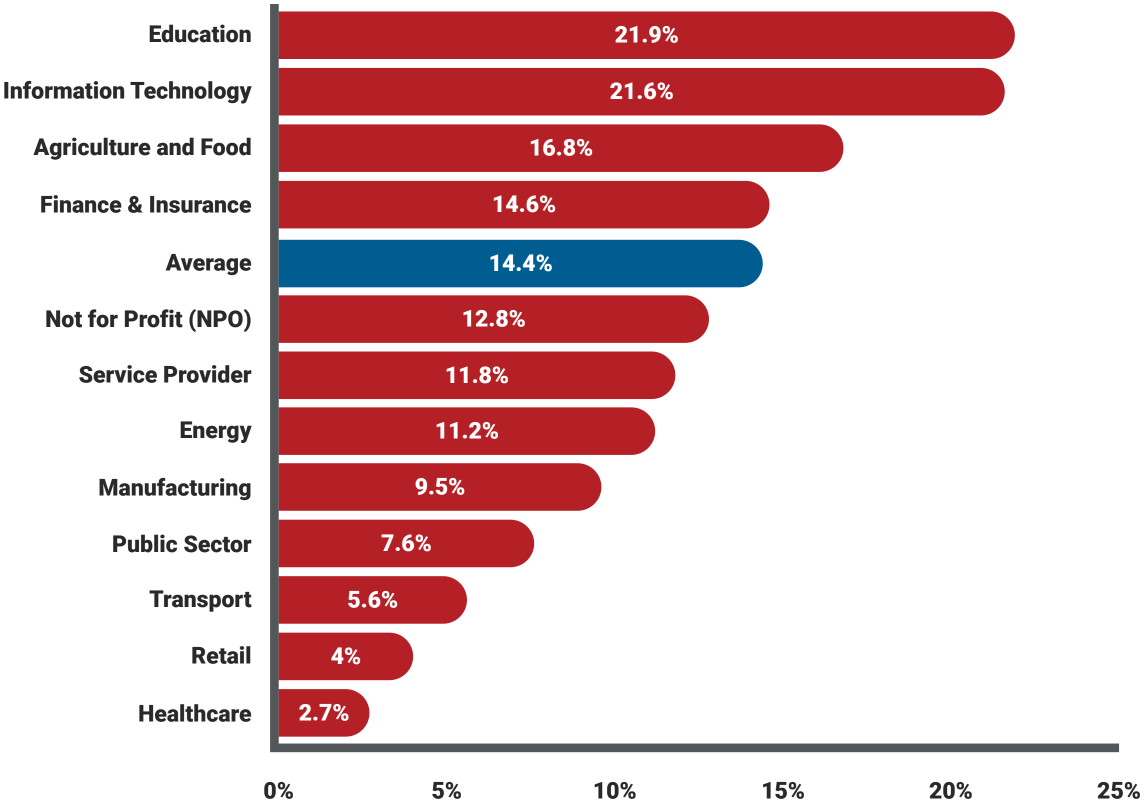
- Agriculture and Food
- Education
- Finance and Insurance
- Information Technology
- Service Provider

CLICKED LINK BY INDUSTRY (%)



Eight organizations finished with a below-average document download rate. The Service Provider sector was in this category despite sporting an above-average click rate. Only two industries, Healthcare and Retail, managed to keep their document download rate under 5%.

DOWNLOAD DOCUMENT BY INDUSTRY (%)

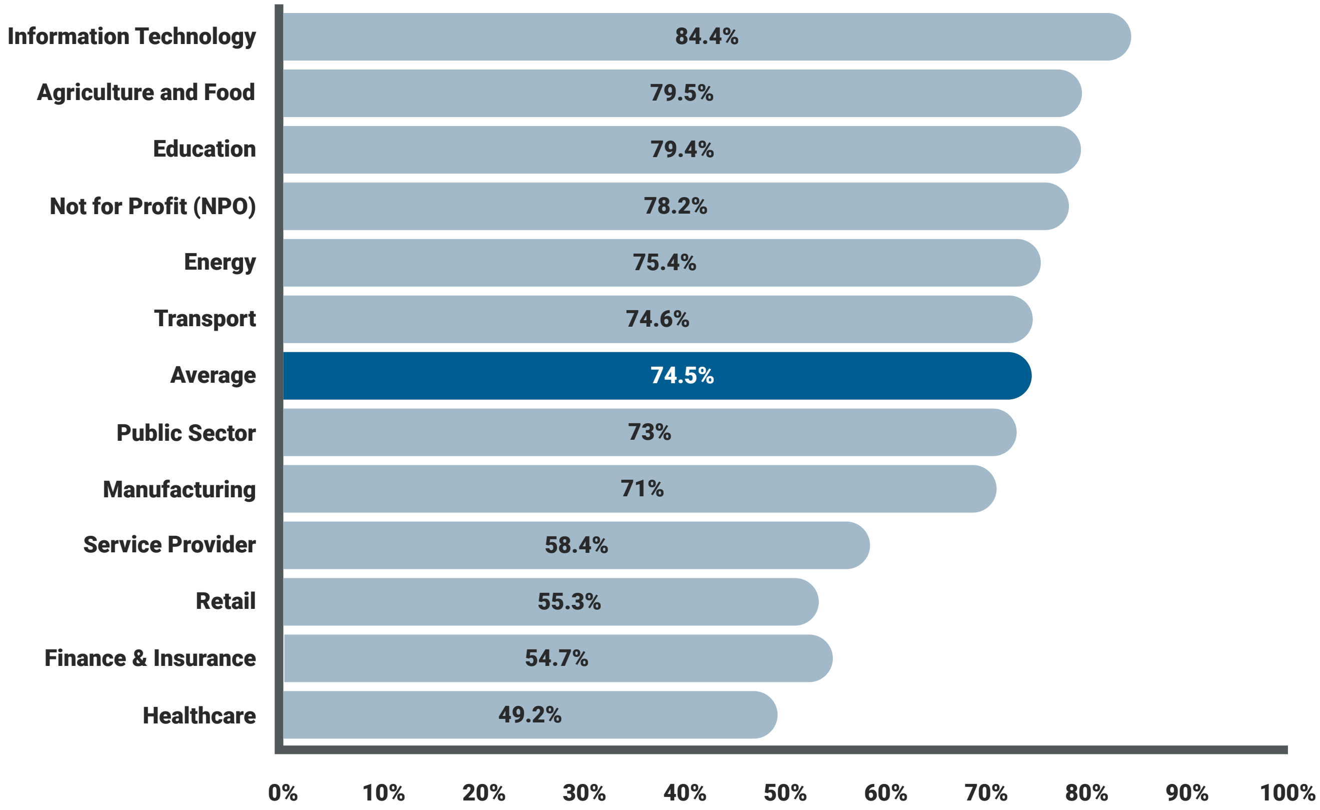


Arguably the biggest surprise from an industry angle is the percentage of clickers who went on to download the simulation's malware file. End users in the Information Technology sector posted a gargantuan click-to-download ratio of over 84%, with Agriculture and Food and Education coming in a close second and third, respectively.

On the other end of the spectrum, less than half of Healthcare end users who clicked followed through and downloaded the file. This number is also under the Terranova Security CISO-cited average of 50%.

These results highlight how, for certain industries, file-sharing is more a part of end users' day-to-day activities, which rendered the phishing simulation more relevant based on their roles. On the other hand, other industries may not use these types of productivity tools every day, potentially making the phishing email easier to pinpoint and report.

CLICKERS WHO DOWNLOADED DOCUMENT BY INDUSTRY (%)

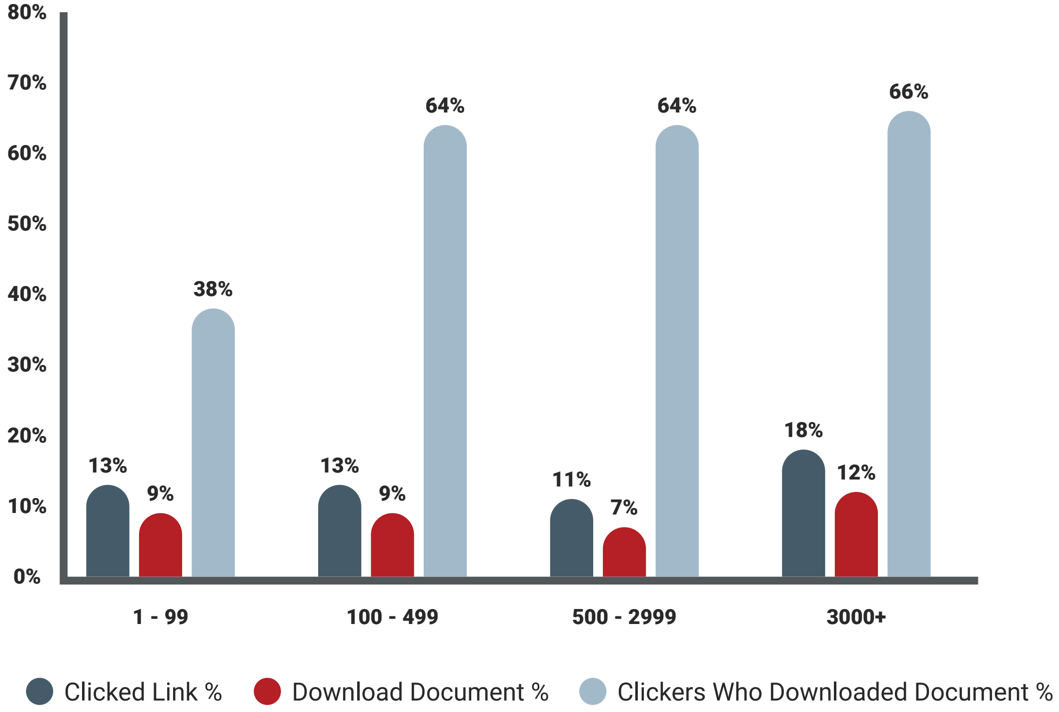


Data breakdown by number of employees: when does size matter?

In the context of security awareness training, this sections' titular question comes up frequently. In short, do more ample internal resources – including budget, staff devoted to related initiatives, and so on – result in lower end user click rates overall? The answer is far more complex than it seems.

The 2021 phishing simulation led to a similar phishing email click rate across all organization size brackets. While all segments saw an overall click rate north of 10%, organizations in the 500-2999 employee count range fared the best at 11%. This segment also performed best when it came to the total number of end users who downloaded the simulation's malware document (7%).

RESULTS BY ORGANIZATION SIZE (%)



Interestingly, organizations with over 3000 employees performed the worst of all size segments, posting an 18% email link click rate and a 12% document download rate. Of all the size brackets, they also featured the largest click-to-download ratio at 66%.

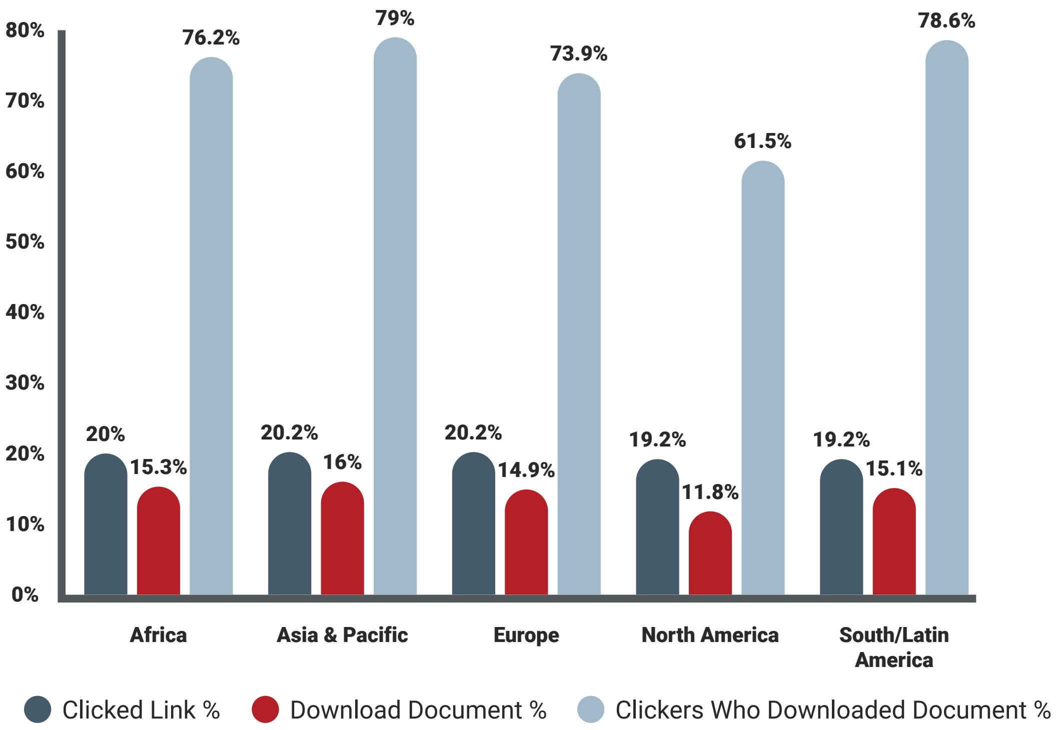
What does this mean? In a broad sense, an organization's security awareness training program strategy and individual initiative execution may matter more than its resources. According to participant data, while organizations with 3000 employees or more were rarely missing a security awareness training solution, they lagged far behind their 500-2999 counterparts in terms of effectiveness. Large organizations have the added challenge of having more users exposed to threats, as well as more users to train and follow up with.

Data breakdown by region: does location makes a difference?

An organization’s region, both in terms of its customer base and where its end users choose to work, can also make an enormous difference in cyber security awareness. Data privacy and compliance regulations, such as GDPR, can influence an organization’s security awareness goals and strategy, as can local or international news coverage of significant data breaches.

However, in the age of remote and hybrid workforces, distributed teams are far more common. As a result, IT personnel must ensure employees understand, recognize, and safeguard sensitive information from hackers. As the 2021 results highlight, this process becoming increasingly more complex to navigate.

RESULTS BY REGION (%)



Of the five regions represented by participating organizations, North America grabbed the top spot overall, claiming both the lowest email link click rate (tied with South/Latin American) and document download rate. As a result, the click-to-download ratio for North American organizations was significantly lower than any of the other regions at 61.5%.

These results are in stark contrast to the 2020 report, which saw North America ranked last compared to other regions. The best performing region from that year’s event, South/Latin America, recorded a middle-of-the-road document download rate and the second-highest click-to-download ratio (78.6%).

After outperforming their North American counterparts in 2020, European organizations posted higher rates across the board in 2021, including a click-to-download ratio that ballooned more than 12 percentage points.

The high click and download rates stemming from the phishing simulation Terranova Security designed in collaboration with Microsoft can be linked back to the real-world quality of the scenario. Phishing threats are constantly changing to mimic content or messages any end user may plausibly encounter in their day-to-day activities. By tapping into this familiarity, attacks similar to this one are becoming harder to spot. And, while North American organizations certainly improved their overall performance year-over-year, their collective security awareness training journey is far from done. As a global leader in many worldwide business communities, it's incumbent on organizations from this region to continually minimize risk through engaging, informative learning opportunities.

On top of that, effective security awareness training must include data from recent cyber attacks and news items, further detailing how hackers operate and the tactics they may use. If those elements aren't present in a training program, the overall end user experience may not communicate updated threat information, which, in turn, can result in a weak knowledge baseline among all employees.

How to Launch Powerful Phishing Simulation Training

Importance of targeting behaviors through risk-based training campaigns

Phishing simulations add a dynamic, learning-by-doing dimension to any security awareness training program. Informative, interactive phishing simulations that reflect current cyber threat realities can help end users solidify their knowledge of cyber threats and put it into practice quickly.

By offering both theoretical and hands-on training, any organization can instantly boost its training program engagement and get more precise insights into the average end user's knowledge of information security best practices. Without the hands-on portion, the theoretical component of any awareness initiative will only go so far. Employees must have the means to put that knowledge into practice.

Maximizing results with risk-based phishing training campaigns

Before designing the specifics of any security awareness training course or phishing simulation, security leaders need to establish a framework that sets the foundation for a defined end user learning path. To help achieve this goal, Terranova Security has identified seven common behaviors targeted by cyber threats, based on Microsoft payloads, that every organization should be mindful of:

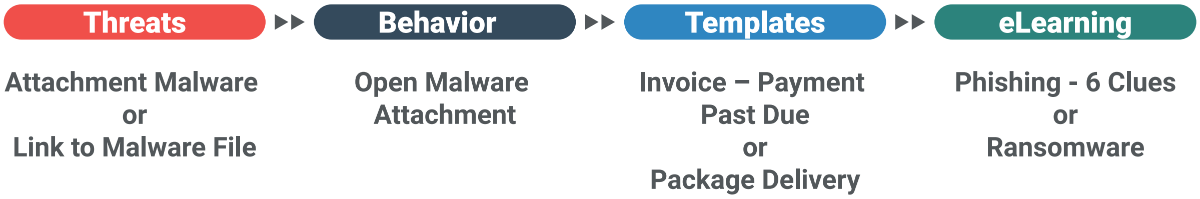
THREATS

- Attachment Malware
- Link to Malware File
- Link in Attachment
- Drive-By URL
- 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



Threats ▸▸ Behavior ▸▸ Templates ▸▸ eLearning

Threats	Behavior	Templates	eLearning
Attachment Malware or Link to Malware File	Open Malware Attachment	Invoice – Payment Past Due or Package Delivery	Phishing - 6 Clues or Ransomware

This illustration depicts the link between a given threat, which, in this case, is a malware attachment or link, to the user behavior which may compromise their sensitive data. Based on the end user behavior(s) you want to address with your awareness training initiative(s), your modules and phishing simulations must work harmoniously to target the right actions and ensure an accurate measure of behavior change.

Terranova Security also recommends using communication tools to encourage participation across all business units once your awareness training is ready to launch. Then, start with a general phishing module that establishes baseline knowledge data across the organization and provides a knowledge-based starting point from which to work.

Ideally, this is followed by a monthly microlearning module that educates users on a specific risk related to your target behavior. Afterward, support the subject matter covered in the microlearning with a related phishing simulation. In the case of ransomware, it may ask the recipient to download an urgent document or software update.

To get actionable, data-driven insights throughout the training program's lifecycle, organizations should target 4–6 simulation deployments per year, with at least four accompanying awareness training activities. Terranova Security recommends aiming for a 5% improvement of the organization's average click rate after completing those 4–6 simulations and related awareness activities over 12 months.

As scenarios vary in complexity, the phishing simulations you choose to launch will impact the click rate. If your users never click on the phishing simulation email links, the deployed scenarios may not be challenging enough. Quality over quantity is a significant consideration here. By safely testing users with high-quality, realistic, and relevant templates, you reduce the possibility of an incorrect action occurring when the threat is real.

How to launch effective phishing simulations

Taking a proactive, data-based approach to security awareness training and phishing simulations can be easier than many organizations may think. To educate users and change key behaviors cyber criminals can look to exploit, 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 click during 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

Next Steps

With fabric-altering changes continuing to affect organizations of all sizes and in all sectors, security awareness training and phishing simulations must be an absolute priority for all organizations.

While an excellent start, sporadic or intermittent bursts of security awareness training are no longer effective. The cyber threat landscape evolves at such a rapid pace that strategies employed by cyber criminals shift frequently and quickly. As a result, organizations must adapt and prioritize the continuous education of their employees to ensure optimal information security.

Giving end users access to high-quality security awareness content – with modules as fun and engaging as they are informative – is an integral part of this journey, as is taking advantage of various communication tools like videos and infographics. Combined with phishing simulations, these assets are the best way to strengthen data protection and reduce risk.

However, before organizations even get to the execution stage, there must also be an acknowledgment of areas for improvement. Once those are identified, determining cyber security goals, such as click rate reduction among all end users, is much more straightforward. Those goals make obtaining all-important buy-in at the executive level that much easier.

Terranova Security recommends leveraging all opportunities to measure and use data about employee awareness, click rates, and industry standards to optimize your awareness training program. Having this information on hand facilitates taking proactive steps to impart lasting, positive behavior change.

Overall, security awareness training is like any other growth-oriented process: it must be consistent and evolve to meet the changing needs and conditions of the world around it. Ongoing training initiatives, both theoretical and hands-on, empower an organization's employee base to safeguard sensitive information against phishing attacks with confidence.

About Terranova Security

Terranova Security is the global security awareness training partner of choice that has been training the world's cyber heroes for more than 20 years. The company empowers organizations worldwide to design programs that change user behaviors, drastically reduce the human risk factor, and counter cyber threats. By providing security leaders with the industry's most innovative, highest-quality awareness training content and real-world phishing simulations, Terranova Security makes it easy to build risk-based campaigns that target the right end user behaviors.

As a result, training initiatives ensure all employees understand critical information security best practices on phishing, social engineering, data privacy, compliance, and much more. This commitment to helping organizations build foundational resilience against cyber threats is also reflected in the Terranova Security partnership with Microsoft. This collaboration embodies both organizations' dual mission to develop initiatives that strengthen the human line of defense in cyber security.

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 www.terranovasecurity.com.

GONE PHISHING TOURNAMENT™

Co-sponsored by

TERRANOVA SECURITY

Microsoft