KnowBe4

PHISHING BY INDUSTRY BENCHMARKING REPORT

2023 EDITION

TABLE OF CONTENTS

Verizon's 2023 Data Breach Investigations Report states that **"74% of all breaches include the human element,** with people being involved either via error, privilege misuse, use of stolen credentials or social engineering." With favorable movement over the prior year, **this renewed focus on the human element is working...but the job is not done.**

INTRODUCTION

Cybercriminals can gain access to a digital environment in a variety of ways. As technical security controls continue to make "hacking in" increasingly difficult, cybercriminals look for less resilient targets: the human layer. As the human layer continues to be the most enticing attack vector, criminals are showing their willingness to search for any weakness, targeting employees in both professional and personal settings. Sadly, most organizations continue to focus on technology-based security layers while ignoring the human layer. Additionally, most humans remain vulnerable because they don't take precautions in their personal lives to prevent being compromised.

Cyber threats continue to grow as criminals rely on the tried and tested attack methods while developing new, more sophisticated ways to infiltrate digital environments and minimize the effectiveness of your human defense layer. To best defend your organization from a cyber attack, employees must have the knowledge, adapted habits and behaviors necessary to drive a culture of security. Training needs to be transformed into something more developed, consistent and instinctive.

We continue to see significant year-over-year increases in phishing attacks across all geographies, industry verticals and organization sizes. Cybercriminals do not discriminate when they consider victims, as carefully constructed attacks target humans both at work and play, day or night through various types of social engineering. Cybercriminals will continue to exploit humans as they determine their next intrusion strategy. As we continue to deal with socioeconomic and health issues globally, we also need to contend with advancements in Artificial Intelligence strengthening a cybercriminals arsenal.

The FBI's 2022 Internet Crime Complaint Center (IC3), ***continued to receive a record number of complaints from the American public: 800,944 reported complaints (2,175+ daily), which was a 5% increase from 2021, with potential losses exceeding $10.3 billion***. Additionally, business email compromise incidents accounted for ***21,832 complaints with an adjusted loss of nearly $2.7 billion***. And these are just the reported incidents. Investment scams and ransomware attacks on critical infrastructures proved to be the most lucrative scams. Industries are grappling with how they can better develop their human defense layer to detect, protect and report suspicious actions before it's too late.

Security leaders who ignore the problem, do the bare minimum, focus only on technology or still rely on old-school training methods leave their organizations vulnerable to a potential attack. Additionally, confusing required compliance training as security awareness training leaves major gaps in employee knowledge and ability. These two areas of focus should be combined to create a holistic and comprehensive learning program that covers all areas that could negatively expose an organization.

Promoting a comprehensive and focused program that includes a variety of content styles/versions, continuous testing and ongoing communication is the right combination to help build a resilient security culture.

With the root cause of the majority of data breaches being traced to the human factor, security leaders who continue to invest solely on technology-based security layers run the risk of overlooking a best practice proven to reduce their vulnerability: security awareness training coupled with frequent simulated social engineering testing. This approach both helps raise the readiness level of humans to combat cyber crime and lays the critical foundation necessary to drive a strong security culture.

As phishing attacks continue to rise, cybercriminals are counting on your employees lacking the necessary knowledge, attention and energy to trick them into getting phished. One over-stressed, distracted, or uneducated employee is all you need to let the bad actors in.

Security leaders need to know what happens when their employees receive phishing emails: are they likely to click the link? Get tricked into giving away credentials? Download a malware-laced attachment? Will they simply ignore the email or delete it without properly notifying their security team? Or will they report the suspected phish and play an active role in the human defense layer?

> Security leaders need to know what happens when their employees receive phishing emails: **are they likely to click the link?**

Each organization's employee susceptibility to these phishing attacks is known as their Phish-prone™ Percentage (PPP). By translating phishing risk into measurable terms, leaders can quantify their breach likelihood and adopt training that reduces their human attack surface.

Understanding Risk by Industry

An organization's PPP indicates how many of their employees are likely to fall for social engineering or phishing scams. These are the employees who might be tricked into clicking on a link, opening a file infected with malware or transferring organizational funds to a cybercriminal's bank account. A high PPP indicates greater risk, as it points to a higher number of employees who typically fall for these scams. A low PPP is optimal, as it indicates the staff is security-savvy and understands how to recognize and shut down such attempts.

In short, a low PPP means that an organization's human firewall is providing security strength rather than weakness. The overall PPP offers even more value when placed in context. After seeing their PPP, many leaders ask questions such as "How does my organization compare to others?" and "What can we do to reduce our Phish-prone Percentage and better equip our team?"

To help organizations evaluate their PPP and understand the implications of their ranking, KnowBe4 conducts an annual study to provide definitive Phish-prone benchmarking across industries. Categorized by industry vertical and organization size, the study reveals patterns that can light the way to a stronger, safer and more resilient security culture.

2023 GLOBAL PHISHING BY INDUSTRY BENCHMARKING STUDY

Though every organization would like to understand how they measure against the rest in their industry, the comparison requires robust data coupled with a scientific, proven method to produce valid results. The struggle to answer the question "How do I compare with other organizations that look like me?" is very real. To provide a nuanced and accurate answer, the 2023 Phishing By Industry Benchmarking Study analyzed a data set of over 12.5 million users, across 35,681 organizations, with over 32.1 million simulated phishing security tests, across 19 different industries.

Methodology For This Year's Study

All organizations were categorized by industry type and size. To calculate each organization's PPP, we measured the number of employees who clicked a simulated phishing email link or opened an infected attachment during a testing campaign using the KnowBe4 platform.

In our 2023 report, we continue to look at the following three benchmark phases:

- **Phase One:** Baseline Phishing Security Test Results
- **Phase Two:** Phishing Security Test Results Within 90 Days of Training
- **Phase Three:** Phishing Security Test Results After One Year-Plus of Ongoing Training

ANALYZING TRAINING IMPACT

To understand the impact of security awareness training, we measured outcomes at these three touchpoints to answer the following questions:

PHASE ONE

If you have not trained your users and you send a phishing attack, what is the initial resulting PPP?

To do this, we monitored employee susceptibility to an initial baseline simulated phishing security test. From that established set of users, we look at any time a user has failed a simulated phishing security test prior to having completed any training.

PHASE TWO

What is the resulting PPP after your users complete training and receive simulated phishing security tests within 90 days after training?

We answered this question by finding when users completed their first training event and looking for all simulated phishing security events up to 90 days after that training was completed.

PHASE THREE

What is the final resulting PPP after your users take ongoing training and monthly simulated phishing tests?

To answer this, we measured security awareness skills after 12 months or more of ongoing training and simulated phishing security tests, looked for users who completed training at least one year ago, and took the performance results on their very last phishing test.

METHODOLOGY AND DATA SET

32.1 Million Phishing Security Tests

12.5 Million Users

35.6 Thousand Organizations

19 INDUSTRIES

- Banking
- Business Services
- Construction
- Consulting
- Consumer Services
- Education
- Energy & Utilities
- Financial Services
- Government
- Healthcare & Pharmaceuticals
- Hospitality
- Insurance
- Legal
- Manufacturing
- Not For Profit
- Other
- Retail & Wholesale
- Technology
- Transportation

ORGANIZATION SIZE RANGES

WHO'S AT RISK: RANKING INDUSTRY VULNERABILITY

The results across the 12.5 million users highlight an all too familiar truth for organizations: failure to effectively train your users leaves them, and your organization, unprepared and vulnerable to social engineering attacks. The PPP data, although slightly more favorable than 2022, continues to show that no single industry across all-sized organizations is doing a good job at recognizing the cybercriminals' phishing and social engineering tactics. When users have not been tested or trained, the initial baseline phishing security tests show how likely users in these industries are to fall victim to a phishing scam and put their organizations at risk for potential compromise.

The overall 2023 PPP baseline average across all industries and size organizations was **33.2%**, an unfavorable increase of nearly one point from 2022. While trends continue to fluctuate and vary across different industries, our research shows that untrained users continue to be the most significant flaw in organizations' cyber defense layer. Humans without the proper knowledge, training and testing leave an organization exposed to crippling cyber attacks.

- Across small organizations (1-249 employees), the top three industries remain the same for a second year running although they have changed rankings. The **Healthcare & Pharmaceuticals** industry, although slightly better than 2022, enters 2023 in the top spot with a **PPP of 32.3%**. **Retail & Wholesale** is second with a **PPP of 31.6%**, flat over prior year. **Education** moves from the first ranked to the third position with a one-point improvement and a **PPP of 31.2%**.
- With mid-sized organizations (250-999 employees), two of the highest risk industries from 2022 remained, while a new one entered the third spot. The **Hospitality** industry exited the risk list and was replaced by **Healthcare & Pharmaceuticals** who moved from the second spot to the first with a **PPP of 35.8%**. We now see the **Healthcare and Pharmaceuticals** industry as the highest at risk for both small- and medium-sized organizations. **Energy & Utilities** also moved up in ranking from third to second with a **PPP of 33.6%**. New to the ranking in 2023 is the **Construction** industry, capturing the third spot with a **PPP of 31.3%**. It's important to mention that both the **Healthcare & Pharmaceuticals** and **Energy & Utilities** industries had slightly better PPPs vs. 2022 ratings, although they remained the industries most at risk.

- For large organizations (1,000+ employees), **Insurance** remains the most at risk industry for the second year running with a **PPP of 53.2%**, relatively unchanged from 2022. The **Energy & Utilities** industry moves from the third spot in 2022 to the second in 2023 with a **PPP of 51.1%**, a slight increase over prior year. Rounding out the top three most at risk industries is **Consulting**, second in 2022, with a **PPP of 48.2%**, a four-point improvement over prior but still extremely risky.
- The winner of the lowest Phish-prone benchmark across small organizations (1-249 employees) was **Legal** with a **PPP of 25.6%**; across mid-sized organizations was **Government** for the second year running with a **PPP of 26.3%**; and across large organizations we again see **Government** with a **PPP of 25.7%**. Although the lowest in the findings, these PPP results strongly indicate that an untrained user base is still vulnerable to phishing attacks.

BASELINE PHISHING SECURITY TEST RESULTS

The initial baseline phishing security test was administered within organizations that had not conducted any security awareness training from the KnowBe4 platform. Users received no warning, and the tests were administered on untrained people going about their regular job duties. The results continue to indicate high risk levels year-over-year:

- Across all industries and all sizes, the average Phish-prone Percentage was **33.2%**, up 1 point from 2022. That means one out of three employees was likely to click on a suspicious link or email or comply with a fraudulent request, about the same outcome as last year.
- The 2023 data that showed the most significant improvement was seen with **Medium Hospitality** organizations, which positively moved from a PPP of **39.4% to 28.5%**. Adversely, the most significant decline was visible in **Large Hospitality** organizations, moving negatively from **20.4% in 2022 to 29.5% in 2023**. The Hospitality industry is a rich target for criminals because of the immense amount of personal identifiable information (PII) they retain, the fact that many are spread out globally providing a large attack surface, and employ workers that are at lower levels of cyber readiness.
- What is most concerning are the PPPs of the following industries in the Large category, which all have PPPs north of 40%: **Banking 43%, Healthcare & Pharmaceuticals 46.7%, Consulting 48.2%, Energy & Utilities 51.1%, and Insurance 53.2%**. Even more concerning is that this list remains unchanged from 2022. This means that employees in these categories have been at a high risk of falling for social engineering attacks for two years straight.

Thoughts: Organizations must stop relying on the minimal investment for their employees. Paying lip service to security awareness training is not effective when trying to keep your organization from human-focused attacks. Security awareness training and testing needs to be offered with a high degree of quality and frequency and be administered in the most efficient manner. Smaller bursts of content delivered more often keeps security top of mind and skills sharpened. Without training and frequent reinforcement, every organization, regardless of size and vertical, is susceptible to phishing and social engineering. Workforces in every industry represent a possible doorway to attackers, no matter how steep the investment in world-class security technology. Investment in both training and technology provides the right mix of coverage.

Phase One

33.2% Initial Baseline Phishing Security Test Results

Organization Size	Initial PPP
1-249	28.1%
250-999	30%
1000+	36.8%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	25.7%	29.4%	43%
Business Services	27%	29.2%	31.6%
Construction	28.8%	31.3%	36.3%
Consulting	27%	31%	48.2%
Consumer Services	29%	30.7%	25.7%
Education	31.2%	29.2%	30.3%
Energy & Utilities	27.9%	33.6%	51.1%
Financial Services	26.2%	28.9%	37.3%
Government	27.7%	26.3%	25.7%
Healthcare & Pharmaceuticals	32.3%	35.8%	46.7%
Hospitality	26.8%	28.5%	29.5%
Insurance	26.1%	31.2%	53.2%
Legal	25.6%	29.5%	35.7%
Manufacturing	28.8%	30.5%	37.4%
Not-For-Profit	27.1%	28.4%	28.9%
Other	31%	35.9%	23.1%
Retail & Wholesale	31.6%	29.9%	42.2%
Technology	25.8%	28.2%	32.9%
Transportation	26.3%	28.5%	33%

PHISHING SECURITY TEST RESULTS WITHIN 90 DAYS OF TRAINING

When organizations implemented a combination of training and simulated phishing security testing after their initial baseline measurement, results dramatically improve. We found that after users complete their first training event, the simulated phishing security test results up to 90 days after that training is completed are more favorable. In those 90 days after completed training events, the average PPP was cut to almost half at **18.5%**, consistent with the studies from the past four years. The dramatic drop in PPP was not specific to a certain industry or organization size, but here are a few interesting data points:

- The most significant reduction was seen in the following organizations: small (1-249 employees) **Banking** experienced a **49.9% decrease** from 25.7% at baseline to 12.9% within 90 days of training. It's worth noting that for the second year running, **Education** saw another sizable decrease of **85.6%**. With mid-size organizations (250-999 employees), **Healthcare & Pharmaceuticals** experienced a **43.3% decrease** from 35.8% at baseline to 20.3% within 90 days of training. Keep in mind that Healthcare & Pharmaceuticals was at the top of the list for the medium size industry most at risk. After applying only 90 days of training they become more favorable. Lastly, with large (1000+ employees) **Insurance** experienced a **65.7% decrease** from 53.2% at baseline to 18.2% within 90 days of training after recording the highest initial baseline PPP. Like we saw in the medium category, the industry with the worst overall PPP, improved to the best overall PPP after only 90 days of training.
- The significant drop from the initial baseline of **33.2% to 18.5%** in phase 2 across all industries proves that, by applying a comprehensive security awareness training program that includes continuous testing and communication, organizations can improve the ability of their users to detect and report malicious activity before it's too late. Strengthening this important human layer in as little as 90 days is a significant advancement in better securing your organization.

Thoughts: After only 90 days of new-school security awareness training, we see a significant improvement in employees' abilities to detect malicious emails across every industry and size of organization. It takes a 90-day investment to raise readiness levels and lower risk. As with any significant change, it takes time to break old habits and create new ones. Once these new habits are formed they become the new normal as a part of the organizational culture and influence how others behave, especially new hires who look to others to see what is socially and culturally acceptable in the organization.

Phase Two

18.5% Phishing Security Test Results Within 90 Days of Training

Organization Size	90-Day PPP
1-249	18.6%
250-999	19.1%
1000+	18.2%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	12.9%	15.3%	16.1%
Business Services	19.6%	21%	19.5%
Construction	20.6%	21.7%	18%
Consulting	19.2%	20.4%	21.7%
Consumer Services	20.2%	20.7%	16.5%
Education	18.4%	19.1%	18.7%
Energy & Utilities	17.9%	17.9%	17.3%
Financial Services	16.4%	17.4%	19.7%
Government	16.9%	16%	15.5%
Healthcare & Pharmaceuticals	20.7%	20.3%	17.5%
Hospitality	20.1%	20.4%	15.8%
Insurance	19.6%	18.1%	18.2%
Legal	17.6%	18%	18.5%
Manufacturing	18.7%	19%	17.8%
Not-For-Profit	20.6%	19.9%	16.5%
Other	20.2%	21.6%	21.3%
Retail & Wholesale	19.5%	19.8%	19.7%
Technology	19.7%	20.1%	18.6%
Transportation	19.9%	21.1%	19.6%

PHISHING SECURITY TEST RESULTS AFTER ONE YEAR-PLUS OF ONGOING TRAINING

At this stage, we measure security awareness skills after 12 months or more of ongoing training and simulated phishing security tests. Our inclusion set contains users who completed training at least one year ago, and we analyze the performance results on their most recent phishing test. The results continue to be dramatic year-over-year, showing that having a consistent, mature awareness training program reduced the average PPP from 33.2% down to **5.4%.** These results were demonstrated consistently across all industry sizes and verticals.

For the third year, the lowest PPP in small organizations (1-249 employees) was **Banking** at **3%**. With Banking being one of the most attacked and regulated industries, the results are no doubt based on the experience they have with cyber crime and the diligence that they have applied to training. In the category of medium organizations, (250-999 employees) the **Hospitality** industry scored **3.8%** after 12 months. This is consistent with the improvement seen in medium Hospitality organizations after 90 days.

The **Legal** industry saw the lowest PPP at **1.8%** for large organizations (1000+ employees). Law firms have unparalleled access to the most sensitive information and will continue to be a prime target for criminals. The increased attack on these data rich organizations will remain constant and relentless. Law firms have increased their adoption of security awareness training and smart technology that can reduce their overall susceptibility to an attack.

After comparing the data, the industries that showed the greatest holistic improvement were both in the large category (1000+ employees): **Insurance**, which went from a benchmark PPP of **53.2%** to **5.7%** after at least 12 months of security awareness training, a 89.2% reduction; the **Energy & Utilities** industry (for the second year in a row), which went from a benchmark PPP of **51.1%** to **4.5%** after one year, a 91.2% reduction. The Energy & Utilities industry will continue as a high yield attack target for cybercriminals because of the immediate, long-term and permanent damage an attack on critical power systems could have.

Also worth mentioning is that Energy & Utility organizations often have remote workforces, relying heavily on outdated technology. With the transfer of delicate, confidential information across a global network grid, the probability of a successful cyber attack goes up. Adversarial nation-states wait ready to attack should they get the opportunity.

Phase Three

5.4% **Phishing Security Test Results After One Year-Plus of Ongoing Training**

Organization Size	12-Month PPP
1-249	4.4%
250-999	5.5%
1000+	5.9%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	3%	4%	4%
Business Services	4.7%	5.9%	5.4%
Construction	4.5%	6.1%	7.3%
Consulting	4.4%	7.5%	10.2%
Consumer Services	4.8%	6%	6%
Education	4.6%	5.5%	5.4%
Energy & Utilities	3.8%	5.6%	4.5%
Financial Services	4.1%	5.9%	5.5%
Government	4%	4%	6.1%
Healthcare & Pharmaceuticals	4.6%	5.3%	5.4%
Hospitality	4.8%	3.8%	8.8%
Insurance	4.5%	5.3%	5.7%
Legal	4.1%	4.7%	1.8%
Manufacturing	4.1%	4.9%	5.9%
Not-For-Profit	5.5%	6.1%	4.9%
Other	5.4%	7.1%	7.3%
Retail & Wholesale	4.1%	5.6%	5.9%
Technology	4.9%	6.4%	6.5%
Transportation	5.4%	8.5%	8%

AVERAGE IMPROVEMENT RATES ACROSS ALL INDUSTRIES AND ORGANIZATION SIZES

After one year or more of security awareness training combined with frequent simulated phishing tests, organizations across all sizes and industries drastically improved. Organizations with 1-249 employees saw an overall improvement rate of **84%** with 12 of 19 industries at or above that average.

Across mid-size organizations (250-999), improvement rates were good with 15 industries coming in at **80% or better**, two industries fell slightly below 80%. One reason for a decrease in favorable movement could be that the initial baseline for some verticals may not have been as bad. So if there was a baseline change from something like 34% initial PPP to 32%, then the overall percent of change over 12 months might be lower. This doesn't mean that anything significant happened other than that the general awareness of phishing scams could be on the rise, impacting the baseline. For large organizations (1,000+), we saw an average improvement rating of **82%**, though three industries experienced 90%+ improvement rates, **Banking, Energy & Utilities and Legal**.

When you look across all industries and sizes, the **82%** average improvement rate from baseline testing to one year-plus of ongoing training and testing is outstanding proof for gaining buy-in to establish a fully mature security awareness training program.

KnowBe4 finds that the industry-wide **33.2% of untrained users will fail** a phishing test.

Organizations that commit to ongoing training are rewarded with swift improvement. Once trained, only 18.5% of users failed within 90 days of completing their first KnowBe4 training. After at least a year on the KnowBe4 platform, only 5.4% of users failed a phishing test.

Average Improvement

82%

Average Improvement Rate Across All Industries and Sizes

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	88%	86%	91%
Business Services	83%	80%	83%
Construction	84%	81%	80%
Consulting	84%	76%	79%
Consumer Services	84%	81%	77%
Education	85%	81%	82%
Energy & Utilities	86%	83%	91%
Financial Services	84%	80%	85%
Government	86%	85%	76%
Healthcare & Pharmaceuticals	86%	85%	88%
Hospitality	82%	87%	70%
Insurance	83%	83%	89%
Legal	84%	84%	95%
Manufacturing	86%	84%	84%
Not-For-Profit	80%	79%	83%
Other	83%	80%	68%
Retail & Wholesale	87%	81%	86%
Technology	81%	77%	80%
Transportation	80%	70%	76%

2023 INTERNATIONAL PHISHING BENCHMARKS

At the international level, we use a slightly different data set that does not include separate industries to determine phishing benchmarks regionally across small, medium and large organizations. We included organizations where a definitive country was associated with the customer account so it could be included in the international benchmark analysis. The same benchmarking phases used to measure Phish-prone Percentages across industries were used for the international data set.

Phase One
Initial Baseline Phishing Security Test Results

Phase Two
Phishing Security Test Results Within 90 Days of Training

Phase Three
Phishing Security Test Results After One Year-Plus of Ongoing Training

		BASELINE			90 DAYS			1 YEAR		
	Organization Size	1-249	250-999	1000+	1-249	250-999	1000+	1-249	250-999	1000+
REGION	North America	28%	30.1%	37.1%	18.5%	19%	18.4%	4.2%	5.1%	5.7%
			TOTAL: 33.1%			TOTAL: 18.6%			TOTAL: 5.1%	
	Africa	30%	29.4%	33.3%	25.2%	22.7%	19.3%	9%	10.5%	5.7%
			TOTAL: 32.8%			TOTAL: 20.5%			TOTAL: 6.6%	
	Asia	32.6%	33.2%	28.8%	20.9%	19.6%	13%	7.3%	7.4%	6%
			TOTAL: 30%			TOTAL: 14.9%			TOTAL: 6.5%	
	Australia & New Zealand	27.1%	30.9%	41.1%	21.1%	19.9%	15.3%	6.3%	7.7%	5.4%
			TOTAL: 34.8%			TOTAL: 17.8%			TOTAL: 6.4%	
	Europe	26.5%	28%	36.2%	19.1%	19.7%	19.4%	6.7%	7.6%	6.1%
			TOTAL: 32.9%			TOTAL: 19.4%			TOTAL: 6.5%	
	South America	34%	27.7%	49.5%	23%	25.8%	18.7%	6.4%	10.2%	5.1%
			TOTAL: 41.1%			TOTAL: 21.3%			TOTAL: 6.9%	
	United Kingdom & Ireland	26.3%	28%	39.6%	18.5%	18.1%	17.6%	6.1%	8.1%	4.9%
			TOTAL: 35.2%			TOTAL: 17.8%			TOTAL: 5.8%	

NORTH AMERICA

By Erich Kron

Most Prevalent Issues

In North America, ransomware continues to threaten organizations of all sizes, across all industries. Given the success of ransomware over the last few years, cybercriminals have not needed to make major changes to their tactics, which continue to create a lucrative and profitable business model for them. We continue to see that the ransomware-as-a-service (RaaS) model comprises a significant amount of the successful attacks in North America.

Because most organizations have become reasonably good at restoring their data, in 2019 ransomware groups began to exfiltrate data to use it as additional leverage. That has now become a bigger focus than the encryption itself. Bad actors know that information is power, and they use the threat of the public release of information as a major source of leverage when it comes time to get paid. Not only is this damaging to an organization's reputation, but the potential fines from regulatory agencies can be crippling. This focus on extortion is one reason the amounts for ransom demands have skyrocketed in the last couple of years.

To make a bad situation worse, according to BlackFog, class action lawsuits are also a cause for concern. Just recently, Dish Network was hit with no less than six law firms pursuing a class action lawsuit against Dish for shareholder losses after their multi-day network outage.

Less publicly visible, but just as devastating a type of cyber crime, business email compromise (BEC) continues to surface as a prolific attack type. One key differentiator of BEC compared to other types of cyber crime is the fact that BEC typically does not include any sort of attachment or link in the email, indicators that many people have become suspicious of, and that technical controls have a chance at spotting. Instead, BEC relies purely on social engineering and emotional manipulation to drive victims to take the attacker's intended action. Not to be forgotten is the increase in VEC or vendor email compromise. These are attacks that originate with a vendor in the supply chain, whose email has been compromised by bad actors and used against their customers. Because there is a level of trust established between the organizations already, and because bad actors will often piggyback on previous legitimate conversations, these attacks can be particularly successful.

While the turmoil of the COVID-19 pandemic is finally calming down, many organizations still struggle with the change to remote workers, now dealing with the technical debt incurred when the pandemic hit. This means many organizations remain in a state of flux while we begin to understand what "normal" looks like. In what appears to be some fallout from the COVID-19 pandemic and the struggling economy, tech organizations are laying off employees in large numbers, adding to a sea of changes already happening in the world. Any time there is this much flux in organizations, there are opportunities for bad actors.

A large area of concern for many is artificial intelligence (AI), which has finally found its way to the main stage, and has done so in a big way with ChatGPT. The fact that ChatGPT can write code, translate languages, correct errors in spelling and grammar and all sorts of other household tasks, is especially disturbing from a cybersecurity standpoint. Using AI to search for vulnerabilities in code or to find ways to get around detection are real and serious threats that organizations need to be considering. While these AI-generated attacks may find their way past technical security controls, humans, when properly educated, far surpass technical controls when it comes to spotting things that are unusual or abnormal in emails, text messages or even phone calls.

Economic Impact

According to a 2021 survey conducted by Cybereason, 58% of organizations in the U.S. suffered significant revenue losses as a direct result of a ransomware attack. In addition, 56% of U.S. organizations reported that their brand was negatively impacted by a ransomware attack. After the attack, 46% of these respondents said they regained access to their data, but some or all of the data was corrupted.

For BEC, in North America and around the world, these easily generated attacks continue to siphon significant amounts of money away from organizations. According to the FBI, in 2022, BEC was responsible for a whopping $2.7 billion in losses – a stunning figure, especially when compared to something like credit card fraud, which we have all heard of and only accounted for $264 million. When it comes to cyber crime, North America, especially the U.S., is a brutal place to be. The FBI reports that Mexico had 1,119 cyber crime victims, Canada had 5,517 victims, and the U.S. alone had 479,181 victims. Within the U.S., California led the pack with 80,666 cyber crime victims within its borders alone, but the next highest, Florida, still had 42,792 victims. Clearly, cybercriminals love to target the U.S.

Typical Organization Profile

The typical organization profile in North America runs the gamut, from small and privately-owned to Fortune 500 organizations, everyone is feeling the impact of cyber crime. While larger organizations typically have more funding for cybersecurity initiatives, they are also more disconnected with respect to employees, making some types of cyber crime easier. It is easier to get a person to purchase gift cards or make wire transfers when the purported requester is not in the same room as the target of the phish.

Cultural Adoption and General Attitudes

There is good news. North Americans are recognizing the threat they face through cyber attacks and are maturing their methods of dealing with them. The shift from simply making people aware of a problem, to embedding security directly into the culture of organizations continues to grow as people realize that simple awareness does not change behavior. Organizations are seriously looking at their overall security culture and working towards improvement. Many organizations are starting to see the parallels between physical safety programs, which include posters, billboards, etc. on how not to be injured while operating machinery or dealing with other physical dangers, and their cyber safety programs. They are beginning to realize that there needs to be a constant and consistent message to employees to help drive home the importance of cybersecurity, just like the messages we use for physical safety. If all goes well, “Check the URL in every message” will be just as familiar to employees as “Wash your hands before returning to work,” or “Hard hats required past this point.”

Fortunately, as the newer, younger generation becomes a part of the workforce, because they have been surrounded by technology since their youth, they often have a better understanding of their role in data protection and cybersecurity than some people who are not fans of technology. This does not mean that these newer generations automatically understand cybersecurity, however, it may be easier for them to grasp their role when properly educated simply because they are already more comfortable with technology.

N. AMERICA	BASELINE	90 DAYS	1 YEAR
1-249	28%	18.5%	4.2%
250-999	30.1%	19%	5.1%
1000+	37.1%	18.4%	5.7%
Average PPP Across All Organization Sizes	33.1%	18.6%	5.1%

Cyber crime is here to stay, and North America is a prime target. Attackers are becoming more advanced as are the tools they use, such as AI. Fortunately, defensive tools and controls are also advancing. However they are not successfully stopping all attacks. It is still critically important for organizations to use a layered defensive approach, one that includes both technical controls and the human layer.

There is no silver bullet to stopping cyber crime. With budgets being cut and economic concerns, it has never been more important for organizations to invest in security controls that require less resources and have the best return on investment. This includes automation wherever possible and efficient workflows, whether with technical tools or non-technical. Year after year, human error, in all its forms, continues to top the list of causes for data breaches and malware infections. However, this problem can be helped dramatically through user education and through the development of effective policies and procedures within organizations.

To defend against BEC attacks, strong policies should be in place that require additional approval(s) for significant funds transfers, or the transfer of sensitive information within the organization, whether it is employee records or intellectual property. This, along with instilling in employees the ability to quickly spot and report potential BEC attacks can go a long way toward fighting these types of attacks.

While ransomware will still continue to claim victims, ensuring that the organization has data loss prevention (DLP) controls in place, regularly testing and securing their backups offline, and educating employees about potential ways that ransomware spreads, can help significantly. In addition, incident response plans that do not include ransomware scenarios are no longer optional.

As training methods continue to mature and new ways to make education and training more relevant and palatable to users become available, employees' ability to protect themselves against cyber crime and scams both at home and at work will continue to improve. Making education relevant to employees in that they understand the risks we are all facing is imperative. It has never been more important to have positive messaging as a part of the education and simulated phishing programs in all parts of the world.

Key Takeaways

- ✓ **While the PPP numbers for North America have increased by approximately one point for the baseline and 90-day marks, the one-year mark is only a fraction of a percentage higher. This conveys the effectiveness of training.** Even when people start at high numbers, such as a 33% click rate, it can still be reduced dramatically, down to about 18.5% in just 90 days. At the end of the year, a 5.4% click rate is still an amazing accomplishment from where it started. This just goes to show that with high-quality training and simulated phishing tests, real improvements can be made to what is often touted as the number one way that data breaches and ransomware infections start.

- ✓ **It is interesting to see that these significant reductions in click rates occur across all sizes of organizations.** The largest organizations made the biggest improvement, dropping from an initial click rate of 37.1% to 5.7% within a year. Of course, that does not mean smaller organizations do not also benefit greatly. For organizations under 250 employees, they also saw drastic reductions, from 28% to 4.2%, the lowest PPP of the organization sizes in North America.

- ✓ **The ability to spot and report phishing emails can be improved significantly in little time among organizations of all sizes when they implement a high-quality security awareness training and simulated phishing program.** These dramatic changes occur regardless of organization size and of their respective industry, underlining the criticality of education in the fight against cyber crime.

UNITED KINGDOM & IRELAND (UK&I)

By Javvad Malik

Most Prevalent Issues

The UK&I region is experiencing a challenging period as they combat multiple crises simultaneously. The global outbreak of COVID-19 has caused significant harm to both public health and the economy, leading to widespread unemployment and declining economic activity. The United Kingdom's departure from the European Union has also posed a significant challenge to the region, bringing with it supply chain issues and significant uncertainties for business owners. Additionally, the ongoing Russia-Ukraine conflict has increased cybersecurity risks and has become an issue of utmost concern to organizations operating in the region.

From a cybersecurity perspective, it's a rather grim picture. Ransomware not only continues, but we are beginning to see just how much of a lasting impact ransomware has on organizations. Government departments and critical infrastructure are increasingly targeted.

Threats to the global supply chain continued to be apparent where attackers accessed target victim organization's networks or systems via third-party vendors or suppliers. Meanwhile, disclosure of the Log4J vulnerability highlighted challenges where weaknesses in IT systems are exploited to deliver successful attacks.

Criminals upped the ante with social engineering attacks by taking advantage of issues, such as government energy grants or tax returns, and were seen to increasingly use SMS and voice-based phishing attacks (smishing and vishing).

The National Cyber Security Centre's (NCSC) annual review states, unsurprisingly, that the most significant threat facing citizens and small organizations continues to be from cyber crime such as phishing, while hacking of social media accounts also remains an issue.

Economic Impact

The true economic impact remains difficult to quantify due to inconsistent and sometimes non-existent reporting metrics. However, from what we do know, the reported costs are just a fraction of the actual figures.

Sophos reports that ransomware attacks are the most prominent, with 13% of UK organizations paying ransom at an average cost of £882,409 ($1.1 million).

But direct costs are not the only thing to consider. After suffering a ransomware attack in October 2020, Hackney Council published its accounts showing the London authority spent over £12 million ($11.7 million) to help it recover from the ransomware attack. Some of the costs included £444,000 ($553,488) on IT consultancy, £152,000 ($189,482) on recovery of the social care system, and £572,000 ($713,052) on the housing register.

Other councils have had it even worse. Gloucester City Council was hit in 2021, and as a result, its museum is unable to access its artifact database to date. While the overall attack is estimated to have cost the council £1 million ($1.2 million), the potential long-term damage to unavailable systems could be far more.

The attacks spotlight the need for the government to invest more in local services, as well as keep a close eye on critical national infrastructure.

Attacks aside, the other big economic impacts are through fines and reporting. Between January 2022 and January 2023, the UK had over 10,000 personal data breach notifications under the General Data Protection Regulation (GDPR).

According to a 2022 National Fraud and Cyber Crime Dashboard, there were 289,330 reports with total losses of £3.7 billion ($4.6 billion). Most of this was fraud as opposed to cyber crime, but the majority of attacks were cyber-enabled.

Typical Organization Profile

Compared to last year, we see the overall PPP across all organizations has taken a jump from 30% to 35.2%. The biggest contributor to this increase are large enterprises with over 1000 employees which went from 32.7% to nearly 40%. There are probably many contributing factors to this increase, ranging from hybrid working models, to staff turnover. However, despite the initial bleak outlook—the silver lining here is that with frequent security awareness training and simulated phishing, the baseline can be drastically reduced to 17.6% in just 90 days and below 5% after a year. Highlighting how effective regular and appropriate training can be regardless of the starting point.

Cultural Adoption and General Attitudes

While threats continue to impact the UK&I, the region is becoming more vigilant about cybersecurity and the importance of educating the workforce and individuals about the role they can play in protecting themselves and their organizations.

Phishing remains the single largest threat vector and is the most popular way ransomware infiltrates organizations. While technical controls are required, the cost and time needed to make these technical changes, especially in underfunded government departments, may take too long. It is imperative that appropriate and timely security awareness and training is rolled out to reduce the risk.

The UK government has spoken about the risks of China for some time now. But with its intent to ban the likes of Huawei and apps like TikTok for official purposes, it seems as if the future of cybersecurity in the region will depend heavily on how China responds. It's also important to remember the continued digital threat Iran and North Korea pose, though admittedly not as sophisticated as China.

Key Takeaways

Cybersecurity remains a huge concern for the UK&I across many fronts. Social engineering is the biggest attack vector, and more needs to be done to promote awareness in organizations and individuals as to the role everyone plays in maintaining security.

With advancements in AI as well as deep fake technologies, we can only imagine how more sophisticated social engineering attacks will become, therefore increasing the need for all organizations across every industry to beef up their defenses.

Three key takeaways are:

- ✓ While ransomware continues to be a menace, **supply chain issues and the geopolitical climate make for an increasingly tricky situation for organizations to stay ahead of.**
- ✓ **The impact of breaches is proving to be more far-reaching in terms of cost and time than previously thought.** Organizations could be paying off the debt of a breach for many years to come. Therefore, stopping attacks becomes an even greater priority.
- ✓ Although some organizations may have a poor starting point, **changing the overall security culture and investing in a solid security awareness and training strategy can provide a rapid return on investment and significantly reduce risk.**

UK & IRELAND	BASELINE	90 DAYS	1 YEAR
1-249	26.3%	18.5%	6.1%
250-999	28%	18.1%	8.1%
1000+	39.6%	17.6%	4.9%
Average PPP Across All Organization Sizes	35.2%	17.8%	5.8%

EUROPE

By Jelle Wieringa

Most Prevalent Issues

The continuing conflict between Russia-Ukraine has impacted societies across Europe. The ENISA Threat Landscape Report 2022 describes an increase in hacktivist activity, its mobilization and aid by nations-state groups during this conflict. Because of the Russia-Ukraine conflict, disinformation has become a favored tool in cyber warfare. We've seen great technological advances in the fields of AI, such as generative AI and machine learning, which make its malicious application more accessible to bad actors. AI-enabled social engineering attacks, disinformation, and deep fakes have become de facto threats that organizations now must protect against.

The most prevalent cyber threats are still ransomware, malware and social engineering. According to the latest "What CEOs talked about" report by IOT-Analytics, economic uncertainties (inflation, recession and interest rates) still dominate what is top-of-mind with organizational leaders. And even though these are very important topics, the continuing threat of cyber crime warrants more attention from the C-suite. Ignoring this leaves the door wide open for threat actors to continue their nefarious activities on unprepared organizations.

Economic Impact

While the economic impact of cyber crime in Europe is hard to accurately determine, it is widely accepted that the impact can have financially devastating consequences.

Under GDPR, organizations that fall victim to data breaches can be forced to pay claim compensation to impacted customers. Legal fees, non-compliance fees, and cost of investigation into the incident can rise into the millions, not to mention the possible reduction in (or cessation of) production, delayed orders and reputational loss with suppliers and customers.

The economic impact of cyber crime applies to all organizations, not just ones that fall victim to a cyber attack. The rising shortage of qualified cybersecurity staff, and the widening skill gap that comes with it, forces organizations to spend more money maintaining security operations. Heavier workloads, unfilled positions and worker burnout all lead to understaffed security organizations. According to the World Economic Forum, the global cybersecurity workforce needs to grow by 65% to effectively defend an organization's critical assets. This leads to an added pressure to the already strained IT security budgets at organizations.

Typical Organization Profile

Unfortunately, this year's PPP data covering Europe shows us that there are many organizations that could improve on their efforts to combat cyber crime. Overall, in Europe, smaller organizations (1–249 employees) score best, with an average PPP across industries before training of 26.5%. Followed by medium (250 – 999 employees) with an industry average PPP of 28% and then large enterprise organizations (1000+ employees) scoring an average of 36.2%.

These results are consistent with those from 2022 showing larger organizations being most vulnerable to cyber attacks. While the efforts of the governing bodies in the European Union continue to update and form new policies like the recent Network and Information Security Directive (NIS2), it does not apply to all organizations, since not all countries are member states of the EU.

Cultural Adoption and General Attitudes

The growing increase in cyber crime throughout Europe, mixed with laws, regulations and legislation put in place to protect organizations and consumers alike, forced many organizations to actively work on their cybersecurity maturity. The ISACA "State of Cybersecurity 2022" indicates that 66% of organizations are actively assessing their cybersecurity maturity level by increasing their assessments to more than once a year.

The increased cost of security, caused in part by the increase in cyber crime and the widening IT security skill gap, forces organizations to "do more with the same, or less." Technology spend alone will not provide a sufficient coverage of the security posture of an organization. Thus, security organizations need to look for other, more efficient and cost effective ways to defend. This movement triggered an increased interest in the importance of a strong security culture, defined as the ideas, customs and social behaviors of an organization that influence its security. Organizations have begun to actively shape their security culture and use this definition as a central and guiding principle to develop their security posture. This gives their existing workforce (e.g. the "people" element within the people-process-technology triad) a more prominent position in their security strategy.

With digital transformation still being a key focus for many European organizations, the top-of-mind approach that security culture brings to security as a business enabler proves alluring for many security organizations. A 2023 report by Deloitte Global Future of Cyber Survey shows that collaboration across cybersecurity, risk management, and business units is critical to neutralizing cyber threats, protecting business value, and sustaining customer trust. This makes security culture an ideal instrument for any organization.

Key Takeaways

Cybersecurity remains one of the biggest concerns to the business continuity of organizations all throughout Europe. With an average PPP of 32.9%, (up from 29.9% in 2022) organizations are still vulnerable to social engineering attacks across all verticals and countries of Europe. It remains vital that we continue our efforts to further increase our resilience and lower our risk posture.

EUROPE	BASELINE	90 DAYS	1 YEAR
1-249	26.5%	19.1%	6.7%
250-999	28%	19.7%	7.6%
1000+	28%	19.4%	6.1%
Average PPP Across All Organization Sizes	32.9%	19.4%	6.5%

Three key takeaways are:

- ✓ **Intensify the efforts to increase the resilience of European organizations.** Geopolitical and economic threats have diverted our attention away from cybersecurity. And with the increase of digitization of organization, the impact of cyber attacks is likely to increase as well.
- ✓ **Focus on educating audiences about the threat and impact of AI-enabled cyber attacks.** With the increased sophistication and developments in machine learning, such as deep fakes and voice biometrics, threat actors now have powerful tools to create misleading content to augment their already dangerous attacks. Because of the increased realism this brings to existing forms of attacks, it is imperative to educate people about these new attack forms.
- ✓ **Increase efforts to build a strong security culture.** The holistic approach it brings to combine security awareness and shape secure behaviors is a proven method to reduce risks and enable business at the same time.

AFRICA

By Anna Collard

Most Prevalent Issues

A region of growth, Africa is rapidly increasing its usage of technology and connectivity. But with growth, prosperity and digitization comes new risks and vulnerabilities that can undermine progress.

According to the KnowBe4 and IDC Report on Cyber Extortion in Africa, nearly 60% of organizations across Southern Africa planned to increase their connectivity and IoT over the next 12 months. This growth unfortunately means a larger attack surface area. The rise of smartphone penetration, online banking mobile payment networks and cryptocurrency is providing criminals across Africa with new targets and avenues of finance. There is a linear relationship between the continent's GDP and cyber crime; as one increases, so does the other. As a result, Africa has had the most exponential growth in cyber crimes over the last few years, particularly among small and medium-sized organizations.

To address rising cyber crime, some African countries have imposed strict regulatory compliance laws, however the majority of African countries have not. Currently, only 15 of 55 African countries have ratified the African Union Malabo Convention, which is a legislative framework to foster data protection and general safeguards against cyber crime; 11 countries have partial laws; and 30 have no meaningful cyber crime laws at all. Governments frequently do not adequately monitor threats, collect digital forensic evidence, and do not prosecute computer-based crime.

As highlighted in last year's report, one of Africa's biggest cybersecurity issues remains the skills shortage. The continent faces a growing lack of certified cybersecurity professionals. Many organizations, agencies and consumers lack cyber awareness and organizations fail to implement basic cybersecurity controls.

We predict that cyber extortion groups and cyber crime syndicates will shift their attention away from the more mature nations like the U.S. towards other regions, including emerging economies like Africa where industries have a large cyber dependency but lack the resources to adequately prevent, remediate or prosecute cybercriminals.

Economic Impact

It is difficult to estimate how much cyber crime really impacts the African economy as incidents and financial impact are not officially disclosed. Most cybersecurity incidents go unreported.

As stated in the 2022 research report by the Global Initiative against Transnational Crime, "The Downside of Digital Revolution," "the spread of digital technology has led to the formation of new organized cybercriminal networks, which now rank among the top threats to African enterprises and is estimated to cost the region's economy billions of dollars per year."

The South African Council for Scientific and Industrial Research (CSIR) expects an increase in cyber attacks on government departments and critical infrastructure, impacting not just private sector organizations but societies and countries' economies. This was the case with the ransomware attack against South Africa's Transnet, a state-owned ports authority enterprise, in 2021. The incident impacted the country's critical maritime infrastructure and undermined South Africa's economic recovery from the COVID-19 pandemic. Attacks against critical infrastructure can result in devastating economic consequences that go beyond the direct losses experienced by the affected organization.

Typical Organization Profile

Africa is a region of considerable geographic, linguistic, cultural and economic diversity. When delving into the state of cybersecurity on the continent, this diversity must be taken into account and can, to some extent, explain the wide variety in the security maturity across different countries and sectors.

Africa's potential as a growth market for business remains underestimated and misunderstood. More than 400 companies in Africa earn annual revenues of $1 billion or more; and they are, on average, faster growing and more profitable than their global peers.

This year's KnowBe4 Phishing By Industry Benchmark Report is based on a total of 337,937 phishing simulation tests delivered across 412 African organizations. Of these, 58% of the organizations are small (1-249 employees), 26% are medium (250-999 employees) and 16% are large organizations (1000+ employees). Most of the data set is derived from organizations in South Africa, followed by Kenya, Nigeria and Botswana.

In Africa, the initial baseline phishing security test results are at an average of 32.8%. That means that before receiving any training, one out of three employees is likely to click on a suspicious link or email or comply with a fraudulent request. Overall PPP varied greatly across African sectors and countries.

Cultural Adoption and General Attitudes

Many African countries face unique and complex socioeconomic landscapes, and the challenges faced internationally are compounded even further on a local level.

For example, South Africa is one of the most unequal countries in the world, resulting in a high rate of poverty and unemployment rate, and increase in its crime rate.

With a median age of just 19.7 years, Africa has the youngest population in the world. And Africa's growing youth is demanding access to global connectivity while driving technology adoption and digitalization: mobile smart device ownership is growing exponentially, social media use is increasing and so is the adoption of cryptocurrencies. According to the International Monetary Fund (IMF), sub-Saharan Africa is the only region in the world where nearly 10% of its gross domestic product is generated through mobile money. People across the continent depend on their mobile devices for remittances, salaries, payments, bills and shopping.

AFRICA	BASELINE	90 DAYS	1 YEAR
1-249	30%	25.2%	9%
250-999	29.4%	22.7%	10.5%
1000+	33.3%	19.3%	5.7%
Average PPP Across All Organization Sizes	32.8%	20.5%	6.6%

KnowBe4's Africa End User Cyber Awareness Survey 2023 uncovered that:

- 71% of the respondents from eight African countries use their mobile data to access the internet, while 63% use their mobile phone for mobile banking and payments
- 68% of the respondents were concerned about cyber crime, however, many lacked some very basic understanding of what type of threats they are exposed to
- 57% of respondents did not know what a ransomware attack is. 21% have experienced a social engineering attack over the phone (vishing) and 32% have lost money because they fell victim to a scam
- 36% said they had fallen victim to a crypto scam, and 57% knew people who had been victims of such scams

Based on a 2022 survey run by KnowBe4 and ITWeb in South Africa, the number one reason for people making security mistakes, such as clicking on a phishing email, was cited as lack of awareness or training (52%), followed by distraction, multitasking and cognitive overload (38%).

Key Takeaways

✓ **The lack of prioritization and investment for cybersecurity amongst both businesses and governments needs to be addressed.** Raising awareness among policy makers and assisting in capacity building efforts should be prioritized.

✓ **Public-private partnerships are needed to assist Africa in its cybersecurity challenges.** Businesses in this region often cannot afford even the most basic security controls. Those that can invest struggle to find those who have cybersecurity skills. The private sector, particularly financial services sectors, possess human capital, infrastructure, capabilities, and expertise in cybersecurity that governments lack.

✓ **Organizations training employees and their customers about security best practices remains critical.** Governments and education institutions need to invest in expanding their security professional capacity as well as making cybersecurity awareness a life skill for every youth entering the workforce.

Africa's potential as a growth market for business remains underestimated and misunderstood. **More than 400 companies in Africa earn annual revenues of $1 billion or more**...

...and they are, on average, faster growing and more profitable than their global peers.

SOUTH AMERICA

By Rafael Silva

Most Prevalent Issues

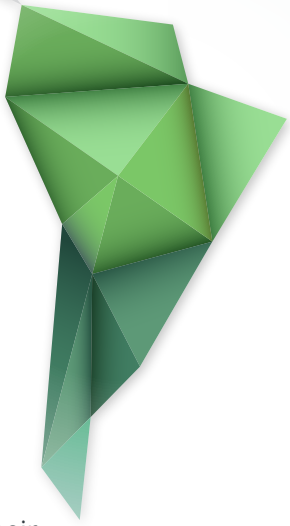
Ransomware, phishing and mobile phone theft are among the top threats of 2022 for both organizations and individuals in Latin America. A report from the Brazilian Agency of Communication (Anatel) revealed that in Sao Paulo, Brazil alone, 553 corporate and personal cell phones are stolen daily.

Latin American organizations experienced a significant increase in ransomware attacks in 2022; however, most organizations have not paid to regain access to their data. According to a study titled "The State of Ransomware 2022" conducted by cybersecurity firm Sophos, 55% of the 200 surveyed organizations in Brazil were targeted by ransomware attacks last year. In comparison, the reported percentage in 2020 was 38%.

In 2022, phishing attacks continued to be a major concern for Latin American organizations and individuals. The increase in remote work and back-to-office due to the COVID-19 pandemic created new opportunities for cybercriminals to exploit vulnerabilities and target unsuspecting users. Cybercriminals consistently pursue critical and sensitive data, such as login credentials, financial information, and personal identification details. This year, they have significantly increased their focus on cryptocurrency phishing, with a 40 percent growth in just one year, as reported by Kaspersky.

Account takeover attacks that are specifically focused on social media and cryptocurrency have substantially increased across Latin America. This is primarily because social media and cryptocurrencies are rapidly gaining notoriety amongst fraudsters and attackers alike. There will be a marked rise in the number of cybercriminals who attempt to gain unauthorized access to social media accounts and cryptocurrencies to use them to perpetrate further acts of fraud and deception.

Economic Impact



Ransomware continues to have a major financial impact on Latin American organizations, causing significant losses. In 2022 alone, a Brazilian e-commerce company fell victim to a ransomware attack, resulting in a staggering loss of $183 million. This number has been on a consistent upward trend year after year.

In 2022, Brazil began imposing fines for privacy violations in order to comply with the General Data Protection Law (LGPD). It is estimated that millions of dollars will be paid to the National Data Protection Authority (ANPG) due to security breaches and privacy violations.

As the digital landscape continues to evolve, Latin American governments and organizations must prioritize investments in cybersecurity and collaborate to develop robust strategies to prevent future attacks and mitigate their financial consequences.

Typical Organization Profile

Some industries are better than others at promoting a security culture, with the Technology and Insurance industries performing better than the Healthcare & Pharmaceutical, Retail & Wholesale industries. There is significant room for improvement in South America, as indicated by the high PPP across the board. In particular, both small organizations (1-249 employees) and enterprise organizations (1000+ employees) have high baseline PPP compared to most other regions around the world.

Alongside its standard yearly phishing statistics per industry, KnowBe4 also puts together an annual security culture report. This data provides interesting viewpoints and context about different sectors. The Hospitality, Education, and Construction industries recorded the lowest scores, only reaching (70), indicating less developed security cultures. The Retail and Wholesale sectors didn't fare much better, registering a slightly higher score of (71). However, industries such as Technology and Insurance, each scoring (76), showcased more advanced and evolving security cultures.

South America with a (73) overall score, has been facing a significant challenge in terms of security culture. However, it is noteworthy that Chile (71), Mexico (77), Colombia (77), and Brazil (72) stand out with high scores, indicating a much higher level of security culture than the other countries.

Organizations operating in South America must take proactive measures to improve their security culture, given the prevailing low scores in most countries. It is crucial to prioritize security measures to ensure the safety and protection of people and assets, as security threats evolve and become more sophisticated.

Cultural Adoption and General Attitudes

Cultural adoption and general attitudes play a critical role in cybersecurity in Latin America. In recent years, the region has experienced a significant increase in cyber attacks. This increase highlights the importance of fostering a positive security culture to increase the security posture for both organizations and individuals.

Cultural adoption refers to the degree to which people and organizations adopt and use cybersecurity practices and technologies. In Latin America, there is a general lack of awareness and understanding of cybersecurity threats, which has resulted in a low level of cultural adoption.

However, attitudes towards cybersecurity are changing in the region, as more people become aware of the risks associated with cyber attacks. Governments and businesses are starting to invest more in cybersecurity initiatives, and individuals are beginning to take steps to protect themselves online.

Sound and useful initiatives are being created, like the national legislation of Costa Rica, which has been revised to provide legal protection for its cyber society, thereby enabling individuals to report violations that were previously not addressed by the law.

Key Takeaways

- ✓ **The growing issue of mobile phone theft in Latin America in 2022 underscores the need to protect sensitive data stored on mobile devices.** Individuals should use strong passwords or biometric authentication, enable remote wiping capabilities, and install security apps to safeguard their devices. Moreover, governments and law enforcement agencies should work together to tackle organized crime related to mobile phone theft and create public awareness campaigns to inform citizens about the risks and preventive measures.
- ✓ **Implementing advanced cryptographic techniques, two-factor authentication (2FA), and hardware keys significantly bolster the protection of your digital assets** to make it increasingly difficult for cybercriminals to succeed. As a convenient and easy-to-use option, hardware keys can be easily integrated into a variety of systems and platforms, making it an accessible choice for users of all technical backgrounds.
- ✓ **Investing in security awareness is crucial for organizations as it helps foster a strong security culture,** empowering employees with knowledge and tools to identify, avoid, and report potential cyber threats, ultimately minimizing the risk of security breaches. By providing comprehensive training and ongoing education, organizations can significantly reduce the likelihood of human error or negligence.

S. AMERICA	BASELINE	90 DAYS	1 YEAR
1-249	34%	23%	6.4%
250-999	27.7%	25.8%	10.2%
1000+	49.5%	18.7%	5.1%
Average PPP Across All Organization Sizes	41.1%	21.3%	6.9%

ASIA

By Jacqueline Jayne

Most Prevalent Issues

The 2023 IBM threat intelligence index reported that "the Asia-Pacific region faced the most cyber attacks during 2022 and that the region accounted for 31% of all incidents monitored in 2022."

Japan was the frontrunner with Emotet malware attacks in 2022. The Japanese National Police Agency reported that the number of cyber crimes hit an all time high in 2022 with 12,369 cases (up from 160 in 2021).

Reports across the region involving extortion are on the rise via business email compromise (BEC) and distributed denial-of-service attacks (DDOS).

According to the 2022 Thales Data Threat Report, APAC Edition, 45% of respondents reported an increase in the number of attacks and interestingly, 77% said they would trust their organization with their own personal data. As with the rest of the world, data breaches are prevalent with 50% of respondents reported that they have experienced a data breach and 32% of those breaches occurred in 2022.

As we can see the overall Phish-prone Percentage across all organization sizes is close to the global percentages. It is encouraging to see the larger organizations with 1000+ employees leading the way by scoring better than the overall regional percentages. This could be attributed to the fact that the larger organizations have an IT department and more than likely a cybersecurity team. These two factors tend to result in a greater understanding of the cyber threat landscape and therefore more of a focus on the need to upskill end users to make better decisions.

Economic Impact

In The State of Financial Crime 2022: Key Takeaways for Asia Pacific Firms, the UN Office on Drugs and Crime (UNODC) reported a 600% rise in cyber crimes in the region.

From a Southeast Asia perspective (Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam), PWCs Global Economic Crime and Fraud Survey 2022 reported that two thirds of incidents involved employees and of those, 34% had lost less than $50,000, 10% lost between $1 million and $5 million, while 9% lost more than $5 million.

Typical Organization Profile

The Asia-Pacific region has a population of 4.3 billion. With over 10 countries, it is one of the world's most diverse regions and home to economies that are at the top of digital and societal developments worldwide. Organizational profiles will be shared across sole ownership, small to medium organizations and enterprise organizations all with the same challenges as every organization globally.

Cultural Adoption and General Attitudes

We have looked for general observations across the entire Asian region and found, via the 2022 Thales Data Threat Report, APAC Edition, that the era of remote working will continue, as will the risks associated with it. Security risks of remote employees continued in 2022 with 33% of respondents "very concerned" and 47% "somewhat concerned."

Key Takeaways

There is still much work to be achieved in relation to the following:

- ✓ There is strength in numbers, and the private and public sectors will need to collaborate across the region
- ✓ All organizations need consistent guidance and support regardless of their size, as they are all a target
- ✓ Implementing ongoing relevant and engaging security awareness training supported with ongoing simulated phishing emails will help bring the desired outcomes

As we can see the overall Phish-prone Percentage across all organization sizes is close to the global percentages. It is encouraging to see the larger organizations with 1000+ employees leading the way by scoring better than the overall regional percentages.

ASIA	BASELINE	90 DAYS	1 YEAR
1-249	32.6%	20.9%	7.3%
250-999	33.2%	19.6%	7.4%
1000+	28.8%	13%	6%
Average PPP Across All Organization Sizes	30%	14.9%	6.5%

AUSTRALIA AND NEW ZEALAND

By Jacqueline Jayne

Most Prevalent Issues

As with previous years, phishing reigned supreme as the most successful attack vector for cybercriminals, with their highest success using ransomware, fraud, financial and identity theft and business email compromise (BEC).

The Australian Cyber Security Centre (ACSC) Annual Cyber Threat Report, received over 76,000 cyber crime reports, or one report every 7 minutes. This is a 13% increase from the previous year, with 67,500 reports.

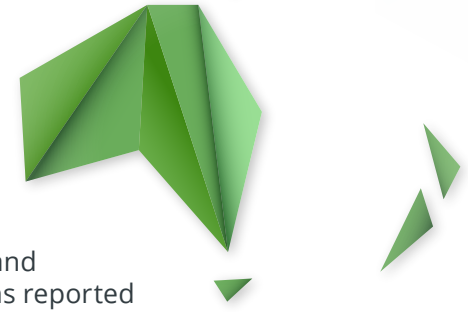
In the period July 1, 2022 to December 31, 2022, the Office of the Australian Information Commissioner (OAIC) shared in their notifiable data breach report that notifications were up 26%, with the top five sectors to notify data breaches being Health service providers with 71 reports, Finance (including superannuation) with 68 reports, Insurance with 42 reports, Legal, Accounting and Management Services with 37 reports and Recruitment agencies with 35 reports. Contact information remains the most common type of personal information involved in breaches.

New Zealand

According to CERT NZ, in 2022, 8,160 incidents were reported, an 8% decrease from 2021. Individuals, small organizations and large organizations from all over New Zealand submitted incident reports.

When they looked at the top incidents, phishing and credential stuffing increased 16% from 2021, scams and frauds increased 15% from 2021, and unauthorized access has increased by 23% from 2021. Interestingly, malware reports decreased by a record 88% since 2021, with the primary reason being the overwhelming amount of FluBot malware reported in that year.

Privacy and data retention has emerged as a major issue with a recent high profile data breach that saw over one million New Zealand records being obtained by cybercriminals.



Economic Impact

AUSTRALIA

According to the Australian Competition and Consumer Commission (ACCC), Australians reported losses of a staggering AUD $526,292,444 to scams in 2022 (up from AUD $323 million in 2021). Remember that these are only the reported scams to the ACCC, with the potential for the total to be significantly higher.

From a business perspective, the ACSCs Annual Cyber Threat Report also noted that the average cost per cybercrime report increased to over AUD $39,000 for small businesses, AUD $88,000 for medium businesses and over AUD $62,000 for large businesses. Financial losses due to BEC increased to over AUD $98 million, with Australian businesses self-reporting an AUD $33 billion loss due to cybersecurity incidents nationwide.

AUSTRALIA & NEW ZEALAND	BASELINE	90 DAYS	1 YEAR
1-249	27.1%	21.1%	6.3%
250-999	30.9%	19.9%	7.7%
1000+	41.1%	15.3%	5.4%
Average PPP Across All Organization Sizes	34.8%	17.8%	6.4%

NEW ZEALAND

New Zealand banks report customers lost a combined total of NZD $183.5 million to scams this year (2022)—an increase of 40% from last year (2021).

According to the 2021/2022 Cyber Threat Report from the National Cyber Security Centre, the National Cyber Security Centre prevented NZD $33 million worth of harm to New Zealand's nationally significant organizations. Plus, "23% of the 350 recorded incidents showed indications of a connection to criminal or financially motivated actors."

Typical Organization Profiles

AUSTRALIA

As of June 30, 2022, 2,569,900 organizations were operating in Australia, dominated by small and medium enterprises (SMEs). Breaking down the SMEs to 97.5% small organizations (0-19 employees) and 2.3% as medium organizations (20-199 employees), with the remaining 0.2% of organizations in Australia having more than 200 employees as defined by the Australia Bureau of Statistics.

NEW ZEALAND

As of Feb 2022, New Zealand had 592,700 enterprises across the region. Small enterprises hold the majority with 97.13% and have between 0 and 19 employees, 1.85% with 20 to 49 employees, 0.57% with 50 to 99 employees and 0.45% with 100+ employees.

Cultural Adoption and General Attitudes

AUSTRALIA AND NEW ZEALAND

Data breaches hit the headlines in 2022, with millions of Australians' and New Zealanders' data being caught up in significant incidents. This has seemingly had little impact on how IT decision makers view the risks to their organizations. In our most recent survey of that cohort in the region, we found that 37% of Australian and 32% of New Zealand IT decision makers say they are concerned about phishing as a risk to their organization. Considering the extremely high success rate for cybercriminals using phishing attacks to gain entry to organizations, this percentage should be much higher.

Key Takeaways

When we consider the responses to who is responsible for cybersecurity, it's clear that IT leaders and organizations across Australia and New Zealand are looking for guidance regarding security issues. There is still much work to be achieved in relation to the following:

- ✓ Educating everyone about basic cyber hygiene must be top of the agenda to bring awareness
- ✓ Providing consistent guidance and support to all organizations regardless of their size, as they are all a target
- ✓ Implementing ongoing relevant and engaging security awareness training supported with ongoing simulated phishing emails will shift us to the desired outcomes

KEY TAKEAWAYS

THE VALUE OF NEW-SCHOOL SECURITY AWARENESS TRAINING

The results from all three phases of the study reveal several conclusions:

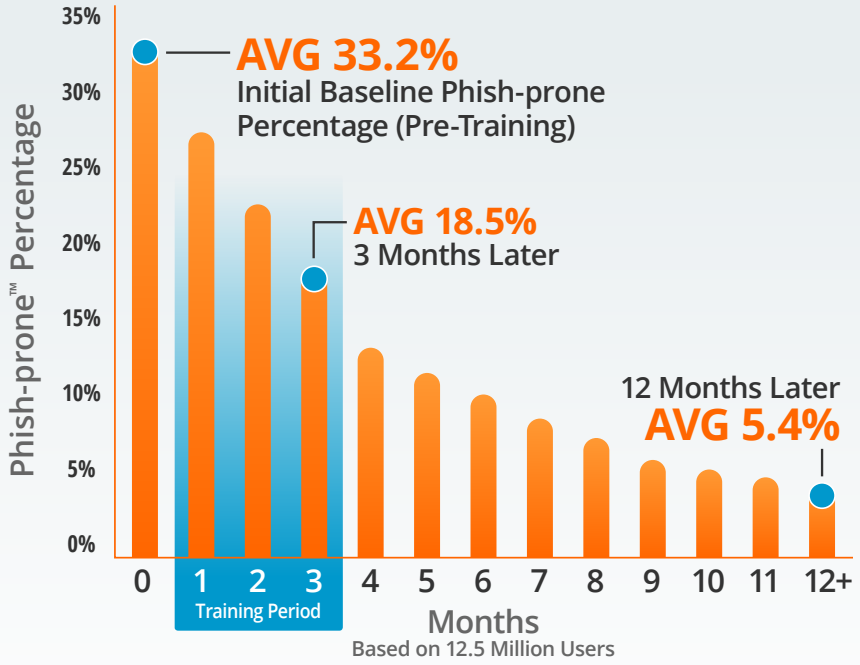
- **Every organization is at serious risk without new-school security awareness training.** With an average industry baseline PPP of 33.2%, organizations could be exposed to social engineering and phishing scams by a third of their workforce at any given time.
- **Any organization can strengthen security through end-user training in as little as three months.** The power of a good training program is to set up a consistent cadence of simulated phishing and social engineering education in a rapid timeframe.
- **An effective security awareness training strategy can help accelerate results for all organizations.** The struggle of some enterprise leaders to successfully implement security training effectively across the organization is not surprising. Leaders can set themselves up for success by assessing their goals and plotting an organizational strategy before rolling out training.

EXECUTIVE TAKEAWAYS

Security and risk management leaders need to understand that in order to favorably change overall security behaviors within their organizations, their programs must have:

- A clearly defined and communicated mandate
- A strong alignment with organizational security policies
- An active connection to overall security culture and human layer of security
- The full support of executives

Without consistent and enthusiastic executive support, raising security awareness within an organization is certain to fail.

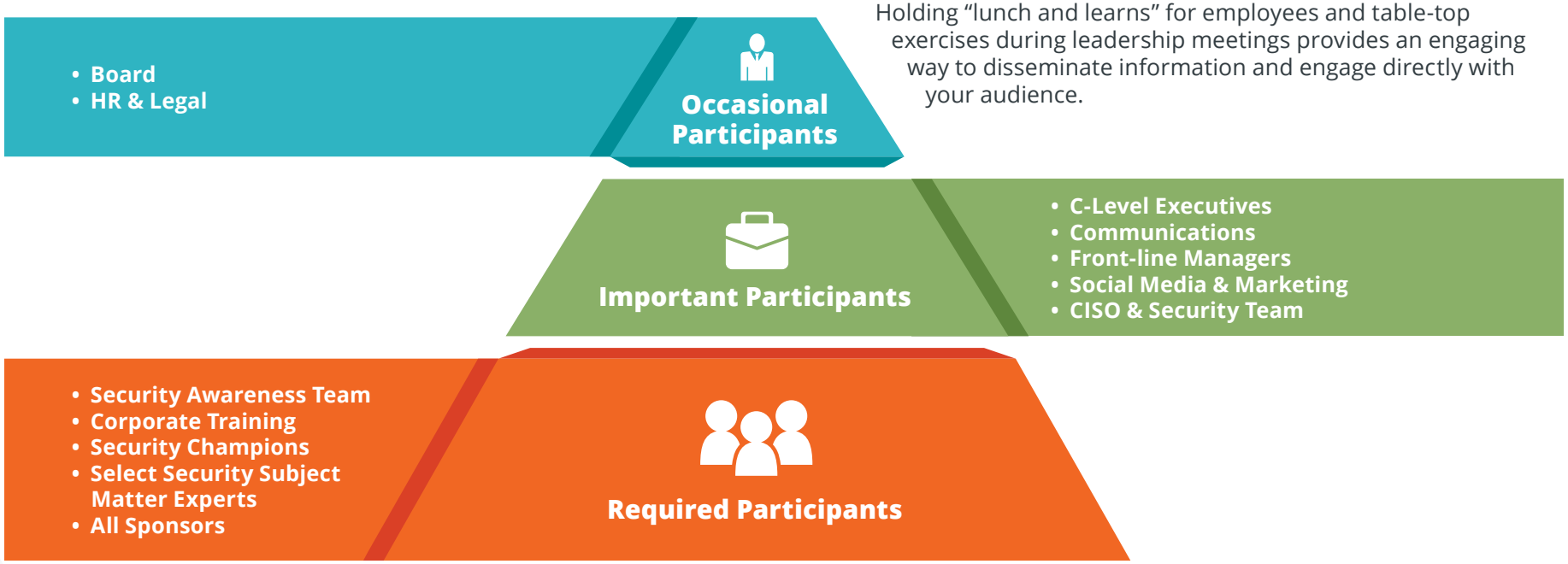


Source: 2023 KnowBe4 Phishing by Industry Benchmarking Report

Note: The initial Phish-prone Percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation. Subsequent time periods reflect Phish-prone Percentages for the subset of users who received training with the KnowBe4 console.

Security and risk management executives can ensure the success of their programs by:

- **Fostering a Security Culture:** The human element is the most critical part of an organization's security infrastructure. All employees should understand what their role and responsibility is to protect the organization and themselves from a cyber attack. Security culture, as defined by KnowBe4, is the ideas, customs and social behaviors of an organization that influence their security. Executives need to ensure they are fostering an environment that is security ready by investing in both the focus of their security awareness training program and the readiness level of their users.
- **Role Modeling:** If you expect your organization to do the right thing, you must lead them accordingly. Executives should be active participants in all aspects of driving security awareness throughout their organizations, which includes participating in the same security awareness training requirements that the rest of their employees are expected to complete.
- **Engaging a Pro:** Security awareness content is unlike any other. Expertise goes into not only the design of the content, but also ensuring that the content leads to a positive learning experience and ultimately favorable secure behavior change. In an industry where content is king, the recommendation is to align with a vendor that can provide you with multiple flavors, versions and varieties that appeal to all different learning styles. Forcing your audience into a singular learning style limits the experience, material consumption and overall retention. It may be tempting to leverage your internal training organization to lead this program development, or to partner with a vendor that provides a one-size-fits-all approach. Both options will lead to a long-term inability to shape your audience's security-related thoughts and actions.
- **Thinking Like a Marketer:** In parallel with content and simulated phishing campaigns, add frequent and relevant messaging in the form of ancillary supporting materials (posters, digital signage, newsletters, etc.) and find opportunities during cross-business meetings and presentations to reinforce the big takeaways. Holding "lunch and learns" for employees and table-top exercises during leadership meetings provides an engaging way to disseminate information and engage directly with your audience.



- **Mobilizing a Security "Culture Carrier" Program:** Most security and risk programs lack the necessary resources to properly engage a global organization. Security "culture carrier" programs go by many different names, such as "Security Champions," "Security Ambassadors," "Security Liaisons," "Security Influencers," and more. Regardless of what you call it, a culture carrier program provides an organizationally dispersed team of advocates who can reinforce security messaging and learning at local levels. The responsibility factor is also in play here. Many employees believe that driving better security behavior is someone else's responsibility. By enrolling local influencers either through manager nomination or volunteering, you create a network of security go-to-people who can relate with local communities and start to help shape the overall security culture.
- **Adding Simulated Phishing Tests:** As we've shared through this research, by adding frequent simulated phishing campaigns to your overall security awareness program, you will increase your employee's resilience to being compromised, and also raise their ability to spot a suspicious email.
- **Increasing Frequency:** At all times, you are either building strength or allowing atrophy. Our research shows that most organizations not seeing favorable behavior change were limiting the frequency of their program (both content and simulated phishing) to annual, twice annual or quarterly. By testing so infrequently, you are essentially conducting moment in time baseline tests that you cannot meaningfully compare. The recommendation is to provide your audience monthly content and simulated phishing campaigns (twice monthly for high risk targets). There needs to be a regular cadence for the appropriate conditioning to take place and for behavior change to take hold. Security and risk management executives may fear that this frequency is too much, but in actuality, it is helping build the right level of security muscle memory to combat the aggressive and ever-changing attack strategies of today and tomorrow. Additionally, human detection and response is the real-time coaching component of security awareness and focuses on detecting and responding to risky human security behavior as it happens. It reinforces security awareness training and allows organizations to gain insight into security risks by tracking risky user activity.
- **Hiring the Right People:** Security awareness programs are often led by security practitioners who were either chosen to take on the task no one wanted or had extra time to deal with this "training" stuff. However, managing a program like this requires a certain level of experience and expertise. Target creative candidates who are aware and well versed in how to drive organizational development and behavior change through learning.
- **Defining Objectives:** Determine upfront what the success criteria of your program are and how you will measure against them. Otherwise it is impossible to measure your program's effectiveness and determine inherent value.
- **Measuring Effectively:** The use of metrics that reinforce desired behaviors is important to help protect systems, employees and data. Don't fall into the trap of selecting too many measurement criteria; that only leads to measuring irrelevant areas and/or under delivering on promised organizational outcomes. Employing measurable data and training that can be frequently quantified and qualified is paramount. Also, ensure that program metrics are connected not only to overall organizational security objectives, but corporate objectives.
- **Motivating Employees:** Be intentional and consistent in how you use positive and negative reinforcement to encourage your audience to complete required training, adhere to security policies and demonstrate ongoing, favorable, secure behavior. Using motivators increases accountability and the employees' overall role in driving a more secure culture.

GETTING STARTED

KnowBe4 is helping tens of thousands of IT pros like you to improve their cybersecurity in fields like finance, energy, healthcare, government, insurance and many more.

With KnowBe4, you have the best-in-class phishing simulation and training platform to improve your organization's last line of defense: **Your Human Firewall**.

We enable your employees to make smarter security decisions, every day. We help you deliver a data-driven IT security defense plan that starts with the most likely "successful" threats within your organization—your employees. The KnowBe4 methodology really works. Ready to get started?

4 STEPS FOR PHISHING YOUR USERS

It's clear that organizations can radically reduce vulnerability and change end-user behavior through testing and training. Take these steps to get your organization on the right track to developing your human firewall.

1. **Conduct Baseline Testing:** Conducting a baseline test is the first step in demonstrating the need for security awareness training to your senior leadership. This baseline test will assess the Phish-prone Percentage of your users. It's also the necessary data to measure future success.

2. **Train Your Users:** Use on-demand, interactive and engaging computer-based training instead of old-school PowerPoint slides. Awareness modules and videos should educate users on how a phishing or social engineering attempt could happen to them.

3. **Phish Your Users:** At least once a month, test your staff to reinforce the training and continue the learning process. You are trying to train a mindset and create new habits. It takes a while to set that in motion. Simulated social engineering tests at least once a month are effective at changing behavior.

4. **Measure Results:** Track how your workforce responds to both training and phishing. Your goal is to get as close to zero percent PPP as possible.

PLAN LIKE A MARKETER, TEST LIKE AN ATTACKER

While every leader can reduce risk by targeting employee PPP, there are several best practices that can bring about lasting change.

Use real-world attack methods

Your simulated phishing exercises must mimic real attacks and methodologies. Otherwise, your "training" will simply give your organization a false sense of security.

Don't do this alone

Involve other teams and executives, including Human Resources, IT and Compliance teams, and even Marketing. Create a positive, organization-wide culture of security.

Don't try to train on everything

Decide what behaviors you want to shape and then prioritize the top two or three. Focus on modifying those behaviors for 12-18 months.

Make it relevant

People care about things that are meaningful to them. Make sure your simulated attacks impact an employee's day-to-day activities.

Treat your program like a marketing campaign

To strengthen security, you must focus on changing behavior, rather than just telling staff what you'd like them to know. Give them the critical information they need, but stay focused on conditioning their security reflexes so your workforce becomes an effective last line of defense.

CONTRIBUTORS

Anna Collard, Senior Vice President of Content Strategy & Evangelist for KnowBe4 Africa.

Joanna Huisman, Senior Vice President of Strategic Insights and Research at KnowBe4.

Jacqueline Jayne (JJ), Security Awareness Advocate for the Asia-Pacific region for KnowBe4.

Erich Kron, Security Awareness Advocate at KnowBe4.

Javvad Malik, Lead Security Awareness Advocate at KnowBe4 based in London.

Rafael Silva, Senior Director of Information Security for KnowBe4.

Jelle Wieringa, Security Awareness Advocate for Europe, the Middle East and Africa (EMEA) EMEA for KnowBe4.

ABOUT KNOWBE4

KnowBe4 is the provider of the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the problem of social engineering through a comprehensive new-school security awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

ADDITIONAL RESOURCES

Free Phishing Security Test
Ready to start phishing your users? Find out what percentage of your employees are Phish-prone with your free phishing security test.

Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad actors do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234)
www.KnowBe4.com | Email: Info@KnowBe4.com