KnowBe4

2023 PHISHING BENCHMARKING

Report For North America

By **Erich Kron**, Security Awareness Advocate at KnowBe4

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.

With geopolitical changes affecting the dynamics of cyber crime, organizations ought to reduce their single biggest cyber risk: the human element. Cybercriminals are counting on your employees lacking the necessary knowledge, attention and energy to trick them into making bad security decisions. One over-stressed, distracted, or daydreaming 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?

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.

To assist geographical regions with evaluating their PPP and understanding the implications of their ranking, KnowBe4 conducts an annual study to provide definitive Phish-prone benchmarking across small, medium and large organizations by geographical regions. This guide provides an overview of the key findings for North America.

2023 Global Phishing By Industry Benchmarking Study

Though every organization would like to understand how they measure against the rest in their industry and geography, the comparison requires robust data coupled with a scientific, proven method to produce valid results. 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 and seven geographic regions.

All organizations were categorized by size and geographical region. 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

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.

2023 International Phishing Benchmarking Results By Geographical Regions

	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+**
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%**		

Most Prevalent Issues Facing North America

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.

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.

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%

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.