KnowBe4

# Phishing Benchmarking Report

## NORTH AMERICA 2025

# Shining a Light on Human Risk and Reducing Phishing Click Rates

## Reducing phishing risk is central to effective human risk management (HRM).

Every successful phishing attack is reliant on a trusted person to carry out a specific action, such as clicking on a hyperlink. If a phishing email gets through technical defenses, it will still fail if the recipient subsequently reports, deletes or does not engage with it.

While enhancing their technical defenses with an AI-powered anti-phishing product, organizations can also significantly reduce their phishing risk through best-practice security awareness training (SAT).

The first step to any effective risk mitigation strategy is to understand your organization's risk profile and how it compares against others of the same industry, organizational size and geographical region. Next, identify how susceptible your organization actually is to phishing risk — and, in particular, who might interact with a phishing email. These insights will enable you to deliver timely and personalized security, such as bespoke training programs and real-time coaching.

KnowBe4's Phishing By Industry Benchmarking Report provides the initial step in this strategy. For this year's report, we analyzed a total of 67,718,305 phishing simulations across 14,508, 441 users in 62,460 organizations over a three-year period to show the Phish-prone™ Percentage (PPP) for organizations across 19 industries and seven geographical regions.

**This guide provides an overview of the key findings for North America.**

# How We Calculate Phish-prone Percentage

The PPP is the percentage of employees within an organization likely to fall for social engineering or phishing attacks. Elsewhere, you might see it described as “phishing simulation click rate.”

## Phase One

### Baseline Phishing Security Test Results

Before any KnowBe4 training takes place, we send an initial phishing simulation. This is used to identify risks and calculate an organization’s baseline PPP.

## Phase Two

### Phishing Security Test Results Within 90 Days of Training

Employees receive KnowBe4’s security awareness training. Another simulation is sent to recalculate the organization’s PPP and measure the effectiveness of the training program.

## Phase Three

### Phishing Security Test Results After One Year+ of Ongoing Training

After 12 months of KnowBe4’s security awareness training, the PPP is calculated again to further quantify the training program’s effectiveness.

# 2025 International Phishing Benchmarks

Across the different regions, the highest baseline PPPs were found in South America (39.1%), North America (37.1%), and Australia & New Zealand (36.8%).

Organizations with 1,000+ employees based in Australia and New Zealand were the most phish prone globally, with 44.6% clicking on simulated phishing hyperlinks. The lowest risk was found in small organizations (1-249 employees) in both Asia and the United Kingdom & Ireland, with one-quarter (24.3%) of employees clicking links.

**All regions achieved average improvement rates over 80%, with North America the highest (89.5%) and South America a close second (88.9%).**

| | | Phase One – Baseline | | | Phase Two – 90 Days | | | Phase Three – 1 Year+ | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Organization Size** | **1-249 Employees** | **250-999 Employees** | **1,000+ Employees** | **1-249 Employees** | **250-999 Employees** | **1,000+ Employees** | **1-249 Employees** | **250-999 Employees** | **1,000+ Employees** |
| **Region** | **North America** | 26% | 31.1% | 42% | 21.1% | 21.2% | 18.5% | 3.7% | 3.9% | 4.1% |
| | | **TOTAL: 37.1%** | | | **TOTAL: 19.6%** | | | **TOTAL: 3.9%** | | |
| | **Africa** | 27.9% | 30.1% | 35.8% | 24.9% | 28% | 20% | 2.2% | 9.2% | 5.1% |
| | | **TOTAL: 34.9%** | | | **TOTAL: 21.1%** | | | **TOTAL: 5.3%** | | |
| | **Asia** | 24.3% | 27.6% | 29% | 18.9% | 19.1% | 17.6% | 5.1% | 4.5% | 5.4% |
| | | **TOTAL: 28.6%** | | | **TOTAL: 17.9%** | | | **TOTAL: 5.2%** | | |
| | **Australia & New Zealand** | 25% | 29.2% | 44.6% | 23.2% | 23% | 16.6% | 3.9% | 6.1% | 4.7% |
| | | **TOTAL: 36.8%** | | | **TOTAL: 19.9%** | | | **TOTAL: 4.9%** | | |
| | **Europe** | 24.9% | 26.7% | 34.9% | 20.7% | 21.6% | 20.5% | 3.9% | 4.4% | 5.3% |
| | | **TOTAL: 32.5%** | | | **TOTAL: 20.7%** | | | **TOTAL: 5%** | | |
| | **South America** | 30.2% | 26.3% | 42.8% | 23.3% | 23.1% | 16.9% | 3.4% | 5.1% | 4.5% |
| | | **TOTAL: 39.1%** | | | **TOTAL: 18.2%** | | | **TOTAL: 4.5%** | | |
| | **United Kingdom & Ireland** | 24.3% | 28.5% | 36% | 22.1% | 22.1% | 17.1% | 4% | 4.1% | 5.3% |
| | | **TOTAL: 32.9%** | | | **TOTAL: 19%** | | | **TOTAL: 4.8%** | | |

# North America | *By Erich Kron*

It's never pleasant to see the initial PPP for the region; however, it is reassuring to see how quickly the numbers can be reduced. This is a testament to the need for a robust SAT program.

This year seemed to be especially challenging for larger North American organizations, which had a pretty significant initial click rate of 42%. Even mid-size organizations seem to struggle with an initial click rate of 31.1%, while smaller organizations were reasonably close to other regions at just shy of 26%.

Put into perspective, this means that in large organizations, more than two out of every five users clicked on simulated phishing attacks.

It's no secret that phishing emails are one of the top threats to organizations across industries. With click rates this high, it is clear that employees are not likely to be looking for social engineering attacks without some guided direction from the organization.

The real success story is how quickly these numbers can improve. Large organizations showed small and medium peers how it's done — with that 42% click rate plummeting to 18.5% after only 90 days of best-practice SAT. While small and medium organizations also showed remarkable reductions, the large organizations took home the prize at the 90-day mark.

Continuing with the trend of plummeting click rates, across all organizations, the average PPP after at least one year of training was 3.9%. This finding underscores the significant improvement that SAT can effect within any organization. Meanwhile, let's not lose track of the fact that in typical organizations, the simulation emails employees receive a year after starting the program are almost always significantly tougher than those they received at the beginning.

While click rate is not an all-encompassing measurement, the improvement rate is a strong indicator that employees are paying attention more and have greatly improved their ability to spot social engineering.

The importance of SAT and improving resilience to cyberattacks is a key initiative in North America. According to Intel 471's 2024 Annual Threat Report, the U.S. and Canada are the #1 and #2 most-targeted countries by ransomware. The truly stunning part is that the U.S. accounted for 51.7% of the 4,205 global attacks analyzed. This is certainly not the kind of attention a country wants.

| North America | Phish-prone Percentage | | |
|---|---|---|---|
| **Organization Size** | **Phase One - Baseline** | **Phase Two - 90 Days** | **Phase Three - 1 Year+** |
| **1-249** | 26% | 21.1% | 3.7% |
| **250-999** | 31.1% | 21.2% | 3.9% |
| **1,000+** | 42% | 18.5% | 4.1% |
| **Average PPP Across All Organization Sizes** | **37.1%** | **19.6%** | **3.9%** |

## Social Engineering Is a Mental Game

Social engineering — the primary way ransomware spreads and the key factor behind BEC attacks and other phishing/vishing/smishing attacks — is an attack on human emotions.

Cybercriminals twist emotions to the point that we fail to see red flags and do things we wouldn't normally do. The hyper-partisan political landscape in the U.S. and Canada has left people in a heightened state of stress and emotion. This makes it easier for bad actors to get people riled up to the point of making errors. As humans, we simply are not good at choosing wisely when emotionally charged, and this is a major reason social engineering is so effective.

## Emotional and Mental Exhaustion Are the Enemy

When we are emotionally drained, we are far less likely to push back on a text message claiming we have an outstanding toll due, or an email saying that our account credentials have expired and we need to re-enter them. With the mental exhaustion we can feel after dealing with political matters at home or on social media, it becomes easy to go into a form of System 1 thinking while at work. In this state, we are much more likely to robotically process tasks than to question them when something is slightly out of the ordinary.

Layoffs and hiring freezes can also leave employees more tired and affect morale as organizations push to do "more with less." Employees may be rushing through tasks just to stay ahead of them, which can also lead to mistakes. Some of these effects can be noted in industries such as Healthcare & Pharmaceuticals, which had a 54.8% initial click rate within large organizations (1,000+ employees) in North America. These are very intelligent people, but the pace at which they work can be detrimental to an employer's cybersecurity standing. Education also tends to suffer, as well, as funding is generally not strong, and many educators are stretched very thin.

## Tools and Education Can Make the Difference

These trends can be countered very effectively by ensuring employees are made aware of the threat, provided the education to spot the threats and have tools deployed to help them identify potentially missed threats. This means consistent, short and impactful education; simulated attacks; and tools designed to help the user understand why certain emails are dangerous, including offering hints that something may be suspicious. Using these methods, the large organizations in healthcare in North America dropped from that staggering 54.8% click rate to an impressive 3.7% in just one year. Results like these show how much an SAT program can affect one of the biggest cyber threats organizations now face.

## Key Takeaways

**No matter how you slice it, organizations across industries in North America are significant targets for ransomware and other cyberattacks.**

- **Due to political and economic issues, people are tired and emotionally drained, and many organizations are asking their employees to do more faster to remain competitive.** These factors make social engineering much easier for bad actors and more difficult for organizations to defend against.
- **North America is one of the most targeted regions for cyberattacks,** meaning organizations need to take the human risk portion of their cybersecurity programs very seriously.
- **Our results show how significantly education and training, along with some practice, can reduce employee click rates.** Given the size of the phishing and social engineering threat, there are few things that can be done to make such a dramatic difference for so relatively little fiscal investment.

For More Information Visit KnowBe4.com

## About KnowBe4

KnowBe4 empowers workforces to make smarter security decisions every day. Trusted by over 70,000 organisations worldwide, KnowBe4 helps to strengthen security culture and manage human risk. KnowBe4 offers a comprehensive AI-driven 'best-of-suite' platform for Human Risk Management, creating an adaptive defence layer that fortifies user behaviour against the latest cybersecurity threats. The HRM+ platform includes modules for awareness & compliance training, cloud email security, real-time coaching, crowdsourced anti-phishing, AI Defense Agents, and more. As the only global security platform of its kind, KnowBe4 utilises personalised and relevant cybersecurity protection content, tools and techniques to mobilise workforces to transform from the largest attack surface to an organisation's biggest asset.

For more information, please visit **www.KnowBe4.com**

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KN0WBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com