KnowBe4
Human error. Conquered.

Data Confirms Value of Security Awareness Training and Simulated Phishing

by Roger A. Grimes &
Dr. Martin J. Kraemer

Data Confirms Value of Security Awareness Training and Simulated Phishing

Table of Contents

A common question we get from potential customers is if security awareness training and simulated phishing tests have proven tangible value in reducing cybersecurity risk. It does. Our data confirms this.

We analyzed records from over 60,000 individual KnowBe4 customer organizations worldwide, comprising 32,604,108 separate individual users, who took a total of 493,871,295 Phishing Security Tests (PSTs) and participated in awareness training at least once a year. We believe this is the largest analysis, in terms of both customers and test numbers, of any study of this kind.

MAJOR FINDINGS

The data is conclusive. Here are the summarized findings:

- Groups that did frequent PSTs performed better in detecting simulated phishing campaigns than groups that did not.
- The more frequently that groups did PSTs, the better the users performed on simulated phishing tests. The more PSTs, the better.
- Groups that did weekly PSTs were 2.74 times more effective in reducing risk than groups that only did less than quarterly PSTs.
- The longer a group trained, the better they did on simulated phishing tests.
- Groups that did both training and simulated phishing tests did the best.

We will cover this data in more detail below. To be clear, we documented these findings regardless of customer industry, location, or types of training (e.g., length, difficulty, media type, delivery method, etc.).

Below is a good representative sample of the data supporting the effectiveness of security awareness training and phishing security tests (PSTs). The table shows the average improvement rate in Phish-prone™ Percentage (e.g., the ability of a user to flag a potential phishing email as a phishing email) depending on training and simulated phishing testing frequency.

The average improvement rate describes the relative improvement in Phish-prone Percentage (PPP) between the first PST and the average PPP for all recorded PSTs given a PST frequency and a training frequency.

Training/ PST Frequency	1 ≥ Monthly	Quarterly	Annually	< Annually	Aggregate (excl. never)
≥ Weekly	96%	84%	88%	89%	89.25%
Bi-Weekly	83%	77%	80%	82%	80.33%
Monthly	74%	71%	74%	74%	73.39%
Bi-Monthly	50%	60%	63%	72%	65.31%
Quarterly	53%	55%	52%	53%	53.00%
< Quarterly	35%	35%	39%	41%	38.95%

Table 1: Average improvement rate of Phish-prone Percentage by average PST frequency and average training frequency (for users active on the platform for five years or more).
The horizontal axis is training frequency, and the vertical axis is phishing frequency.

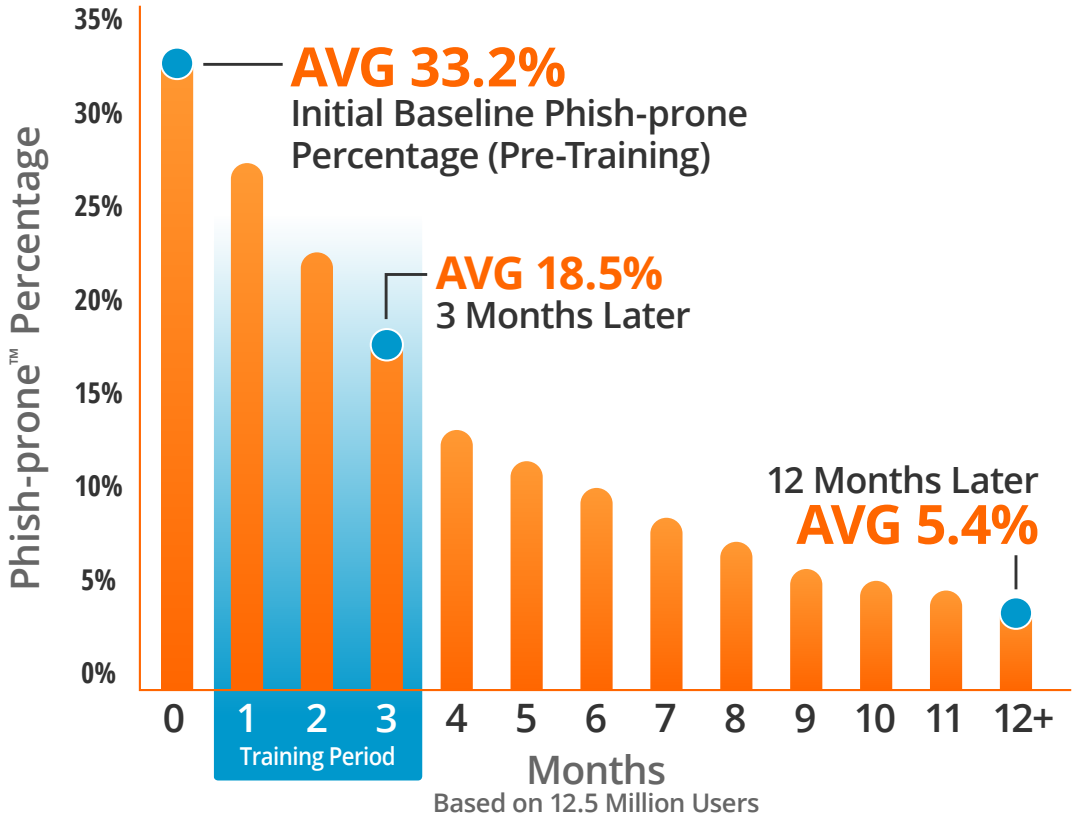
Fact: Groups that did both training and simulated phishing tests did the best.

For example, users who were given both monthly or more frequent security awareness training and weekly or more frequent phishing simulated tests had their Phish-prone Percentage rate improve by 96%, better as compared to any other less trained and tested group. Although there are some minor exceptions, all groups that trained or tested more did better than groups that trained or tested less, in general. Interestingly, according to the data, the influence from more frequent phishing tests is more impactful than from more frequent training, but the increase of frequency of both provided the best outcomes.

Based on the data, everyone should be conducting frequent simulated phishing tests as part of their security awareness training program to get the best impact.

KnowBe4 Phishing by Industry Benchmark Report

We are not surprised by the results. Our customers' data has long shown that continued simulated and frequent phishing tests result in less of their users clicking on and responding to those tests (i.e., "failing") over time. Organizations without any training and simulated phishing tests often have 30% or higher percentage of their users who would likely click on and treat a simulated phishing test (or real phishing email) as a non-malicious email. After training and frequent simulated phishing tests, the PPP rate would often fall to around 5% within a year of training and PSTs. (See the 2023 results below)



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.

This 82% drop in the Phish-prone Percentage from new customers who now use security awareness training and simulated phishing testing has been fairly consistent over the years. And we have many customers with Phish-prone Percentages consistently below 5%. We knew training and PSTs, which we consider a very important type of training, worked at reducing cybersecurity risk. It is why KnowBe4, Inc., is one of the largest and fastest-growing cybersecurity companies in the world.

Simulated phishing tests are a big part of training.

Each year, we release our annual Phishing by Industry Benchmarking Report. Here is the 2023 edition: https://info.knowbe4.com/phishing-by-industry-benchmarking-report

This year's report analyzed a data set of 12.5 million users across 35,681 organizations with over 32.1 million simulated phishing security tests. As shown above, we also consistently see large drops in the Phish-prone Percentage after just the first three months.

You can view a webinar that discusses Phish-prone Percentages per industry here, Phishing by Industry Benchmarking Study findings and best practices: https://info.knowbe4.com/pib-2023

Data in the 2023 Phishing by Industry Benchmarking report came from anonymized training and PST customer campaigns from March 3, 2011 to January 1, 2023.

DATA DETAILS

We have data on our customers and end users since the beginning of KnowBe4 over 13 years ago, although the data in this whitepaper is based on anonymized data collected over the last 10 years. This data accounts for over 493M individual simulated phishing tests from over 60,000 individual KnowBe4 customer organizations worldwide with over 32M users.

This section of the report will display the raw data behind the summary statement of findings above. Before we begin, let's define some terms and acronyms that are data labels:

- **PPP** = Phish-prone Percentage. Percentage of users who negatively interacted with a phishing security test (PST) message. Usually via email but can be from other media types such as SMS, voice calls, or USB tests.
- **Phishing Security Test (PST)**. A simulated phishing test is designed to appear as a rogue phishing message but is solely used to test the recipient's ability to spot a real phishing message. Opening a simulated phishing message is not necessarily a "failure" but clicking on an embedded link or performing any requested action (e.g., to providing login credentials, downloading a file, executing a program, etc.) is considered a test failure.
- **Training**. Assigned educational sessions. Could be via email, web, video, contest, quiz, gaming, PDF poster, etc. Most training is done via interactive modules and/or live action videos. KnowBe4 also considers PST high-quality training (and so should you), but not for the purposes of the data in this whitepaper. In this paper, training is not PSTs.
- **Aggregate (Agg).** Total number in a particular collection of data.
- **Frequency (Freq).** How often a training or PST was performed:
    - **Aggregate >= Weekly PST.** PSTs given weekly or more often.
    - **Aggregate Bi-Weekly PST.** PSTs given every two weeks.
    - **Aggregate Monthly PST.** PSTs given monthly.
    - **Aggregate Quarterly PST.** PSTs given quarterly.
    - **Aggregate <Quarterly PST.** PSTs given less than once a quarter.
    - **Aggregate Everything.** All PSTs no matter when given.
- **User Age.** How long the user had been using our system, in years. Max is 13 years.

Frequency Matters

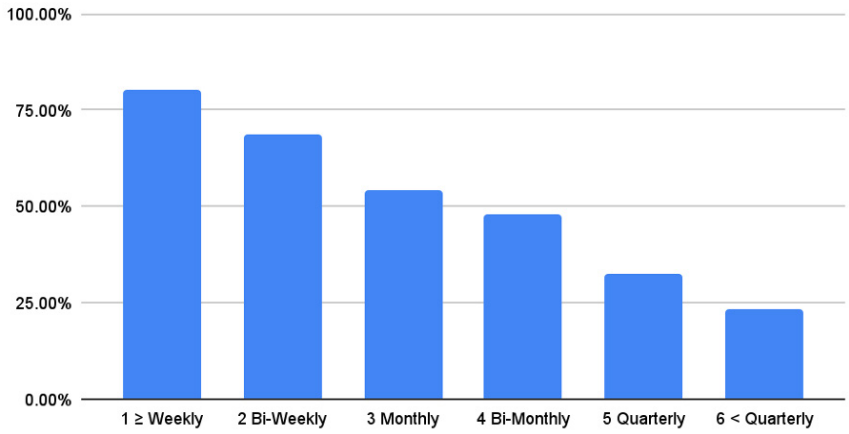
Fact: Groups that did frequent PSTs performed better in detecting simulated phishing campaigns than groups that did not.

The data shows great value in customers doing frequent simulated phishing campaigns. That statement of fact is derived from this data:

Avg PST Frequency	First PST		Latest PST		Lifetime PSTs			Sample Size
	# of Fails	PPP%	# of Fails	PPP%	# of Fails	# Received	PPP%	
Aggregrate ≥ Weekly PST	22,123	9.04	4,997	2.04	560,117	31,253,102	1.79	244,841
Aggregate Bi-Weekly PST	216,185	10.94	94,823	4.80	3,257,015	95,377,935	3.41	1,976,981
Aggregate Monthly PST	711,892	11.96	363,578	6.11	6,676,093	121,771,620	5.48	5,953,628
Aggregate Bi-Monthly PST	1,179,605	12.26	642,506	6.68	10,446,663	163,520,367	6.39	9,620,102
Aggregate Quarterly PST	640,906	13.26	431,178	8.92	3,425,455	38,389,891	8.92	4,834,048
Aggregate ≤ Quarterly	1,388,454	13.92	1,149,548	11.52	4,654,018	43,548,380	10.69	9,974,508
Aggregate Everything	**4,159,165**	**12.76**	**2,686,630**	**8.24**	**29,019,361**	**493,871,295**	**5.88**	**32,604,108**

If all the data is not clear in a quick glance, the following bar chart shows the average improvement rate of the user's Phish-prone Percentage as the frequency of a phishing simulated test increased.

(Fig. 2b) Average improvement rate of PPP by average PST frequency



In all categories, as the frequency of PSTs increases, the Phish-prone (failure) Percentage falls. For example, over a lifetime of PSTs (meaning all PSTs given to a particular user), the average user's PPP is 10.69% when done less than quarterly, but falls to 8.92% with quarterly PSTs, to 6.39% with bi-monthly PSTs, then 5.48% and 3.41%, and finally to 1.79% with subsequent PSTs done weekly or more. That is an incredible decrease in risk, considering untrained, untested users' PPPs for most organizations are usually 30% or above. With frequent weekly or more PSTs, you can get the users' "click rate" down to below 2%.

That is a demonstrably 80% improvement in risk reduction from using one cybersecurity defense tool!

Fact: The more frequently that groups did PSTs, the better the users performed on simulated phishing tests. The more PSTs, the better.

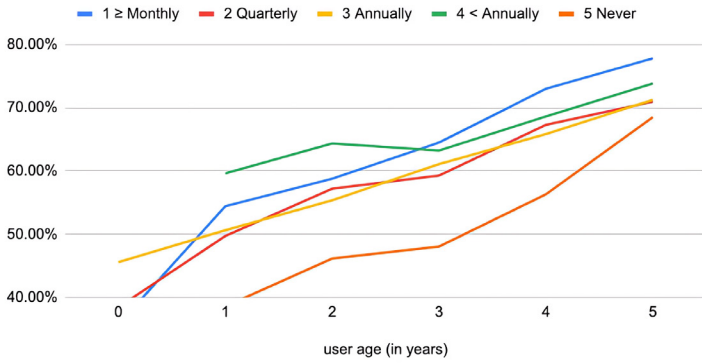
This fact comes from the same data. All groups that did monthly, bi-weekly, and weekly or more frequent PSTs did better than the groups that did further apart intervals. The more PSTs that were conducted, the lower the PPP rate. As the first table showed, groups that did weekly or more PSTs had an improvement rate of 96% and groups that did less than quarterly PSTs only had a 35% improvement rate. This means that the groups that did weekly or more PSTs decreased phishing risk 2.74 times better than the less than quarterly group.

Longer Training Matters

Fact: The longer a group trains, the better they did on simulated phishing tests.

The data shows that users who had been using KnowBe4's training performed better (i.e., had high rates of correctly spotting simulated phishing tests) the longer they had been using our system and the more frequently they received training (as evidenced by the chart to the right). The percentage shown is the improvement in Phish-prone Percentage with user age. User age is the number of years the user has been using our system.

Average improvement rate of PPP by average training frequency and user age



Inside Man: Special Success Case With Netflix-Style Training

"The Inside Man" is KnowBe4's Netflix-style series of training videos. These live-action videos are high quality, use career actors, and are filmed on real sets with professional crews. In short, they are as close to a professional television series as you are going to come by in security awareness training. No other competitor has anything close to this series. Our users love them. We frequently get requests from admins and users asking when the next season will be out.

Imagine, users *asking* for more computer security training!

This is a link to a promo for Season 5 with 12 episodes: https://blog.knowbe4.com/knowbe4-announces-new-12-episode-security-awareness-video-series-the-inside-man

Below is the data from our users who have watched at least one episode or more of "The Inside Man." You can see that before watching it, the average viewer had a PPP of 13% - 17%. After watching at least one episode, their PPP dropped to 5% - 8% and kept dropping as the number of episodes they watched increased.

Users that watched at least one episode in addition to other training							
	Total episodes ever watched	**Before watching any episodes**	**After watching 1+ episode**	**After watching 10+ episodes**	**After watching 20+ episodes**	**After watching 50+ episodes**	**Sample Size**
Aggregate PPP	**1-9**	16.85	7.72	--	--	--	6,665,967
	10-19	14.87	7.57	6.46	--	--	1,139,830
	20-49	14.15	6.66	6.15	5.50	--	640,670
	50+	13.10	5.51	5.21	5.01	4.43	133,274
Agg PPP change over time since before watching first episode	**1-9**	--	-9.13	--	--	--	6,665,967
	10-19	--	-7.31	-8.41	--	--	1,139,830
	20-49	--	-7.49	-8.00	-8.65	--	640,670
	50+	--	7.59	-7.89	-8.09	-8.67	133,274

Our data (shown below) showed that even users who only viewed "The Inside Man" as their only training within the KnowBe4 system benefitted. Even after only one episode of "The Inside Man", users' untrained PPP went from 8% - 11% to 5% - 7%, and eventually down to 4% if they watched 50 or more episodes.

Users whose ONLY training was episodes of Inside Man							
	Total episodes ever watched	**Before watching any episodes**	**After watching 1+ episode**	**After watching 10+ episodes**	**After watching 20+ episodes**	**After watching 50+ episodes**	**Sample Size**
Aggregate PPP	**1-9**	10.76	6.89	--	--	--	387,544
	10-19	10.25	6.72	6.45	--	--	191,072
	20-49	9.27	5.42	5.23	5.23	--	174,192
	50+	7.97	4.86	4.99	5.11	3.96	4,310
Agg PPP change over time since before watching first episode	**1-9**	--	-3.87	--	--	--	387,544
	10-19	--	-3.53	-3.80	--	--	191,072
	20-49	--	-3.85	-4.03	-4.04	--	174,192
	50+	--	-3.11	-2.98	-2.85	-4.01	4,310

Although we do not recommend watching only "The Inside Man", (we recommend changing training selections and types regularly to keep content fresh to users), exclusively using "The Inside Man" with no other KnowBe4 training content, decreased PPP significantly on its own. Highly enjoyable and educational.

Note: A small segment of customers use our content outside our platform by importing our training modules into their organization's own Learning Management System, so although they may show in our data as having only watched Inside Man, they may have completed training modules that were not tracked in our system.

Use of AI Within KnowBe4

Another common question we hear is if artificial intelligence (AI) can improve anti-phishing defenses? The answer is a definitive yes. KnowBe4 uses AI in many ways including a feature we introduced in 2017 known as Artificial Intelligence Driven Agent or AIDA™. AIDA uses artificial intelligence to determine what simulated phishing templates to send to users. Templates are the text, look, and feel of our simulated phishing, often created to mimic in-the-wild, real-world phishing emails. Customer admins can pick (or create) their own phishing templates to test users with, enable full random selection, or allow AIDA to select the templates.

KnowBe4 AI-Driven Phishing

Using AIDA results in higher PPP failure rates.

We analyzed failure rates of 1) admin-selected, 2) full random, and 3) AIDA-selected templates of nearly 650 million simulated phishing tests across over 46,000 different phishing template uses. AIDA-selected templates caused higher user PPP failure rates (7.1%) versus the other two (2.7%).

As stated, AIDA leverages machine learning to recommend and deliver informed and personalized phishing campaigns based on your users' training and phishing history. This enables you to automate the dynamic selection of unique phishing security test templates for your users, creating a campaign for each of your users to make sure every user receives simulated phishing tests personalized to their individual level.

Phishing templates are rated from 1- to 5-star difficulty levels. AIDA automatically selects the best, personalized templates, and when indicated, the next higher difficulty level. That causes the initially higher failure rates. However, over time that continually increases your user's ability to spot attacks and proves out to strengthen your security culture.

KnowBe4 uses AI in several other features, including the new PhishER Plus (https://blog.knowbe4.com/introducing-phisher-plus-anti-phishing-defense), to help detect phishing and other malicious attacks. So, when you hear the media talking about all the damage that bad actors are likely to cause with AI, remember the "good actors", including KnowBe4, were using AI years before and have used AI to improve user experiences and to decrease your cybersecurity risk.

Note: Data included only 19,475 templates that were used by both traditional and AIDA-enabled simulated phishing campaigns. 601,468,868 user experiences involved traditional selection methods and 48,299,578 experiences involved AIDA-selected templates.

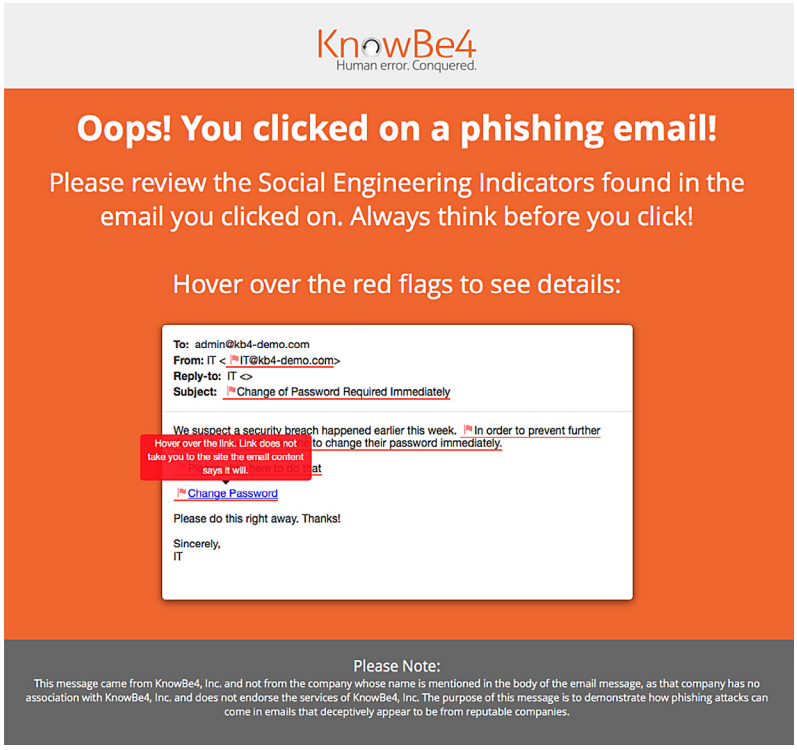
For more information on AIDA, see: https://blog.knowbe4.com/knowbe4-fresh-content-updates-from-april-including-new-ai-driven-phishing-feature

OUR BEST PRACTICE TRAINING AND PST RECOMMENDATIONS

Using the KnowBe4 methodology provides you with immediate, measurable, and fastest cybersecurity risk reduction. It includes these best practices:

- Security awareness training should have an executive sponsor from senior management (i.e., CEO, CFO, CIO, CSO, etc.) and that executive sponsor should make it known to all that taking security awareness training and participating in the PSTs is expected, and for the good of the whole organization.
- Give all new employees in-depth, broad security awareness training (SAT) during onboarding. This training should comprise popular social engineering and hacking subjects and ideally last between 30-60 minutes in total length. This needs to be repeated at least once a year.
- Also, give all users shorter, at least monthly training, with the topic lasting three to five minutes in length. Ideally, the topic should be about a current attack or risk.
- Training should include a variety of types, including videos, posters, quizzes, and gaming.
- PSTs should be sent monthly or more frequently. The data shows that the more often a PST is sent, the lower the PPP. Of course, administrators will need to appreciate the need not to cause user frustration by sending out too many PSTs. How often is too much? That is up to each organization and administrator based on user and management feedback.

- Users failing a PST should immediately be presented with what they missed that should have indicated the PST was phishing test. See example below:



- When doing PSTs, let everyone know that you do them, how frequently, but not when you will do them.
- When doing PSTs, it is best to do randomized delivery (templates and send-time) to users and do not send the same simulated phishing message to all users at the same time.
- It is okay to inform management ahead of time that there will be future PSTs, but not exactly when or what the messages will be.
- Do not send a PST that contains content that is likely to cause more grief than good (for instance promising raises, bonuses, or promotions, etc.). There are plenty of good PST subjects that can be used to test users without making them mad.
- Implement an easy way for users to report suspected real and simulated phishing emails within your organization. We recommend our free Phish Alert Button: https://www.knowbe4.com/free-phish-alert
- Users who fail multiple PSTs should be given more training and even perhaps 1:1 coaching. The consequences for failing more PSTs in a given time (say a year) should result in more training, but not be seen as punishment. The goal is to help all users become part of your human firewall and become assets to the organization. Everyone can be taught to be better at recognizing phishing attacks.
- During the initial roll-out of your security awareness program, you can set up an instant feedback channel, such as through Microsoft Teams or Slack. Use emotional intelligence if they fail a test for the first time and manage their expectations with empathy.

Related Resources

If you are interested in everything you can do to prevent social engineering and phishing, check out this whitepaper: https://info.knowbe4.com/comprehensive-anti-phishing-guide

Check out Building a Security Awareness Program to Help Defend Against Cyber Extortion and Ransomware: https://info.knowbe4.com/wp-security-awareness-program-cyber-extortion-ransomware

Here is an example security training awareness guide: https://info.knowbe4.com/wp-example-sat-policy-guide

What About Other Studies That Did Not Show Improvements With Training and Simulated Phishing Tests

We have come across a few studies by other independent researchers who questioned the value of security awareness training. While we do not discount any other person or study's experiences and findings, each of those studies used relatively small data sets, were of limited duration, and either did not indicate whether they consistently followed best practices or did not follow best practices. We believe our data (nearly 500M records gathered over 13 years) is the best data set on the subject.

Top Learning: Customers who perform frequent training and simulated phishing test campaigns significantly and best reduce the risk of their co-workers falling for phishing attacks.

LIMITS OF THIS STUDY

We looked at nearly 500M separate user records as they related to training, PSTs, and PPP rates. However, we did not include all data that we have in our enormous databases. This was done to adhere to customers who decline to share their data and scenarios that might result in skewed data, such as new users with less than a day of use on the system. We are including the data filters we did use (below) to be transparent about what types of data sets were not included in the data.

Data included:

- PST campaign runs received by at least 25 users (smaller data sets would likely skew results drastically)
- PST campaign runs which were not marked as "hidden" by their admins
- PST campaign runs which were not part of Scam of the Week or Scam or Security Hints and Tips of the Week templates (which are not testing PSTs)
- Users had to be on the system at least one full day
- Users had to be not archived or suspended by admins
- Accounts that are active, paid, and allow analytics
- Accounts without test/demo/seed domains

Further:

- We did not track how different lengths, content types, or quality of training content impacted risk rates. All training and simulated phishing campaign instances were counted identically for the purposes of this study. It is assumed, however, that better quality training and simulated phishing content would lower risk more than poor and/or short-length content.
- Training and PSTs are not independent of each other. In large percentage of instances, a failed PST resulted in required training, such that both the failed PST and the training then resulted in the future lower PPP rates. We cannot isolate and attribute what portion of the future lower PPP rate was attributed to training versus PST.
- We recommend to our customers to increase simulated phishing training difficulty (i.e., complexity, maturity, etc.) over subsequent tests as users begin to "score" well on the early, easier-to-recognize tests, likely making it harder for tested users to "pass" subsequent phishing tests. For the purposes of this study, every simulated phishing test regardless of complexity was counted identically. But readers should assume that the results from constantly difficult simulated phishing tests over time would have resulted in even lower phish prone rates.
- We do not analyze data on how our customers versus non-customers compare against real-world phishing attacks (this would be the ultimate data to collect to prove the efficiency of PSTs and training, but we do not have data on non-customers). We are researching ways to get this type of comparative data and hope to present the findings in a future whitepaper.

With these caveats, we believe our very large data set of almost 500M individual records from over 13 years strongly supports the case of using PST and training to significantly reduce cybersecurity risk. Further, the more you train and test, the better you reduce cybersecurity risk.

FOR MORE INFORMATION

How PhishER and PhishER Plus Works

First, users report phishing threats. These are ingested by PhishER and PhishML triages to identify clean emails from spam and threats. The PhishER Admin then determines if threats should be added to their organization's private blocklist. KnowBe4's Threat Research Lab then verifies each threat before adding it to the Global Blocklist.

The Global Blocklist syncs to the mail servers of PhishER Plus customers to block known threats before they can reach other organizations. If a threat sneaks by before being added to the Global Blocklist, Global PhishRIP will remove and quarantine the message from all PhishER Plus customers' inboxes.

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free 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 guys do

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

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 ongoing problem of social engineering through a comprehensive new-school 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.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

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

01D10K01