KnowBe4
Human error. Conquered.

2020 Phishing Attack Landscape and Industry Benchmarking

The data you need to know

Perry Carpenter
Chief Evangelist & Strategy Officer
KnowBe4, Inc.

Perry Carpenter

Chief Evangelist & Strategy Officer

KnowBe4
Human error. Conquered.

About Perry

- MSIA, C|CISO
- Author of *Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors*
- Former Gartner Analyst leading research and advisory services to CISOs, Security Leaders, and security vendors around the world
- Led security initiatives at Fidelity Information Services, Alltel Telecommunications, and Wal-Mart Stores
- Lover of all things:
  - Security
  - Psychology
  - Behavioral Economics
  - Communication Theory
  - Magic, misdirection, and influence

About KnowBe4

- The world's most popular integrated new-school Security Awareness Training and Simulated Phishing platform, over 32,000 customers worldwide
- Founded in 2010
- Recognized as a Leader in the Gartner Magic Quadrant for Computer-Based Training (CBT) with the highest and furthest overall industry position for ability to execute and completeness of vision.
- Recognized as a Leader in the Forrester Wave for Security Awareness and Training Solutions with the highest overall industry position.
- Our mission is to train your employees to make smarter security decisions so you can create a human firewall as an effective last line of defense when all security software fails…

Which it will!

The question every executive asks…

Agenda

1. The phishing problem
2. Phishing benchmark data by industry
3. International phishing benchmark data by region
4. Actionable tips to create your “human firewall”

Agenda

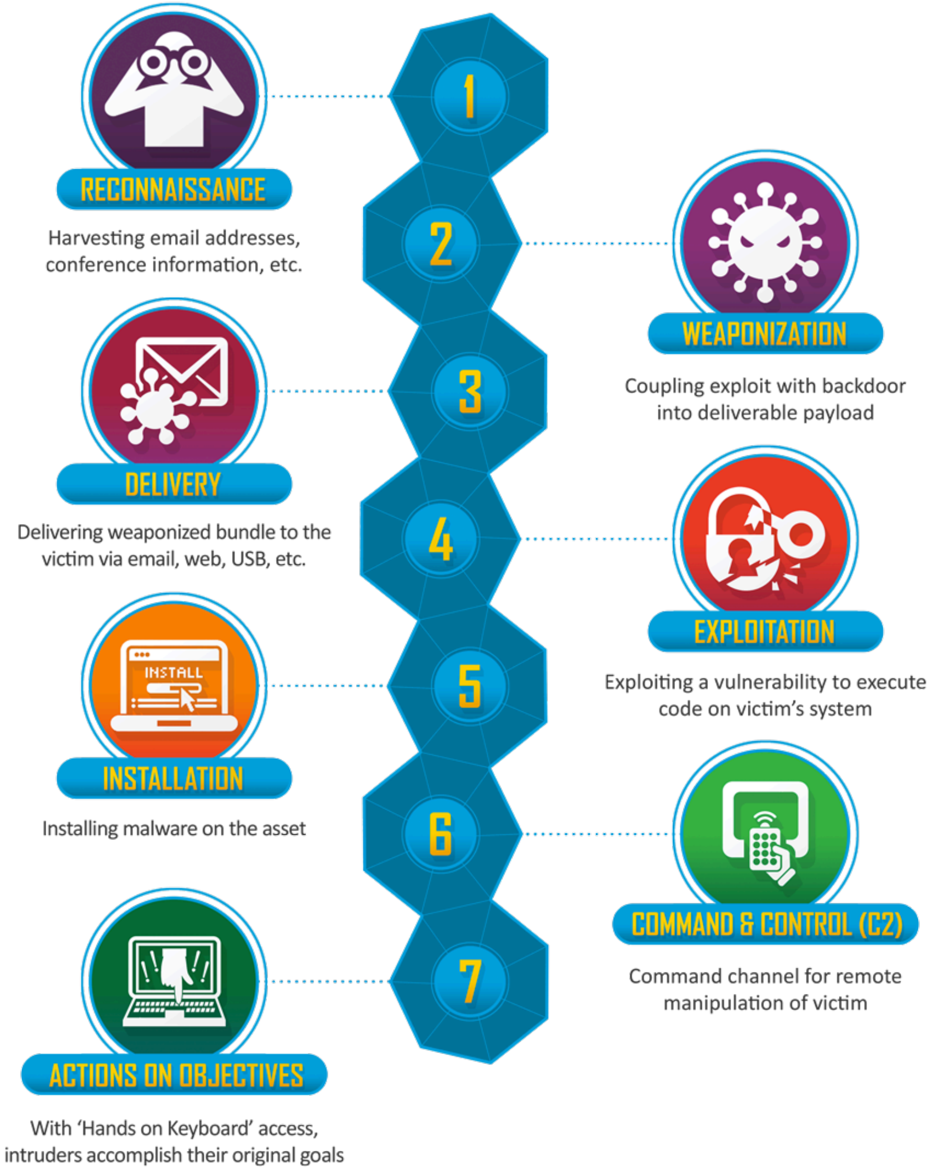
1. The phishing problem
2. Phishing benchmark data by industry
3. International phishing benchmark data by region
4. Actionable tips to create your “human firewall”

Cybercriminals rely on phishing *because it works…*

ACCORDING TO VERIZON'S 2019 DATA BREACH INVESTIGATION REPORT, **PHISHING WAS THE #1 THREAT ACTION** USED IN SUCCESSFUL BREACHES LINKED TO SOCIAL ENGINEERING AND MALWARE ATTACKS.

the Cyber Kill Chain

Attackers generally follow these steps to compromise an organization



RECONNAISSANCE

Harvesting email addresses, conference information, etc.

WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

INSTALLATION

Installing malware on the asset

COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

Agenda

1. The phishing problem
2. Phishing benchmark data by industry
3. International phishing benchmark data by region
4. Actionable tips to create your "human firewall"

METHODOLOGY AND DATA SET

17 thousand organizations

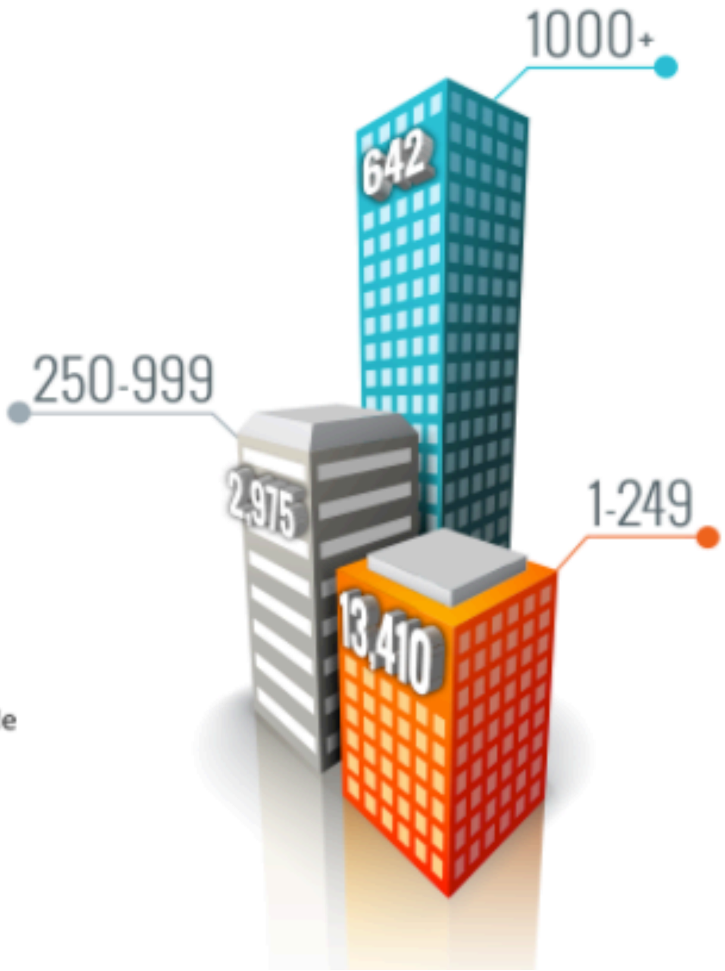
4 million users

9.5 million phishing security tests

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



All **17,000** customers were using the KnowBe4 platform according to the recommended best practices for a new-school security awareness approach:

- Running an initial **baseline** test
- Training their users through **realistic** on-demand, interactive training
- **Frequent simulated testing** at least once a month to reinforce the training

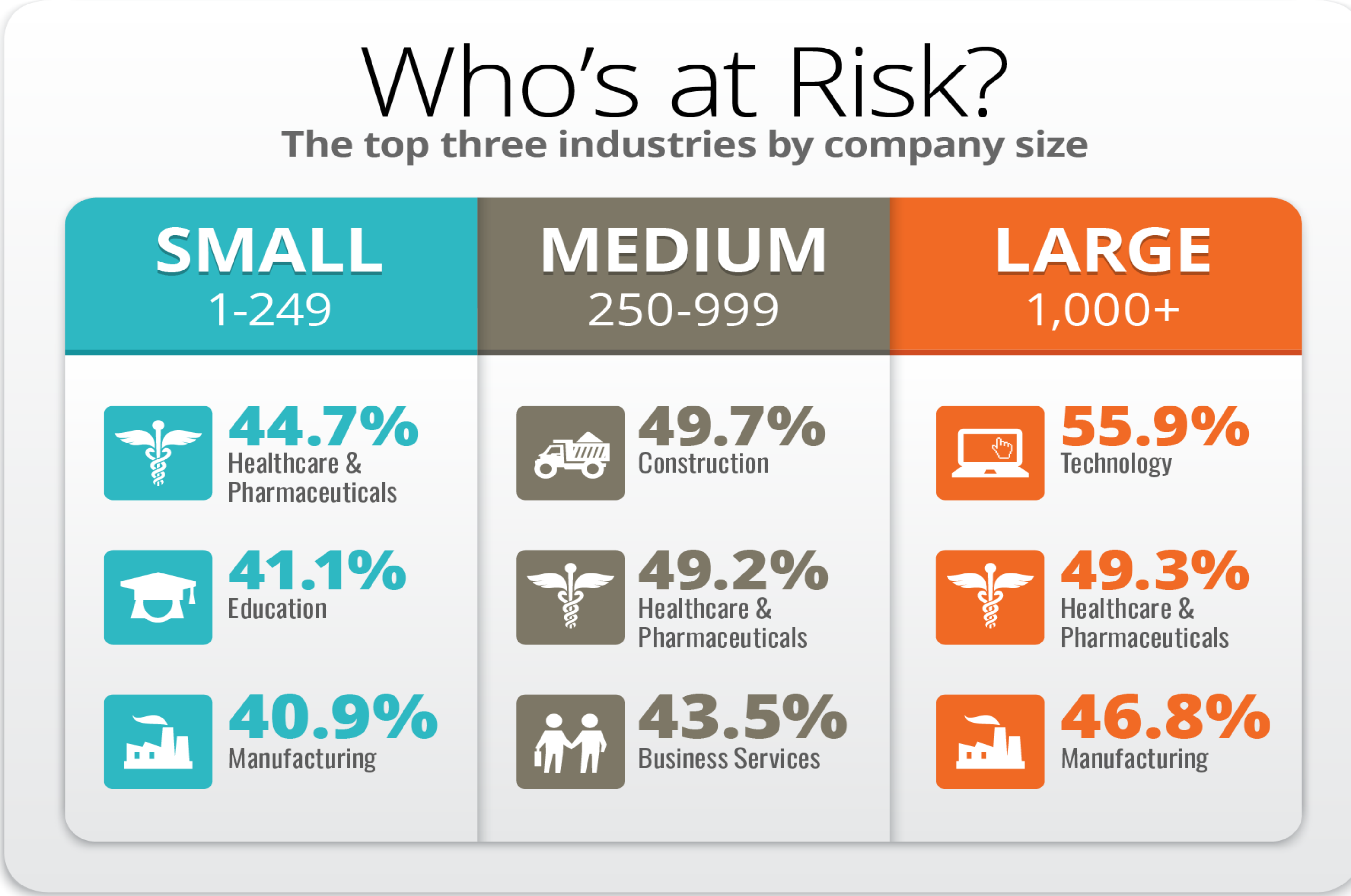
Three-Phases of Measurement

1 **Phase One: If you haven't 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.

2 **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 look for all simulated phishing security events up to 90 days after that training is completed

3 **Phase Three: What is the final resulting PPP after your users take ongoing training and monthly simulated phishing tests?** We measured security awareness skills after 12 months or more of ongoing training and simulated phishing security tests and look for users that completed training at least one year ago and take the performance results on their very last phishing test.

RISKY BUSINESS



Who’s at Risk?

The top three industries by company size

SMALL 1-249	MEDIUM 250-999	LARGE 1,000+
44.7% Healthcare & Pharmaceuticals	49.7% Construction	55.9% Technology
41.1% Education	49.2% Healthcare & Pharmaceuticals	49.3% Healthcare & Pharmaceuticals
40.9% Manufacturing	43.5% Business Services	46.8% Manufacturing

Benchmark Phish-prone Percentage by Industry

CALCULATING PHISH-PRONE PERCENTAGE BY INDUSTRY

Phase One: Baseline Phishing Security Test Results

The initial baseline phishing security test was administered within organizations that hadn't conducted any security awareness training. Users received no warning and the tests were administered on untrained, unaware people going about their regular job duties.

The results indicated a high-risk level. Across all industries and all sizes, the average Phish-Prone percentage was **37.9%**. That means **1 out of 3 employees** was likely to click on a suspicious link or email or obey a fraudulent request, about the same outcome as last year.

It's interesting (and maybe scary) to see that no organization performed well without training. Very few industries were under 30% in "Phish-Prone" employees: Banking - Small and Large at 29.8% and 27.4% respectively, Business Services - Large 27%, Government - Large at 26%, Legal - Medium at 26.8% and Transportation - Large at 27.2%.

The inescapable conclusion: Absent of training, 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.

Phase One

37.9% **Initial Baseline Phishing Security Test Results**

Organization Size	Initial PPP
1-249	36.8%
250-999	37.5%
1000+	39.2%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	29.8%	36.5%	27.4%
Business Services	35.8%	43.5%	27.0%
Construction	38.3%	49.7%	45.1%
Consulting	31.5%	37.6%	32.1%
Consumer Services	38.2%	30.6%	39.2%
Education	41.1%	34.4%	31.7%
Energy & Utilities	39.6%	41.2%	39.2%
Financial Services	32.1%	35.9%	43.9%
Government	33.8%	30.0%	26.0%
Healthcare & Pharmaceuticals	44.7%	49.2%	49.3%
Hospitality	32.1%	37.5%	39.2%
Insurance	39.2%	37.9%	39.2%
Legal	34.1%	26.8%	39.2%
Manufacturing	40.9%	37.7%	46.8%
Not-For-Profit	39.4%	38.1%	39.2%
Other	35.3%	41.0%	28.0%
Retail & Wholesale	40.4%	37.1%	36.5%
Technology	33.2%	30.5%	55.9%
Transportation	36.8%	43.2%	27.2%

Results Within 90 Days of Testing

Phase Two: 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 testing, results changed dramatically. We find when users completed their first training event and look for all simulated phishing security events up to 90 days after that training is completed. In those 90 days after completed training events, the Phish-Prone percentage was **cut nearly in half to 14.1%**, consistent with both the 2018 and 2019 studies.

The dramatic drop in Phish-Prone percentages was not specific to a certain industry or organization size. But a few interesting data points:

- The most drastic reduction was seen in the 1,000+ organizations where **Technology** organizations experienced a **39% decrease** within 90 days of training after recording one of the highest initial baseline PPP's at 55.9%.
- Other significant reductions were seen in the 1,000+ organizations where **Manufacturing** organizations experienced a **33.3% decrease** and **Healthcare & Pharmaceuticals** organizations, who had the second highest PPP at 49.3%, experienced a **31.8% reduction** within 90 days after training.
- The **significant drop from 37.9% to 14.1%** for all industries proves that a security awareness training program can pay meaningful dividends in building a strong human firewall as part of your defense-in-depth IT security posture—even within the first three months.

Phase Two

14.1% Phishing Security Test Results Within 90 Days of Training

Organization Size	90-Day PPP
1-249	13.2%
250-999	14.3%
1000+	14.7%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	10.4%	10.9%	11.8%
Business Services	14.2%	13.8%	11.5%
Construction	14.2%	17.7%	16.1%
Consulting	11.1%	17.6%	11.0%
Consumer Services	15.1%	15.3%	13.2%
Education	13.6%	17.1%	18.5%
Energy & Utilities	12.5%	13.2%	14.7%
Financial Services	11.1%	12.2%	12.1%
Government	13.9%	15.1%	14.0%
Healthcare & Pharmaceuticals	15.9%	15.7%	17.5%
Hospitality	12.9%	17.4%	14.7%
Insurance	13.3%	16.0%	16.1%
Legal	13.3%	13.6%	14.7%
Manufacturing	14.3%	15.6%	13.5%
Not-For-Profit	14.9%	12.4%	15.0%
Other	13.2%	11.1%	13.6%
Retail & Wholesale	13.7%	13.2%	17.3%
Technology	12.2%	13.9%	16.8%
Transportation	10.9%	12.9%	14.7%

Results after 1 Year+ of Ongoing Training

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

At this stage, we measured security awareness skills after 12 months or more of ongoing training and simulated phishing security tests and look for users that completed training at least one year ago and take the performance results on their very last phishing test. The results were dramatic, showing that having a consistent, mature awareness training program took the average PPP from 37.9% all the way down to 4.7%—demonstrating dramatic effectiveness across all industry sizes and verticals.

Originally, we saw that large enterprise organizations scored better PPPs in their initial baseline test. In the final phase of the study, it became clear that these same organizations needed more time to turn the ship around and move in the right direction. This is likely due to the complexity of addressing different departmental and regional needs. There were two exceptions: Technology and Healthcare & Pharmaceuticals industries. These industries, representing the two highest overall baseline PPPs, experienced the most significant, favorable movement after 12 months from 55.9% to 5%, nearly a 51% reduction and 49.3% to 5.2%, a 44% reduction respectively.

A globally dispersed workforce can also introduce language differences and cultural nuances that lead to a longer roadmap for testing. Often enterprise security leaders will roll out a new security awareness training program to three or four departments first to monitor outcomes and adjust their strategies. This approach helps them incorporate lessons learned into their program, but also explains the slower response to reduction in Phish-Prone percentages.

Phase Three

4.7% **Phishing Security Test Results After One Year-Plus of Ongoing Training**

Organization Size	12-Month PPP
1-249	3.9%
250-999	4.8%
1000+	5.8%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	3.0%	4.3%	3.5%
Business Services	3.6%	5.0%	2.1%
Construction	3.9%	4.8%	3.8%
Consulting	3.4%	4.3%	5.8%
Consumer Services	5.1%	5.2%	6.9%
Education	4.0%	4.6%	4.8%
Energy & Utilities	5.4%	4.9%	5.2%
Financial Services	3.3%	4.6%	6.3%
Government	4.4%	4.2%	5.8%
Healthcare & Pharmaceuticals	4.3%	3.9%	5.2%
Hospitality	5.0%	4.1%	6.2%
Insurance	3.5%	4.0%	4.6%
Legal	4.8%	3.5%	5.4%
Manufacturing	4.2%	5.6%	5.7%
Not-For-Profit	4.8%	3.3%	6.0%
Other	4.3%	5.0%	5.8%
Retail & Wholesale	3.7%	6.5%	7.5%
Technology	3.5%	4.5%	5.0%
Transportation	3.9%	4.8%	5.4%

The Results are in:

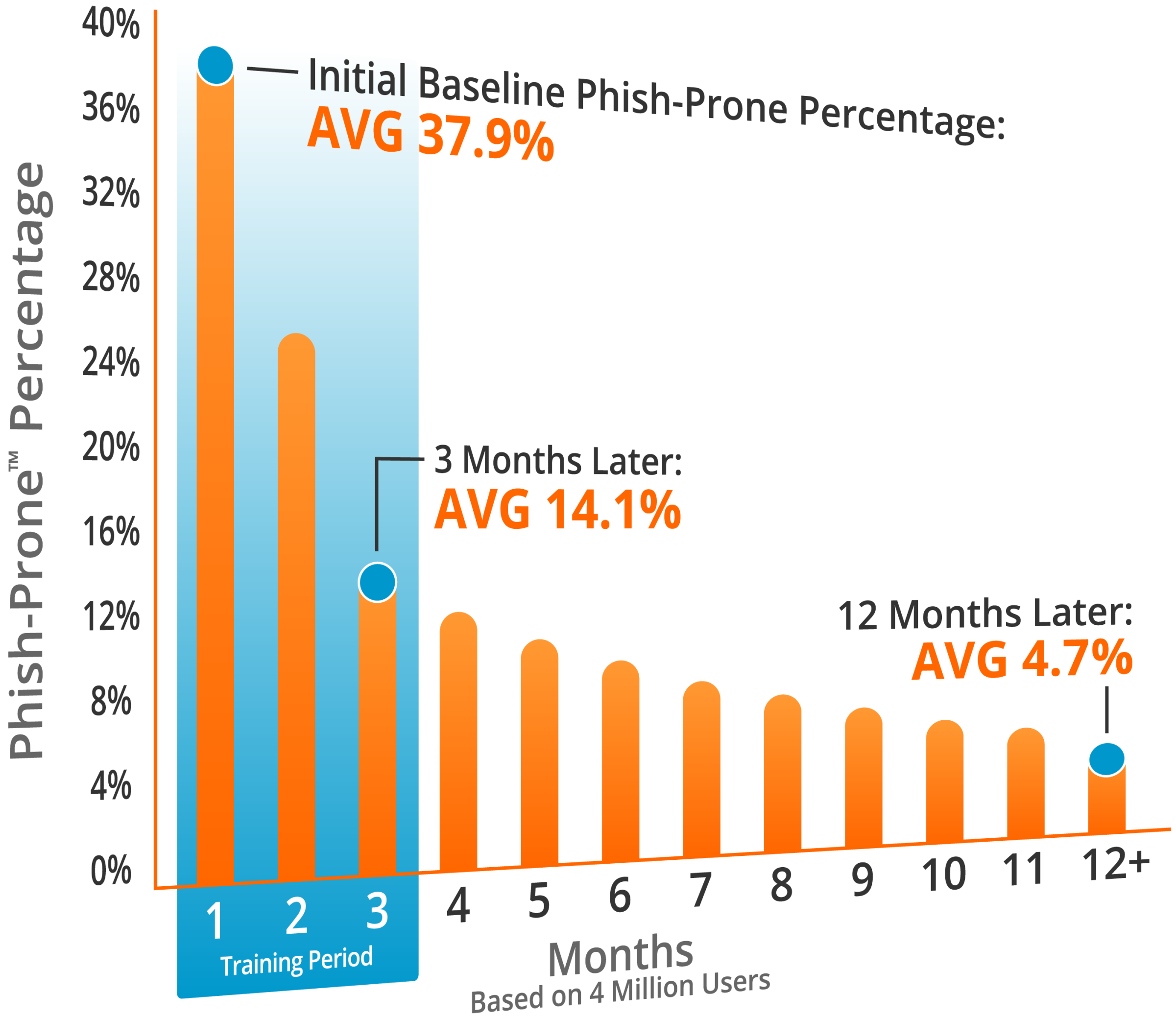
and they are dramatic

KnowBe4
Human error. Conquered.

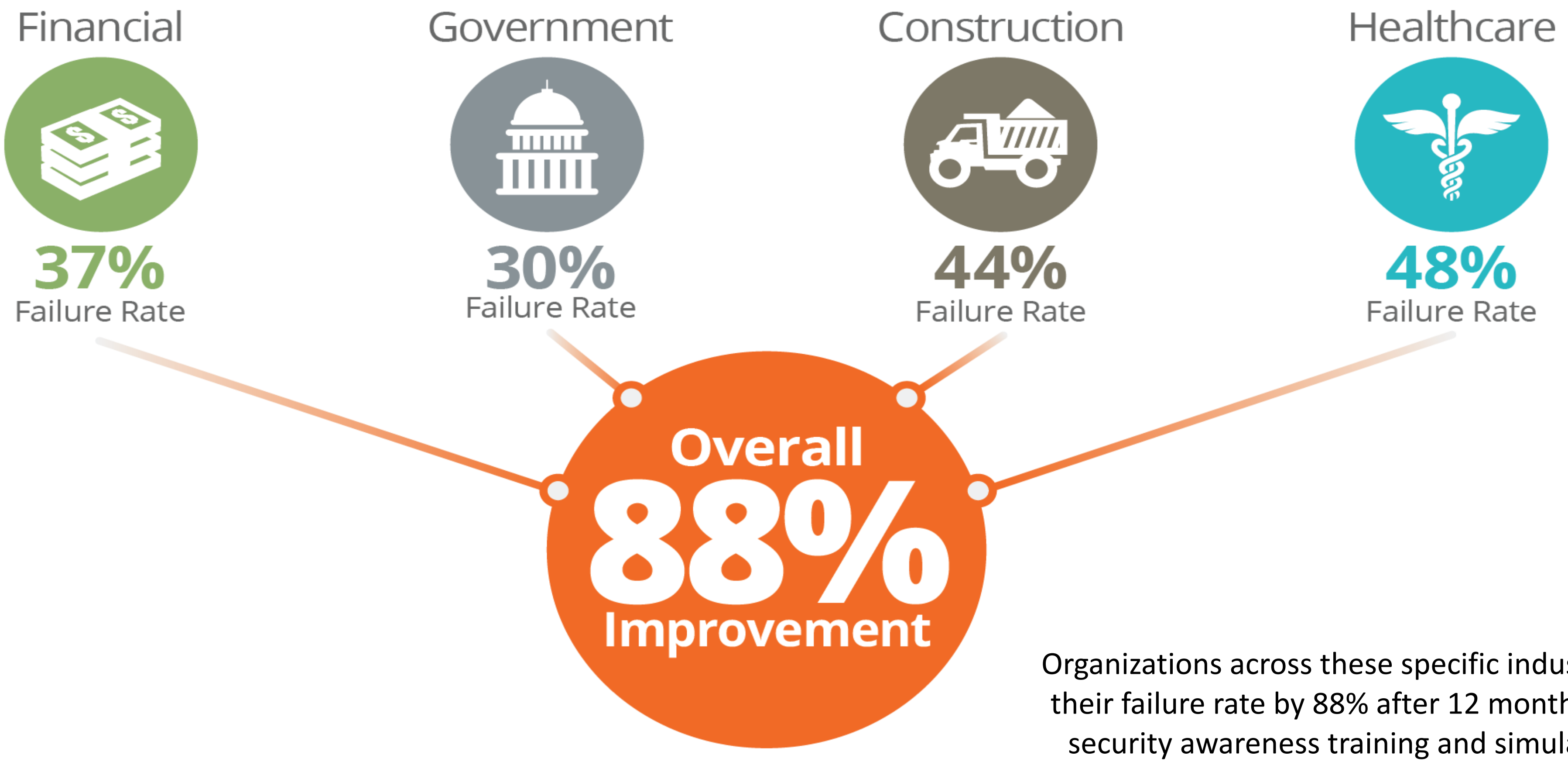
Security Awareness

+ Frequent simulated phishing training

= Drastically improved phishing resiliency



Our Behavior-Based Approach Works



Financial

37%
Failure Rate

Government

30%
Failure Rate

Construction

44%
Failure Rate

Healthcare

48%
Failure Rate

Overall
88%
Improvement

Organizations across these specific industries improved their failure rate by 88% after 12 months of combined security awareness training and simulated phishing using KnowBe4. (Based on weighted averages across all organization sizes. Percentages rounded.

Putting the results into perspective

Average Improvement Rates Across All Industries and Organization Sizes

It's evident that 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 continued to achieve the **best overall improvement with eleven out of the nineteen industries coming in at 90% or more.**

Across mid-size organizations, improvement rates were good with **most industries coming in at 85% or better,** three industries fell slightly below 85%. For large organizations, we see a wider range of improvement rates with the **lowest improvement rate at 68% and the highest at 93%.**

When you look across all industries and sizes, the **87% 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 industry-wide 37.9% of untrained users will fail a phishing test.

Only 14.1% of those same users will fail within 90 days of completing their first KnowBe4 training. After at least a year on the KnowBe4 platform only 4.7% of those users will fail a phishing test.

Average Improvement

87%

Average Improvement Rate Across All Industries and Sizes

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	90%	88%	87%
Business Services	90%	89%	92%
Construction	90%	85%	92%
Consulting	89%	89%	64%
Consumer Services	87%	83%	71%
Education	90%	87%	85%
Energy & Utilities	86%	88%	92%
Financial Services	90%	87%	86%
Government	87%	86%	78%
Healthcare & Pharmaceuticals	90%	92%	89%
Hospitality	85%	92%	71%
Insurance	91%	89%	93%
Legal	86%	87%	91%
Manufacturing	90%	85%	88%
Not-For-Profit	88%	91%	89%
Other	88%	88%	66%
Retail & Wholesale	91%	83%	79%
Technology	90%	85%	91%
Transportation	90%	84%	80%

Agenda

1. The phishing problem
2. Phishing benchmark data by industry
3. International phishing benchmark data by region
4. Actionable tips to create your "human firewall"

2020 International Results

2020 INTERNATIONAL PHISHING BENCHMARKS

At the international level, we used a slightly different data set which does not include separate industries to determine phishing benchmarks 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: Baseline Phishing Security Test Results

The initial baseline phishing security test was administered within organizations that hadn't conducted any security awareness training.

Phase Two: Phishing Security Test Results Within 90 Days of Training

Phase two evaluates organizations who have conducted baseline testing and then progressed to using a combination of training and simulated phishing exercises within a 90-day period. The data indicates that this combination cuts the Phish-Prone percentage **more than half for most regions**.

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

For phase three, we measured after 12 months or more of ongoing training and simulated phishing security tests. The results are in line with the industry benchmarking results, showing that having a consistent, mature awareness training program took the average PPP down to single digits—**demonstrating effectiveness across all organizational sizes and regions**.

		BASELINE			90 DAYS			1 YEAR		
REGION	Organization Size	1-249	250-999	1000+	1-249	250-999	1000+	1-249	250-999	1000+
	Africa	31.7%	26.9%	29.6%	23.5%	16.3%	22.2%	4.3%	2.7%	5.8%
			TOTAL: **29.2%**			TOTAL: **21.8%**			TOTAL: **5.3%**	
	UK & Ireland	28.7%	27%	22.8%	13.8%	13.6%	14.1%	3.8%	6.1%	4.1%
			TOTAL: **26.7%**			TOTAL: **13.9%**			TOTAL: **4.7%**	
	Europe	30.5%	31.9%	27.1%	17.5%	16.9%	13.4%	5.8%	7.4%	***
			TOTAL: **29.5%**			TOTAL: **15.3%**			TOTAL: ***	
	APAC (Oceanic & Australia)	28.5%	34.9%	25.1%	17.6%	18%	14%	5.2%	6.7%	***
			TOTAL: **29.1%**			TOTAL: **17%**			TOTAL: **6.2%**	

***Insufficient data to calculate accurate PPP

- Africa -
81.9%
Improvement

AFRICA

Of all the international data, African citizens appear to be the most vulnerable. As outlined in KnowBe4's African Cybersecurity Research Whitepaper, "From ransomware to phishing, to malware and credential theft, users are not protecting themselves adequately because they mistakenly believe themselves to be informed, ready, and prepared. Of Africans surveyed, 53% think that trusting emails from people they know is good enough; 28% have fallen for a phishing email and 50% have had a malware infection; 52% don't know what multifactor authentication is; and 64% don't know what ransomware is and yet believe they can easily identify a security threat."

On a continent where half a billion citizens are connected to the Internet, and with this number increasing to an estimated 1 billion by 2022 (half a billion more untrained users), this emerging economy is very attractive to cybercriminals for a number of reasons:

1. High degree of digitization of economic activities
2. High unemployment rates drive youths to illegal activities
3. Mobile connectivity, such as the pervasiveness of WhatsApp and it's use for fake news dissemination
4. Immature understanding of the current cyber situation and need
5. Talent gap

AFRICA	BASELINE	90 DAYS	1 YEAR
1-249	31.7%	23.5%	4.3%
250-999	26.9%	16.3%	2.7%
1000+	29.6%	22.2%	5.8%
Average PPP Across All Organization Sizes	29.2%	21.8%	5.3%

The good news is that when organizations adopt an ongoing security awareness and simulated phishing program for a period of 12 months or more, we see the overall PPP drop from 29.2% to 5.3%. This shows that if organizations commit to raising the readiness levels of their employees, they will have a workforce that is more effective in preventing cyberattacks.

- UK&I -

82.4%

Improvement

UNITED KINGDOM & IRELAND

The latest cyberattack trend data in the UK show that the majority of data breaches in 2019 began with a phishing attack. Security consulting firm CybSafe analyzed three years of the UK's Information Commissioner's Office (ICO) cyber breach data from 2017 – 2019. Out of nearly 2,400 reported data breaches, over 1,000 – 45.5% – of attacks were initiated by a phishing attack. According to the report, phishing dominated over unauthorized access, ransomware, malware, and misconfigurations. This preponderance of phishing being the initial attack vector is consistent with the ICO's 2018 data as well, indicating that cybercriminals continue to see phishing as a staple tactic because it just works.

In December 2018, a survey conducted by Censuswide found that 14% of Irish office workers – approximately 185,000 people – have fallen victim to a phishing scam. Additionally, "1) millennials (17%) were most often victims of a phishing scam compared to 6% of Gen X and 7% of Baby Boomers; 2) Almost half (48%) of generation X, those aged 42-54, have been targeted by a phishing scam – with spear phishing believed to be a major contributing factor; 3) 44% of Irish office workers aged 54 and over have clicked on links or attachments from an unrecognized email sender; 4) 20% of survey respondents have never received security awareness training or simulated phishing."

UK & IRELAND	BASELINE	90 DAYS	1 YEAR
1-249	28.7%	13.8%	3.8%
250-999	27%	13.6%	6.1%
1000+	22.8%	14.1%	4.1%
Average PPP Across All Organization Sizes	26.7%	13.9%	4.7%

KnowBe4 regional benchmark data shows that by implementing a new-school approach to security awareness training, organizations in the United Kingdom and Ireland region were able to reduce their PPP from 26.7% to 4.7% in 12 months.

- Europe -
Incomplete data set, yet trending favorably as expected

EUROPE

According to Europol's European Cybercrime Centre (EC3), the European Police Office which is the official intelligence agency of the European Union, in 2018, "75% of EU Member States had active investigations into phishing, while Europol stakeholders consistently highlighting phishing or related attacks as the single most common attack vector with 65% of all reported cases". Additionally, the European Payments Council reported that "social engineering attacks and phishing attempts are still increasing and they remain instrumental often in combination with malware, with a shift from consumers, retailers, Subject Matter Experts to company executives, employees (through "CEO fraud"), financial institutions and payment infrastructures and more frequently leading to authorized push payments fraud."

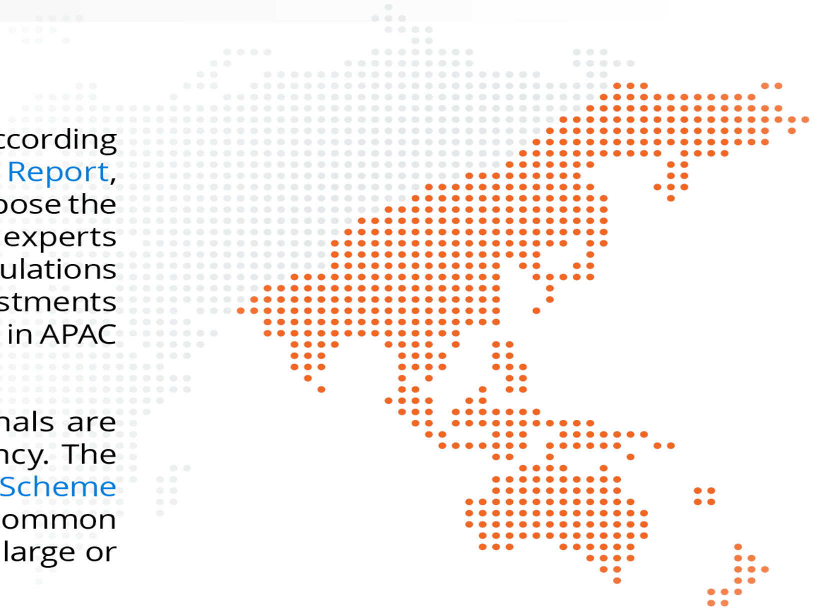
EUROPE	BASELINE	90 DAYS	1 YEAR
1-249	30.5%	17.5%	5.8%
250-999	31.9%	16.9%	7.4%
1000+	27.1%	13.4%	***
Average PPP Across All Organization Sizes	29.5%	15.3%	***

***Insufficient data to calculate accurate PPP

Due to KnowBe4's recent expansion into the EU, there was not enough data gathered yet to perform a statistically sound analysis for a valid 12+ month period for the 1,000+ size organizations. This additional data should be available in the next report. That being said, with the European data so closely mirroring the North American data, we anticipate the EU Large Account 12+ month data to follow that trend. We look forward to continuing to add to the volume of phishing-related data that we are able to gather from this important region.

- APAC -
78.7%
Improvement

ASIA-PACIFIC



Cybercrime continues to be an increasing risk when doing business across APAC. According to Marsh & McLennan Companies Asia Pacific Risk Center's Cyber Risk in Asia Pacific Report, "rapidly growing connectivity and the accelerating pace of digital transformation expose the APAC region, and make it particularly vulnerable to cyber exploitation." In addition, experts note that there is a lack of transparency in APAC which "results in weak cyber regulations and enforcements by authorities, as well as low cyber awareness and security investments among corporations." As a result, the report shows that organizations and individuals in APAC are 80% more likely to be targeted by hackers than other parts of the world.

Whether it's Australia, New Zealand or any other country across APAC, criminals are increasingly using social engineering to access systems and steal data and currency. The Office of the Australian Information Center shared in its Notifiable Data Breaches Scheme 12-Month Insights Report that "phishing and spear phishing continue to be the most common and highly effective methods by which entities are being compromised—whether large or small—in Australia or internationally."

APAC	BASELINE	90 DAYS	1 YEAR
1-249	28.5%	17.6%	5.2%
250-999	34.9%	18%	6.7%
1000+	25.1%	14%	***
Average PPP Across All Organization Sizes	29.1%	17%	6.2%

***Insufficient data to calculate accurate PPP

With a baseline PPP beginning at 29.1% and decreasing to 6.2% after 12+ months of ongoing new-school security awareness training and simulated phishing, we see that – as with customers in other regions – KnowBe4 APAC customers are successfully helping their employees make smarter security decisions, every day.

Agenda

1. The phishing problem
2. Phishing benchmark data by industry
3. International phishing benchmark data by region
4. Actionable tips to create your “human firewall”

People are a critical layer within the fabric of our Security Programs

Security Awareness and Secure Behavior are NOT the Same Thing

Traditional awareness programs fail to account for the *knowledge-intention-behavior gap*

KnowBe4
Human error. Conquered.

There are Three Realities of Security Awareness

1

Just because I'm **aware** doesn't mean that I **care**.

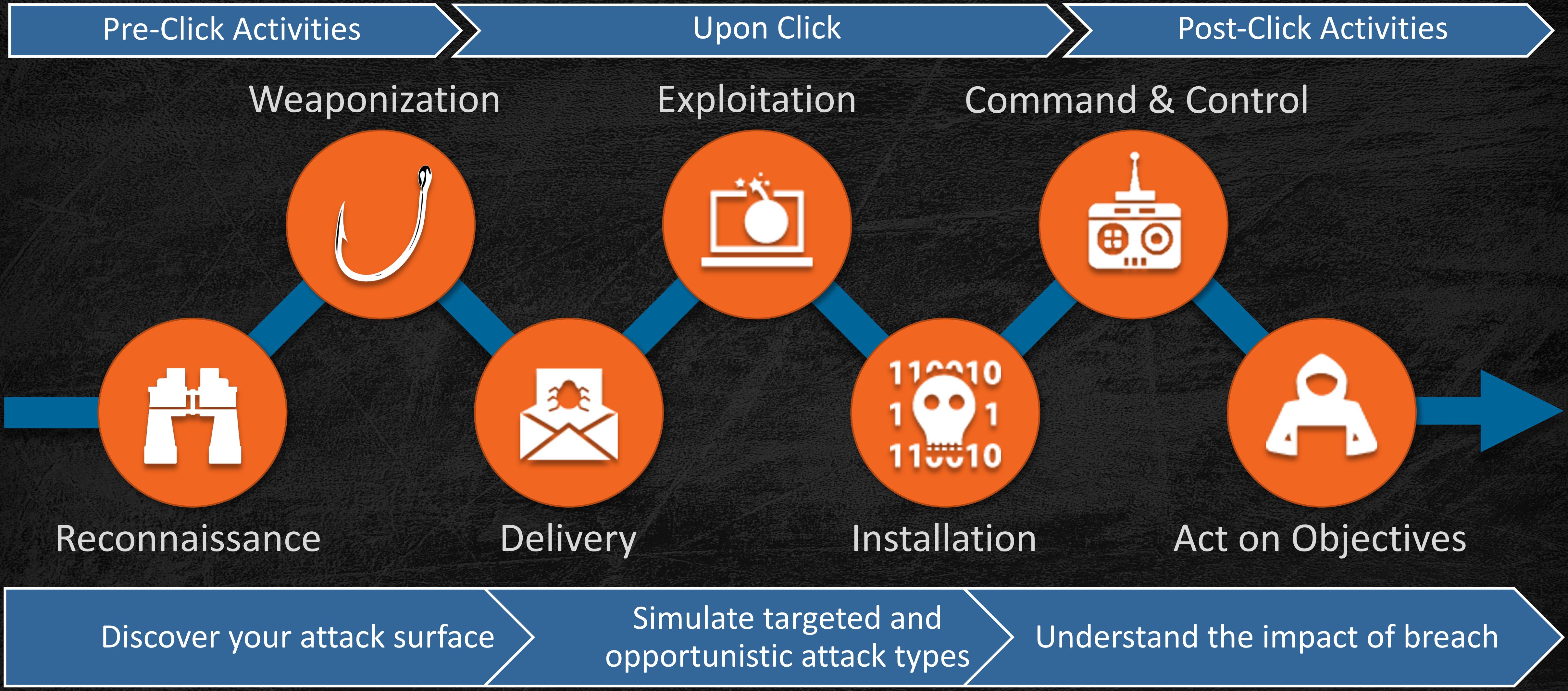
2

If you try to work **against** human nature, you will **fail**.

3

What your employees **do** is way more important than what they **know**.

Train by Simulating the Steps taken by Attackers



Pre-Click Activities

Upon Click

Post-Click Activities

Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command & Control

Act on Objectives

Discover your attack surface

Simulate targeted and opportunistic attack types

Understand the impact of breach

Bait the **hook!**

- Understand the types of email subjects that will realistically test your users susceptibility to phishing.
- Know the types of 'in the wild' phishing scams that are occurring so that you can work to inoculate your users!

Social Engineering

-- effective phishing lures --

Greed

Curiosity

Self Interest

Money

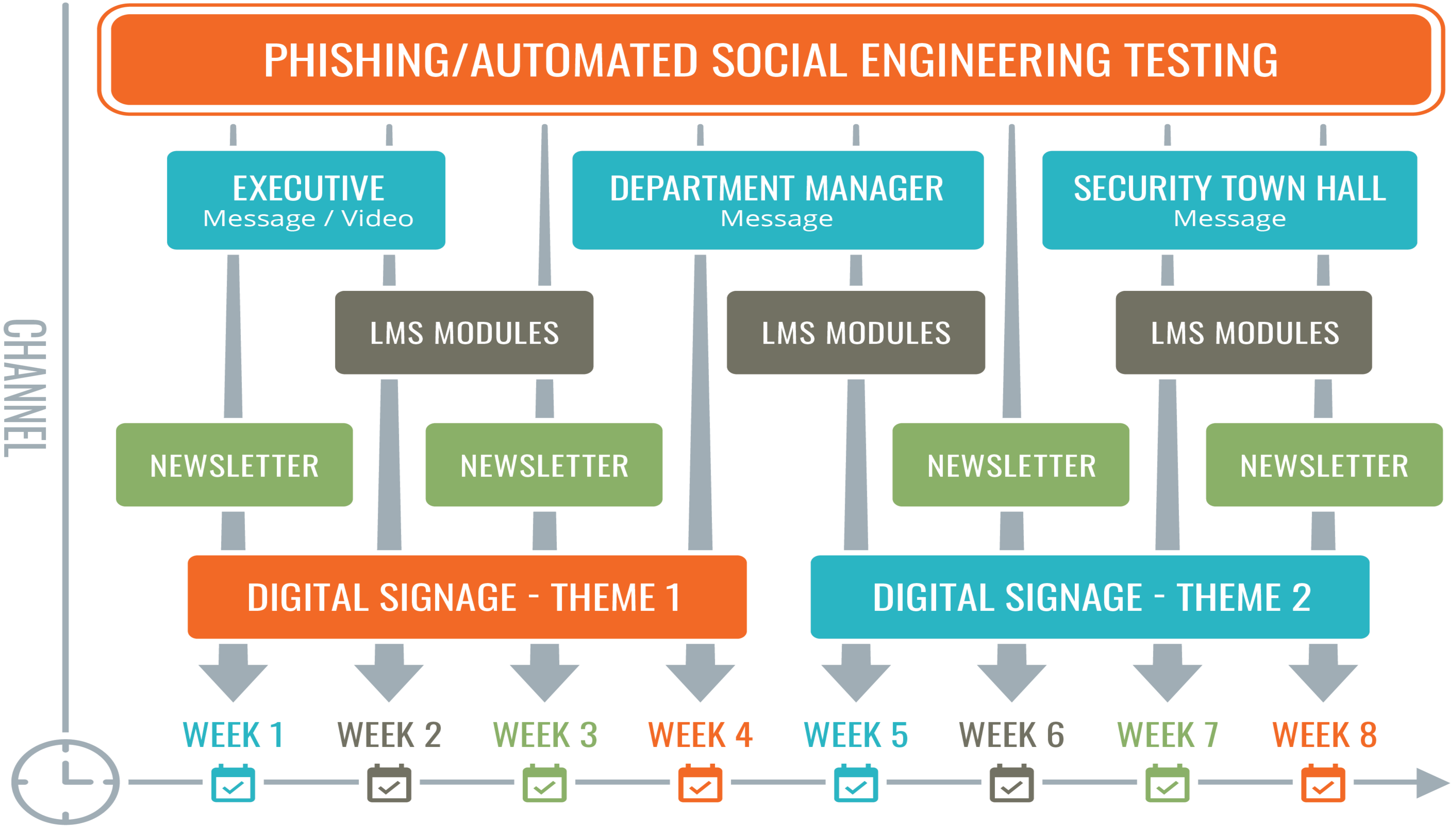
Urgency

Fear

Helpfulness

Hunger

Plan like a Marketer. Test like an Attacker.

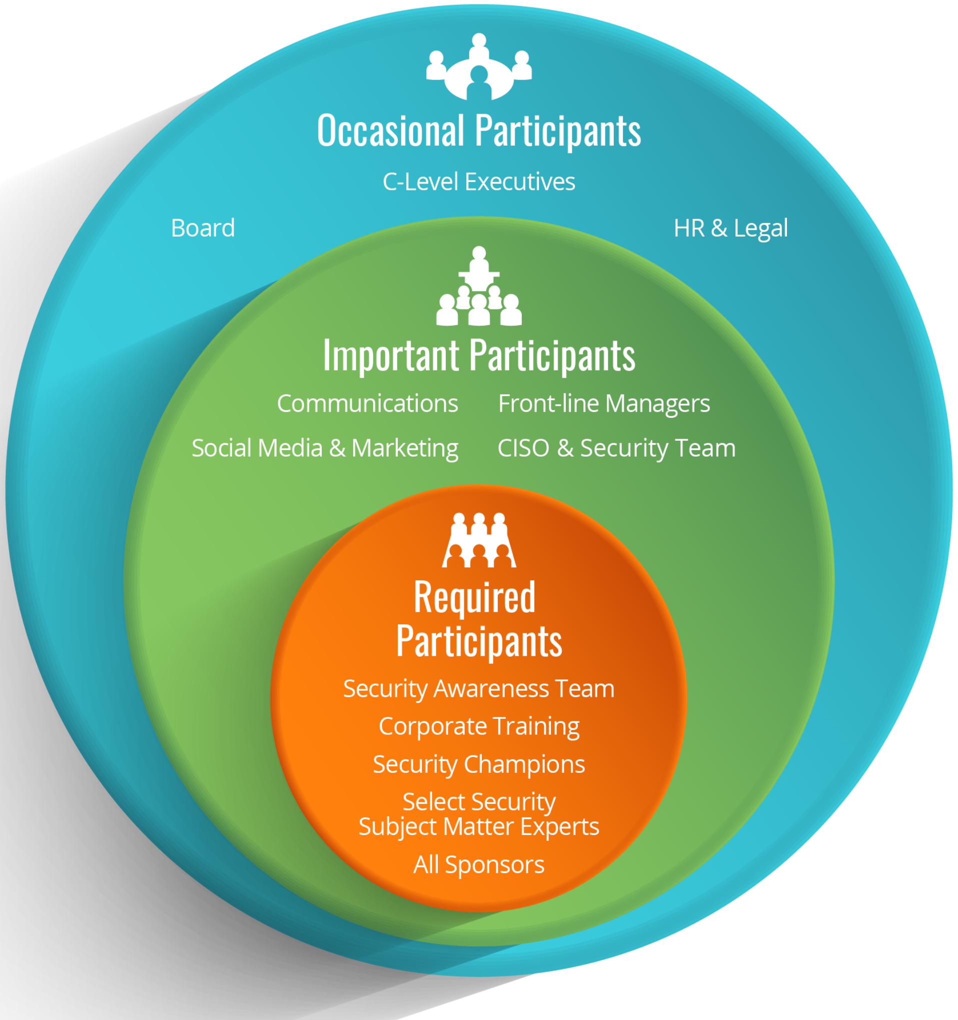


Final Thoughts

- Humans are the de-facto top choice for cybercriminals seeking to gain access into an organization.
- Security Awareness and frequent simulated social engineering testing is a proven method to dramatically slash your organization's phish prone percentage.
- Effectively managing this problem requires ongoing due diligence, but it *can* be done and it isn't difficult. We're here to help.

Some Executive Takeaways

- ✓ Role Modeling: If you expect your organization to do the right thing, you must lead them accordingly.
- ✓ Engaging a Pro: 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.
- ✓ 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 take-aways.
- ✓ Mobilizing a Security "Culture Carrier" Program_ Provides an organizationally dispersed team of advocates that can reinforce security messaging and learning at local levels.



Occasional Participants

C-Level Executives

Board

HR & Legal

Important Participants

Communications

Front-line Managers

Social Media & Marketing

CISO & Security Team

Required Participants

Security Awareness Team

Corporate Training

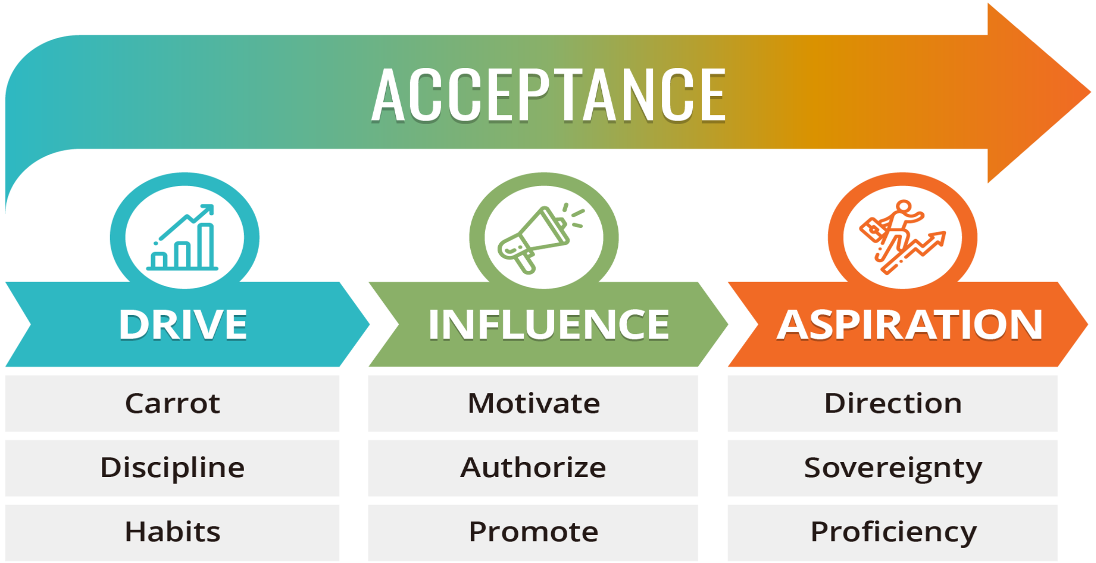
Security Champions

Select Security Subject Matter Experts

All Sponsors

Some Executive Takeaways

- ✓ **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 mischievous email.
- ✓ **Increasing Frequency:** tent and simulated phishing campaigns (twice monthly for high risk targets).
- ✓ **Hiring the Right People:** Target creative candidates that 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 protecting systems, employees and data.
- ✓ **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.



ACCEPTANCE

DRIVE	INFLUENCE	ASPIRATION
Carrot	Motivate	Direction
Discipline	Authorize	Sovereignty
Habits	Promote	Proficiency

A Security Awareness Training Program that Works!

Baseline Testing

We provide baseline testing to assess the Phish-prone™ percentage of your users through a free simulated phishing attack.

Train Your Users

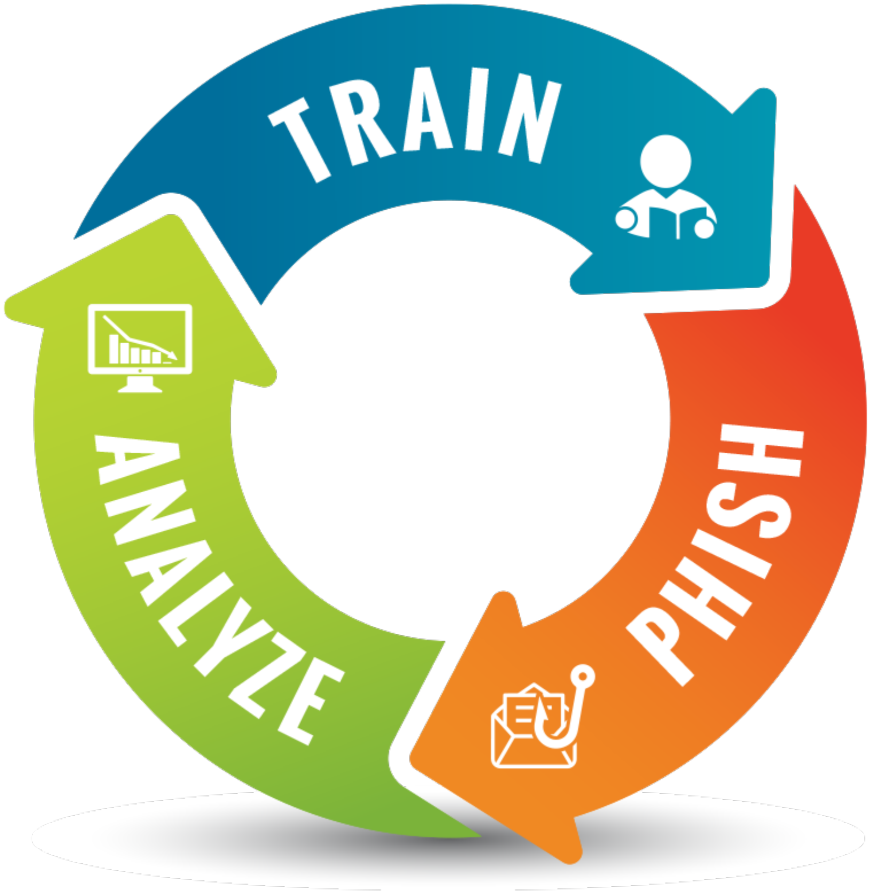
On-demand, interactive, engaging training with common traps, live hacking demos and new scenario-based Danger Zone exercises and educate with ongoing security hints and tips emails.

Phish Your Users

Fully automated simulated phishing attacks, hundreds of templates with unlimited usage, and community phishing templates.

See the Results

Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!



Thank You

KnowBe4

Human error. Conquered.