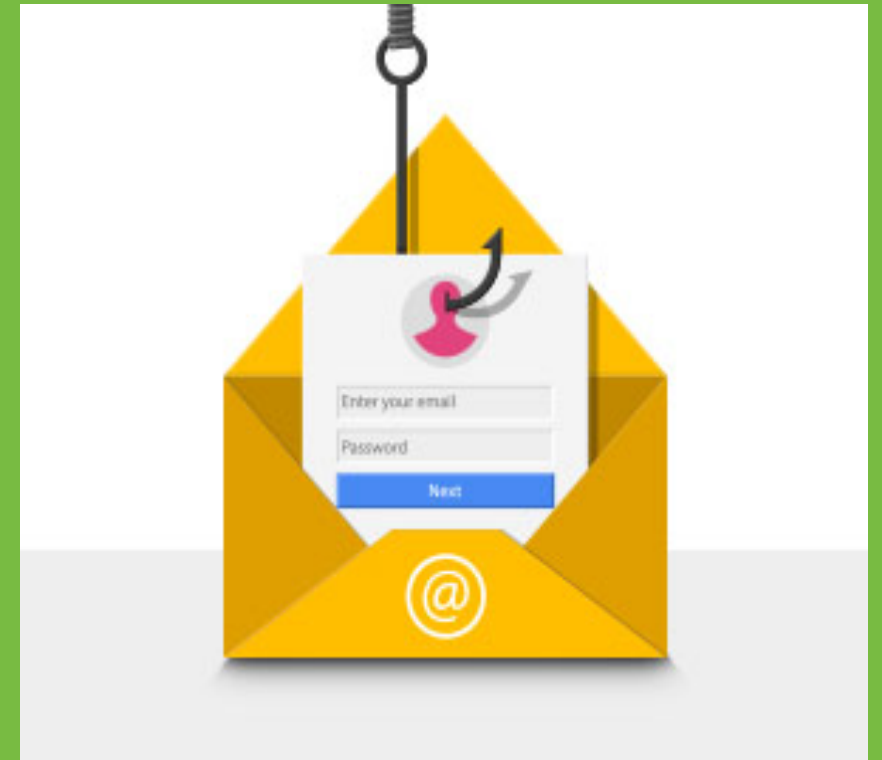


Are You Preparing End Users For Phishing Attacks?

Presented by ASMGi and KnowBe4

September 12, 2019



Today's Presenters - *Are You Preparing End Users For Phishing Attacks?*

Steve Roesing

President, CEO, ASMGi

sroesing@asmgi.com



Cienne Blackburn

Channel Account Manager, KnowBe4

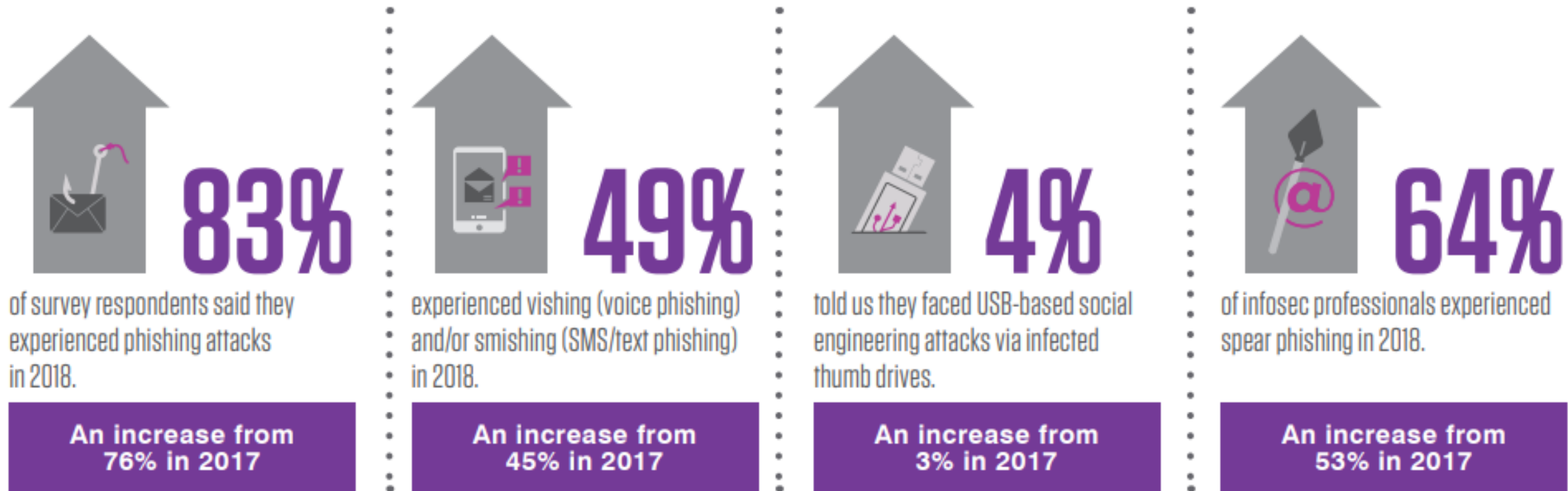
cienneb@knowbe4.com



Stats are staggering ... Phishing is not slowing down anytime soon



2019 State of the Phish: From over 15,000 InfoSec professionals surveyed ...



How relevant is Security Awareness Training ?

Compliance:

PCI-DSS: 12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.

HIPAA: 164.308 (a)(5)(i) – Implement a security awareness and training program for all members of its workforce (including management).

CobiT: PO7.4 Personnel Training – Provide IT employees with appropriate orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls and security awareness at the level required to achieve organizational goals.

Frameworks:

NIST: NIST SP 800-50, Building an Information Technology Security Awareness and Training Program / NIST SP 800-53, AT 1-5: Security Awareness and Training Policy and Procedures, Security Awareness Training ...

ISO/IEC 27001, 2: 8.2.2 – All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

CIS: Organizational Controls: CIS 17 –Implement a Security Awareness and Training Program

A Holistic Approach to Cyber Security



Total Solution = 3 Pillars

Program




Technology



Operations




Building a Security Awareness Program


 **ASAP** | Automated Security Awareness Program

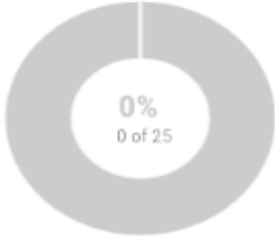
[Download PDF](#) [Change Start Date](#) [Reset My Program](#)

Your Security Awareness Program Tasks


Based on your questionnaire feedback, we have generated the following tasks that need to be completed for you to get the most out of your Automated Security Awareness Program.










 Task List

 Calendar



Click each task to learn more about recommended settings and best practices



1. Engage your stakeholders <i>(Estimated Duration: 1 day)</i>	Due on July 25, 2017	
2. Customize your KnowBe4 console <i>(Estimated Duration: 30 minutes)</i>	Due on July 26, 2017	
3. Whitelist the KnowBe4 mail servers <i>(Estimated Duration: 1 day)</i>	Due on July 28, 2017	
4. Import your users <i>(Estimated Duration: 1 day)</i>	Due on July 31, 2017	
5. Create and complete a baseline phishing campaign <i>(Estimated Duration: 1 hour)</i>	Due on August 4, 2017	
6. Review the results of your phishing test <i>(Estimated Duration: 30 minutes)</i>	Due on August 8, 2017	
7. Communicate the Security Awareness Program with your employees <i>(Estimated Duration: 4 hours)</i>	Due on August 9, 2017	
8. Install the Phish Alert Button (PAB) <i>(Estimated Duration: Variable)</i>	Due on August 14, 2017	
9. Review and select a primary training module <i>(Estimated Duration: 4 hours)</i>	Due on August 15, 2017	

KnowBe4 Product Suite to Manage Security and Compliance Issues



Security Awareness Training Platform

Discover how you can enable your employees to make smarter security decisions with training and simulated social engineering.



PhishER

Learn how you can identify and respond to reported email threats faster and automate your email incident response plan.



KCM GRC Platform

Find out how you can efficiently and effectively manage risk and compliance and get insight into gaps in your security plan.



Free Tools

Learn how you can identify potential vulnerabilities in your organization and stay on top of your defense-in-depth plan.

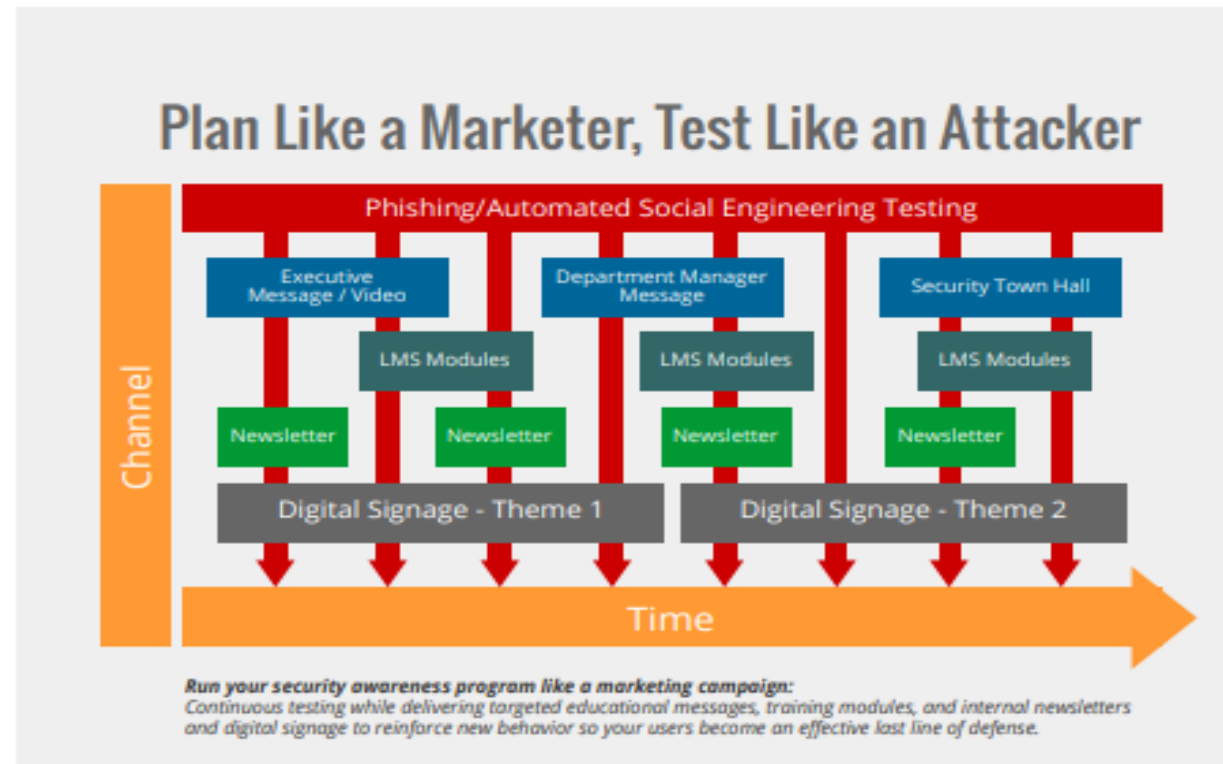
Executing the plan ...

2019 Phishing By Industry Benchmarking Report

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.

- 1 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.
- 2 Don't do this alone.** Involve other teams and executives, including Human Resources and IT and even Marketing. Create a positive, company-wide culture of security.
- 3 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.
- 4 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.
- 5 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 secure reflexes so your workforce becomes an effective last line of defense.



Executing the plan ...

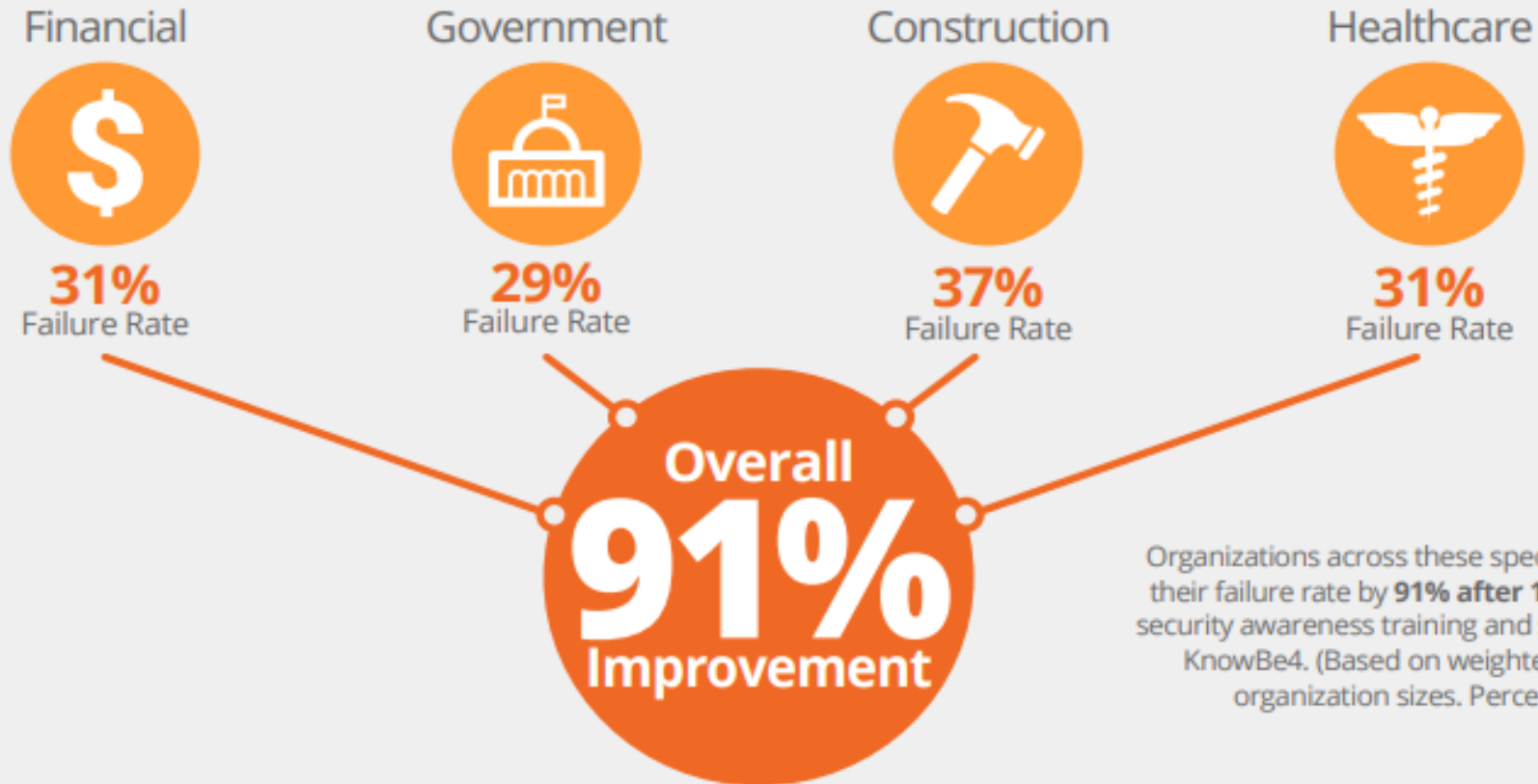
4 Steps for Phishing Your Users

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-style 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 Phish-prone as possible.

Results...

Average Initial Phish-prone Percentage By Industry



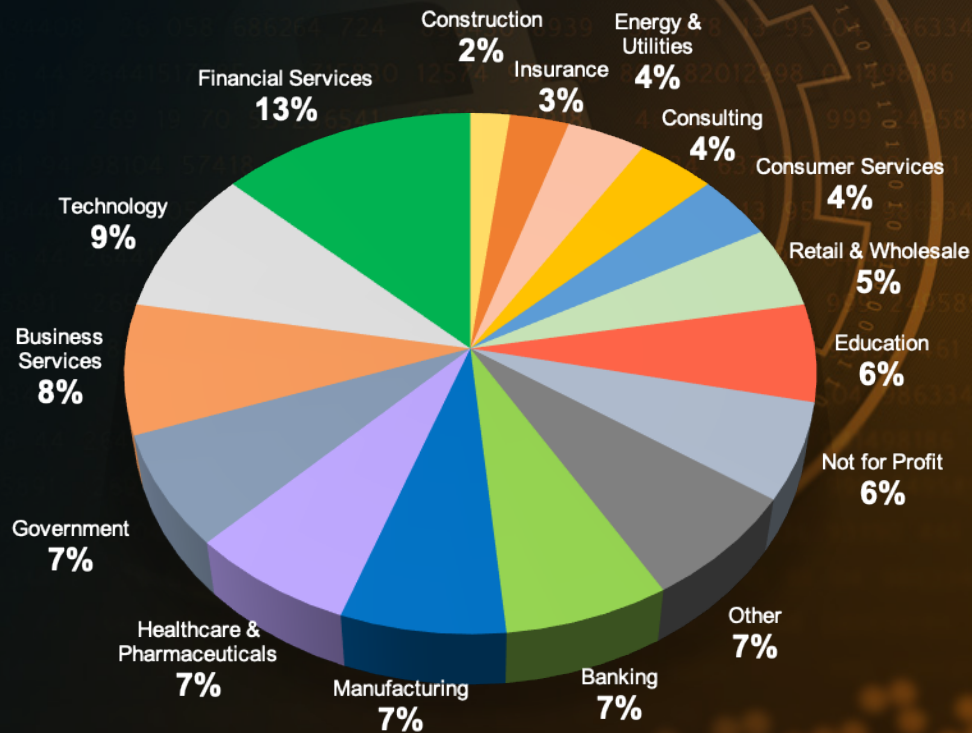


KnowBe4
Human error. Conquered.

KnowBe4 Mission

Enable your employees to make smarter security decisions, every day

Over
27,000
Customers



About KnowBe4

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- KnowBe4 helps tens of thousands of organizations manage the ongoing problem of social engineering
- KnowBe4 provides an affordable, easy-to-use GRC tool that helps organizations cut down audit time and manage your compliance and risk projects faster than ever



A staggering

91%

of successful data breaches start with
a spear phishing attack

Users Are the Last Line of Defense

- 91% of successful data breaches start with a spear phishing attack
- 30% of data breaches are caused by repeat offenders from within the organization



\$133K

The Costs of Breaches and Ransomware Attacks

- 34% of businesses hit with malware take a **week or more** to regain access to their data
- The **average cost** of a ransomware attack on businesses is **\$133,000**
- 75% of companies infected with ransomware are running **up-to-date** endpoint protection

CEO Fraud and BEC Caused

\$12.5B

In Identified Global Losses

BEC Attacks Are Growing

- **Business Email Compromise (BEC)** increased 136% in identified global exposed losses between Dec. 2016 and May 2018
- These attacks often contain **no links, no attachments** and no spelling or grammar errors.

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

KnowBe4
is the
8th Layer in
Security

i.e. Building the
HUMAN FIREWALL



Platform for Awareness Training and Testing

- 1 Train Your Users
- 2 Phish Your Users
- 3 See the Results



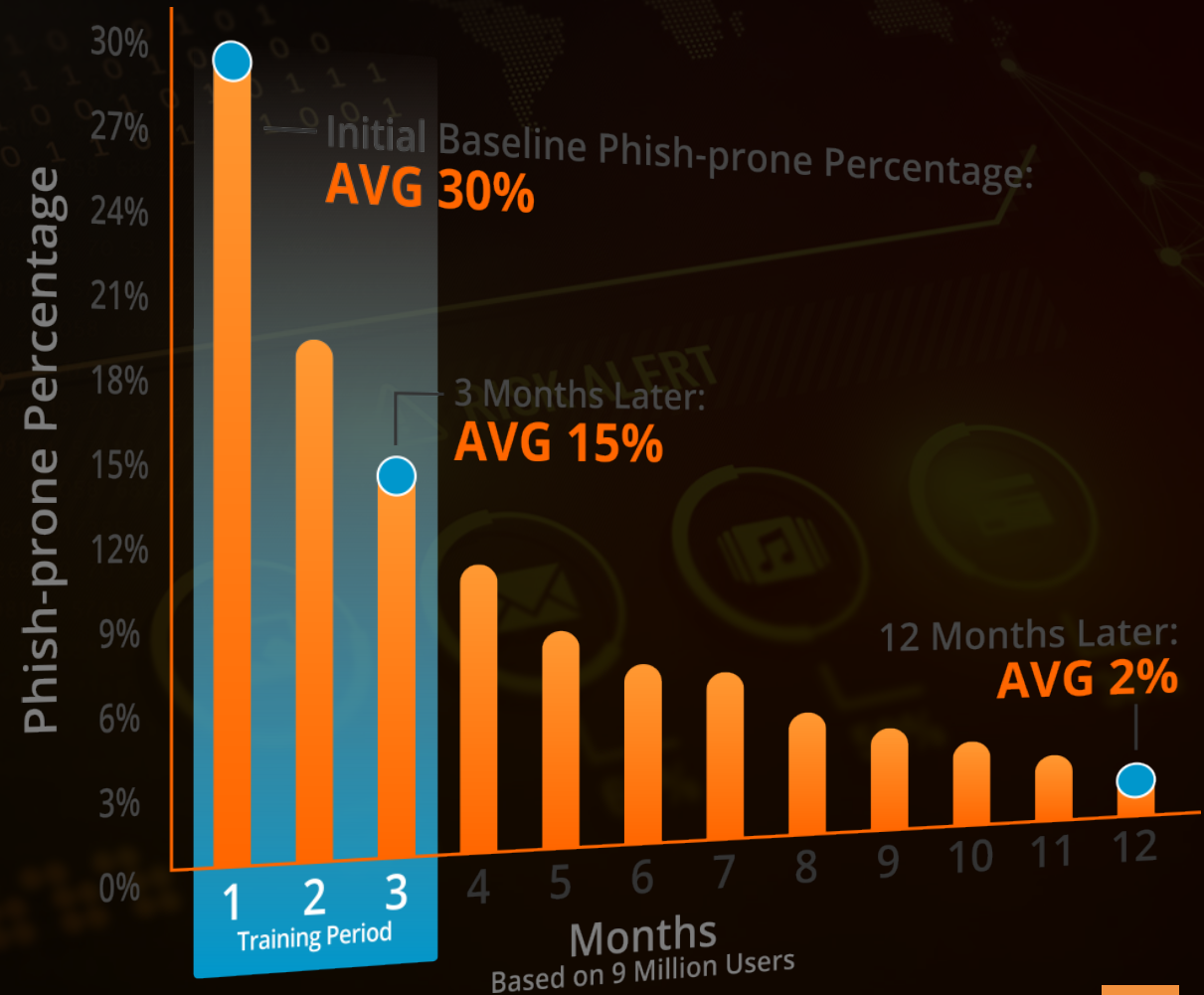
- Reduced Malware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

127% ROI

With a One-Month Payback

FORRESTER®

Generating Industry-Leading Results and ROI





KnowBe4
Human error. Conquered.

Thank You

Upcoming Webinars and Events



Events

- ◆ *September 25th 4PM - **Cyber Security Issues in Higher Education***
panel discussion at the Union League of Philadelphia
- ◆ *October 21-25 - **Information Security Summit***
at The Cleveland I-X Center

Webinars

- ◆ *September 18 - **Setting the Trap: Crafty Ways The Bad Guys Use Pretexting To Own Your Network***
presented by KnowBe4
- ◆ *October 3 - **Securing Your Endpoints – Why Are Businesses Getting Hit With So Much Malware?***
presented by ASMGi and Malwarebytes
- ◆ *October 10 - **Where Will You Compute Securely?***
presented by ASMGi and Flexential
- ◆ *October 17 - **Do You Know Where Your Data Is And Who Is Accessing?***
presented by ASMGi and Heureka



QUESTIONS?



Thank You!

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Fax: 216.274.9647

Email: info@asmgi.com

www.asmgi.com