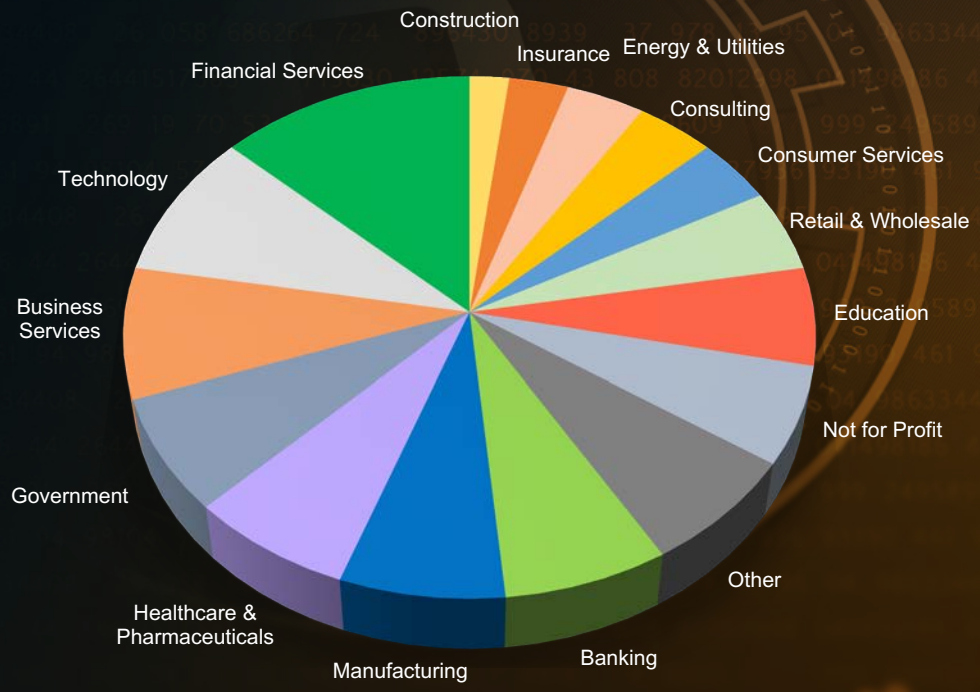

KnowBe4
Human error. Conquered.
KnowBe4 is the world’s largest security awareness training and simulated phishing platform that helps you manage the ongoing problem of social engineering.

Over

39,000

Customers



About Us

- 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
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- Winner of five consecutive Inc. 500 awards

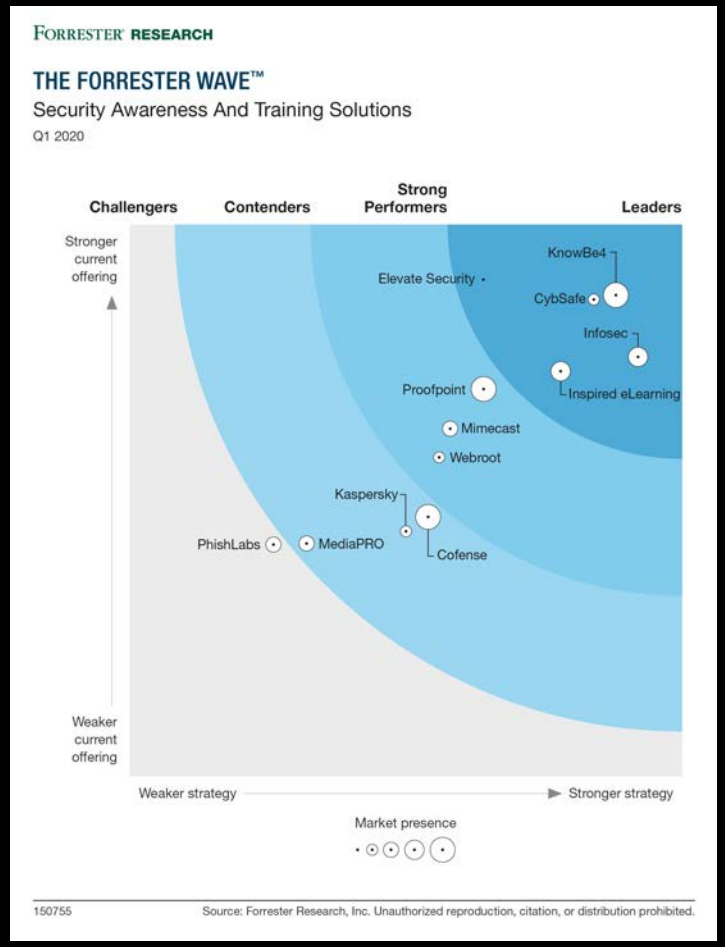
CYBERSECURITY 500 WORLD'S HOTTEST SECURITY COMPANIES

AMERICA'S FASTEST-GROWING Inc. 500 PRIVATE COMPANIES

Entrepreneur | cultureIQ TOP COMPANY CULTURES 2017

KnowBe4 Named a Leader in The Forrester Wave™: Security Awareness and Training Solutions, Q1 2020

KnowBe4 received the highest scores possible in 17 of the 23 evaluation criteria, including learner content and go-to-market approach.



Using a 23-criteria evaluation, the Forrester Wave ranks 12 vendors in the security awareness and training market based on their current offering, strategy, and market presence.

The Forrester Wave™: Security Awareness and Training Solutions, Q1 2020, Forrester Research, Inc., February 25, 2020

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

Customers Are Building a Modern Security Stack....

People

Infrastructure

Devices

Network

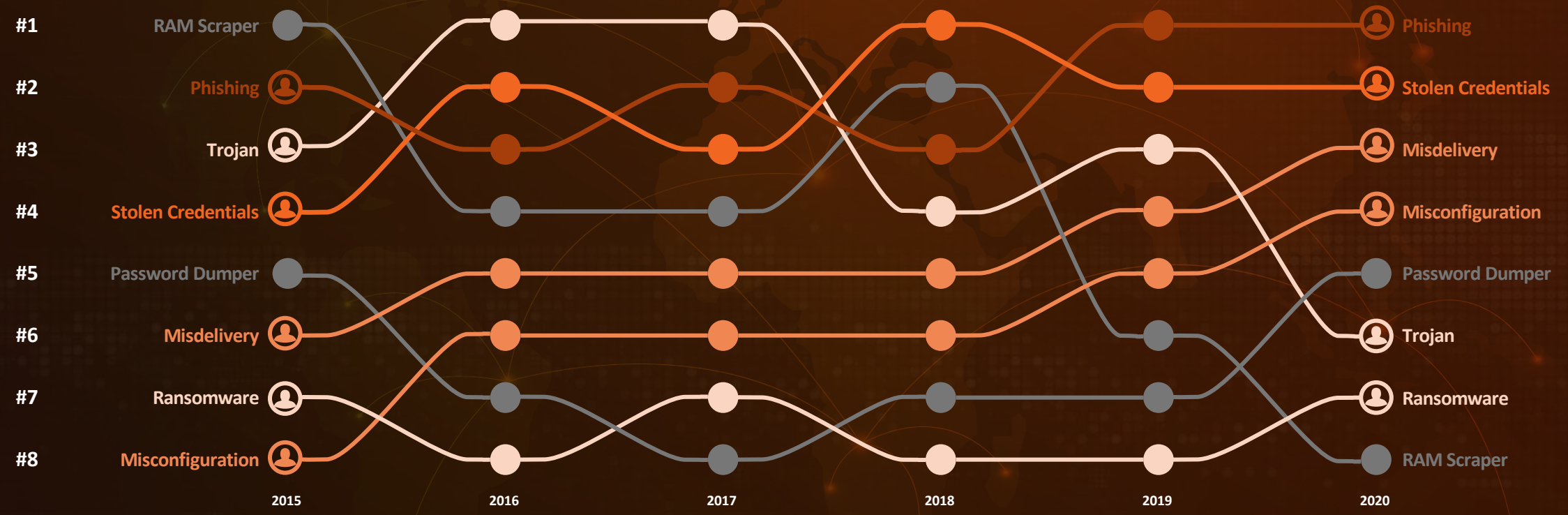
...That Starts With the Human

Your Employees Are Your Last Line Of Defense

- **91%** of successful data breaches started with a spear phishing attack
- Losses to **CEO Fraud** (aka Business Email Compromise**) increased by 48%** in Q2, 2020
- **W-2 Scams** social engineer Accounting/HR to send tax forms to the bad guys
- **Ransomware** damage costs predicted to reach $20 billion by 2021

Humans Have Always Been the Weakest Link in Security

Rank of Select Threat Action Varieties in Breaches Over Time
Ranking



The human layer represents a **high value and probability target** at **low time and cost** to implement for attackers

Source: Verizon 2020 Data Breach Investigations Report

KnowBe4
Human error. Conquered.

HOW CEO FRAUD IMPACTS YOU

THE START

Attackers see if they can spoof your domain and impersonate the CEO (or other important people)

Bad guys often troll companies for months to gather the data necessary in pulling off a successful attack

THE PHISH

Spoofed emails are sent to high-risk employees in the organization

To: Finance Department

Urgent wire transfer request! Please send $100,000 to new acct #987654-3210

To: CFO

Please pay this time-sensitive invoice. I'm on vacation and will be unavailable, no need to respond. - Your CEO

To: Human Resources

I need a PDF copy of ALL employee W-2s for the IRS ASAP!

THE RESPONSE

Target receives email and acts without reflection or questioning the source

I better get this payment to the new account!

It's from the CEO, I'll take care of this for him!

Sounds important. I'll send these right away!

THE DAMAGE

Social engineering was successful, giving hackers access to what they were after

Causing fraudulent wire transfers and massive data breaches

THE RESULT

The fallout after a successful attack can be highly damaging for both the company and its employees

Resulting damage:

- ✔ **Money is gone forever in most cases and only recovered 4% of the time**
- ✔ **CEO is fired**
- ✔ **CFO is fired**
- ✔ **Lawsuits are filed**
- ✔ **Intangibles - tarnished reputation, loss of trust, etc.**

So... Think Before You Click!

SECURITY AWARENESS TRAINING | www.KNOWBE4.COM

How Can We Protect Our Organization?

- **Users are unaware of the internet dangers** and get tricked by social engineering to click on a malicious link in a (spear)phishing email or opening an email attachment they did not ask for.

- Employees have a false sense of security and believe their **anti-virus** has them covered. With the firehose of spam and malicious email that attack your network, **7-10% make it past your filters**.

- Surprisingly often, **backups** turn out not to work or it takes days to restore a system.

- Today, an essential, additional security layer is to have your employees be your **last line of defense.**

How Do You Manage the Ongoing Problem of Social Engineering?

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

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

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

Develop a Fully Mature Awareness Program

- **Awareness Training** on its own, typically once a year, is far from enough.
- **Simulated phishing tests** of groups of employees doesn't work on its own either.
- But **together,** done frequently, and reinforcing each other, they can be combined to greatly **increase effectiveness**.

KnowBe4
Human error. Conquered.

Train Everyone

- In order to create a security culture and change the behavior of your employees, you have to ***train everyone***, from the board room to the lunchroom, and include the training in the onboarding of every new employee.
- This should be ***on-demand, interactive, engaging*** and create a thorough understanding of how cybercriminals operate.
- Employees need to understand the mechanisms of:
  - Spam
  - Phishing
  - Spear phishing
  - Malware
  - Ransomware
  - Social engineering

And be able to apply this in their day-to-day job.

Baseline Phishing Test

- Security awareness training can be undermined due to difficulty in measuring its impact. “**You can’t manage what you don’t measure**”

- It is vital to **establish a baseline** on phishing click-through rates. This is easily accomplished by sending out a simulated phishing email to a random sample of personnel.

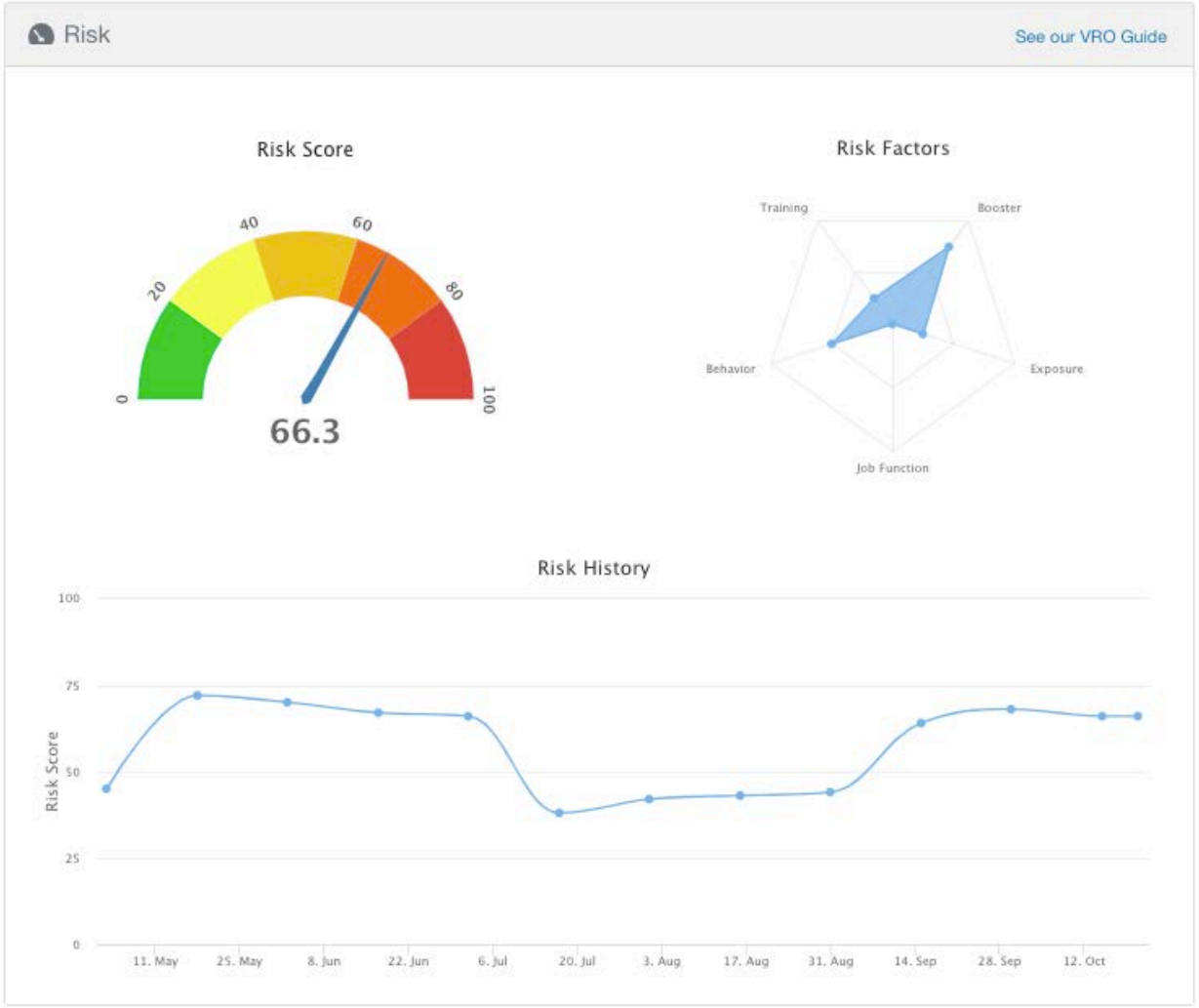
- You find out the number that are tricked into clicking. This is your baseline **“Phish-prone percentage”** that you use as the catalyst to kickoff your training campaign.

Virtual Risk Officer™

- **Identify risk** at the user, group, and organizational level to enable you to make data-driven decisions for your security awareness plan.

- With Virtual Risk Officer's **Risk Score**, answer questions like:
  - What users are the most vulnerable to a phishing attack?
  - What groups haven't had any training?
  - What types of phishing templates are my users most prone to clicking?
  - What are my highest-risk groups?

- Risk Score enables you to take action and **implement security awareness mitigation plans** for high-risk user groups

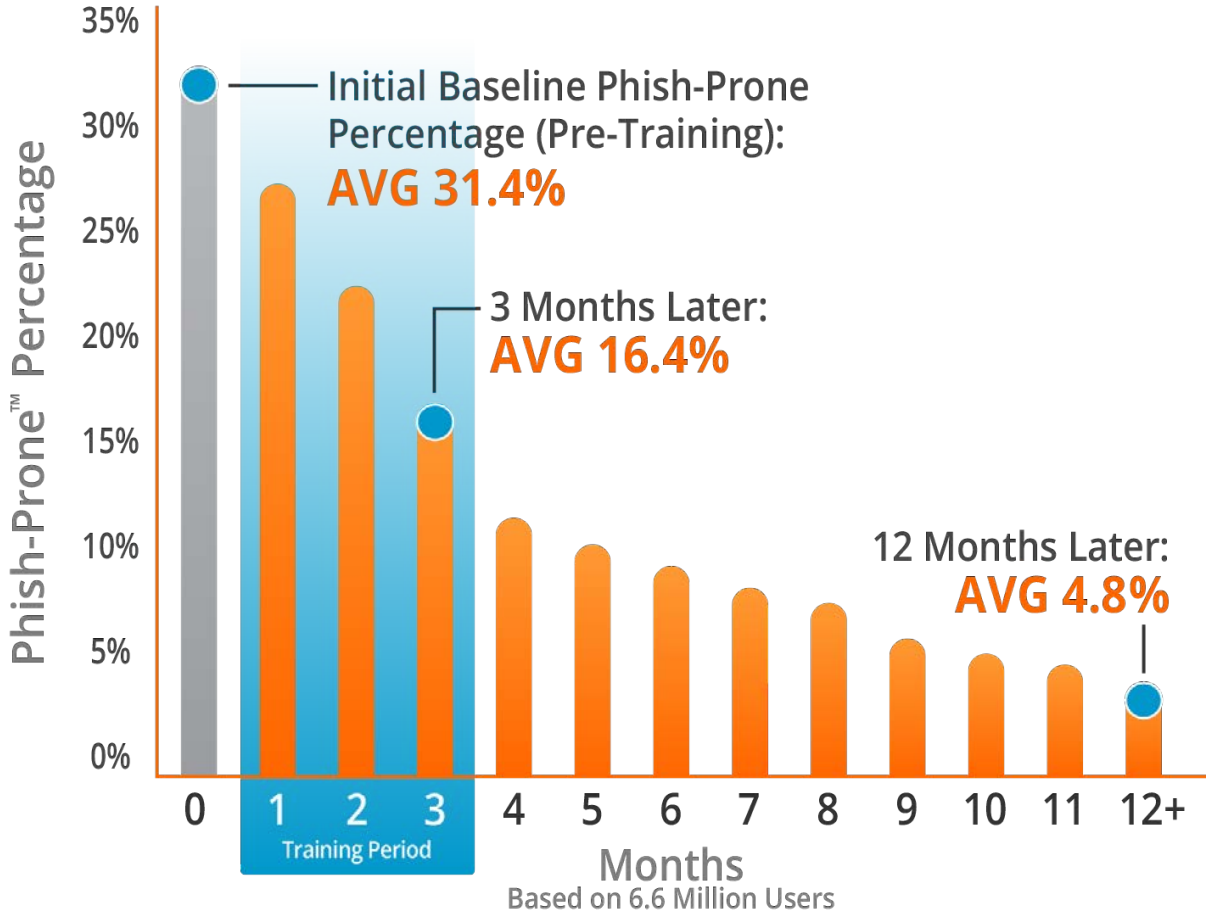


Continue to Test Employees Regularly

- Even when testing confirms that phishing susceptibility has fallen to nominal levels, **continue to test** employees frequently to keep them on their toes, **with security top of mind.**
- The **bad guys are always changing the rules**, adjusting their tactics and upgrading their technologies.
- **Analyze your phishing data**. Continue to train and phish your users with more advanced tactics such as attachments and landing pages where they are asked to enter data.
- Over time, **increase the difficulty of the attacks**, KnowBe4 has 8,000+ templates rated by difficulty from 1 to 5.

KnowBe4 Security Awareness Training Works

Effectively managing this problem requires ongoing due diligence, but it *can* be done and it isn't difficult. ***We're here to help.***



Source: 2021 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.

KnowBe4
Human error. Conquered.

KnowBe4

Human error. Conquered.