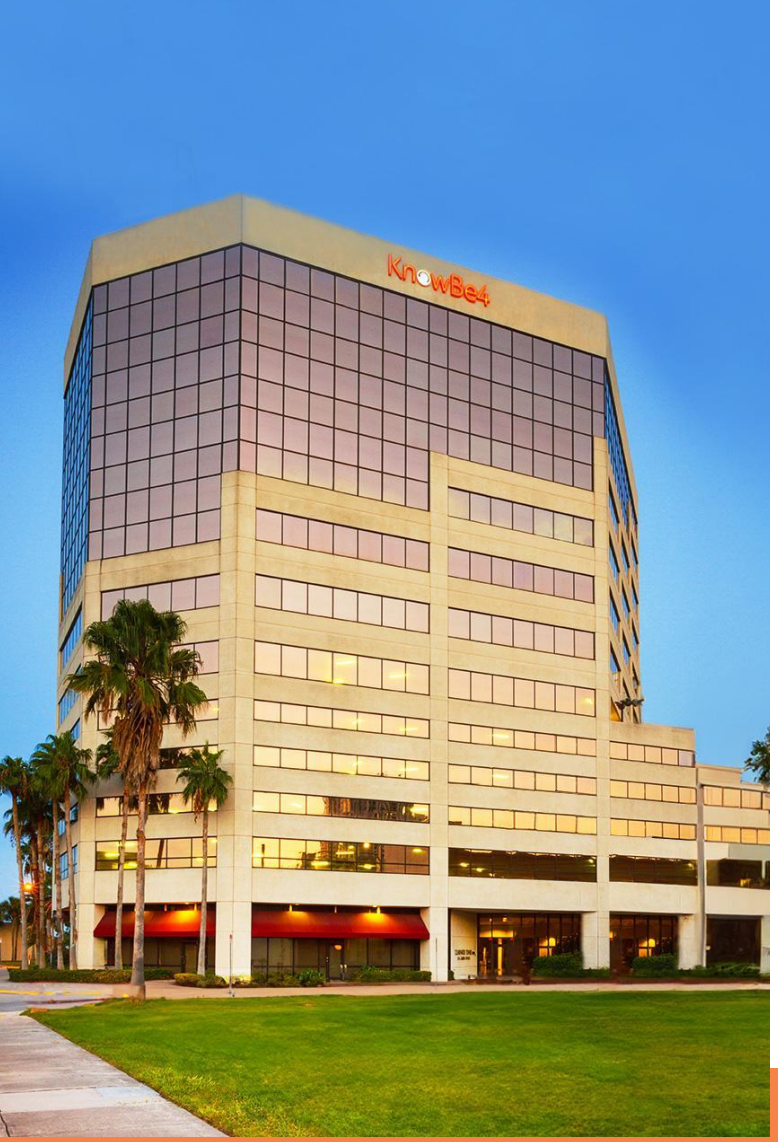
SUNY Implementation plan



Agenda

- Introductions
- Security Culture Maturity Model
- Implementation Phases
- Support Model
- Q&A

KnowBe4

Introductions

KnowBe4 & NewPush – Strategic Partners

SUNY and NewPush/KnowBe4 have contracted into a 5-year agreement for Human Risk Management.

- Centralized Purchasing & Contract Management, through the office of the CTO
- Streamlined engagement and support model
- Knowledge sharing, an interactive SUNY community
- Product Updates, Industry Awareness
- Consulting, Troubleshooting, Best Practices, Q&A

Meet Your Partner Teams

KnowBe4

Onboarding, Implementation, Best Practices, Roadmap

- Max Brannen
  Customer Success Manager (Enterprise)MBA,SACP,CCPA
- Leslie Portis
  Customer Implementation Specialist (New Universities)
- Miesh Blankenship
  Account Manager (ENT/Strategic)

NewPush

Operational Support, Troubleshooting, Best Practices, Product capabilities

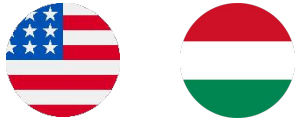
- Zsofia Csaba-Toth
  Director of Operations
- Dino Minuti
  COO / Sales & Engagement Manager

Company Snapshot

newpush®

NewPush is a managed security services provider (MSSP) committed to empowering enterprises with comprehensive, cutting-edge cybersecurity solutions with a dedicated Human Risk Management practice.

Global HQ in Baltimore (US) and European HQ in Budapest (HU)
Privately held



International presence in **US, EU, LatAm**

20+ years
providing Cloud Services and Security solutions as a service

HITRUST* CSF Certified

PCI DSS COMPLIANT

SOC II TYPE II AICPA SOC

5,000+
SMB to Fortune 1000 clients across **major industries**

Better Business Bureau Certified MBE
Accredited Since: 4/7/2004
Years in Business: 21

A+ Rating BBB ACCREDITED BUSINESS

Global delivery capabilities in Baltimore, Budapest, Denver, and Santiago

SAM.GOV®

CAGE code

8THJ1

* Staff with CISSP, HITRUST CCSFP, HITRUST CHQP certification, SOC II with HITRUST Framework

KnowBe4 – The #1Platform for Human Risk Management

70k

Nearly **70,000 organizations** rely on KnowBe4 so employees remain vigilant of social engineering

50m+

50 million plus users everyday engage with the KnowBe4 platform to stay protected from bad actors

17m+

17 million email messages quarantined as malicious by PhishER Plus

7

KnowBe4

Next Steps

Security Culture Maturity Model - What is it?

SCMM

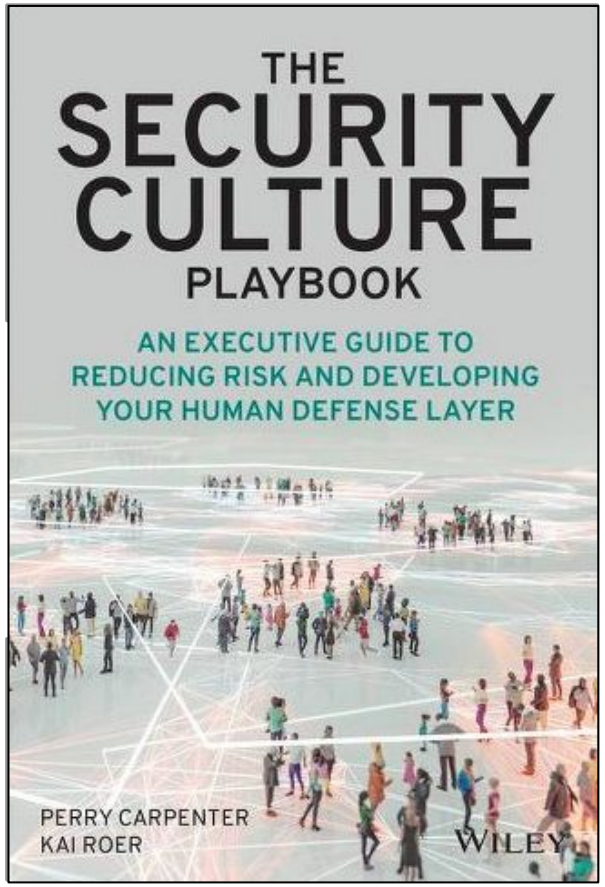
Link to resource

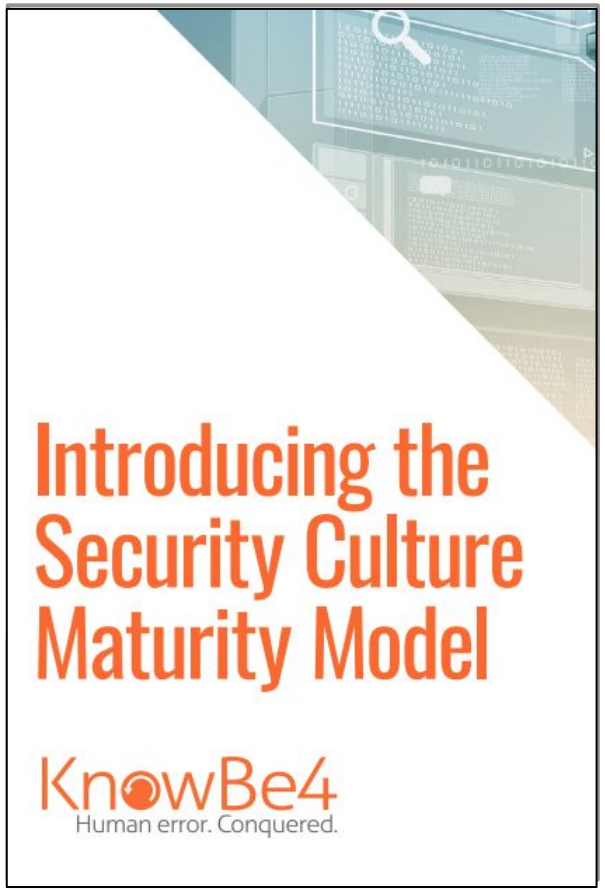
Security Culture

is defined as the ideas, customs and social behaviors of a group that influence its security.

Security Culture Maturity Model

is an evidence-driven framework for understanding and benchmarking the current security related maturity of an organization.





Security Culture Maturity Model

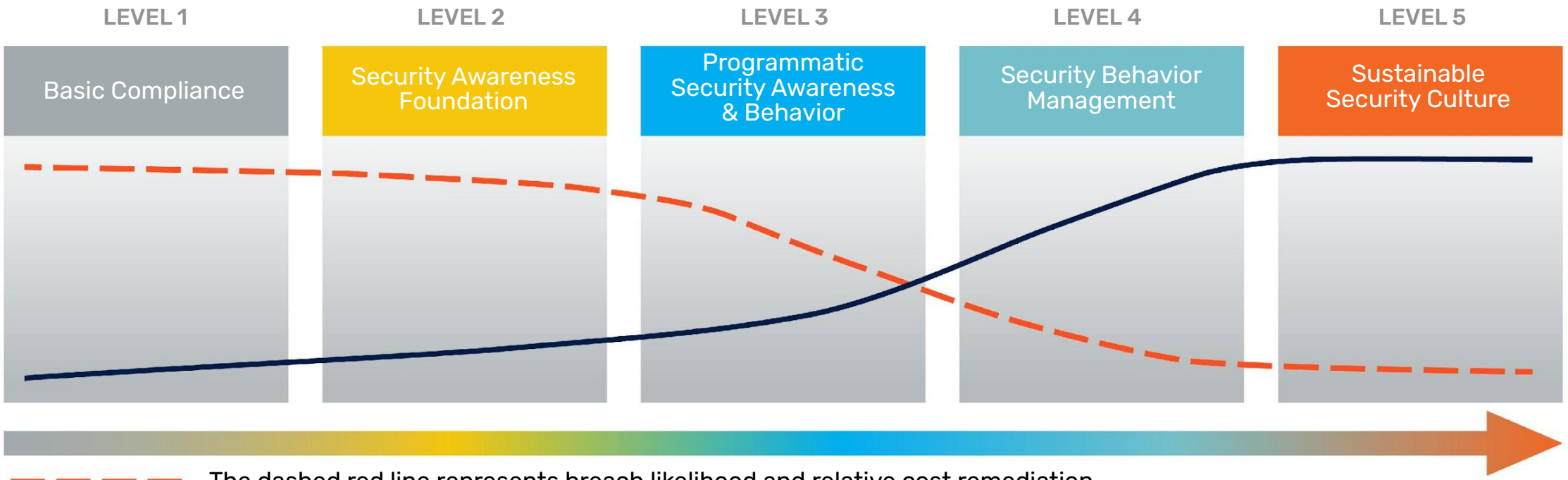
Level 1	**Basic compliance**	• "Checking a box" • Annual training • Limited buy-in
Level 2	**Security Awareness Foundation**	• Annual + New Hire training • Monthly phishing simulations • Leadership buy-in
Level 3	**Programmatic Security Awareness & Behaviors**	• Additional SAT tools added to program (SAPA/SCS) • Quarterly & Remedial Training + Monthly simulated phishing • Leadership driven Security Awareness focus
Level 4	**Security Behavior Management ("The Human Firewall")**	• Continuous training across a variety of delivery methods and audiences • Integrated tools and resources to increase SA footprint • Full organizational buy-in from top to bottom
Level 5	**Sustainable Security Culture**	• Programs that intentionally measures, shapes and reinforces the security culture • Multiple methods of behavior-based encouragement • Security values woven through fabric of entire organization

Future

Develop A Strong Security Culture To Reduce Risk

A strong security culture means more secure employee behaviors and reduced organizational risk.

As security awareness, behavior and culture increases, the likelihood of human-related breach and cost of remediation decreases.



Source: KnowBe4

KnowBe4

Implementation Phases 1-5

Implementation Phases and Timeline

Prerequisites needed prior to implementation phases.

Whitelisting

Users uploaded in the console via CSV or Active Directory/SCIM Integration

---

Onboarding Phase 1 August 5th at 3pm- First Call (Note, if you haven't phished or trained

1. Test whitelisting (send phish test to small group of users to verify whitelisting is updated and emails can be delivered from KB4 to your environment.) -
2. Branding The Knowbe4 Console/Logo
3. Blind Baseline Phishing Test. - Asses the overall knowledge of the organization (likelihood of users to fall for a phishing attack)
4. Inform Local Users of Program (Leadership to educate users of the program/ongoing phishing and training being assigned)
5. Assign Initial Training with 1-2 weeks after launching your baseline phishing test

   office Hours 8/15 12-1pm

Automation Phase Next -September 16th at 12pm

1. Turn on Monthly (Recommended) or Quarterly Phishing Campaigns
2. Use Dynamic Clickers Training for employees who fail a phishing campaign - Clickers 1,2,3,4 and 5
3. SEI landing page (Social Engineering Indicators - shows employees "Red Flags" They should of looked out for prior to clicking on the phishing simulations
4. Discuss Phish Alert Button Deployment-

   Office Hours 9/23 11-12pm

Stage 3 - Continued Knowledge Phase October 20th at 3pm

1. These emails are designed to go out weekly or bi-weekly for supplemental training and awareness. Scam of the week is an automated newsletter that is sent to help employees both personally and professionally in Cybersecurity awareness.

   No office Hours for this Phase

Implementation Phases and Timeline

Data Collection Phase November 3rd 2pm-3pm - During this time we do not make any changes in the console, we allow the console to bake in the changes and begin to identify our highest risk users based on phishing activities.

AMA- Group think to discuss best practices in the Suny organization, what is working well from a messaging perspective and an AMA for KnowBe4 on what questions they have for us.

(Compliance Plus/ Student Edition demos) Miesh

Diversification Phase December 4th 11am-12pm - Establish trends and identify high risk and advanced users and phish using the following recommendations.

High-risk users: Users who have failed more phishing simulations will receive easier phishing templates until they fall below an acceptable risk threshold.

1. Recommended Bi-weekly Phishing campaigns 1-3 star templates

Advanced users phishing: Users who have demonstrated mastery in the phishing program will receive harder phishing templates to align with their skills

1. Recommended Monthly Phishing Campaigns 4-5 star templates

New hire phishing: Ramp-up approach to their phishing simulations and onboarding training

1. Easier templates are used during days 30-60 of onboarding - Biweekly 1-2 star templates
2. Medium-level difficulty introduced from days 61-90 Bi-weekly/monthly 3 star template

Office Hours December 12th 12-1pm

Stage 1 - Onboarding Phase

During this phase, schools are provided with recommendations on how to leverage the KnowBe4 console, what resources were needed to allow for emails to be delivered in their environment, and how to effectively deploy KnowBe4 security awareness training program.

Note if a school has not phished yet this would be the first call to have these schools on.

Whitelist Testing

Console Branding

Baseline Phishing Test

Initial Training Campaigns

Leadership Communication

Note - If a school has already completed this phase on their own, they would skip and reconnect on later program initiatives/recommendations this phase is designed to get schools get familiar with the console and begin phishing/training users.

Stage 2 - Automation Phase

During this phase, Schools are shown how to optimize KnowBe4's console to leverage automated workflows with phishing simulations, dynamic remedial training, and content recommendations across all state agencies.

Introduced full automation of phishing simulations

Recommended monthly cadence for Phishing Simulations
Automated training for "clickers" (1-5 fails)

Best practices and recommendations

Phishing template categories
Attack vectors
Social Engineering Indicators landing pages

Remedial training recommendations

Training content selection
Completion timelines
How to focus on highest risk users

Stage 3 - Continued Knowledge Phase

Schools are advised to add informational communication to supplement phishing and training. This provides employees regular updates on personal and professional cybersecurity threats.

Implement Scam of the Week newsletters

These emails are designed to go out weekly or bi-weekly for supplemental training and awareness.

Stage 4 - Data Collection Phase

Schools are advised not to make changes to the consoles allowing for benchmarking and assessing of individual console performance to tailor future programs at the individual agency level to gather the required data for Phase 5 implementation.

Instead of a traditional call, we will conduct an "***Ask Me Anything"*** session:

Topics covered:
Data Gathered
Common challenges
Frequently encountered situations in their organization

Stage 5 - Diversification Phase

Using the data gathered from Phase 4 and prior, the diversification phase of implementation is for empowering organizations to tailor their security awareness program for various user groups, significantly reducing human-related security risks, and meeting employees where their understanding in phishing simulations are.

Note - This phase is designed to be the framework and blueprint for a level 4 on the Security Culture Maturity Model.

This phase focuses on three key areas:

High-risk users:

Users who have failed more phishing simulations will receive easier phishing templates until they fall below an acceptable risk threshold.

Advanced users phishing:

Users who have demonstrated mastery in the phishing program will receive harder phishing templates to align with their skills

New hire phishing

Ramp-up approach to their phishing simulations and onboarding training

Easier templates are used during days 30-60 of onboarding,

Medium-level difficulty introduced from days 61-90

KnowBe4

Support Model

Who do I contact?

KnowBe4 questions on console (How do I do this, why should I do this, best practices?)

New Campus Onboarding – Contact Max Brannen at maxb@knowbe4.com

Tier 1 operational questions- Contact NewPush at support@newpush.com

NewPush- Problem examples:

- KnowBe4 platform or specific modules or features are unavailable
- Phishing simulations are failing to send or track results.
- Training assignments are failing for a group of users.
- Inaccurate or missing data in reports.
- Integration with other systems (e.g., HR systems) is broken.
- Number of users are unable to log in or access training.

Information request examples:

- Information about available features or planned features
- We can point to the right support article or help understand the steps and relations between settings
  - Guide on campaign setup
  - Help in user management settings
- Advice on optional settings and learning experience
- Advice on modules

KnowBe4

Questions?

KnowBe4

Additional Resources

Addition Products

Human Risk Management + Expansion Options

- ***Diamond Upgrade*** *- 1500+ training modules, Multiple publishers, Call Back Phishing, AI Driven Phishing, AI Recommended Optional Learning and PasswordIQ*
- ***PhishER Plus**** *- AI/Machine Learning categorizes reported emails. Includes: PhishRIP, PhishFLIP, Threat Intel(Webroot) and built-in interfaces to VirusTotal and Crowdstrike Falcon. 24x7x365 automation.*
- ***Compliance Plus*** *- 700+ HR/Compliance modules for the price that HR typically pays for a single module.*
- ***Egress Defend/Prevent/Protect*** *- Cloud Email Security Suite continually assesses human risk & dynamically adapt security controls.*
- ***SecurityCoach*** *- Detects and responds to risky end user behavior to provide immediate feedback*
- ***AIDA*** *- AI Defense Agents currently featuring: Automated Training, Template Generation, Knowledge Refreshers and Policy Quizzes (Diam)*

KnowBe4
Human error. Conquered.

KnowBe4 Student Edition Training Topics Include:

Computer and Mobile Security Vulnerabilities

Our cyber threat awareness training empowers students to confront not only malware risks, but also the broad spectrum of computer and mobile security vulnerabilities. It offers insight into cyber defense strategies, such as regular system updates, the use of reputable software and the adoption of savvy online practices to safeguard against an ever-evolving array of digital threats.

Password Security Weaknesses

Our password security training examines common password security weaknesses. The training emphasizes the critical need for robust, complex passwords, password management tools, and multi-factor authentication to fortify user accounts against unauthorized access.

Phishing Attacks

Our phishing training tackles the surge of sophisticated attacks, such as job fraud emails aimed at students. Using examples from student inboxes, it teaches students how to identify these deceptive tactics that can compromise personal information and guides students to exercise vigilant cyber etiquette.

Social Media Dangers

Our social media training emphasizes the importance of recognizing and avoiding oversharing to prevent adverse outcomes such as loss of privacy, reputational damage and identity theft. The training reinforces that school computers should be used for academic purposes, helping students to understand how to safeguard their digital well-being.

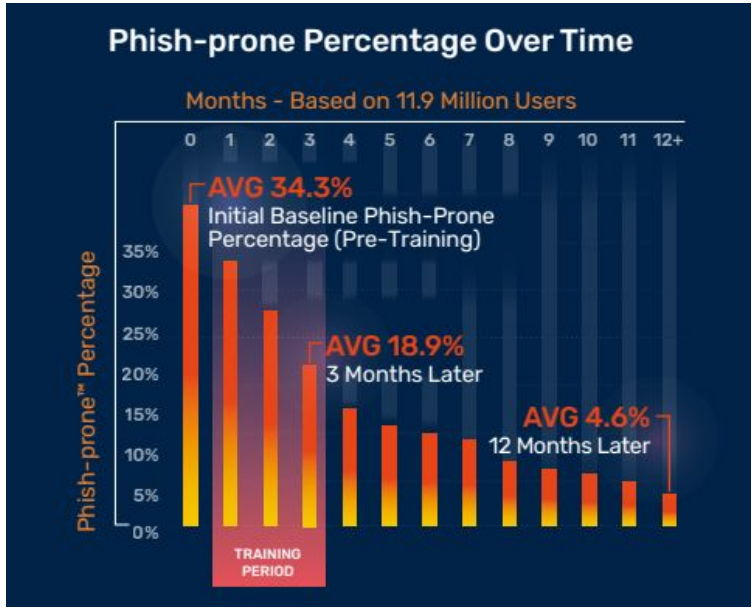
Campus Thefts and Scams

Our secure behavior training confronts the realities of campus thefts and scams, underscoring the necessity of shredding confidential materials such as past applications and unneeded documents. The training highlights the importance of maximizing privacy settings on personal accounts and encourages regular data backups to mitigate potential losses from deceptive activities.

Travel and Off-campus Data Security Thefts

Students gain a crucial layer of protection against data theft when they're equipped with the knowledge to work securely off-campus or while traveling. This training explores how to leverage VPNs for secure communications, navigate public Wi-Fi with caution and effectively secure devices and personal information while engaging in academic pursuits or conducting homework off campus.

Phishing by Industry Benchmarking - 2025



How We Calculate Phish-prone Percentages

67.7M
Phishing Security Tests

14.5M
Users

62.4K
Organizations

Security Culture Report

2024

NEW this year!

Expanded analysis for six global regions plus an in-depth worldwide overview

Security Culture

Trends over time and regional breakdowns of security culture around the world

Scoring

The best and worst scoring industries

Best Practices

Improve your organization's security culture

KnowBe4

THANK YOU!