knowbe4

SUNY
Implementation Phase 5

Program Diversification Phase
Dec 4th, 2025

Meet Your KnowBe4 Team

- **Max Brannen**

  Customer Success Manager (Strategic)
  MBA, SACP, CCAP

- **Miesh Blankenship**

  Account Manager (ENT/Strategic)

Implementation Phases Recap

© 2025 KnowBe4, Inc. All rights reserved.

Phase 1 – Onboarding Phase

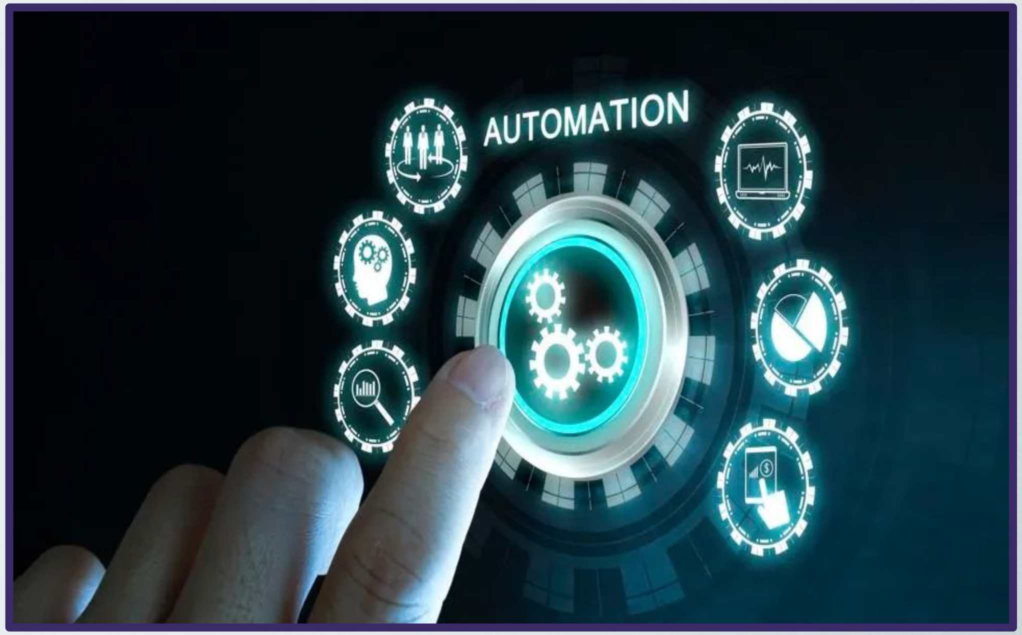
During this phase, Child Accounts are provided with recommendations on how to leverage the KnowBe4 console, what adjustments are needed to allow for emails to be delivered in their environment, and how to effectively deploy a KnowBe4 security awareness training program.

- **Whitelist testing**
- **Console Branding**
- **KnowBe4 Academy Admin Training**
- **Baseline Phishing Test**
- **Initial Training Campaigns**
- **Leadership Communication**

© 2025 KnowBe4, Inc. All rights reserved.

Phase 2 - Automation Phase (Foundational Program)

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



- **Best practices and recommendations**
    - Phishing template categories
    - Attack vectors
    - Social Engineering Indicators landing pages (Branded)

- **Remedial training recommendations**
    - Training content selection
    - Completion Timelines
    - How to focus on highest risk users

- **Full automation of phishing simulations and Remedial Training**
    - Set up recurring monthly Phishing Simulations
    - Implement automated training for "clickers" (1-5 fails)

© 2025 KnowBe4, Inc. All rights reserved.

Phase 3 - Continued Knowledge Phase

Organizations are advised to add informational communication to supplement phishing and training. This provides employees with 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.
- **Targeted Training Plan**
  - Work with KnowBe4 courseware team to come in and create a targeted training plan and roadmap for training requirements and or NIST and or CMCC Training Requirements
  - Consider launching the SAPA assessment to benchmark users knowledge of specific areas for future training/communication.
- **Intranet Portal with Optional Learning**
  - Pick short effective and fun video modules to supplement learning

© 2025 KnowBe4, Inc. All rights reserved.

Phase 4 - Data Collection Phase

Organizations are advised, initially, not to make changes to the consoles. This will allow for benchmarking and the proper assessment of user population- and program performance, to tailor future program level for Phase 4 (program diversification).

GROUP AMA and Best Practices call - Scheduled for November 3rd at 2pm Eastern Time

Max Brannen- Customer Success Manager (Strategic)

Rose Martinez -Snr. Security Awareness Content Specialist

Miesh Blankenship - Account Manager (ENT/Strategic)

© 2025 KnowBe4, Inc. All rights reserved.

Phase 5 - Program Diversification Phase

The diversification phase empowers organizations to tailor their security awareness program, relevant to targets and expectations, significantly reducing human-related security risks.

- **High-Risk User Phishing:**
  - Users who have failed more phishing simulations will receive easier phishing templates until they fall below an acceptable risk score
- **Advanced User Phishing:**
  - Users who have demonstrated mastery in the phishing program will receive harder phishing templates to align with their skills
- **Quarterly Credential Phishing Campaigns:**
  - Implement quarterly campaigns that run concurrent with the monthly phishing test, testing exclusively on password theft to the entire organization.
- **New Hire Phishing**
  - Ramp-up approach to their phishing simulations and onboarding training. Strategic ramp up for new hires joining the SUNY team
- **Role Based Training**
  - Tailored training programs with micro modules that are relevant to roles and user groups.
- **Culture Initiatives**
  - Gamification
  - Reward programs
  - Cyber Champions Program

© 2025 KnowBe4, Inc. All rights reserved.

Program Diversification Phase

© 2025 KnowBe4, Inc. All rights reserved.

New Hire Phishing

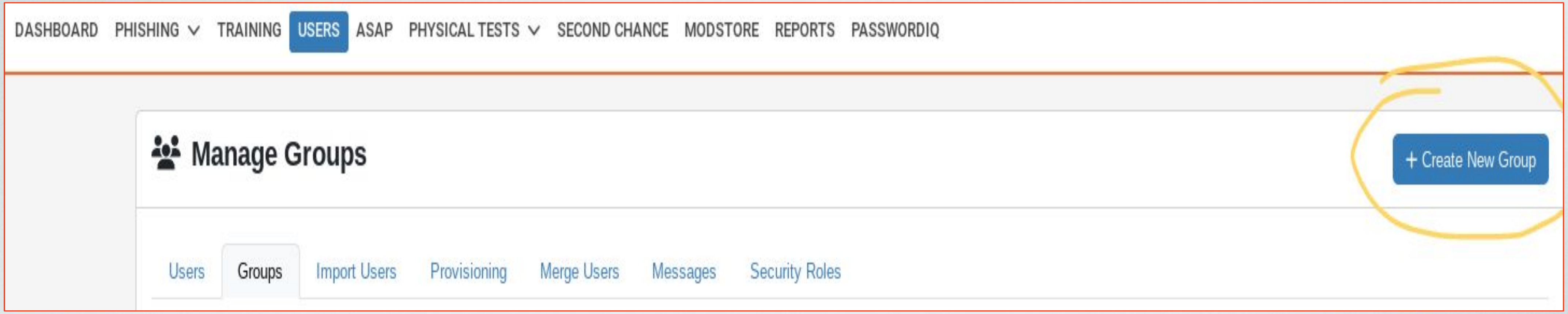
© 2025 KnowBe4, Inc. All rights reserved.

Creating Smart Groups

Log in to your KSAT account

Navigate to the Users tab

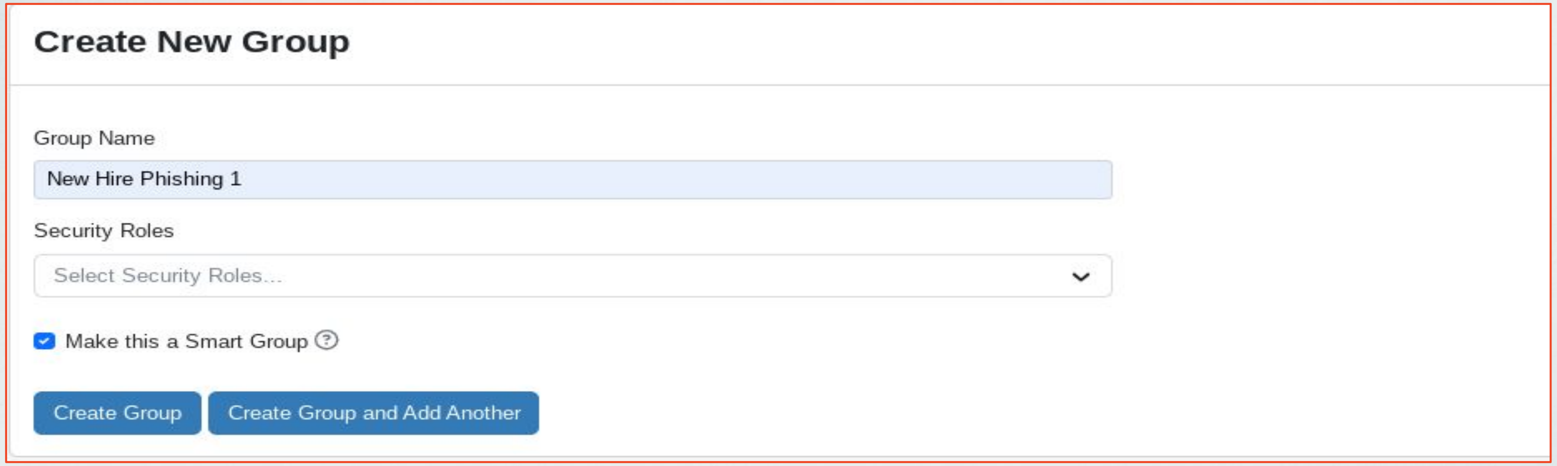
Create a new Group



© 2025 KnowBe4, Inc. All rights reserved.

Creating The Smart Group For New Hire Phishing

Name The Group New Hire Phishing 1 and select the option “Make This a Smart Group.”



Create New Group

Group Name

New Hire Phishing 1

Security Roles

Select Security Roles...

☑ Make this a Smart Group

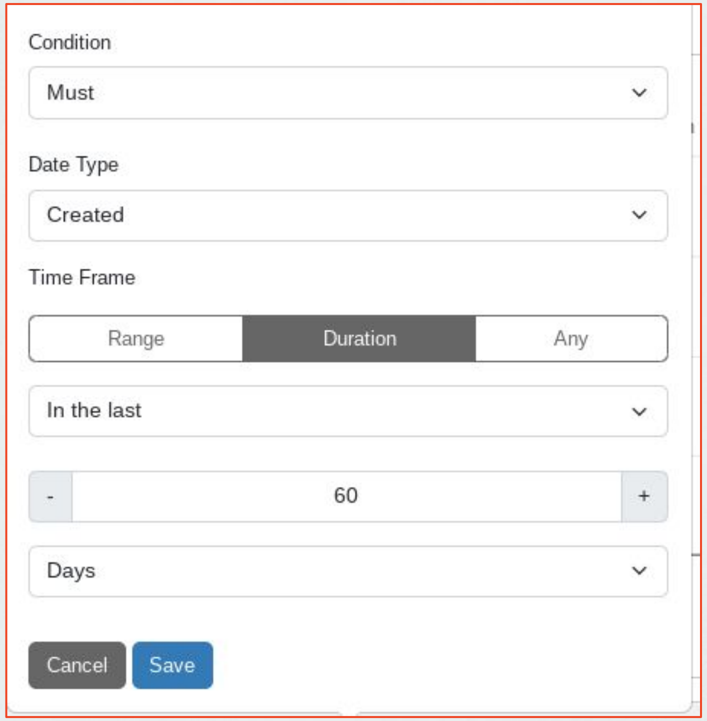
© 2025 KnowBe4, Inc. All rights reserved.

Creating The Smart Group For New Hire Phishing

Criteria for New Hire Phishing 1

User Date User Must Have Been Created In the last 60 Days

User Must Not Have Been Created In The Last 30 days.



Condition: Must

Date Type: Created

Time Frame: Range | [✓ Duration] | Any

In the last

60

Days

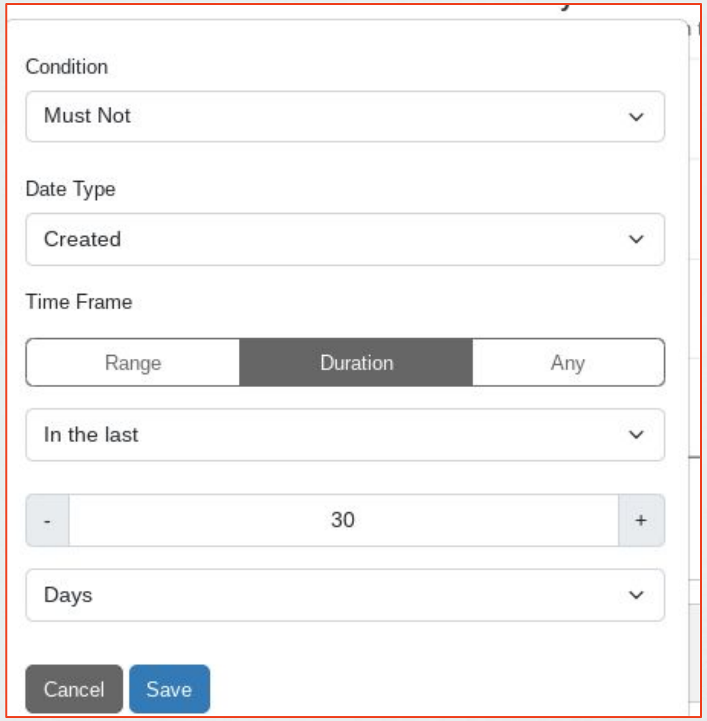
© 2025 KnowBe4, Inc. All rights reserved.

Creating The Smart Group For New Hire Phishing

Criteria for New Hire Phishing 1

User Date User Must Have Been Created In the last 60 Days

User Must Not Have Been Created In The Last 30 days.



Condition: Must Not

Date Type: Created

Time Frame: Duration

In the last

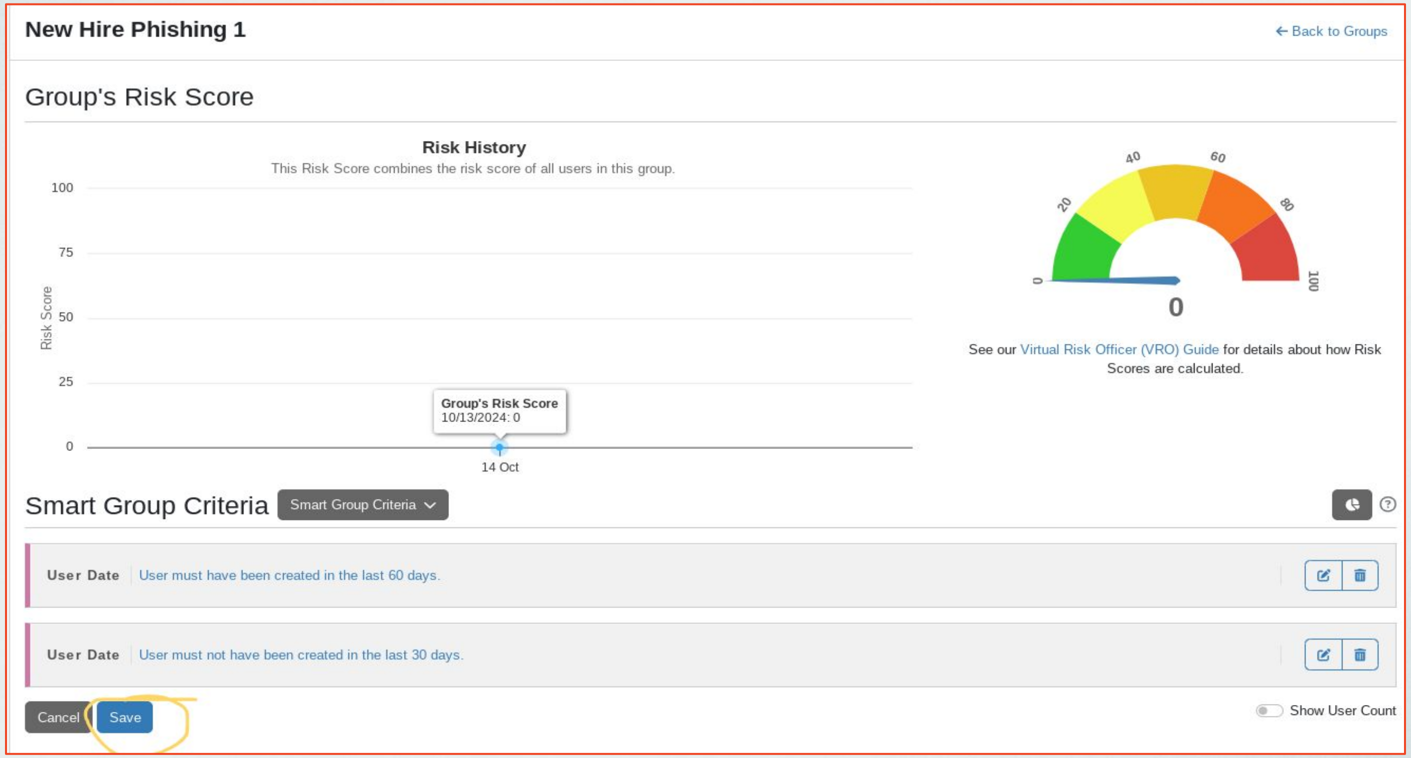
30

Days

© 2025 KnowBe4, Inc. All rights reserved.

Creating The Smart Group For New Hire Phishing

Once you have both criterias saved, MAKE SURE your hit the blue save button at the bottom of the screen!



New Hire Phishing 1

Group's Risk Score

Risk History

This Risk Score combines the risk score of all users in this group.

Group's Risk Score
10/13/2024: 0

See our Virtual Risk Officer (VRO) Guide for details about how Risk Scores are calculated.

Smart Group Criteria

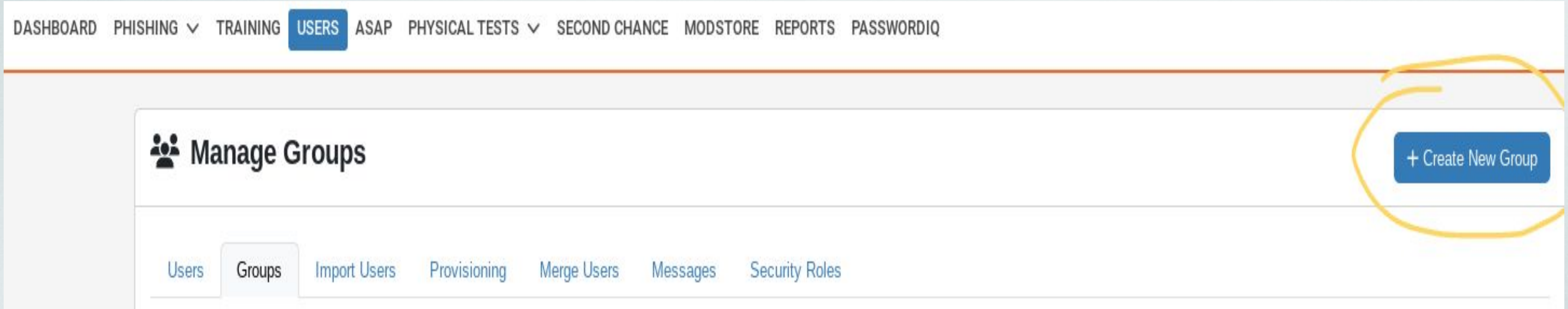
User Date — User must have been created in the last 60 days.

User Date — User must not have been created in the last 30 days.

© 2025 KnowBe4, Inc. All rights reserved.

Creating The Smart Group For New Hire Phishing 2

Login to the Knowbe4 console- Go to “Users tab” and create a “New Group”



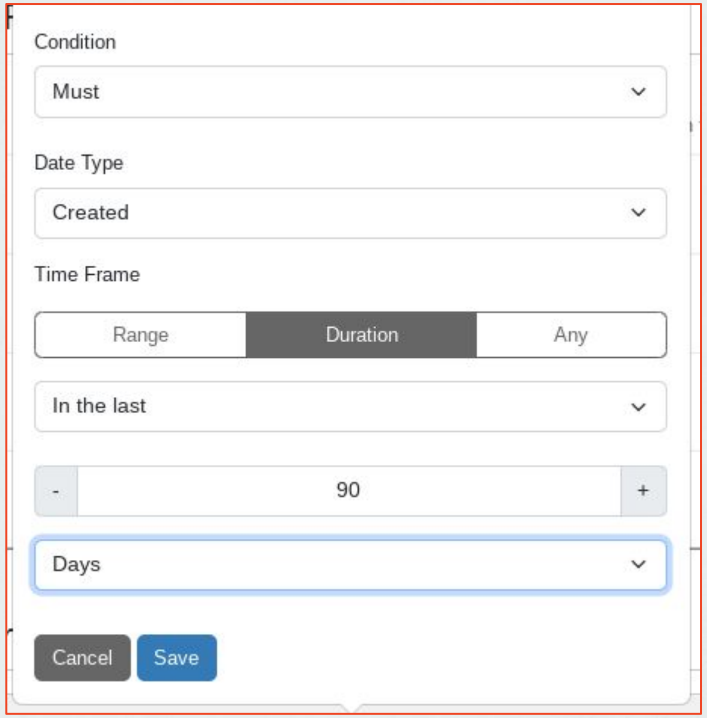
© 2025 KnowBe4, Inc. All rights reserved.

Creating The Smart Group For New Hire Phishing

Criteria for New Hire Phishing 2

User Date User Must Have Been Created In the last 90 Days

User **Must Not Have Been** Created In The Last 60 days.



Condition: Must

Date Type: Created

Time Frame: Range | **Duration** | Any

In the last

- 90 +

Days

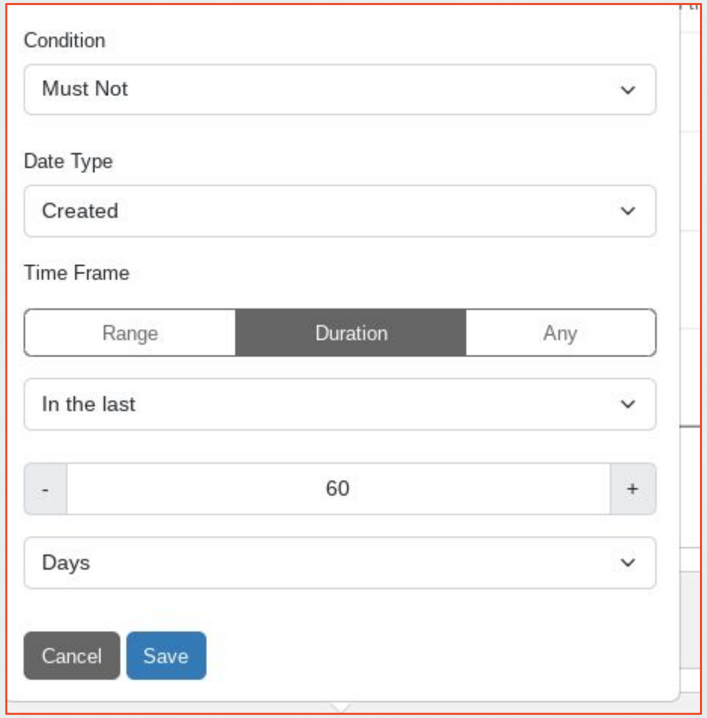
© 2025 KnowBe4, Inc. All rights reserved.

Creating The Smart Group For New Hire Phishing

Criteria for New Hire Phishing 2

User Date User Must Have Been Created In the last 90 Days

User **Must Not Have Been** Created In The Last 60 days.



Condition
Must Not

Date Type
Created

Time Frame
Duration

In the last

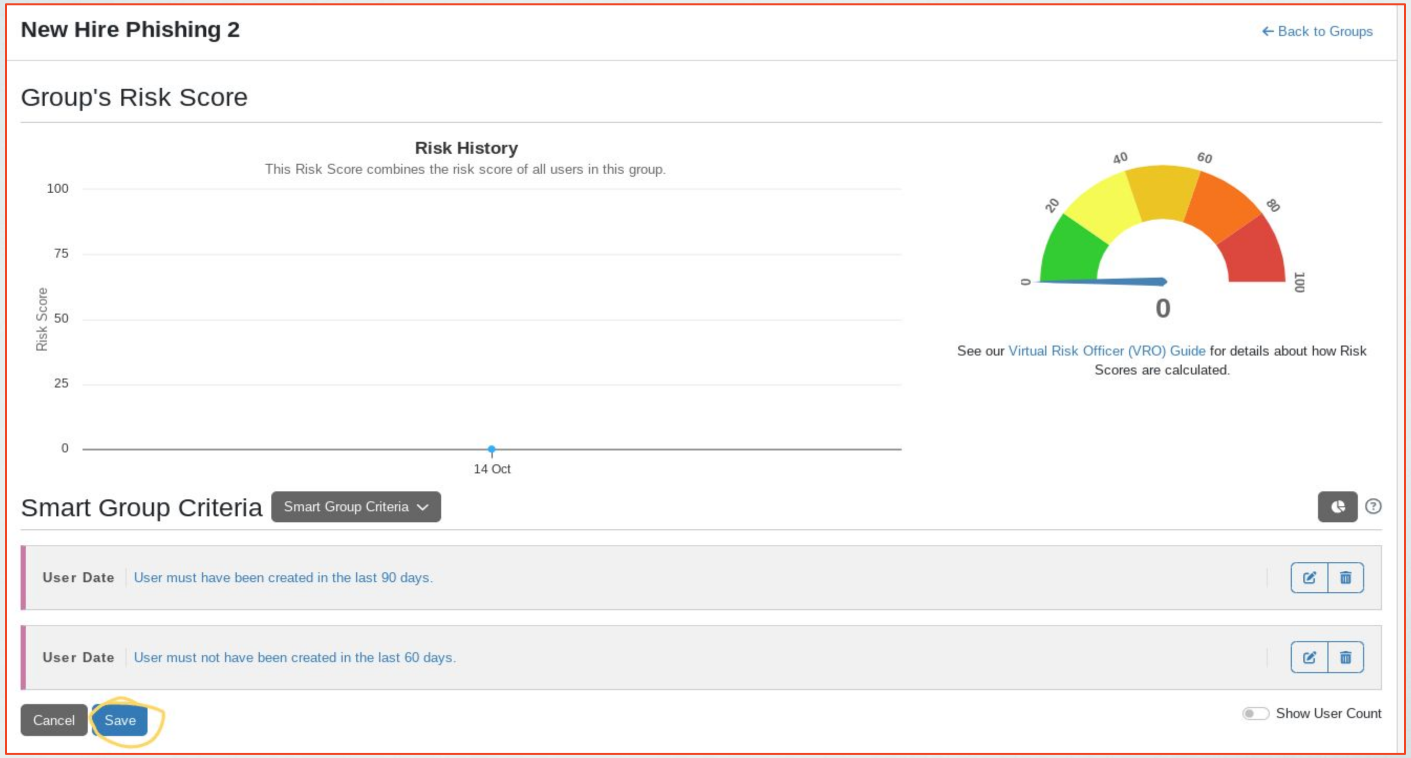
60

Days

© 2025 KnowBe4, Inc. All rights reserved.

Creating The Smart Group For New Hire Phishing

Once you have both criterias saved, MAKE SURE your hit the blue save button at the bottom of the screen!



User Date | User must have been created in the last 90 days.

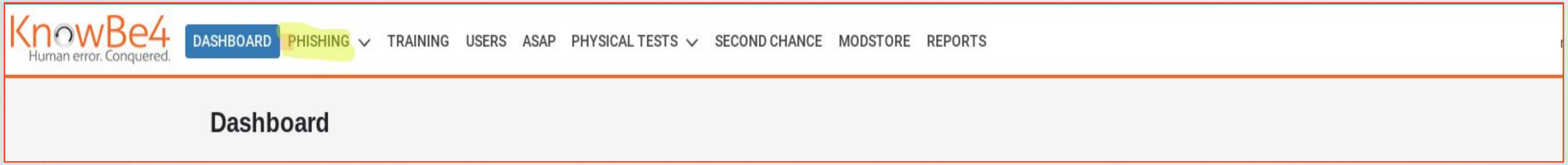
User Date | User must not have been created in the last 60 days.

Creating New Hire Phishing Campaigns

© 2025 KnowBe4, Inc. All rights reserved.

Creating Phishing Campaigns

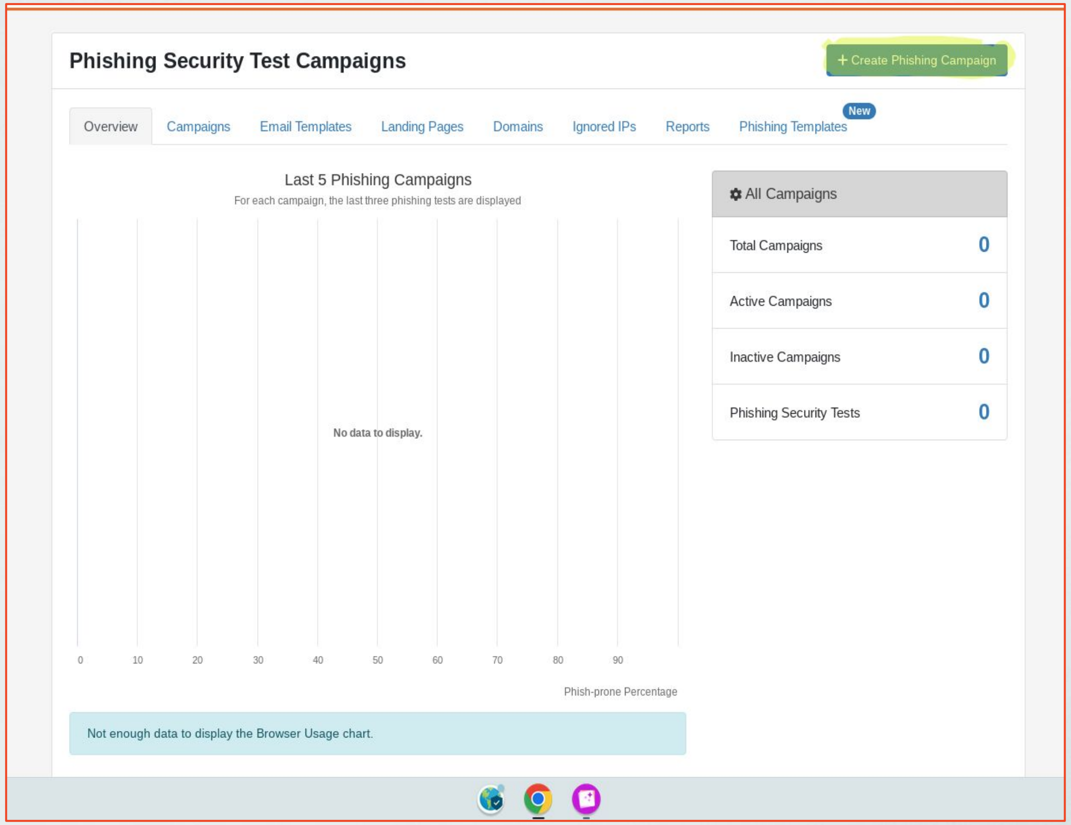
Login to your Knowbe4 Account and Click the subtab “Phishing” at the top of your page.



© 2025 KnowBe4, Inc. All rights reserved.

Creating Phishing Campaigns

Login to your Knowbe4 Account and Click the subtab “Phishing” at the top of your page.



Last 5 Phishing Campaigns

For each campaign, the last three phishing tests are displayed

No data to display.

Not enough data to display the Browser Usage chart.

All Campaigns	
Total Campaigns	0
Active Campaigns	0
Inactive Campaigns	0
Phishing Security Tests	0

© 2025 KnowBe4, Inc. All rights reserved.

Creating The New Hire Phishing 1

Name the campaign under campaign name “New Hire Phishing 1
Choose to send to “New Hire Phishing 1”

Select Frequency Bi-Weekly

Choose desired Start Time and Date we want the campaign to go live

Send emails over 2 weeks

Track Activity for 1 day

Turn on Track Replies to Phishing Emails

Template categories- Education, Reported Phishes Of The Week, Brand Knockoffs

Difficulty Rating 1-2 Stars

Landing Page- SEI Landing Page (Translatable) (Branded) (Platinum and Diamond Only)

Leave Add clickers to field blank/select group

Select Box, send an email report to account admins after each phishing test.

Creating The New Hire Phishing 2

PRO TIP - Clone the New Hire Phishing Campaign 1
Name the campaign under campaign name “New Hire Phishing 2
Choose to send to “New Hire Phishing 2

Select Frequency “Bi-weekly”
Choose desired Start Time and Date we want the campaign to go live

Send emails over 2 weeks

Track Activity for 1 day

Turn on Track Replies to Phishing Emails

Template categories- Reported Phishes Of The week, Banking and Finance,Online services, Social Networking, current event of the week, current event of the month, mail Notifications,

Difficulty Rating 3 stars only

Landing Page- SEI Landing Page (Translatable) (Branded) (Platinum and Diamond Only)

Leave Add clickers to field blank/select group

Select Box, send an email report to account admins after each phishing test.

Dynamic Phishing Creating The Groups

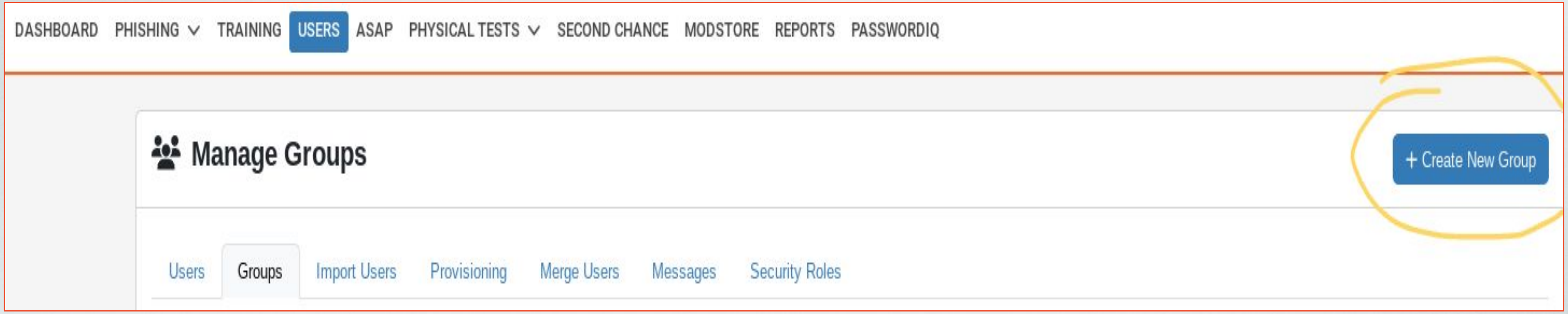
© 2025 KnowBe4, Inc. All rights reserved.

Creating Smart Groups For Advanced User Phishing

Log in to your KSAT account

Navigate to the Users tab

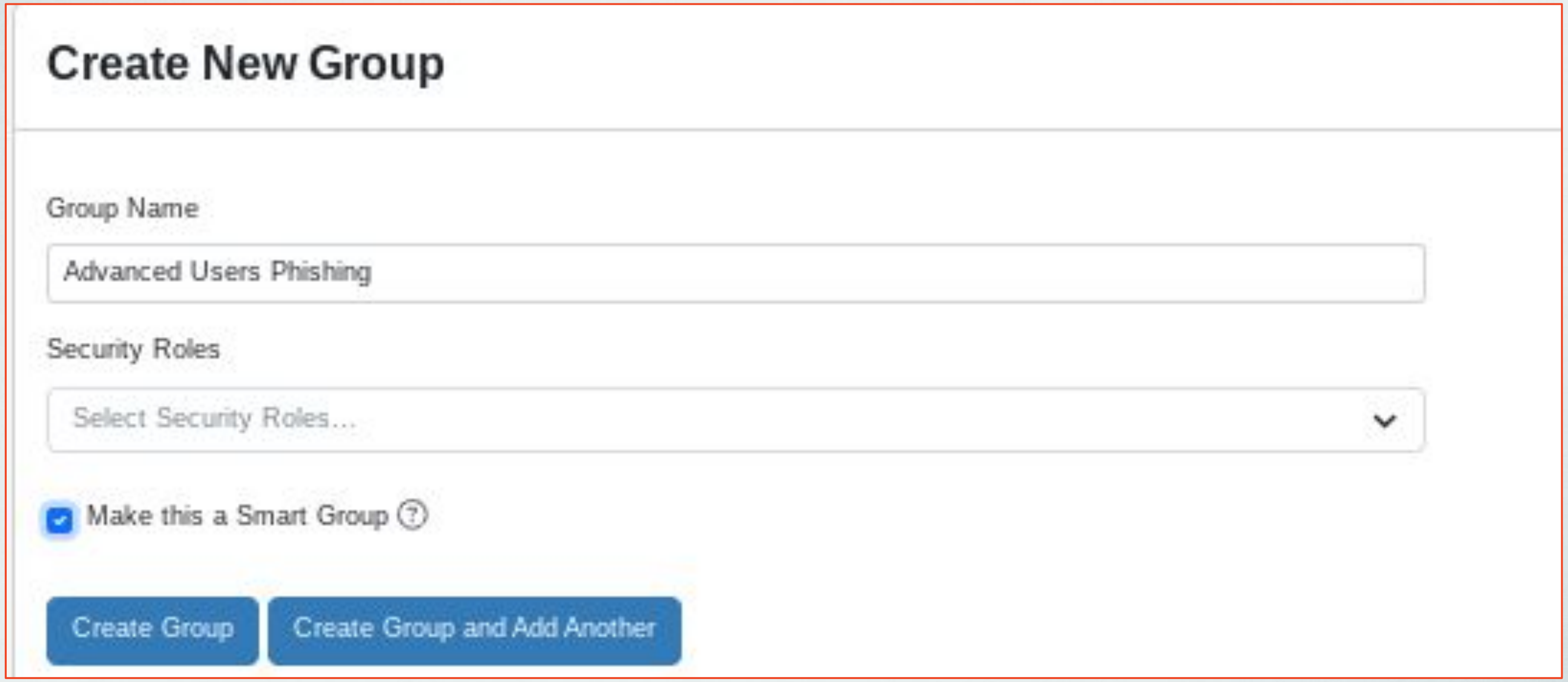
Create a new Group



© 2025 KnowBe4, Inc. All rights reserved.

Creating The Smart Group For Advanced User Phishing

Name The Group Advanced Users and select the option “Make This a Smart Group.”



Create New Group

Group Name: Advanced Users Phishing

Security Roles: Select Security Roles...

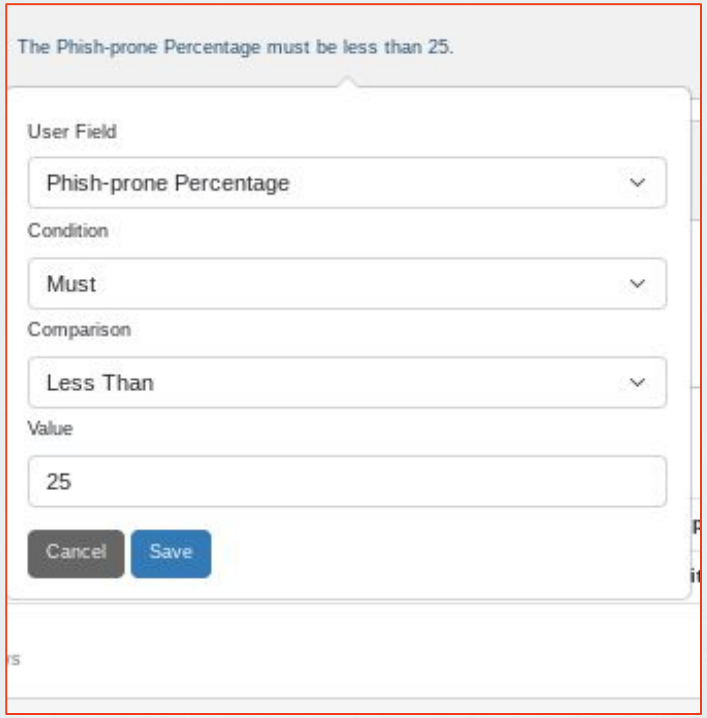
☑ Make this a Smart Group

Creating The Smart Group For Advanced User Phishing

Criteria for Advanced User Phishing

User Field- Phish Prone Percentage Must Be Below, 25%

User date- User Must Not have been created in the last 90 Days.



The Phish-prone Percentage must be less than 25.

User Field: Phish-prone Percentage

Condition: Must

Comparison: Less Than

Value: 25

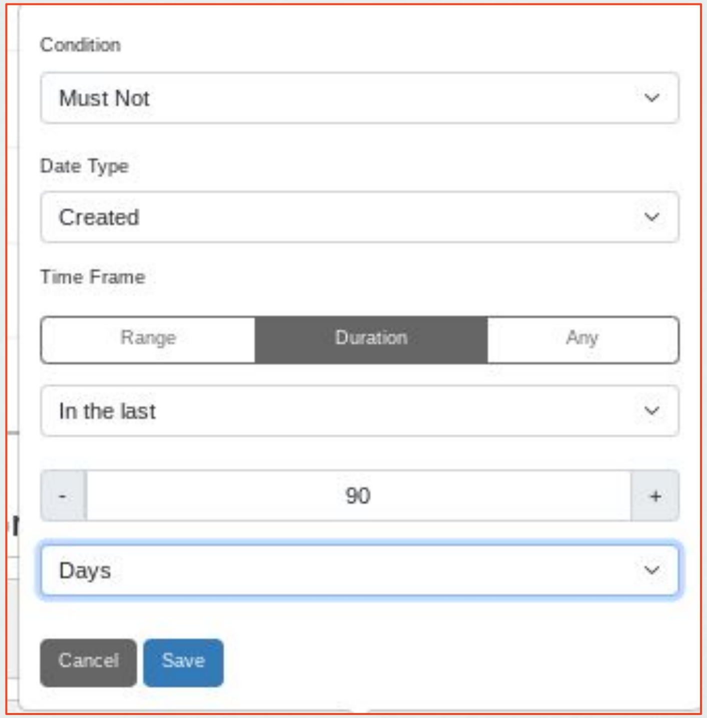
© 2025 KnowBe4, Inc. All rights reserved.

Creating The Smart Group For Advanced User Phishing

Criteria for Advanced User Phishing

User Field- Phish Prone Percentage Must Be Below, 25%

User date- User Must Not have been created in the last 90 Days.



Condition: Must Not

Date Type: Created

Time Frame: Range [✓ Duration] Any

In the last

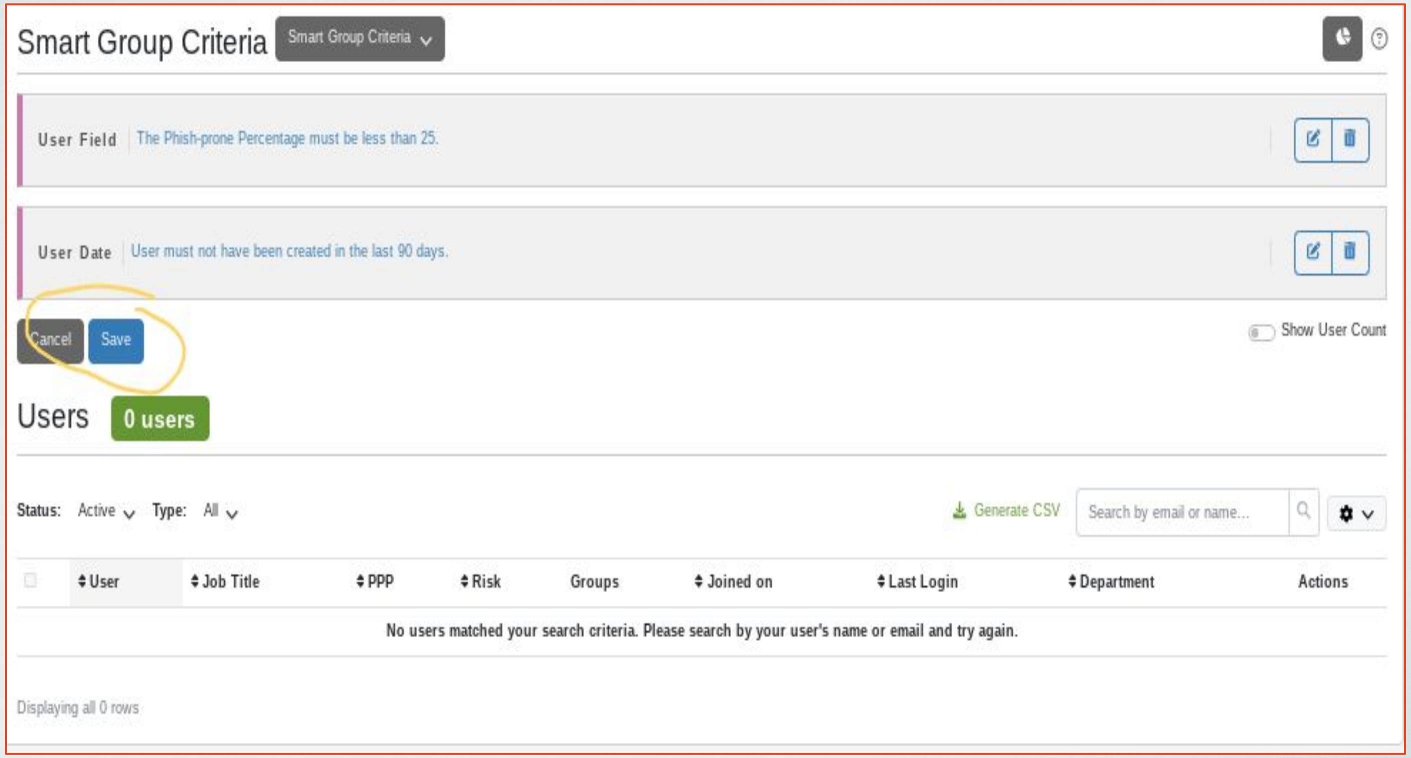
90

Days

© 2025 KnowBe4, Inc. All rights reserved.

Creating The Smart Group For Advanced User Phishing

Once you have both criterias saved, MAKE SURE your hit the blue save button at the bottom of the screen!



Smart Group Criteria

User Field | The Phish-prone Percentage must be less than 25.

User Date | User must not have been created in the last 90 days.

Cancel Save

Show User Count

Users 0 users

Status: Active Type: All

Generate CSV

Search by email or name...

	User	Job Title	PPP	Risk	Groups	Joined on	Last Login	Department	Actions

No users matched your search criteria. Please search by your user's name or email and try again.

Displaying all 0 rows

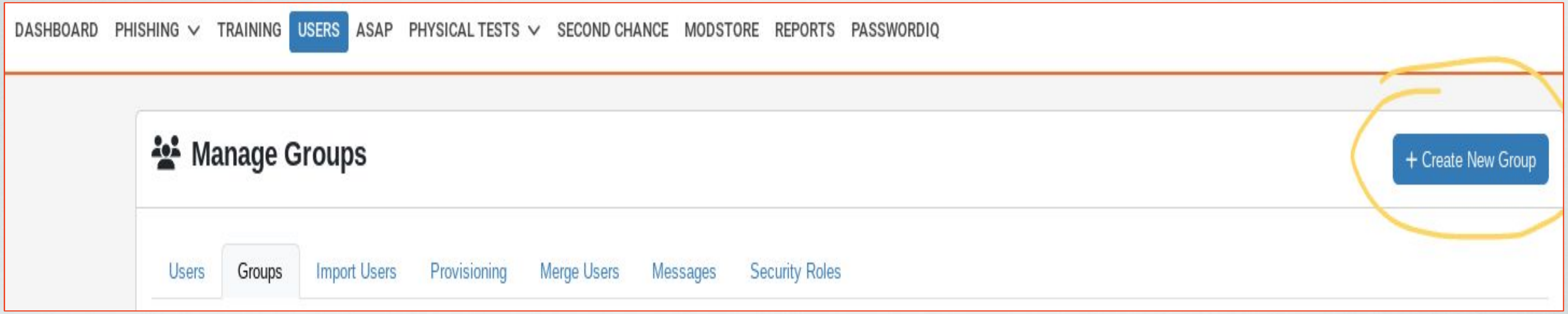
© 2025 KnowBe4, Inc. All rights reserved.

Creating Smart Groups For High Risk User Phishing

Log in to your KSAT account

Navigate to the Users tab

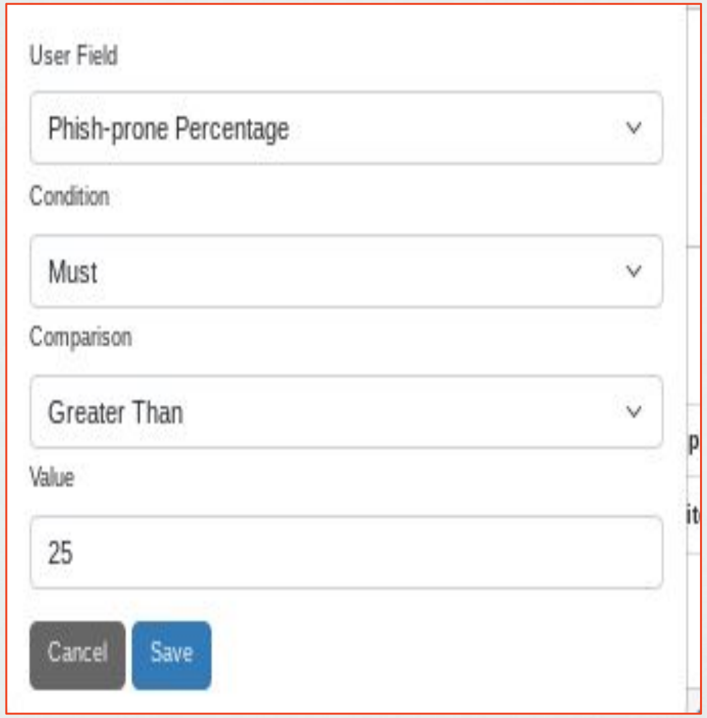
Create a new Group



© 2025 KnowBe4, Inc. All rights reserved.

Creating The Smart Group For Advanced User Phishing

Criteria for High Risk User Phishing
User Field- Phish Prone Percentage Must Be Greater Than, 25%
User date- User Must Not have been created in the last 90 Days.



User Field
Phish-prone Percentage

Condition
Must

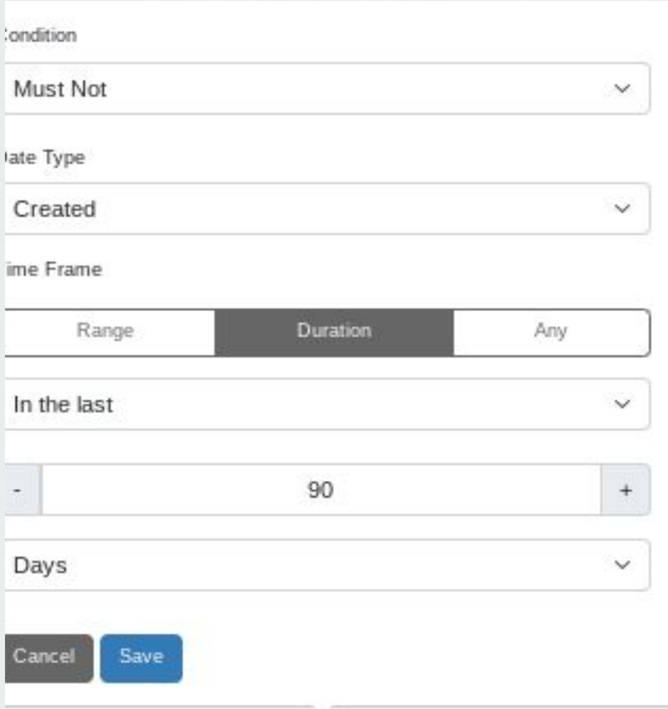
Comparison
Greater Than

Value
25

© 2025 KnowBe4, Inc. All rights reserved.

Creating The Smart Group For Advanced User Phishing

Criteria for High Risk User Phishing
User Field- Phish Prone Percentage Must Be Greater Than, 25%
User date- User Must Not have been created in the last 90 Days.



ondition
Must Not

ate Type
Created

ime Frame
Range | Duration | Any

In the last

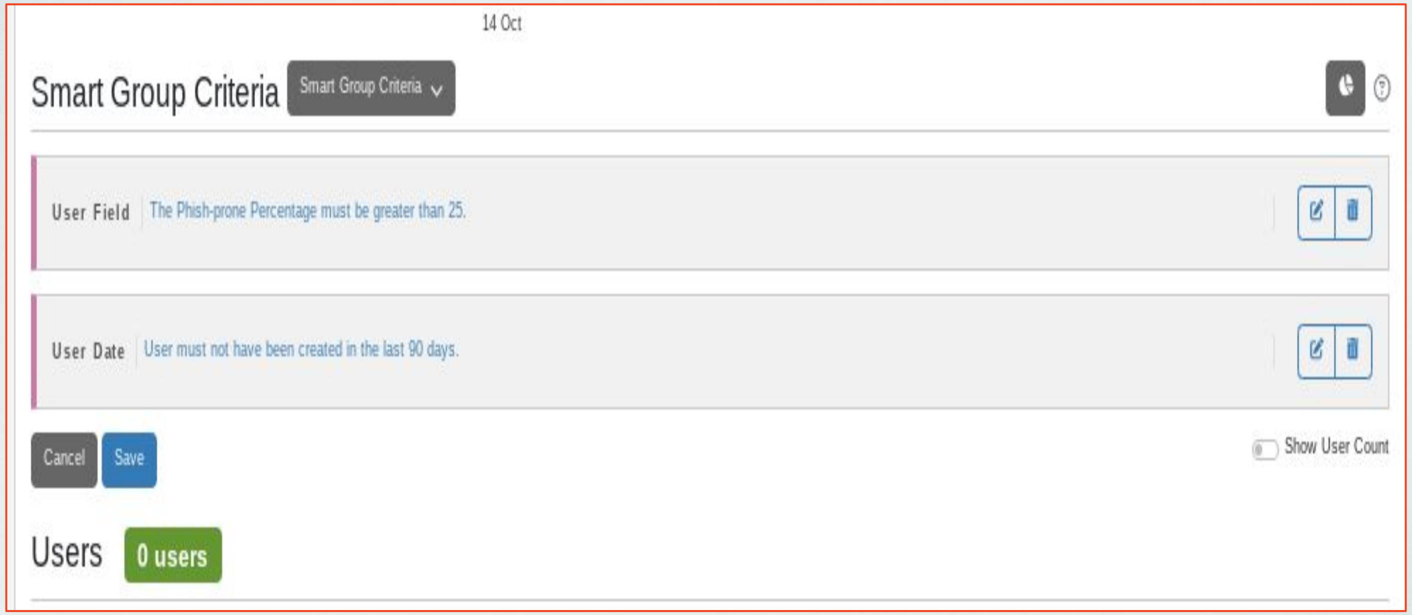
- 90 +

Days

© 2025 KnowBe4, Inc. All rights reserved.

Creating The Smart Group For High Risk User Phishing

Once you have both criterias saved, MAKE SURE your hit the blue save button at the bottom of the screen!



14 Oct

Smart Group Criteria

User Field The Phish-prone Percentage must be greater than 25.

User Date User must not have been created in the last 90 days.

© 2025 KnowBe4, Inc. All rights reserved.

Creating Advanced + High Risk Users Campaigns

© 2025 KnowBe4, Inc. All rights reserved.

Creating The Advanced User PHishing

PRO TIP - Clone the High Risk Users Campaign
Name the campaign under campaign name Advanced Users 25% Below PPP
Choose to send to Advanced User Phishing

Select Frequency “Monthly”
Choose desired Start Time and Date we want the campaign to go live

Send emails over 3 weeks

Track Activity for 1 day

Turn on Track Replies to Phishing Emails

Template categories- Reported Phishes Of The week, Banking and Finance,Online services, Social Networking, current event of the week, current event of the month, mail Notifications,

Difficulty Rating 3,4, and 5 stars

Landing Page- SEI Landing Page (Translatable) (Branded) (Platinum and Diamond Only)

Leave Add clickers to field blank/select group

Creating The High Risk Users Phishing

Name the campaign under campaign name “New Hire Phishing 1
Choose to send to High Risk Users 25%+ PPP

Select Frequency Monthly
Choose desired Start Time and Date we want the campaign to go live

Send emails over 3 weeks

Track Activity for 1 Week

Turn on Track Replies to Phishing Emails

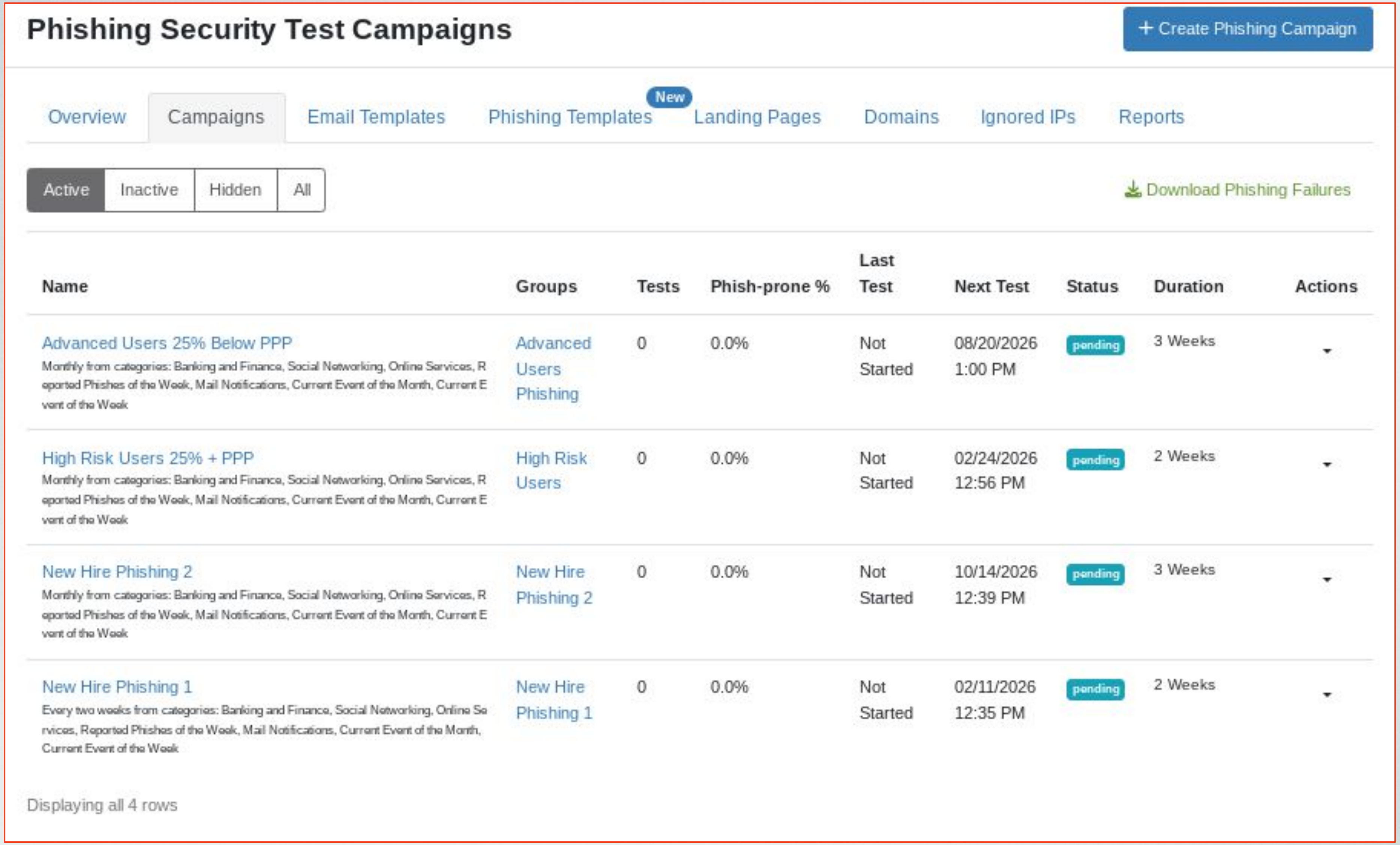
Template categories- Reported Phishes Of The week, Banking and Finance,Online services, Social Networking, current event of the week, current event of the month, mail Notifications,

Difficulty Rating 1-3 Stars

Landing Page- SEI Landing Page (Translatable) (Branded) (Platinum and Diamond Only)

Leave Add clickers to field blank/select group

By the end your Phishing test should look like this



Phishing Security Test Campaigns

Name	Groups	Tests	Phish-prone %	Last Test	Next Test	Status	Duration	Actions
Advanced Users 25% Below PPP Monthly from categories: Banking and Finance, Social Networking, Online Services, Reported Phishes of the Week, Mail Notifications, Current Event of the Month, Current Event of the Week	Advanced Users Phishing	0	0.0%	Not Started	08/20/2026 1:00 PM	pending	3 Weeks	▾
High Risk Users 25% + PPP Monthly from categories: Banking and Finance, Social Networking, Online Services, Reported Phishes of the Week, Mail Notifications, Current Event of the Month, Current Event of the Week	High Risk Users	0	0.0%	Not Started	02/24/2026 12:56 PM	pending	2 Weeks	▾
New Hire Phishing 2 Monthly from categories: Banking and Finance, Social Networking, Online Services, Reported Phishes of the Week, Mail Notifications, Current Event of the Month, Current Event of the Week	New Hire Phishing 2	0	0.0%	Not Started	10/14/2026 12:39 PM	pending	3 Weeks	▾
New Hire Phishing 1 Every two weeks from categories: Banking and Finance, Social Networking, Online Services, Reported Phishes of the Week, Mail Notifications, Current Event of the Month, Current Event of the Week	New Hire Phishing 1	0	0.0%	Not Started	02/11/2026 12:35 PM	pending	2 Weeks	▾

Displaying all 4 rows

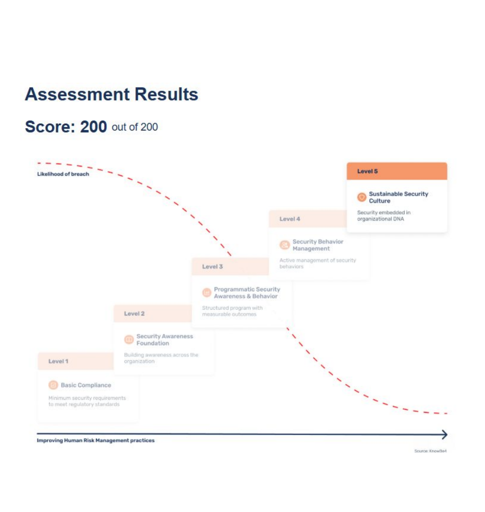
Additional Resources

© 2025 KnowBe4, Inc. All rights reserved.

Program Maturity Assessment Tool

Created by security culture expert **Perry Carpenter**, the PMA offers a structured, practical self-assessment framework focused on Human Risk Management (HRM).

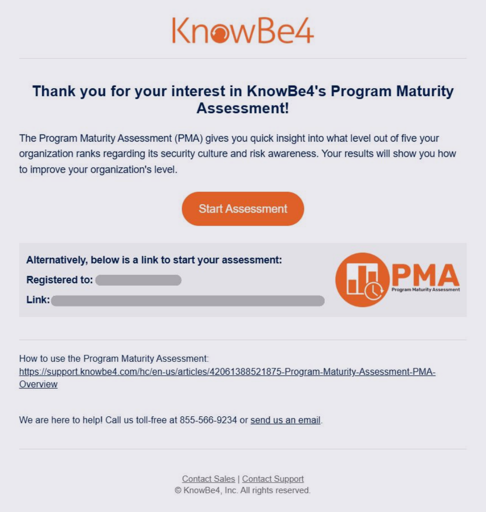
KnowBe4's Program Maturity Assessment tool measures and strengthens an organization's security culture across critical human risk dimensions. As human actions are targeted and exploited by attackers with increased sophistication, organizations need clarity on what is working and how to measure improvement.



Assessment Results

Score: 200 out of 200

Likelihood of breach
Level 5
Sustainable Security Culture
Security embedded in organizational DNA
Level 4
Security Behavior Management
Active management of security behaviors
Level 3
Programmatic Security Awareness & Behavior
Structured program with measurable outcomes
Level 2
Security Awareness Foundation
Building awareness across the organization
Level 1
Basic Compliance
Minimum security requirements to meet regulatory standards
Improving Human Risk Management practices
Source: KnowBe4



KnowBe4

Thank you for your interest in KnowBe4's Program Maturity Assessment!

The Program Maturity Assessment (PMA) gives you quick insight into what level out of five your organization ranks regarding its security culture and risk awareness. Your results will show you how to improve your organization's level.

Alternatively, below is a link to start your assessment:

Registered to: [redacted]

Link: [redacted]

How to use the Program Maturity Assessment:
https://support.knowbe4.com/hc/en-us/articles/42061388521875-Program-Maturity-Assessment-PMA-Overview

We are here to help! Call us toll-free at 855-566-9234 or send us an email.

Contact Sales | Contact Support
© KnowBe4, Inc. All rights reserved.

> "Your employees' knowledge, beliefs, values, and behaviors will be the difference between protection and breach."

https://www.knowbe4.com/free-cybersecurity-tools/program-maturity-assessment

© 2025 KnowBe4, Inc. All rights reserved.

KnowBe4 Academy!

The KnowBe4 Academy is an education platform where admins can learn how to successfully use and integrate KnowBe4's products. In the academy, admins can follow various learning paths for different areas of KnowBe4, including KSAT, PhishER, and SecurityCoach.

- On the **Home** page, you can view our introductory courses, such as KnowBe4 101and PhishER 101.
- View our **Knowledge Base,** connect on the **KnowBe4 Community**, or go to **KnowBe4.com.**
- On the **Topics** page, you can view all of your learning topics organized by category. You can even click **Follow** to receive notifications when new lessons are added to the topic.
- The **Library** page allows you to view all of your academy content.

KSAT 101

Learn how to implement security awareness training (SAT) and simulated social engineering campaigns for your users to minimize potential data breaches.

PhishER 101

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

Free Tools 101

Learn about KnowBe4's free tool offerings, including the Phish Alert Button (PAB) and Automated Security Awareness Program (ASAP).

© 2025 KnowBe4, Inc. All rights reserved.

Resources

SUNY Resources
https://cpd.suny.edu/knowbe4-webinar-series/past-webinars/

© 2025 KnowBe4, Inc. All rights reserved.