knowbe4

2026 Cybersecurity Awareness Month

Resource Kit Strategy Dossier

WEEK 1
WEEK 2
WEEK 3
WEEK 4

MISSION BRIEF:

2026 Cybersecurity Awareness Month

Your mission, should you choose to accept it: Equip your team with the intel they need to stay ahead of global threat actors.

Make full use of this year's load-out of cybersecurity tools, equipment and specialists as part of an elite team known as "the Workforce Risk Division." As a member of the WRD, you'll help your users embark on four week-long missions each focusing on a specific cyber threat.

Transforming your workforce into a frontline defense force just got a lot easier. We've done the heavy lifting with a free collection of resources.

This campaign-in-a-box for Cybersecurity Awareness Month casts your employees as "Secret Agents" in the campaign against cybercrime. In addition to free training modules and supporting posters and documents, we've included four "Specialist" Character Cards that personify the skills needed to navigate today's threat landscape. You'll also find four pre-built table-top exercise scenarios designed to be run in person or virtually to help your team build resilience against threats to come.

Your Equipment

Our kit web page gives you:

FOR YOUR EYES ONLY

For Your Eyes Only

- **Webinar:** How to Secure AI Adoption in Your Organization
- **Whitepaper:** Securing The Hybrid Workforce: Protecting Humans and AI Agents in a New Era
- **Four topic-based tabletop exercise** scenario documents
- **Web-based Security Awareness Weekly Planner**, which organizes all the user-facing assets below into weekly planned themes for use throughout October available here:

WEEKLY PLANNER

For Your Agents

Access all courses and content via the links provided until **October 31, 2026.**

- **Six free interactive training or video modules**
  - Smishing Frenzy (Available in 35 languages)
  - A Deepfake Social Engineering Attack (Available in 35 languages)
  - Protecting Intellectual Property (Available in 12 languages)
  - Strong Passwords, Secure Accounts (Available in 35 languages)
  - Hack-Proof Habits Audiocast (Available in 12 languages)
  - Pursuit of Privacy Game (Available in 13 languages)
- **Four Workforce Risk Division Specialist character cards/posters**
- **Four posters and digital signage assets perfect for reminders on key concepts**

Workforce Risk Division 101

For WRD agents, the constant struggle against bad actors is hard enough, so we've tried to make enlisting new agents as easy as possible. To start, each piece of content is aligned to a general theme to focus on for each of the four full weeks in October. Each week, consider sharing one or more of these content types:

- **Video or interactive training module**
- **Poster/Info Document**
- **WRD Specialist character card**
- **Tabletop exercise document**

We'll walk you through each week's theme in more detail later in the dossier, but here's the summary:

- **Week 1:** Phishing and Social Engineering
- **Week 2:** AI Safety and Deepfakes
- **Week 3:** Data Security and Passwords
- **Week 4:** Incident Reporting

For help visualizing how it all fits together, check out our Security Awareness Planner, available here:

WEEKLY PLANNER

Use the planner as single access point for the WRD assets made available to you.

WRD Specialist Profiles

The missions are set; now it's time to meet the specialists. Brief your users on the four sets of skills they'll need for the cyber-ops across Cybersecurity Awareness Month with these four specialist profiles. Each has a piece for what it takes to tackle the month's missions. The rest is up to your users.

PHISHING/SOCIAL ENGINEERING

GHOST

MOTTO:

TRUST,
BUT VERIFY...
THEN
VERIFY AGAIN

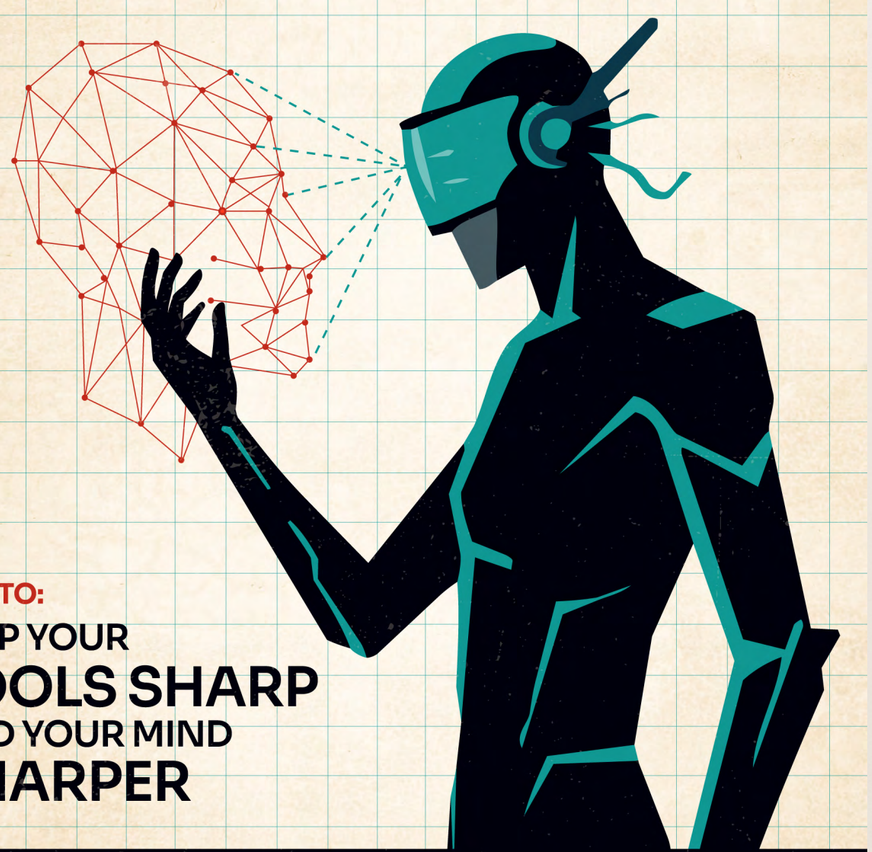
ROLE: COUNTER-INTELLIGENCE SPECIALIST

SPECIALTY: SPOTTING PRETEXTING AND SOPHISTICATED SOCIAL ENGINEERING

ADVICE: IF AN EMAIL CREATES A FALSE SENSE OF URGENCY, IT'S PROBABLY A TRAP

AI THREATS/SAFETY

GADGET



MOTTO:

KEEP YOUR
TOOLS SHARP
AND YOUR MIND
SHARPER

ROLE: TECH SPECIALIST

SPECIALTY: AI SAFETY AND DEEPFAKE DETECTION

ADVICE: USE A CODE WORD WITH FAMILY OR COLLEAGUES TO VERIFY IDENTITY DURING SUSPICIOUS "URGENT" CALLS

DATA SECURITY AND PASSWORDS

LOCK N KEY

MOTTO:

[REDACTED]

ROLE: CRYPTOGRAPHER

SPECIALTY: PASSKEYS, MFA AND ENCRYPTION

ADVICE: YOUR PASSWORD SHOULDN'T BE A WORD; IT SHOULD BE A STORY ONLY YOU KNOW

PAGE

INCIDENT REPORTING

SCOUT

MOTTO:

IF IT WALKS LIKE A
DATA BREACH
AND TALKS LIKE A
DATA BREACH;
YOU BETTER TELL SOMEONE

ROLE: FIELD OPERATIVE

SPECIALTY: INCIDENT REPORTING AND PHYSICAL SECURITY

ADVICE: IF YOU SEE SOMETHING, SAY SOMETHING

PAGE

Bringing Everyone to the Table

We've provided four comprehensive lesson plans to help guide your team through tabletop exercises simulating security crises.

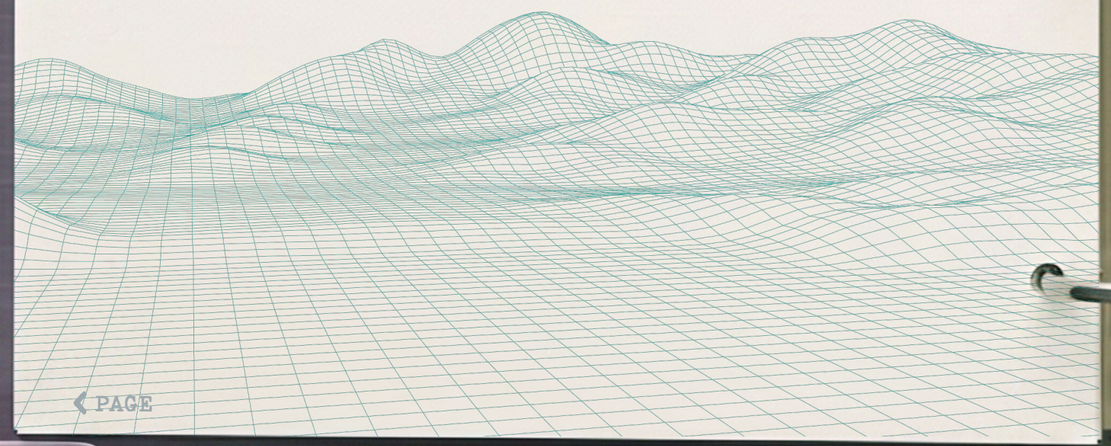
The goal is to accommodate users of any technical level, focusing on role identification, decision-making and team coordination. Activities include prioritizing response checklists and conducting realistic scenario simulations with complications. Your people will learn established incident response procedures, cross-functional communication and adaptability during security incidents through practical exercises and structured debriefing sessions.

Here are some field-ready suggestions to make the most out of these assets:

1. Manager's Mission-in-a-Box:
Share these assets with department heads with a *Director's Briefing* note. Suggest they pick a topic most relevant to their department and run a 30-minute *Rapid Response* version during an existing weekly sync meeting.

2. The Remote-First Hack Attack:
For a majority remote workforce, use the *Scenario Card* sections of the tabletop assets as poll questions during regular all-hands video conference meetings in October as quick pop quizzes. Discuss the previous week's results on the next week's meeting to see how your people fared.

3. The Instant-Message *Choose Your Own Adventure*:
Pick a day of the week and drop one *Scenario Card* into your infosec or security awareness channel on your internal messaging app of choice. The first agent to "Report the Incident" correctly, explaining why it's an issue and what could be done about it, in the thread could win a themed prize or other incentive as your organization allows.



Advice from the WRD Eggheads: Campaign Strategies

The team of behind-the-scenes scientists and researchers at the HDR may not get out much, but they know their stuff. The minds behind all these assets have seen the following core campaign strategies work for organizations of all sizes:

Think Like a Handler, Deploy Like a Field Agent
Your objective is changing risky behavior, not just information transfer. Consider how world-class intelligence agencies build "deep cover" narratives; they use multiple touchpoints to reinforce a single truth. That's why we've authorized enough assets for a multi-channel "surround sound" approach. By deploying different media (videos, games, and briefings) throughout the week, you're conditioning their security reflexes through regular engagement. This is how you turn passive employees into a hardened last line of defense.

Recruit Assets from Every Sector
No intelligence operation succeeds in a vacuum. To build a truly resilient security culture, you must recruit allies from beyond the IT perimeter. Use October to activate "Sleepers" in HR, Legal and Marketing. Show them that they have a high-stakes role in the WRD. When security messaging comes from a trusted peer in their own department rather than just "the IT guy," the intelligence is much more likely to be integrated.

Prioritize Mission-Critical Intel
Don't compromise your agents by providing too much "mission critical" intel. If you dump too much data at once, they could burn out and start clicking through briefings just to clear their queue. Instead, identify the two or three most critical vulnerabilities in your organization and focus your fire there. Our weekly mission themes—Phishing, AI Safety, Passwords and Reporting—are designed to build a well-rounded agent. Focus on the mission at hand, secure the objective and save the deep-dive intel for future operations.

While the assets in this kit should by no means take the place of a comprehensive security awareness training program, these resources are designed to be easily shared and deployed in ways that will reach your people in the most impactful way possible.

Mission by Mission Breakdown

Below you'll find content broken out by week with suggested content to feature plus associated email text.

By now you'll hopefully have some ideas or strategies in mind for how you want to tackle the month. No matter how you build out your campaign, we suggest an introductory email sent out October 1, or even the last week of September.

Here's some sample copy:

Suggested Subject Line:
[MISSION START] Your Induction into the Workforce Risk Division

2026 CYBERSECURITY AWARENESS MONTH | **MISSION START**

knowbe4

Workforce Risk Division: Initiation Briefing

Good morning agents,

In the high-stakes world of global cyber-espionage, you are the primary target—and our strongest line of defense.

Only the most vigilant and well-trained operatives can withstand the surge of AI deepfakes, sophisticated social engineering and the digital shadow-war lurking behind every corner of our network.

The field is dangerous, and you shouldn't operate in a vacuum. Fortunately, we've authorized a series of intel sessions to ensure you're prepared for the mission ahead.

THE MISSION:

This October, we are recognizing Cybersecurity Awareness Month by inducting every member of our team into the Workforce Risk Division (WRD). Throughout the month, you will be briefed by four specialists—each representing a critical pillar of our security culture.

Prepare for a four-week deployment where every mission represents a new layer of intelligence to master.

Keep your wits about you this month for **[Insert planned activities or themes here. Use the ideas in this User Guide for inspiration!]**

If you have any questions, contact **[insert contact person]**.

Your First Briefing Drops Monday. Stand by, Agent, and good luck.

WEEK 1

Phishing And Social Engineering

The most sophisticated spies don't break in; they talk their way in. This week focuses on the subtle red flags of social engineering that technical filters might miss and how to spot them.

Here's a summary of the assets for this week:

Training Module - Smishing Frenzy

This seven-minute module introduces the dangers of smishing, or text-message-based phishing, and shows how your users can avoid becoming another victim of this type of cyberattack.

Your employees will learn:

- **How cybercriminals can use social engineering through text messages**
- **What smishing typically looks like**

ACCESS ASSET

Tabletop Exercise Asset - Unmasking Phishing and Whaling Attacks

This tabletop exercise equips employees to identify and respond to sophisticated phishing and whaling attacks. Participants analyze a simulated CEO fraud email to differentiate between AI-generated false trust indicators and true behavioral warning signs. Designed for all employee levels to practice applying critical thinking and your organization's official procedures.

Two Downloadable Assets

- **Don't Get Hooked: Report Every Phishing Attempt –** Poster-style reminder of common signs of a phishing email and what to do if you suspect something phishy
- **Your Role in Internet Security –** Infographic-style asset reminding users of the most common cybercrime tactics and how to avoid them

WEEK 1 ASSETS

Sharing the Content

Here's some sample email text from specialist Ghost to use when sharing the training module for this week:

Suggested Subject Line:
[MISSION WEEK 1] Intercepting the "Smishing" Threat

knowbe4

Intercepting the "Smishing" Threat

2026 CYBERSECURITY AWARENESS MONTH | **MISSION WEEK 1**

Good morning agents,

Specialist codename **Ghost** reporting.

Our mobile devices are now the primary targets for external interference. The enemy has expanded from your inbox to your pocket.

THE MISSION:
Complete the "Smishing Frenzy" briefing. This training module introduces the dangers of smishing, or text-message-based phishing, and shows you how to avoid becoming another victim of this type of cyberattack.

You'll learn:

- **How cybercriminals can use social engineering through text messages**
- **What smishing typically looks like**

Access It Here (https://training.knowbe4.com/modstore/view/af44ce18-ea58-47c9-a352-fb1f277ec903)

If you have any questions, send a communique to **[insert contact person]**.

Stay safe out there. Look out for additional briefings this month.

Ghost out.

PAGE

WEEK 2

AI And Deepfakes

Delve into the seedy underbelly of AI to teach users how bad actors use generative tools to create perfect clones and scripts. Your agents must rely on their most valuable asset, their critical thinking skills, to verify what's real.

Here's a summary of the assets for this week:

Video Module - A Deepfake Social Engineering Attack

This six-minute video module features members of the cast of the popular security awareness series "The Inside Man" demonstrating how cybercriminals are using AI voice cloning and video deepfake technology to impersonate people you may know.

Your employees will learn:

- **How cybercriminals can use deepfakes and social engineering to compromise an organization's defenses through simple requests**
- **Red flags to watch for to protect yourself and your organization from sophisticated deepfake attacks**

ACCESS ASSET

Training Module - Protecting Intellectual Property

This 10-minute training module, available from the KnowBe4 Compliance Plus library, explains the importance of intellectual property, or IP.

Your employees will learn:

- **What IP is and why it is so valuable**
- **How to protect IP from theft, infringement and accidental exposure, including via use by artificial intelligence**

ACCESS ASSET

Tabletop Exercise Asset - The AI Prompt Challenge

This tabletop exercise equips employees to identify the risks of using unsafe prompts in the workplace. Participants will analyze AI prompts to select which ones are safe and which ones put private data at risk. Designed for all employee levels to practice critical thinking and following their organization's policies.

PAGE

WEEK 2
WEEK 3
WEEK 4

Two Downloadable Assets/Digital Signage

- **Real or Fake? Spotting Deepfakes –** Poster-style reminder to use context clues and critical thinking to help identify deepfakes in the wild
- **Phishing Gets Smarter: How AI Is Changing Online Scams –** Infographic-style asset that explains how AI is making phishing scams harder to detect

WEEK 2 ASSETS

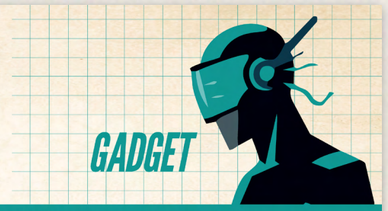
Sharing the Content

Here's some sample email text from specialist Gadget to use when sharing our suggested featured asset for this week: the "A Deepfake Social Engineering Attack" module.

Suggested Subject Line:
[MISSION WEEK 2] **Seeing Through the Deepfake**

knowbe4

Seeing Through the Deepfake



2026 CYBERSECURITY AWARENESS MONTH | **MISSION WEEK 2**

Good morning agents,

Specialist **Gadget** reporting in.

It rusts my toolkit to see leaps in AI tech used for evil. Bad actors are using the latest in AI voice cloning and video deepfakes to impersonate leadership and colleagues. Anyone they can duplicate that will get them the access and data they need to complete their own nefarious missions is fair game.

THE MISSION:
Complete the *Deepfake Social Engineering Attack* video briefing. This module features vital intel from "The Inside Man" experts demonstrating how cybercriminals are using AI voice cloning and video deepfake technology to impersonate people you may know.

You'll learn:

- **How cybercriminals can use deepfakes and social engineering to compromise an organization's defenses through simple requests**
- **Red flags to watch for to protect yourself and your organization from sophisticated deepfake attacks**

Access It Here (https://training.knowbe4.com/modstore/view/0451be1f-0531-4724-a664-21f109be6308)

If you have any questions, contact **[insert contact person]**.

Keep your tools sharp and your mind sharper. Look for additional briefings this month.

Gadget signing off.

WEEK 3

Data Security And Passwords

Sensitive data is currency in the modern world; and bad actors are willing to do anything to get it. Make sure your agents know the value of what they protect and what's at stake if it gets out. This week focuses on using password managers and MFA to ensure that even if an agent is compromised, the agency's data stays encrypted.

Here's a summary of the assets for this week:

Mobile-First Training Module - Strong Passwords, Secure Accounts

This five-minute module, designed for use on mobile devices, details the importance of secure passwords and passphrases in your users work and home lives.

Your employees will learn:

- **Tips on creating strong, secure passwords and using passphrases effectively**
- **How to avoid common security mistakes that leave accounts vulnerable**
- **Best practices for securing passwords and passphrases**

ACCESS ASSET

Tabletop Exercise Asset - The Password Guessing Game

This tabletop exercise gives employees a simulated role as a hacker to experience cracking weak passwords. Participants will examine social media posts and try to guess their owners' passwords only from the information shared online. This exercise demonstrates how the combination of oversharing online and having weak password practices makes it easier for bad actors to brute-force their way into accounts.

Two Downloadable Assets/Digital Signage

- **Strong Passwords Protect Your Online Peace –** Poster-style asset focusing on the importance of strong passwords
- **Sensitive Data: Keep it Secret, Keep it Safe –** Infographic-style document explaining the basics of keeping sensitive information secure and why to do so

WEEK 3 ASSETS

Sharing the Content

Here's some sample email text *from* specialist Lock and Key to use when sharing the training module for this week:

Suggested Subject Line:
[MISSION WEEK 3] **Securing the Vault**

Good morning agents,

Specialist **Lock and Key** checking in from… well, that's under lock and key.

A secret is only as safe as its lock. We're going back to basics with proper password protocol. What may sound like trainee-level intel does not make it any less important. Our most complex vaults are useless if left open.

THE MISSION:
Complete the "Strong Passwords, Secure Accounts" mobile training module. Learn why passphrases beat passwords and how to eliminate the common mistakes that leave our perimeter open.

You'll learn:

- **Tips on creating strong, secure passwords and using passphrases effectively**
- **How to avoid common security mistakes that leave accounts vulnerable**
- **Best practices for securing passwords and passphrases**

Access It Here (https://training.knowbe4.com/modstore/view/c0ee0966-ff3a-4fc2-93bb-2a632811140b)

If you have any questions, send an encrypted communication to **[insert contact person]**.

As my favorite wizard says: Keep it secret. Keep it safe.

LK

WEEK 4

Incident Reporting

In the Workforce Risk Division, keeping ears to the ground is a vital part of an operation. No agent can get through any mission alone, so it's crucial your agents know the importance of telling the team when something doesn't seem quite right. This week ensures every agent knows exactly how to signal for backup when they see something suspicious.

Here's a summary of the assets for this week:

Audiocast - Hack-Proof Habits: Reporting

This 15-minute audiocast, split into five and 10-minute modules, discusses the importance of reporting security threats.

Your employees will learn:

- **Potential barriers to reporting that can occur when faced with a security threat**
- **Why reporting is such a critical step in fighting cybercrime**
- **A decision-making process they can use to analyze situations and choose safe actions**

ACCESS PART 1 ACCESS PART 2

Game - Pursuit of Privacy

This 15-minute interactive game will improve your users' understanding of international data privacy laws through a challenging, globe-trotting adventure that will sharpen their compliance knowledge.

Your employees will learn:

- **The importance of data privacy regulations**
- **Different regional and international approaches to data privacy**

ACCESS ASSET

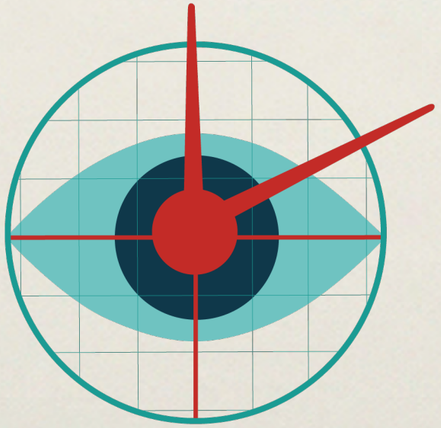
Tabletop Exercise Asset - Incident Response

This comprehensive incident response lesson plan guides corporate employees through tabletop exercises simulating security crises. The practice accommodates participants of any technical level, focusing on role identification, decision-making and team coordination. Activities include prioritizing response checklists and conducting realistic scenario simulations with complications. Participants will learn established incident response procedures, cross-functional communication, and adaptability during security incidents through practical exercises and structured debriefing sessions.

Two Downloadable Assets/Digital Signage

- **One Report, Shared Protection -** Poster-style asset that highlights the importance of promptly reporting suspicious emails to protect personal information, colleagues and client data
- **Phishing, Physical Security, and Data Breaches, Oh My! -** Infographic-style asset reminding users why immediately reporting security concerns stops small issues from becoming major incidents

WEEK 4 ASSETS



Sharing the Content

Here's some sample email text from specialist Scout to use when sharing the audiocast and game module this week:

Suggested Subject Line:
[MISSION WEEK 4] Keeping the Team Informed

knowbe4

Keeping the Team Informed

2026 CYBERSECURITY AWARENESS MONTH | MISSION WEEK 4

Good morning agents,

Scout reporting in with a final sit-rep and briefing.

Our missions only succeed if the WRD knows what's happening on the ground and in the wild.

Reporting incidents isn't snitching. It's passing along vital intel so our teams can secure the perimeter and keep bad actors at bay.

Your fourth and final briefing is two-fold:

THE MISSION:

Listen: Hack-Proof Habits: Reporting. Master a core infosec decision-making process to analyze threats in real-time

Access Part 1 (https://training.knowbe4.com/modstore/view/ad7bb017-916b-442f-b1e7-4f96bf6b202f)

Play: The Pursuit of Privacy. Travel the world (virtually) and test your knowledge of global data privacy practices to learn more about what's at stake when it comes to potential breach incidents

Access Part 2 (https://training.knowbe4.com/modstore/view/a5ec90a8-956b-4675-8c63-c336812752e7)

If you have any questions, ping **[insert contact person]**.

Scout signing off on behalf of the whole WRD team.

MISSION DEBRIEF:

Keeping Workforce Risk Top-of-Mind

The leadership team at the WRD expects this mission dossier and provided assets has helped you equip your people with the skills and tools needed to turn away cyberthreats of all types.

Establishing and maintaining a strong security culture is an ongoing mission. Real behavior change for the better means a strategy that turns your largest attack surface— your workforce — into your biggest asset, thereby reducing workforce risk.

Think of these assets as a complement to a comprehensive approach to security awareness and training. If you're interested in how KnowBe4 can help you take the next step, contact us.

For more assets and intel for you and your users throughout cybersecurity awareness month be sure to follow and mention @KnowBe4 on social media. Use the hashtag #CyberAware to stay in the loop throughout Cybersecurity Awareness Month.


knowbe4