Cybersecurity Awareness Month

2023

KnowBe4

Resource Kit User Guide

WELCOME TO YOUR 2023 CYBERSECURITY AWARENESS MONTH KIT!

Thank you for requesting KnowBe4's 2023 Cybersecurity Awareness Month Kit. We've built this kit to help you drive home the importance of cybersecurity and keeping safe from malicious social engineering attacks for your employees.

Cyber threats can be scary, and for good reason. Malware can be lurking in a suspicious email your users get convinced to click. All it takes is one crack in the door of your network to let all the wrong ones in; spear phishing witches, ravenous ransomwolves, you name it!

But never fear! While torches, pitchforks and silver bullets never put down a data breach, a resilient security culture in your organization is your best bet for keeping the beasts at bay. We've put together a set of resources you can use throughout the entire month of October to help your users keep up their cybersecurity defenses.

With **suggested campaign ideas** and an **interactive planner**, our Cybersecurity Awareness Month Kit has what you need to run an engaging security awareness training campaign all month long!

What You Get

The kit web page gives you access to these resources:

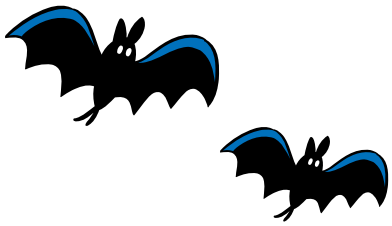
For You

- On-Demand Webinar: *Critical Considerations When Choosing Your Security Awareness Training Vendor*
- Whitepaper: *The Security Culture How-to Guide*
- **Interactive Security Awareness Weekly Planner**, which organizes all the user-facing assets below into weekly planned themes for use throughout October available at this link: https://www.knowbe4.com/cybersecurity-awareness-weekly-training-planner-p

For Your Users

Access all courses and content via the links provided until October 31, 2023.

- 4 video modules
    - *Security Culture and You*
    - *KnowBe4 Pretexting - "Tech Support" Social Engineering (Available in 36 languages)*
    - *Understanding URLs (Available in 35 languages)*
    - *When You Report, We Get Stronger - PAB (Available in 12 languages)*
- 5 free interactive training modules
    - *Eight Ways to Strengthen and Secure Your Passwords Today (Available in 35 languages)*
    - *Micro-module: Introduction to Ransomware (Available in 10 languages)*
    - *Social Media: Staying Secure in a Connected World (Available in 35 languages)*
    - *Danger Zone game (Available in 34 languages)*
    - *2023 Common Threats (Available in 36 languages)*



- 5 cyber-monster character cards and posters
- 4 cybersecurity and security awareness tip sheets
- 4 Security Hints and Tips newsletters
- 4 posters and digital signage assets perfect for reminders on key concepts

Access all posters, tip sheets, and other digital assets via this single file download.

What to Do

The same principles we built this kit around also underpin any good security awareness training program. Key concepts you should keep in mind are:

Treat Your Program Like a Marketing Campaign

To strengthen security, you must focus on changing employee 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 security reflexes so your workforce becomes an effective last line of defense. Bringing varied content across multiple channels will go a long way toward achieving this goal. That's why we've packed this kit with enough assets to deploy multiple resources per week throughout October.

Work with Colleagues in Other Departments

Use October as an opportunity to involve people and resources from throughout your company, including HR and even Marketing, to strengthen your organization-wide security culture. More than just your infosec team has a stake in a strong cybersecurity posture.

Focus Training on a Few Key Risks

Decide what behaviors you want to shape and then prioritize the top two or three. The themes we've developed per week in October are a perfect starting place to focus on the threats that impact your organization the most and build off for later security awareness initiatives.

While the content 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 employees in the most impactful way possible.

With that said, read on for campaign ideas for sharing these resources and sample email text to get you started!

Campaign Ideas to Get You Started

We hope our interactive **Security Awareness Planner** makes the thought of providing a month's worth of security awareness content way less scary! With this tool, available here: https://www.knowbe4.com/cybersecurity-awareness-weekly-training-planner-p, you can access all content included in our Cybersecurity Awareness Month Kit all in one place!

We've aligned each piece of content to a general theme to focus on each of the four full weeks in October. Each week we suggest sharing one or more of these content types:

- Video or interactive training module
- Infographic
- Poster
- Awareness Tip Sheet
- Cyber-monster character card

We've offered some suggested themes per week based on the content presented in the interactive planner (explained in more detail below)

- Week 1: Security Culture
- Week 2: Ransomware
- Week 3: Social Media and AI
- Week 4: You Can Make a Difference

Cyber-Monster Cards

This year we've included a set of five **cyber-monster cards and associated posters**. Each spooky creature personifies a key cyber threat that can be tied into each week's theme.

The cards are meant to bring a little fun to the month of October, which just so happens to end on Halloween. Though senses of humor can vary, our customers and colleagues typically find a light-hearted approach to some cybersecurity training topics pays dividends.

Our pack of cyber-monsters have hidden throughout this user guide, lurking behind paragraphs and images. Find them all and be among the first to tell us at https://info.knowbe4.com/cyber-monsters which page each is on, and you'll be entered to win a limited edition printed set of the cards and posters! Happy hunting!

How should they be used you might be wondering? We're glad you asked! Let your imagination run wild, but here are some ideas to get you started:

- **Monster Hunting:** Organize a scavenger hunt around your office (or internal shared drive or intranet) to find the hidden cyber-monster cards. The employee who finds them all first wins!
- **Dressed to Kill:** Plan a Halloween costume contest and encourage employees to dress up as one of the cyber-monsters. Fan favorite voting is encouraged!
- **Guess that Monster:** Use Google Forms or other online survey tools to build an educational quiz based on the cyber-monster traits. Offer incentives, like small prizes or recognition, for those who score well to encourage participation.

Meet the Monsters

Find descriptions of each character below, with access to cards and posters themselves available from the same web page where you downloaded this guide:

Count Hackula

Whether by brute force or the charm of social engineering, Count Hackula is desperate to drain your networks of vital personal identifiable information (PII). Ensure your systems are safe from this monster with secure passwords and employees who know enough to see past Count Hackula's mesmerizing gaze.

Spoofy Steve

Wrapped in ancient layers of digital cloth, Spoofy Steve hides his scammy intentions from all but the most insightful of employees. Use well-honed social-engineering-spotting skills to avoid his tricks as he pretends to be a coworker or supervisor asking for sensitive information.

Breachatrix le Phish

This sister of the night has her evil eye set on the most valuable of targets; C-suite and finance managers beware! Breachatrix le Phish will swoop in to cast her spear phishing spells to steal secrets and treasure but can be warded off with a resilient security culture in your organization.

Ransomwolf

Lurking in that innocent-looking file attachment you just downloaded, Ransomwolf is ready to gobble up all your important files, bounding from folder to folder through the forest of your network. Unlike other werewolves, Ransomwolf is invulnerable to "silver bullets." Organizations need both regular backups and a well-trained employee base to keep this monster at bay. Don't wait until this monster turns into something worse!

Frankenphisher

Frankenphisher is stitched together from all the most dangerous pieces of phishing emails; compromised links, malicious attachments, you name it! Before he gets a chance to bust down the door of your network, make sure your people know what makes a phishy email phishy.

Security Hints and Tips Newsletters

The kit also includes four Security Hints and Tips Newsletters designed to stand on their own as informational emails or even internal blog posts. These can augment or replace the suggested emails we have for each weekly theme. The links and topics for these newsletters are listed below:

- **Google Yourself**
- **Unsafe Email Attachments**
- **Stay Safe on Social Media**
- **Unexpected Emails**

Consider connecting each theme to a "Question of the Week" or "Point to Ponder" to get your employees thinking about the topics and content. One way to proceed would be to feature one of the videos or interactive modules per week via email, while sharing the supporting digital signage and infographics via your internal social media, chat channels (Slack or Microsoft Teams, for example) or intranet; wherever your employees spend the most time.

Remember these are just suggestions! You know your organization and people best, so use these assets however you see fit. The beauty of the variety of resources available in our kit is all the different directions you could go to promote cybersecurity best practices this month.

No matter how you build out your campaign, we suggest an introductory email sent out Oct. 1, or even the last week of September. Here's some sample copy:

Suggested Subject Line: *Welcome to Cybersecurity Awareness Month 2023!*

Cyber threats can be scary, and for good reason. Malware could be lurking in any suspicious email that finds its way into your inbox.

Fortunately, we know how to keep bad actors and monstrous malware at bay. But we can't do it without your help!

That's why we're recognizing Cybersecurity Awareness Month this October by sharing tips to promote a strong and resilient security culture in our organization. To turn away cyber attacks, a little knowledge teamed with critical thinking skills can go a long way!

Stay tuned this month for ***[Insert planned activities or themes here. Use the ideas in this User Guide for inspiration!]***

If you have any questions, feel free to reach out to [insert contact person].

Thanks, and have a cyber secure October!

Below find the contents of each week in detail plus suggested content to feature.

Week 1 Campaign - Security Culture

The first suggested campaign theme is about establishing a strong culture of security in your organization. As we like to say, every organization has a security culture; it's the quality of it that matters. **Security culture** is defined as the ideas, customs and social behaviors of a group that influence its security.

Your employees' knowledge, beliefs, values and behaviors will be the difference between protection and breach. That's why focusing on security culture is so important. An organization's employees are at the center of everything; they can either be easy prey or they can become an effective human layer of defense.

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

Video Module - Security Culture and You

Access Link: https://training.knowbe4.com/modstore/view/561dccec-1cba-4015-80b8-23ba0a3eaa26

Mobile-First Training Module - Eight Ways to Strengthen and Secure Your Passwords Today

This four-minute video explores how building a strong security culture can help protect both organizations and employees' homes from cyber attacks.

Your employees will learn:

- What security culture is and why it's important
- What a strong security culture looks like in practice
- Their role in building a strong security culture

Access Link:
https://training.knowbe4.com/modstore/view/5c215964-f416-4e56-9dd0-31ce7619de5a

3 Downloadable Assets/Digital Signage

- *Stop! Look! Think!*—Poster-style reminder to stay alert to cyber risks
- *Why Security Awareness Training?*—Poster-style reminder about the importance of employee training on cybersecurity
- *Pump Up Your Password Strength!*—Poster-style graphic with easy-to-digest password best practices

Sharing the Content

Here's some sample email copy to use when sharing our suggested featured asset for this week: the *Security Culture and You* training video. Alternatively, we suggest using the ***Google Yourself*** newsletter this week.

Suggested Subject Line: *Our Security Culture Depends On You!*

Whether you know it or not, you play a major role in our organization's security culture.

That may sound intimidating, but chances are you're already doing your part. Reporting a phishing email to our IT team, discussing a news-making cyber attack with a coworker; that's security culture at work!

To help kick off Cybersecurity Awareness Month, we're sharing a short video discussing the basics of cybersecurity culture. Watch this video to learn:

- *What security culture is and why it's important*
- *What a strong security culture looks like in practice*
- *Your role in building a strong security culture*

Check it out here:
https://training.knowbe4.com/modstore/view/561dccec-1cba-4015-80b8-23ba0a3eaa26

You and your coworkers are a vital part of our cybersecurity program. Remember: No one gets through life alone!

If you have any questions, feel free to reach out to ***[insert contact person]****.*

Thanks, and look for more cybersecurity content all this month!

Week 2 Campaign - Ransomware

The second week's suggested campaign theme focuses on ransomware. Still a devastating type of malware for any organization, ransomware attacks cause downtime, data loss and possible intellectual property theft. Phishing emails remain a leading cause of ransomware entry, meaning your employees have a key role to play in keeping it out of your network.

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

Video Module - Tech Support Scam/Pretexting Featuring Kevin Mitnick

This five-minute video module features Kevin Mitnick and Rachel Tobac (social engineer and the CEO / Co-founder of SocialProof Security) roleplay a social engineering attack using pretexting. Pretexting is a form of social engineering where the attacker lies to obtain restricted information.

Your employees will learn:

- How bad actors can compromise an organization's network by pretending to be a member of the tech support team
- Why the software details of their work computers should be kept private
- Warning signs that someone may be trying to glean information about your organization's network or computers

Access Link:
https://training.knowbe4.com/modstore/view/c033863b-b521-11e9-84bf-123d7cbdf51c

Interactive Training Module - Introduction to Ransomware

This five-minute micro-module takes an employee through the basics of ransomware, the different methods used to infect a machine, and how hackers trick unsuspecting users into downloading infected files. The module includes video-based lessons and a brief quiz.

Your employees will learn:

- How unexpectedly ransomware can show up
- The typical ransomware extortion process
- Tactics cybercriminals use to get ransomware on networks
- What to watch out for

Access Link:
https://training.knowbe4.com/modstore/view/5372c0ab-04cb-47a2-a0f3-20df870948bf

3 Downloadable Assets/Digital Signage

- *You Can't Go Back*—Poster-style reminder of how risky a single click on a suspicious email can be
- *Ransomware Invaders*—Poster-style graphic in the style of "Space Invaders" where ransomware is the target
- *Major Keys to Ransomware Protection*—Infographic summarizing important ways to avoid and combat ransomware

Sharing the Content

Here's some sample email copy to use when sharing our suggested featured asset for this week: the training module *Introduction to Ransomware*. Alternatively, we suggest using the ***Unsafe Email Attachments*** newsletter this week.

Suggested Subject Line: *Don't Let Ransomware Lock You Out!*

We won't sugarcoat it: Ransomware can make even the most hardened IT pro shake in their boots.

That's why we need your help to keep baddies from locking out our network! For Cybersecurity Awareness Month this year, we're sharing a short training course that explains the basics of ransomware, the different methods used to infect a machine, and how hackers trick unsuspecting users into downloading infected files.

Check out this course to learn:

How unexpectedly ransomware can show up

The typical ransomware extortion process

Tactics cybercriminals use to get ransomware on networks

What to watch out for

Access it here:
https://training.knowbe4.com/modstore/view/5372c0ab-04cb-47a2-a0f3-20df870948bf

If you have any questions, feel free to reach out to ***[insert contact person]****.*

Thanks, and look for more cybersecurity content all this month!

P.S. Check out this infographic for important ways to avoid and combat ransomware:

[Insert link to "Major Keys to Ransomware Protection" asset]

Week 3 Campaign - Social Media and AI

The third week's suggested campaign theme focuses on social media threats and the rise of AI. Hackers have not shied away from social media as a hunting ground to target victims and perpetuate scams. Additionally, the rising popularity of AI tools means employees must be even more vigilant about what they see and share online.

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

Video Module - Understanding URLs

This two-minute video module breaks down the parts of a URL to show how hackers can manipulate them to their gain and everyone else's loss.

Your employees will learn:

- The fundamental parts of the URL structure
- What makes a URL received in an email or other means suspicious

Access Link:
https://training.knowbe4.com/modstore/view/9e96a153-a5a0-428c-abe1-d24cbe71386d

Interactive Training Module - Social Media - Staying Secure in a Connected World

This eight-minute module explores ways to keep employees and your organization safe from bad actors using social media to target victims and perpetuate scams. This module includes scenario-based instruction and a brief quiz.

Your employees will learn:

- The prevalence of social media use
- The variety of ways cybercriminals use social media to target victims
- Specific examples of how to protect themselves and your organization

Access Link:
https://training.knowbe4.com/modstore/view/71970510-f7b1-4f24-ad5c-567f7dd181a6

3 Downloadable Assets/Digital Signage

- *Deepfakes*—Poster-style reminder about the prevalence of deepfakes and the importance of the "trust but verify" concept
- *Risks of Social Media Sharing*—Poster-style asset with easy-to-digest reminders about social-media-related risky behaviors to avoid
- *What Are AI Chatbots?*—Poster-style asset with five tips for using AI chatbots with cybersecurity in mind

Sharing the Content

Here's some sample email copy to use when sharing the suggested featured asset for this week, the interactive training module: *Social Media - Staying Secure in a Connected World*.

Alternatively, we suggest sharing the ***Stay Safe on Social Media*** newsletter this week.

Suggested Subject Line: *Share with Care on Social Media!*

Could that beyond-belief animal video you just liked and shared have been too good to be true?

The combination of social media and AI-generated content has made major sharing platforms a prime hunting ground for scammers and cybercriminals. All the more reason to keep your wits about you and think twice before you share!

That's why our next offering for Cybersecurity Awareness Month is all about social media. In this video, we'll cover:

- *The popularity of social media and its risks*
- *The crafty ways cybercriminals target their victims*
- *Simple and specific tips to shield ourselves and our organization*

Check it out here:
https://training.knowbe4.com/modstore/view/71970510-f7b1-4f24-ad5c-567f7dd181a6

Let's stay one step ahead of those scammers! Tune in to the training, keep your personal information secure, and remember, we've got each other's backs!

If you have any questions, feel free to reach out to ***[insert contact person]****.*

Stay tuned for more Cybersecurity Awareness Month activities!

P.S. For a primer on AI tools and how to use them securely, check out this infographic:

[Insert link to "What Are AI Chatbots" asset]

Week 4 Campaign - You Can Make a Difference

The fourth and final week's suggested campaign theme is the importance of your employees' actions on an individual level. Everyone in an organization is ultimately part of the cybersecurity team, both through their actions *and* inactions. Make sure they're doing the right things and avoiding the wrong ones!

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

Video Module - When You Report, We Get Stronger - PAB

This short video module emphasizes the importance of reporting suspicious emails using standard company policies. The key message is, ***"When you report, we get stronger."***

Your employees will learn:

- The importance of their role in keeping the whole organization cyber secure
- That trusting their gut and reporting a suspected phishing email is better than doing nothing at all

Access Link:
https://training.knowbe4.com/modstore/view/04781289-4926-460b-8cd1-2e75ee69aaff

Free Offer: To make it even easier for your employees to report phishing emails, we offer a free **Phish Alert Button** that can be installed in your email client. Once installed, users can click a button to report real phishing emails, which are then directly forwarded to your incident response or IT teams.

Consider introducing the Phish Alert Button once you have it installed and educate your users on why it's important to report suspicious emails using this training video.

Find out more about our Phish Alert Button here!

Interactive Game - Danger Zone

This web-based game is set in an office where a nefarious hacker is trying to get to an unlocked computer. Your employees will be asked to answer security awareness training-related questions correctly, which will move them closer to the workstation. If they answer incorrectly, the hacker will move closer. The goal: Stop the hacker, get to that workstation, and save the organization!

Access Link:
https://training.knowbe4.com/modstore/view/e883204e-cd6b-417b-b371-40014e27ada1

3 Downloadable Assets/Digital Signage

- *Make it a Habit… PAB It!*—Poster-style to get into the habit of using the Phish Alert Button (PAB) to report phishing emails
- *Be an Email Superhero*—Poster-style reminder of the power all employees have to think before they click
- *Social Engineering Red Flags*—Infographic that calls out important characteristics of a phishing email to look out for

Sharing the Content

Here's some sample email copy to use when sharing our suggested featured asset for this week: the *Danger Zone* Mini-Game. Alternatively, we suggest using the ***Unexpected Emails*** newsletter this week.

Suggested Subject Line: *[Mini-Game] Can You Keep the Hacker from Breaching our Network?*

RED ALERT!

A hacker has made it inside our offices and has spotted an unlocked workstation.

Can you use enough cybersecurity knowledge to stop the hacker before they compromise our network?

In this browser-based mini-game, answer security awareness training-related questions correctly, and you will move closer to the workstation. Answer incorrectly, and the hacker will move closer. Stop the hacker, get to that workstation, and save the organization. Game on!

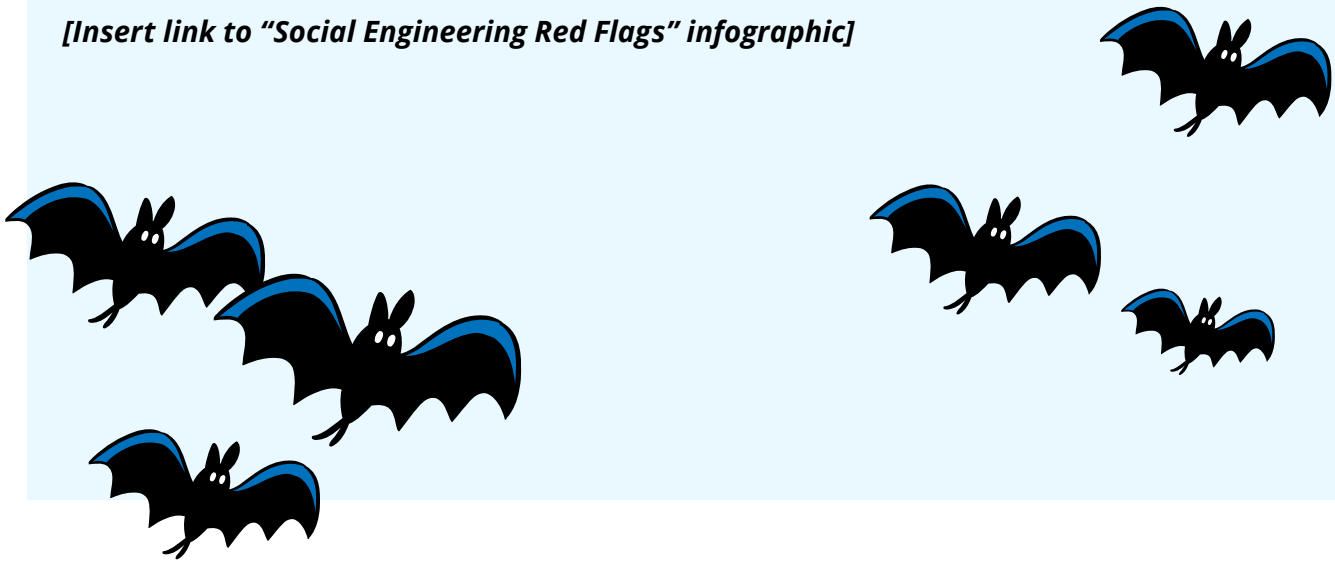
Check it out here:
https://training.knowbe4.com/modstore/view/e883204e-cd6b-417b-b371-40014e27ada1

If you have any questions, feel free to reach out to ***[insert contact person]****.*

Thanks, and remember: Think before you click!

P.S. Need some hints to help thwart the hacker? Check out this infographic:

[Insert link to "Social Engineering Red Flags" infographic]



KEEPING CYBERSECURITY TOP-OF-MIND

We hope the resources in this kit help you drive important lessons about cybersecurity and the responsibilities we all share for keeping bad actors at bay.

Think of this kit as a complement to a full-fledged training and awareness initiative. If you're interested in how KnowBe4 can help you build out a security awareness training program and work toward addressing the ongoing problem of social engineering, contact us!

For more resources, tips, and news 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!

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

01D08K01