Cybersecurity Awareness Month

2023

KnowBe4

Customer 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 a **web-based planner**, our Cybersecurity Awareness Month Kit has what you need to run an engaging security awareness training campaign all month long!

What You Get

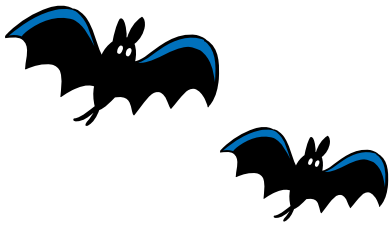
The kit web page gives you access to these resources:

For You

- On-Demand Webinar: *2023 Phishing By Industry Benchmarking Report*
- Whitepaper: *Building an Effective and Comprehensive Security Awareness Program*
- **Web-Based 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-dc
- Select support documentation from the KnowBe4 Knowledge Base
- A selection of new simulated phishing landing pages templates:
    - Phishing Template: *UPS: We attempted to deliver your item*
    - Phishing Template: *Scheduled Maintenance*
    - Phishing Template: LinkedIn: *Hoyt Waller sent you a message on LinkedIn*
    - Phishing Template: *Chase: Security Alert: Unusual Debit Card Activity Detected*
    - Landing Page: *How to Avoid the Cyber Monsters*
    - Landing Page: *That was scary!*

For Your Users

- 4 video modules
    - *Kickoff: Overview Cyberattacks (Available in 35 languages)*
    - *Security Snapshots: Pretexting (Available in 34 languages)*
    - *QR Codes: Safe Scanning (Available in 35 languages)*
    - *Security Culture and You*
- 4 interactive training modules



  - *Introduction to Data Protection (Available in 35 languages)*
  - *Beating Ransomware (Available in 34 languages)*
  - *How To Spot a Deepfake (Available in 10 languages)*
  - *Phish or Treat game (Available in 34 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 courses and content via your KnowBe4 ModStore until October 31, 2023. Diamond subscription levels will have access to this content from the resource kit landing page until the end of October. Look for the Carousel on the ModStore homepage for all this month's content in one place.

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 organization, 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 web-based Security Awareness Planner makes the thought of providing a month's worth of security awareness content way less scary! Check it out at this link: https://www.knowbe4.com/cybersecurity-awareness-weekly-training-planner-dc, and see a whole month's worth of content laid out by week.

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 planner (explained in more detail starting on page 7)

- Week 1: Data Protection
- 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 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

We've also included four **Security Hints and Tips Newsletters** as email templates accessible in your KnowBe4 platform designed to stand on their own as informational emails or even internal blog posts. Suggested Security Hints and Tips Newsletters are available in your KnowBe4 console under the Phishing Tab in Email Templates>System Templates under the Security Hints & Tips category. These can augment or replace the suggested emails we have for each weekly theme. The topics for these newsletters are listed below:

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

For more details on using the newsletters for your campaigns, check out our support article here: https://support.knowbe4.com/hc/en-us/articles/4405521758355.

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!

Getting Started in Your KnowBe4 Console

Using the KnowBe4 console, you can add all these modules to one campaign or individual campaigns depending on your preference to make the training required or optional for your users. For more information on setting up campaigns, read this Knowledge Base article:

https://support.knowbe4.com/hc/en-us/articles/204948207-Creating-and-ManagingTrainingCampaigns#CREATING

With the **Optional Learning** feature, you can allow your users to self-select which courses to take. Find out more about this process in this Knowledge Base article:

https://support.knowbe4.com/hc/en-us/articles/1500002656002

When you log in and go to the ModStore home page, look for the Cybersecurity Awareness Month Featured Content at the top of the page. We also created a special Cybersecurity Awareness Month Topic under the Popular Topics search filter. You'll see all the content bundled together to make it easy to choose available content and add to your campaign.

Below find the contents of each week in detail plus suggested content to feature. **All content is available at the Diamond subscription leve by searching the module/asset name in your ModStore.**

Week 1 Campaign - Data Protection

The first suggested campaign theme is focused on the importance of data protection. After all, the "security" part of cybersecurity is about keeping personal and sensitive information, both of your organization and individual employees, secure. Your employees need to know the role they play in keeping valuable data out of the hands of cybercriminals.

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

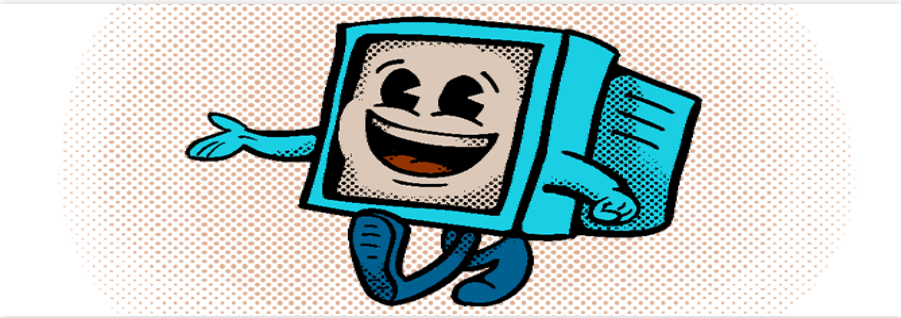
Video Module - Kickoff: Overview Cyberattacks

This two-minute video provides an overview of the most widespread cyber attack methods and helps drive home the importance of data security overall.

Your employees will learn:

- What data security is and why it's important
- How cybercriminals get into networks
- Their role in protecting data

Interactive Training Module - Introduction to Data Protection



This 11-minute module discusses the basics of data privacy and data protection in simple terms and includes real-world examples, interactive practice exercises and a short quiz.

Your employees will learn:

- What personal information is
- General privacy principles
- The types of data that need protection
- How to identify threats to data
- What happens when we fail to protect data

3 Downloadable Assets/Digital Signage

- *You Are a Target* - Infographic-style asset describing the various ways cybercriminals use social engineering
- *Spot the Phish* - Poster-style reminder of what phishing emails can look like
- *Avoid Becoming a Social Engineering Victim: Four Questions to Ask Yourself* - Poster-style asset summarizing key questions to keep in mind when a social engineering attempt is suspected

Sharing the Content

Here's some sample email copy to use when sharing our suggested featured asset for this week: the *Introduction to Data Protection* interactive module. Alternatively, we suggest using the ***Google Yourself*** newsletter this week.

Suggested Subject Line: *We Are All Data Protectors*

Cybersecurity and protecting personal data go hand-in-hand.

Think about it: Cybercriminals try to trick, lie and steal with social engineering to get their hands on personal information; yours and our organization's. The "security" in cybersecurity is really all about data!

That's why for the first week of Cybersecurity Awareness Month, we're launching a short video to walk you through the basics of data privacy and data protection.

Check out this interactive course to learn:

- *What personal information is*
- *The types of data that need protection*
- *How to identify threats to data*
- *What happens when we fail to protect data*

Secure data means the wellbeing of our organization. Secure data means peace of mind for you, both at work and at home.

So the mission is clear: Don't let bad actors near it!

Be on the lookout for email instructions from our learning console on how to access this course.

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

Thanks, and have a cyber secure October!

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.

Video Module - Security Snapshots: Pretexting

This two-minute video vignette tells the story of Alex, a seasoned performer who applies his skills not the stage or screen, but to social engineering. He pretends to be anyone he needs to be to collect sensitive information over the phone.

Your employees will learn:

- How cybercriminals use phone-based trickery to steal sensitive information or access
- The signs of a social engineering attempt
- Why they should be skeptical of unexpected urgent email or phone requests, especially if they involve money

Mobile-First Training Module - Beating Ransomware

This four-minute module, designed for use on a mobile device, teaches employees about the basics of ransomware with interactive practice exercises and a short quiz.

Your employees will learn:

- How ransomware works
- How criminals use ransomware to hijack file and systems
- Warning signs of a ransomware attack

3 Downloadable Assets/Digital Signage

- *Major Keys to Ransomware Protection* - Infographic summarizing important ways to avoid and combat ransomware
- *Protecting Data Across Borders* - Poster-style reminder that data protection is everyone's responsibility
- *Reality Bytes - Ransomware Gangs* - Newsletter-style reminder of how ransomware works and who it targets

Sharing the Content

Here's some sample email copy to use when sharing our suggested featured asset for this week: the mobile-friendly training module *Beating 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*

Be on the lookout for email instructions from our learning console on how to access this course.

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, including through the use of QR codes. 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 - QR Codes: Safe Scanning

This four-minute video module explains when and why QR codes become dangerous and how to protect yourself against them.

Your employees will learn:

- The good and bad uses of QR codes
- How they can be used to download malware
- Steps to take to use QR codes responsibly

Interactive Training Module - How To Spot a Deepfake

This five-minute training module explores the basics of deepfake technology and how dangerous it can be in the wrong hands. The module includes video lessons and a brief quiz.

Your employees will learn:

- What makes a deepfake
- Tips on how to spot them

3 Downloadable Assets/Digital Signage

- *How To Spot a Deepfake* - Infographic-style reminder about what makes a deepfake and common telltale signs
- *Deepfakes* - Poster-style asset reminding users of the “trust but verify” concept when it comes to deepfakes
- *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: *How To Spot a Deepfake*. Alternatively, we suggest sharing the ***Stay Safe on Social Media*** newsletter this week.

Suggested Subject Line: *Did That Celebrity REALLY Say That?*

As if cybercriminals didn't make modern life tough enough, now they're out to get us to doubt our very eyes and ears.

We're talking about deepfakes; an emerging technology bad actors are latching on to as part of their ever-evolving social engineering schemes.

Deepfakes are digital versions of people, manipulated to make it seem like they are saying things they're not actually saying. Since this is the perfect breeding ground for scams, we're sharing this brief training video all about them to help you suss out the real from the fake.

Check out this course to learn:

- *What makes a deepfake*
- *What makes them risky*
- *Tips on how to spot them*

Be on the lookout for email instructions from our learning console on how to access this course.

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

Thanks, and have a cyber secure October!

P.S. For a primer on deepfakes you can download and keep for yourself, check out this infographic:

[Insert link to "How To Spot a Deepfake" 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 - Security Culture and You

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

Interactive Game - Phish or Treat!

This web-based game will teach your employees the dynamics of social engineering schemes. The emphasis is on phishing attacks: scams received via email that try to trick your employees into clicking on a malicious link or downloading malware without their knowledge. The ultimate objective is for your employees to recognize the red flags of a phishing attack and avoid becoming a victim.

3 Downloadable Assets/Digital Signage

- *Data Breaches and You* - Infographic-style reminder of ways to prevent data breaches and what to do if a data breach is suspected
- *Do You Think Before You Click?* - Poster-style reminder for employees to think before they click
- *Click with Care* - Infographic with tips on what to look for in a phishing email

Sharing the Content

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

Suggested Subject Line: *[Mini-Game] Do You Know What Makes a Phishing Email Phishy?*

POP QUIZ HOT SHOTS!

You just got an email coupon from a brand you love with a killer deal. But something about it seems off... The "from" address doesn't look right, and the deal sounds a little too good to be true.

What do you do? What. Do. You. DO?

Emails like this are exactly the sorts of messages we all get every day, and the focus of our final Cybersecurity Awareness Month activity: Phish or Treat! This mini-game presents sample emails you have to mark as "phish" or "legit."

Can you spot them all? Only one way to find out!

Be on the lookout for email instructions from our learning console on how to access this game.

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

Thanks, and remember: Think before you click!

P.S. Check out this infographic for tips on what to look for in a phishing email:

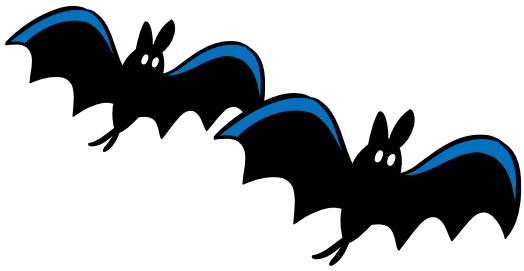
[Insert link to "Click with Care" asset]

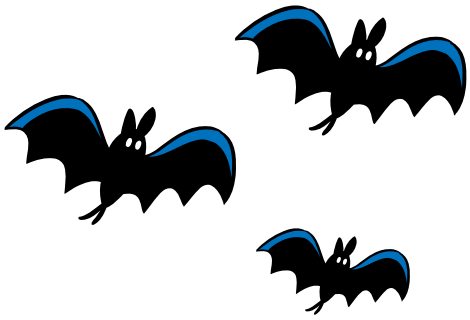
KEEPING CYBERSECURITY TOP-OF-MIND

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.

Use this kit as a complement to your existing training and awareness initiatives. If you're interested in how KnowBe4 can help you continue to build out your security awareness training program further, please contact your Customer Success Manager. They are ready to help!

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