KnowBe4
Human error. Conquered.

# 2021 Cybersecurity Awareness Month Customer Resource Kit User Guide

# WELCOME TO YOUR 2021 CYBERSECURITY AWARENESS MONTH KIT!

Thank you for requesting KnowBe4's 2021 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.

Between vacations, working from home, and coming back to something resembling "normal" from the pandemic, we wouldn't be surprised if you haven't been able to devote much time to plan for Cybersecurity Awareness Month in October.

Not to fear, we've got you covered! We put together resources and suggested courses you can use from the KnowBe4 platform to help your users keep up their cybersecurity defenses throughout the month, no matter where they are.

## What You Get

The kit web page gives you access to these resources:

**For You**

- On-Demand Webinar: *Empowering Your Human Firewall: The Art and Science of Secure Behavior*
- Whitepaper: *Building an Effective and Comprehensive Security Awareness Program*
- 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-c
- Our Advanced Phishing Tips resource to help you get the most out of your simulated phishing campaigns
- Select support documentation from the KnowBe4 Knowledge Base
- A selection of new simulated phishing landing pages and corresponding Security Hints & Tips templates:
    - Stay Safe While Working on Mobile Devices
    - Stay Safe While Working from the Office
    - Stay Safe While Working in Public Locations
    - Stay Safe While Working from Home

**For Your Users**

Select courses available per your subscription level. Preview these modules in your ModStore

- **Silver Level:**
    - 2021 Social Engineering Red Flags*
    - Your Role: Internet Security and You*

- **Gold Level and Above; All Silver Courses Plus:**
    - Mobile Device Security
    - 2021 Danger Zone Mini-game
    - Creating Strong Passwords
    - Staying Safe in the Cloud
- **2 Kevin-Mitnick-led Cybersecurity Demo Videos**
    - Password Management
    - Pretexting - Fake IT Password Demo*
- 4 infographics on avoiding social engineering and cybercrime
- 4 posters and digital wallpapers perfect for reminders on key concepts
- 4 cybersecurity awareness tip sheets

To view the kit, bookmark this link for quick reference:

https://info.knowbe4.com/cybersecurity-awareness-month-resource-kit

## What to Do

With the employee-facing resources provided, we've tried to provide a good variety in terms of both format and topic. Variety of content will get your message to resonate, and should be a part of any security training and awareness initiative.

While the content in this kit should by no means take the place of whatever security awareness training program you're currently running, these resources are designed to be easily shared and deployed throughout Cybersecurity Awareness Month 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 copy to get you started!

## Campaign Ideas to Get You Started

We have lots of ways to supplement the resources in this kit to make this the best Cybersecurity Awareness  Month ever!

Try using our recommended email templates, themed landing pages, and Cybersecurity Awareness Month newsletters in weekly simulated phishing campaigns. See our How to Engage Users During Cybersecurity Awareness Month Knowledge Base article (https://support.knowbe4.com/hc/en-us/articles/4405521758355) for a brief overview and detailed instructions.

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.

**Available to KnowBe4 Silver customers through October 31, 2021 with direct access links via the resource kit web page.*

Here's some sample copy:

**Suggested Subject Line: Welcome to Cybersecurity Awareness Month 2021!**

In our uber-connected world, it seems like cybercriminals and malicious links creep around every corner. News stories of ransomware attacks and data breaches costing millions of dollars fly past our feeds almost constantly.

We get it; it can be overwhelming. With so much information bombarding us, it can be hard to focus on the right actions to take to keep information secure.

That's why we're recognizing Cybersecurity Awareness Month this October by sharing tips to stay cyber secure, both at work and at home. 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!

We've taken the guesswork out of putting together a month's worth of security awareness content with our interactive Security Awareness Planner. With this tool, available at this link: (https://www.knowbe4.com/cybersecurity-awareness-weekly-training-planner-c), 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 weeks in October. Each week we suggest sharing one or more of these content types:

- Infographic
- Video or training course
- Posters
- Cybersecurity tip sheets
- Additional suggested training courses available to Gold Subscription Level and above customers

## 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-Managing-Training-Campaigns#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.

We've included campaign topics and ideas for each of the four weeks below.

**First Week Campaign:**

*Social Engineering Course*

The opening week of Cybersecurity Awareness Month is all about phishing and social engineering. This set of assets features an interactive, web-based course called *2021 Social Engineering Red Flags* that will teach your employees:

- How to identify different types of social engineering attacks
- How to identify red flags to be on the lookout for
- What actions to take to protect themselves and your organization

Here's some sample email copy to spread the word:

**Suggested Subject Line: Get to Know These Social Engineering Red Flags**

Ever get an email that just seemed off? An invitation to click on a link from a stranger, or a weird request from a usually trustworthy source?

Chances are these were examples of **social engineering**, cybercriminals' attempts to manipulate, influence or deceive you into taking some action that isn't in your own best interest or in the best interest of our organization.

Good cybersecurity practices and knowing social engineering when you see it go hand in hand. So this Cybersecurity Awareness Month, we're sharing this training course covering the ins and outs of social engineering. You'll learn:

- The different types of social engineering attacks cybercriminals use
- Key signs of social engineering
- What actions to take to avoid making yourself or or organization the latest victim of a cyber attack

**[For Gold, Platinum, and Diamond customers]**

Be on the lookout for an email notification of your enrollment in this training course and click the link to log in and begin the training.

**[For Silver customers]**

**[Insert this direct link for your users to access this course]**

https://www.knowbe4.com/cybersecurity-awareness-course

Stay tuned for more cybersecurity tips all month long!

### *Phishing Bounty Activity*

As a month-long opportunity to keep your employees engaged, try a Catch-the-Phish contest! With the reminders found in the first week's Email Phishing Red Flags infographic, offer your employees a challenge: The employee who reports the most suspected phishing emails throughout October receives a prize!

You could even set up weekly video conference calls and invite employees to share any notable phishing attempts they've received (sneakiest phish, most obvious phish, etc.).

If actual prizes aren't in the budget, a little organization wide recognition can go a long way. If there's one thing (most) people love almost as much winning stuff, it's being recognized for winning stuff.

This is a perfect opportunity to use the Phish Alert Button that comes with your subscription. When installed in your email client, users can click a button to report real phishing emails, which are then directly forwarded to your incident response or IT teams.

Find out more about our Phish Alert Button here:

https://support.knowbe4.com/hc/en-us/articles/208969608-Phish-Alert-Button-PAB-Product-Manual

Here's some sample email copy for this activity:

**Suggested Subject Line: Calling All Phish Hunters!**

Do you have what it takes to reel in a big phish and win a prize? Take part in our Phish Hunt game and find out!

All this month to recognize Cybersecurity Awareness Month, we're offering a phishing email bounty! Keep a close eye on your inbox for any suspected phishing emails that may come in. If you find one you think fits the bill, simply click the phishing hook icon you see at the top header of your email window **[Not using the Phish Alert Button yet? Learn more in our support article!]**.

At the end of the month we'll hold a raffle and randomly choose one phish hunter to win our prize! The more actual phishing emails you report, the more chances you have to win. Our prize consists of **[insert prize description]**.

To help spot the phishing attempts, check out these infographics:

*Red Flags of Rogue URLs*
https://www.knowbe4.com/hubfs/CybersecurityAwarenessMonth2021/Downloads/RedFlagsofRogueURLs.pdf

*Email Phishing Red Flags infographic*
https://www.knowbe4.com/hubfs/CybersecurityAwarenessMonth2021/Downloads/CyberRedFlags.pdf

**[Or access it in the ModStore and add to your training campaign].**

### *Mobile Device Security*

As an additional course option **for Gold level and above subscribers**, we've included a Mobile Device Security course. This course teachers your users:

- How hackers can use mobile devices to wreak havoc
- The dangers surrounding Bluetooth, WiFi, apps, and even human error
- How to protect your organization from these threats

Here's some sample email copy:

**Suggested Subject Line: The Power to Turn Away Cybercriminals is in Your Hands!**

Everyone partakes in the occasional scroll through their smartphone during short breaks throughout the day or during lunch.

But did you know, all totaled, the average person spends two and half hours per day on their phone?

All that scrolling time means more opportunities for hackers to sneak in to access personal data or insert malware on your device if you click the wrong link.

That's why we're taking this Cybersecurity Awareness Month to highlight a training course all about mobile device security and how to make sure your smartphone doesn't get outsmarted by hackers!

In this 10-minute course, you'll learn:

- How hackers can use mobile devices to wreak havoc
- The dangers surrounding Bluetooth, WiFi, apps, and even human error
- How to protect your organization from these threats

Be on the lookout for an email notification of your enrollment in this training course and click the link to log in and begin the training.

This Cybersecurity Awareness Month, the power to thwart cybercriminals is literally in your hands! Use it!

## Second Week Campaign

### *Pretexting - Fake IT Password Demo Lunch and Learn*

The theme for the second week is all about the variety of social engineering tactics beyond phishing that bad actors can use to gain access to your network. The focus of this week is a short video starring KnowBe4's own hacking expert Kevin Mitnick (available in the ModStore in the Cybersecurity Awareness Month topic group and via Vimeo at this link: https://vimeo.com/340994716) demonstrating how easy it is to use pretexting (impersonating someone via email or phone to steal information) to get access to your organization's network.

Consider hosting the 5-minute video on a shared space and playing during a lunch-and-learn for the entire organization. Some questions to ask after the video to generate healthy discussion include:

- What were the first signs something was not right?
- What should you do in this situation?
- Has anyone here encountered such an attempted scam, either at work or at home?

Here's some sample copy for this activity:

**Suggested Subject Line: Do You Know A Social Engineering Scam When You See It?**

Hackers aren't just about convincing people to click on links and download malware.

Sometimes the right set of questions from a seemingly trustworthy source can lead to cybercriminals on our network without a single click.

That's why we're featuring a brief video for the second week of Cybersecurity Awareness Month all about pretexting, which often involves bad actors impersonating someone via email or phone to steal information.

Join us ***[insert time and date of showings here]*** for a lunch-and-learn screening of a demonstration showing how hackers can use pretexting to gain access to sensitive information over the phone, followed by some discussion afterward.

Stay tuned for more Cybersecurity Awareness Month activities!

### *Danger Zone Game*

As an additional option **for Gold level and above subscribers**, we've included an interactive game in the Cybersecurity Awareness Month topic group. In this game, users answer wide-ranging questions about cybersecurity topics in an attempt to keep a cybercriminal away from an unlocked workstation and out of your organization's network.

Here's some sample email copy:

**Suggested Subject Line: [Mini-Game]: Can You Keep the Hacker Off Our Network?**

RED ALERT! RED ALERT! [Cue Star Trek red alert sound!]

A hacker has made their way inside our organization and has spotted an unlocked workstation! Can you beat the hacker to the computer before they get a chance to steal personal data and wreak havoc on our network?

It is a race against time! In this mini-game, answer cybersecurity-related questions correctly, and you will move closer to the workstation. Answer incorrectly, and the hacker will move closer.

Be on the lookout for email instructions from our learning console for how to start playing this game!

We're sharing this game to recognize Cybersecurity Awareness Month this month. Stop the hacker, get to that workstation, and save the organization. Game on!

### Third Week Campaign

*Everyone Has A Role to Play In Cybersecurity*

The featured asset this week is another interactive course, this time called *Your Role: Internet Security and You*. This course seeks to help the average employee to understand today's threat landscape and see that the threats out there are more common than they might think. With this course your employees will learn:

- That every employee is a target of potential cybercrime
- The active role they play in keeping your organization safe from cybercrime
- The different types of attacks out there and how they can spot such attacks

Here's some sample email copy to share this course:

**Suggested Subject Line: Remember Your Role When it Comes to Internet Security**

Though the world is edging its way back to normal, there's unfortunately one thing the pandemic never slowed down: Cybercriminals.

Those seeking to make a quick buck off companies like ours with social engineering attacks and malware seemed to double their efforts this year. This makes regular reminders about the role you play in keeping our organization cybersecure all the more important.

That's why we're taking this Cybersecurity Awareness Month to share a training course that will help you make smarter security decisions every day and help prevent a cybercrime attack that could put you and our whole organization at risk. You'll learn:

- That every employee is a target, and cybercrime is more common than you think
- The active role you play in keeping our organization safe from cybercrime
- The different types of attacks out there and how you can spot them

**[For Gold, Platinum, and Diamond customers]**

Be on the lookout for an email notification of your enrollment in this training course and click the link to log in and begin the training.

**[For Silver customers]**

**[Insert this direct link for your users to access this course]**

https://www.knowbe4.com/cybersecurity-awareness-month-course

### *Creating Strong Passwords*

As an additional course option **for Gold level and above subscribers**, we've included a course about password best practices that teaches employees:

- How weak password use can lead to much larger problems
- Important rules for creating new passwords
- The best ways to keep your passwords secure

Here's some sample email copy to share this course:

**Suggested Subject Line: How Secure Are Your Passwords?**

Passwords have become a necessary evil to secure our digital lives.

Cybercriminals know well the tendency of all of us to use easy passwords that we can remember, or reuse passwords across multiple accounts. No wonder, then, that a whopping 81 percent of data breaches used stolen or weak passwords.

That's why we're taking Cybersecurity Awareness Month to highlight the importance of secure password use and highlight a specific training course that teaches about this important issue.

In this 10-minute course, you'll learn:

- How weak password use can lead to much larger problems
- Important rules for creating new passwords
- The best ways to keep your passwords secure

Be on the lookout for an email notification of your enrollment in this training course and click the link to log in and begin the training.

Stay tuned for more cybersecurity awareness content all this month!

## Fourth Week Campaign

### *Poster/Tip Sheet Scavenger Hunt*

For the fourth and final week of Cybersecurity Awareness Month, we suggest wrapping up activities with a poster or tip sheet scavenger hunt using the PDF assets we've provided.

Insert links to the four Cybersecurity Awareness Month posters and/or tip sheets found in the Cybersecurity Awareness month topic group into the sections of your internal policies related to the asset topic.

If you're not already, you can use the Policy Management feature in your KnowBe4 platform to store, distribute, and track the various acknowledgments and agreements required of the employees in your organization. Learn more about this feature in the Knowledge Base article: https://support.knowbe4.com/hc/en-us/articles/360001641907-How-to-Create-and-Manage-Policies-in-Your-KnowBe4-Console

Incentivize trying to collect these assets, similar to the Phishing Bounty activity from Week 1. The non-so-secret goal here is to re-familiarize your employees with your security-related policies and what other resources you might have on your intranet.

Consider taking it one step further and ask your employees to provide one thing they learned about each of the sections of policies where the assets were "hidden." Think of it as a micro-book report, with some treasure hunting mixed in!

Here's some sample email copy for this activity:

**Suggested Subject Line: Let the Virtual Scavenger Hunt Begin!**

As part of Cybersecurity Awareness Month, we're hosting a virtual scavenger hunt! Hidden throughout our InfoSec policy we've linked four poster-style graphics as reminders of key cybersecurity topics, such as phishing or cybercriminals posing as organizational leaders to trick you into revealing sensitive information (known as CEO fraud).

The challenge: Take a stroll through the policy linked here **[insert internal policy link]** and see if you can find all four posters. If you collect all four, reach out to **[insert appropriate email address here]** for a prize!

One catch: You have to include one thing you learned from the policy in your email. We didn't want to make it that easy!

Happy hunting!

### *Staying Safe in The Cloud*

As an additional course option **for Gold level and above subscribers**, we've included a course about cloud tools that teaches employees:

- What "the cloud" actually means
- What risks come along with using this technology
- Tips and strategies for using the cloud securely

Here's some sample email copy for this course:

**Suggested Subject Line: Keep a Silver Lining of Cybersecurity When Using the Cloud**

Use of cloud technology is not all unicorns and rainbows.

Putting files and information "in the cloud" is commonplace these days but should still be approached with caution.

Why? There is no such thing as a completely safe cloud. The way you use the cloud can have a significant impact on our organization and your personal information.

In honor of Cybersecurity Awareness Month this month, we're sharing a brief training course to help you keep cybersecurity top of mind when using cloud devices and tools.

With this course you'll learn:

- What "the cloud" actually means
- What risks come along with using this technology
- Tips and strategies for using the cloud securely

Be on the lookout for an email notification of your enrollment in this training course and click the link to log in and begin the training.

This Cybersecurity Awareness Month, let a cyber secure mindset be your silver lining when using the cloud!

## Keeping Cybersecurity Top-of-Mind

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

Think of this kit as a complement to whatever training and awareness initiative you have running through the KnowBe4 platform.

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, and use the hashtag #CyberAware to stay in the loop throughout the month!

## Additional Resources

**Free Weak Password Test**
Find out how many weak passwords are in your network

**Free Domain Doppelgänger**
Identify potential look-alike domains and see if your organization's domain has an evil twin

**Free Browser Password Inspector**
Find out which users are putting your organization at risk with browser-saved passwords

**Free Compliance Audit Readiness Assessment**
Find out your organization's readiness for a CMMC compliance audit

## 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, and vishing 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