KnowBe4
Human error. Conquered.

2021 Cybersecurity Awareness Month 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 a set of resources you can use throughout the entire month to help your users keep up their cybersecurity defenses, no matter where they are.

What You Get

The kit web page gives you access to these resources:

For You

- On-Demand Webinar: A Master Class on IT Security: Roger Grimes Teaches You Phishing Mitigation
- Comprehensive Anti-Phishing Guide E-Book
- Interactive Security Awareness Weekly Planner, which organizes all the user-facing assets below into weekly planned themes for use throughout October: https://www.knowbe4.com/cybersecurity-awareness-weekly-training-planner-p

For Your Users

- Free Interactive Course: *Social Engineering Red Flags* (available in 10 languages)
- Free Interactive Course: Your Role: *Internet Security and You* (available in 34 languages)
- 2 expert-led videos on pretexting and password management
- 4 infographics on avoiding social engineering and cybercrime
- 4 cybersecurity awareness tip sheets
- 4 posters and digital wallpapers perfect for reminders on key concepts

What to Do

With the employee-facing resources, 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 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 copy to get you started!

Campaign Ideas to Get You Started

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 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-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 weeks in October. Each week we suggest sharing one or more of these content types:

- Infographic
- Video or interactive training course
- Poster
- Cybersecurity Awareness Tip Sheet

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 organization the latest victim of a cyber attack

Check out the course here: https://www.knowbe4.com/cybersecurity-awareness-course

Stay tuned for more cyber security 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.

We just happen to have a free downloadable tool called the **Phish Alert Button** that would make this activity even easier! 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!

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, take a screenshot of it and send it to ***[insert appropriate email address here, such as a member of your InfoSec team].***

[**Use this alternative copy if you've installed our Phish Alert Button:** 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.]

To help spot the phishing attempts, check out this infographic:

- Email Phishing Red Flags [***Upload to your own intranet or share our link:***]

www.knowbe4.com/hubfs/CybersecurityAwarenessMonth2021/Downloads/CyberRedFlags.pdf

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]***.

Second Week Campaign

Pre-Texting 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 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 scammers 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!

Third Week Campaign

Everyone Has A Role to Play In Cybersecurity

The featured asset this week is another interactive course, this time called Y*our Role: Internet Security and You*. This course seeks to help the average employee 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

Check out the course here:
https://www.knowbe4.com/cybersecurity-awareness-month-course

Fourth Week Campaign

Tip Sheet/Poster 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. Upload the four posters and/or tip sheets to your intranet or other internal document repository and link to them from sections of your internal policies related to the asset topic.

Incentivize trying to collect them all during the last week, similar to the Catch-the-Phish Contest above. 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!

For the final week 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 organization 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!

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 compliment 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, 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

01SCSB33R01