KnowBe4
Human error. Conquered.

2022 Cybersecurity Awareness Month Resource Kit User Guide

WELCOME TO YOUR 2022 CYBERSECURITY AWARENESS MONTH KIT!

Thank you for requesting KnowBe4's 2022 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.

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, no matter if they're still working from home or have begun to slowly transition back to the office.

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: *It's More Than Phishing: How to Supercharge Your Security Awareness Training*
- 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-p

For Your Users

Access all courses and content via the links provided until October 31, 2022.

- 4 free interactive training modules
  - *2022 Social Engineering Red Flags (Available in 35 languages)*
  - *Danger Zone mini-game (Available in 34 languages)*
  - Mobile-friendly *Phishing: Don't Get Reeled In (Available in 35 languages)*
  - *Internet Security When You Work From Home (Available in nine languages)*
- 4 training videos
  - *Understanding URLs (Available in 34 languages)*
  - Three video hacking demonstrations featuring Kevin Mitnick *(Available in 36 languages)*
    - Pretexting and credential harvesting (with Phil Hendrie)
    - Tech support scam/pretexting
    - Two-factor authentication attack
- 8 Security Docs and Awareness Tips assets on avoiding social engineering and cybercrime
- 4 Security Hints and Tips newsletters
- 4 posters and digital signage assets perfect for reminders on key concepts

What to Do

When it comes to reinforcing messaging and delivering it at a time when it is most relevant to the employee, we can learn a lot from marketers. When companies launch marketing campaigns, they don't just put out one ad a year and hope they get lucky.

In learning terms, this means connecting with the learner with a variety of content delivered at regular intervals. That's why we've packed this kit with enough assets to deploy multiple resources per week throughout October. From posters used as desktop backgrounds to training videos deployed during lunch and learns, make variety the spice of life this Cybersecurity Awareness Month!

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

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:

- Video or interactive training module
- Infographic
- Poster
- Awareness Tip Sheet

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

- Week 1: Cyber Secure at Work
- Week 2: Watch Out for That Phish
- Week 3: More Than Just Phishing
- Week 4: Cyber Secure at Home

We've also included 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:

- Social Engineering Study Guide: https://www.knowbe4.com/hubfs/CybersecurityAwarenessMonth2022/PDFs/SocialEngineeringStudyGuide_EN-US.pdf
- Uncovering and Reviewing Links: https://www.knowbe4.com/hubfs/CybersecurityAwarenessMonth2022/PDFs/UncoveringReviewingLinks_EN-US.pdf

- Protect Your Personal Information: https://www.knowbe4.com/hubfs/CybersecurityAwarenessMonth2022/PDFs/ProtectPersonalInfo_EN-US.pdf
- Keeping Your Passwords Squeaky Clean: https://www.knowbe4.com/hubfs/CybersecurityAwarenessMonth2022/PDFs/KeepingPasswordsClean_EN-US.pdf

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 suggestions are just that; 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 2022!*
>
> *Though threats to cybersecurity may regularly make the news, we know how to guard against them. But we can't do it without your help!*
>
> *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!*

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

Week 1 Campaign - Cyber Secure at Work

The first suggested campaign theme is all about keeping secure while at work. A no-brainer perhaps, but with offices all over beginning to reopen after two years into the COVID-19 pandemic, we wanted to provide assets so you could focus on the fundamentals the first week.

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

Training Video - Understanding URLs

This roughly 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 Mini-Game - Classic 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

- *Cybercrime Happens Way More Than You Think!* - Infographic that includes noteworthy stats on just how common cyber attacks are
- *Stop! Look! Think!* - Poster-style reminder to stay alert to cyber risks
- *Security Doc: Your Role* - Poster-style reminder of your employees' responsibilities in identifying and reporting potential social engineering attacks

Sharing the Content

Here's some sample email copy to use when sharing our suggested featured asset for this week: the *Classic Danger Zone Mini-Game*. Alternatively, we suggest using the ***Uncovering and Reviewing Links*** 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 look for more cybersecurity content all this month!

P.S.

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

[Insert link to "Cybercrime Happens Way More Than You Think" asset]

Week 2 Campaign - Watch Out For That Phish

The second week's suggested campaign theme focuses on phishing. Still the most common method for bad actors to compromise networks and organizations, phishing cannot be discussed enough when it comes to security awareness training content.

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

Training Video - Credential Harvesting Attack featuring Kevin Mitnick and Phil Hendrie

This roughly four-minute video course features Phil Hendrie (voice actor and radio personality) teaming up with Kevin Mitnick (world-renowned security consultant, public speaker, and author) to portray a social engineering attack using pretexting. Pretexting is a form of social engineering where the attacker lies to obtain restricted information or access. Phil roleplays a vishing attack (phone-based phishing), after which Kevin explains how Phil, as the attacker, used social engineering to trick an unsuspecting user to enter their email login credentials into a fake website.

Your employees will learn:

- How bad actors can trick their victims into giving up sensitive information with little more than a friendly voice and information gleaned from social media
- Red flags to watch out for when requests for login information are involved

Access Link: https://training.knowbe4.com/modstore/view/ea0422f8-31db-4ff3-b7af-605a92220680

Mobile-First Module - Phishing: Don't Get Reeled In

This interactive module, designed for use on a mobile device, will show your employees some ways that cybercriminals use phishing to try to reel them in and break into your organization's computer networks. Your employees will also learn tips for staying safe that can be used both at work and at home and test their knowledge with a built-in quiz.

Your employees will learn:

- Why cyber criminals use phishing in the first place
- How employees can fall for the bait
- Tips for staying secure

Access Link: https://training.knowbe4.com/modstore/view/f6b2ae7d-a1b6-47ae-98e1-0ff0f561d322

3 Downloadable Assets/Digital Signage

- *When In Doubt, Check It Out!* - Infographic that reminds employees of the risks of sharing questionable information online
- *Be An Email Superhero* - Poster-style reminder to think before clicking on a suspicious-looking email
- *Social Engineering Red Flags* - Infographic that calls out important characteristics of a phishing email to look out for

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!

Sharing the Content

Here's some sample email copy to use when sharing our suggested featured asset for this week: the mobile-first module *Phishing: Don't Get Reeled In*. Alternatively, we suggest using the **Social Engineering Study Guide** newsletter this week.

Suggested Subject Line: *Don't Let Phishing Reel You In!*

What's sneaky, pervasive and (cybercriminals hope) read all over?

We're talking about phishing emails!

Jokes aside, phishing remains a top threat to organizations like ours. All it takes is one of us to click on one phishing email for our whole organization to have a bad time.

Don't let the baddies reel you in! For Cybersecurity Awareness Month this year, we're sharing a *mobile-friendly training course that explores ways cybercriminals use phishing to try to reel us in and break into our organization's network.*

Check out this course to learn:

- *Why cybercriminals use phishing in the first place*
- *How employees can fall for the bait*
- *Tips for staying secure, both at work and at home*

Access it here: https://training.knowbe4.com/modstore/view/f6b2ae7d-a1b6-47ae-98e1-0ff0f561d322

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 reminders on what a phishing email looks like:

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

Week 3 Campaign - More Than Just Phishing

The third week's suggested campaign theme focuses on other social engineering methods beyond phishing. Emails are only one tool in the cybercriminal's toolbox, meaning your employees need to be knowledgeable about multiple social engineering tactics and strategies to keep your organization secure.

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

Training Video - Tech Support Scam/Pretexting Featuring Kevin Mitnick

This roughly five-minute video module features Kevin Mitnick (world renowned security consultant, public speaker and author) 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. Rachel demonstrates and explains how an attacker can gain information about your organization's defenses by pretending to be a member of the tech support team and how this can lead to your organization's network being compromised.

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 - 2022 Social Engineering Red Flags

This course explains how to spot the red flags and signs of danger associated with common social engineering methods.

Your employees will learn:

- 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

Access Link: https://training.knowbe4.com/modstore/view/8cf6b700-4965-42f1-b42e-f108207e37aa

3 Downloadable Assets/Digital Signage

- *Sensitive Identifiable Information: If You Handle It, Protect It!* - Infographic that reminds employees of the many varieties of sensitive data
- *You Can't Go Back* - Poster-style reminder of how risky a single click on a suspicious email can be
- *How to Block Mobile Attacks* - Infographic illustrating how to keep sensitive secure while using a mobile device

Sharing the Content

Here's some sample email copy to use when sharing the suggested featured asset for this week, the video training module: *Tech Support Scam/Pretexting Featuring Kevin Mitnick*. Here we suggest hosting a lunch-and-learn session with the video training module played on a shared space 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?

In addition to the lunch-and-learn, we suggest sharing the ***Protect Your Personal Information*** newsletter this week to reinforce the importance of keeping sensitive information out of the hands of hackers.

Suggested Subject Line: *Do You Know Pretexting 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 third 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 learn how to overcome technical defenses over the phone, followed by some discussion afterward.*

Stay tuned for more Cybersecurity Awareness Month activities!

Week 4 Campaign - Cyber Secure at Home

The fourth and final week's suggested campaign theme is keeping cybersecurity top of mind at home; both when working and in the everyday lives of your employees. This includes a focus on two-factor authentication, reporting phishing emails and sound internet security practices when working from home.

Here's a summary of the assets for this week (including two training modules):

Training Video - Two-Factor Authentication Attack

In this approximately five-minute video module, Kevin Mitnick demonstrates how having two-factor authentication set up can still leave you vulnerable to a phishing attack if you don't stop, look, and think before taking action on a phishing link.

Your employees will learn:

- How attackers can get around two-factor authentication via an attached or linked-to document, such as a resume
- Red flags of a suspicious email related to a seemingly legitimate two-factor authentication request

Access Link: https://training.knowbe4.com/modstore/view/c033ab92-b521-11e9-84bf-123d7cbdf51c

Interactive Training Module - Internet Security When You Work From Home

This interactive module helps your employees understand the benefits and challenges of working from home and trains them to stay secure online while doing so.

Your employees will learn:

- Steps to keep their home and devices secure for home work
- Best practices for working from home successfully

Internet Security When You Work From Home
10 tips for keeping safe online when working away from the office

Access Link: https://training.knowbe4.com/modstore/view/2d445877-b4dc-442c-9c0f-997551131b7d

3 Downloadable Assets/Digital Signage

- *Don't Become a Victim!*- Infographic summarizing a variety of social engineering attacks and how to watch out for them
- *Ahh, Secure at Home!* - Poster-style reminder of important actions to keep in mind when working from home
- *Pump Up Your Password Strength* - Poster-style reminder of key things to keep in mind when it comes to password security

Sharing the Content

Here's some sample email copy to use when sharing the suggested featured asset for this week, the interactive training module: *Internet Security When You Work From Home*. Alternatively, we suggest using the ***Keeping Your Passwords Squeaky Clean*** newsletter this week.

Suggested Subject Line: *Keep Cybersecurity Top of Mind While Working from Home*

More than two years into a global pandemic that has changed so much about daily life, and you're likely still reading this email from your home office.

Working remotely has become a way of life for many over the last two years. Once a luxury, working from home has become all but a necessity and has brought with it many information security risks and challenges.

That's why we're taking the last week of Cybersecurity Awareness Month to share a training course offering a refresher on staying secure online while working from home. You'll learn:

Some common technology problems to stay aware of when working from home

Basic necessary steps to secure your home environment for remote work

Essential best practices to implement for success while working remotely

Check out the course here: [https://training.knowbe4.com/modstore/view/2d445877-b4dc-442c-9c0f-997551131b7d]

Thanks for helping us make this a great Cybersecurity Awareness Month!

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