

2024 Cybersecurity Awareness Month Customer Resource Kit User Guide

From our friends at

KnowBe4

A fun interpretation from
our award-winning series,
“The Inside Man.”

Cybersecurity Awareness Month at Khromacom*

Welcome to the official Khromacom Cybersecurity Awareness Month handbook!

Technology is everywhere, helping us out in all aspects of our lives, at work and at home. But as technology evolves, the need for vigilance and awareness also increases. Threats like phishing, social engineering and malware are more common than ever, so we each need to play a part in keeping our networks safe.

I know from personal experience how many major incidents have been narrowly avoided in the past, and I can say from personal experience that even the smallest of actions can have huge and far reaching consequences. Security awareness should be an integral part of every work day, of course, but October is **Cybersecurity Awareness Month**—the perfect time to ensure you and your teams are security conscious and acting safely.

Cyber risks abound, inside and out. That's why we've prepared an entire kit of free resources to help you keep employees and teammates alike informed, in close collaboration with our partners at KnowBe4. With **suggested campaign ideas, world class content** and a **web-based planner**, this kit has what you need to run an engaging security awareness training campaign for an entire month!

Cheers,

Mark Shepherd

IT Security Manager
Khromacom



**The Khromacom name is used as reference to "The Inside Man" series and is completely fictional. We're just having a little fun!*

The Resources

The kit web page gives you access to these resources:

For You

- On-Demand Webinar: *Reality Hijacked: Deepfakes, GenAI, and the Emergent Threat of Synthetic Media*
- Whitepaper: *The Role of AI in Email Security*
- **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:
info.knowbe4.com/resources/free-cybersecurity-resource-kits/cybersecurity-awareness-month-kit-weekly-training-planner-d
- Select support documentation from the KnowBe4 Knowledge Base
- A selection of new simulated phishing email templates and landing pages
 - Phishing Template: *Google Drive: Security Update*
 - Phishing Template: *OpenAI: You have been invited to a ChatGPT Team*
 - Phishing Template: *Mobile Phone Security*
 - Phishing Template: *Microsoft 365: Help us protect you - Security advice for your email account*
 - Landing Page: *Inside Man New Recruits: "Basic Oops!"*
 - Landing Page: *Inside Man: "Basic Oops!"*
 - Landing Page: *Inside Man New Recruits: SEI Rules to Stay Safe Online*
 - Landing Page: *Inside Man: SEI Rules to Stay Safe Online*

For Your Users

Search for all provided courseware and content in your KSAT console.

- 4 video modules
 - *Reality Bytes - Business Email Compromise (BEC) (Available in 13 languages)*
 - *Confessions of a ChatGPT Novice (Available in 12 languages)*
 - *Security Snapshots - "Travel Travails" (Travel Security) (Available in 35 languages)*
 - *Incident Response: First Steps (Available in 35 languages)*
- 4 interactive training modules
 - *The Inside Man: New Recruits Game*
 - *Generative AI: Intelligent and Dangerous? (Available in 12 languages)*
 - *Cyber Essentials Series: Working Remotely (Available in 13 languages)*
 - *Reporting Security Incidents (Available in 35 languages)*
- 4 The Inside Man character cards and posters
- 4 cybersecurity and security awareness tip sheets
- 4 Security Hints and Tips messages
- 4 posters and digital signage assets perfect for reminders on key concepts

Messaging Like a Khromacomster for Cybersecurity Awareness Month

At Khromacom, we make a pretty big deal out of Cybersecurity Awareness Month every October. So big, in fact, that we've built a web-based **Security Awareness Planner** at this link: info.knowbe4.com/resources/free-cybersecurity-resource-kits/cybersecurity-awareness-month-kit-weekly-training-planner-d, so you can access all content included in this Cybersecurity Awareness Month Kit all in one place!

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

- Video or interactive training module
- Infographic
- Poster
- Awareness tip sheet
- Khromacom employee card



Printed posters
are great for
around the
office or used as
trading cards.

Gotta
collect them all!
- AJ

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

- **Week 1:** Understanding Cyber Threats and Their Impact
- **Week 2:** AI and Deepfakes
- **Week 3:** Mobile Device, Travel Security and Remote Workers
- **Week 4:** Incident Response

Security Awareness the Khromacom Way

Sound cybersecurity principles are Khromacom principles. These principles underpin any good security awareness training program and form the core around which we've built this training kit. As a Khromacomster tasked with managing security awareness, 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 Cybersecurity Awareness Month in October.

Collaborate With Colleagues in Other Departments

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

Focus Training on a Few Key Risks

Decide what behaviors you want to shape and then prioritize the top two or three. The themes we've developed per week in Cybersecurity Awareness Month 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!

Security Hints and Tips Messages

We've also included four **Security Hints and Tips Messages** in your KnowBe4 platform 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 topics for these messages are listed below:

- How to Keep Your Organization Safe in and Out of the Office
- The Dangers of AI Art and Deepfakes
- How Secure is Your Mobile Device?
- How to Handle Suspicious Emails

For more details on using the messages 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.



Some fantastic tips
in here, Mark!
- Fiona

Week-by-Week Security Awareness Content

We at Khromacom are nothing if not flexible. Remember all these ideas 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 throughout the month.

No matter how you build out your Cybersecurity Awareness Month efforts, 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 2024!*

As Cybersecurity Awareness Month approaches in October, we're rolling out a month's worth of engaging training content to strengthen our organization's defenses against ever-evolving cyber threats.

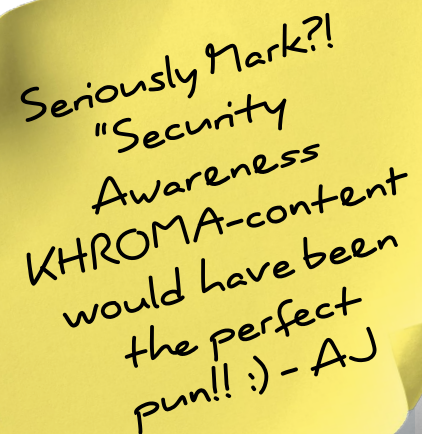
This year, we're focusing on the educational original drama series "The Inside Man," produced by our partners at KnowBe4. Through episodic videos and engaging scenarios, you'll learn how to identify and thwart even the most sophisticated cyber attacks, fortifying our organization's overall security posture.

[Insert more details on 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]**.*

Stay tuned for more updates as we dive into Cybersecurity Awareness Month. Together, we can become a formidable human defense against cyber threats and ensure the continued protection of our organization's assets and data.

Thanks, and have a cyber secure October!



Seriously Mark?!
"Security
Awareness
KHROMA-content
would have been
the perfect
pun!! :) - AJ

Weekly Dose of The Inside Man

As part of a Diamond subscription, you get access to all five seasons of “The Inside Man.” If you’ve not gotten a chance to watch yet, Cybersecurity Awareness Month is the perfect time! If you’ve already hooked on the series, we recommend sharing two-four episodes per week of the series in whichever season you’re currently in.

Get People Talking

While every organization is different, we recommend delivering this content in a fun way. Suggestions include: an after-work event, lunch and learns, team socials, popcorn parties, or any kind of event with snacks. Groups of 15-30 are optimal for discussion but larger groups that are well facilitated can also be conducted with success. Document attendance for your records with a sign-in sheet or virtual signup and attendance records.

Here are some sample discussion questions to get your people thinking about the themes and content of the show:

- Who is your favorite character and why? OR who do you most identify with in the episodes we just watched?
- What do you feel like are the key lessons that can apply to our organization’s cybersecurity environment?
- What is one thing you took away from these episodes that you can use for your personal cybersecurity?
- What are you most looking forward to in the next set of episodes? Or what are you looking forward to in the next season of the series?

Spreading the Word

In the ModStore there are movie-style posters for each season that can be posted in common areas to advertise your showing and used as promotional material. We’ve also provide brand new character posters and cards as part of this kit!

Trailers are also available in the ModStore that can be used to grow excitement for your event by placing them on the organization intranet or playing them during organization-wide meetings.

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 content in the “Featured Content” section. 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 by searching the module/asset name in your ModStore.



Below find the contents of each week in detail.

Week 1 Campaign - Understanding Cyber Threats and Their Impact

The first suggested campaign theme is all about the variety of cyber threats out there and why employee knowledge of them must be as varied as the content in this kit.

Alternatively, we suggest using the **How to Keep Your Organization Safe in and Out of the Office** message this week.

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

Reality Bytes - Business Email Compromise (BEC)

Video Module



This 4-minute video explains the basics of a specific type of social engineering known as business email compromise, or BEC. Your employees will learn:

- Red flags of BEC
- Steps they should take to protect your organization

THE INSIDE MAN NEW RECRUITS

Interactive Mini-Game



“The Inside Man: New Recruits” makes your users part of the series as they help protect the Khromacom corporation from possible hackers. They’ll be recruited by series lead Mark Shepherd and interact with many other characters as they complete challenges related to password security, document handling, physical security, social media sharing, phishing and more.

Your employees will learn:

- What cyber risks can be around the office
- How to secure sensitive data from prying eyes
- What sharing securely on social media looks like
- Common phishing email warning signs

3 Downloadable Assets/Digital Signage

- *The Human Firewall Manifesto* - Poster-style asset that presents a human firewall manifesto establishing the principles of what it means to be a strong, security-aware individual, regardless of job title or responsibilities
- *Don't Let Them Phish Your Inbox* - Poster-style reminder for users to think before they click
- *QR Codes: Enjoy Safe Scanning* - Infographic-style poster that provides best practice security tips so users can scan QR codes safely

Week 2 Campaign - AI and Deepfakes

The second week's suggested campaign theme focuses on the risks associated with AI and deepfakes. Cybercriminals are diving into AI to make the world more dangerous for the rest of us. From deepfakes to AI-generated phishing emails at scale, this emerging technology has become a powerful weapon in the arsenals of bad actors around the world. Alternatively, we suggest using the **The Dangers of AI Art and Deepfakes** message this week.

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

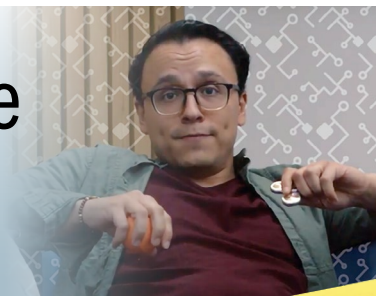
Confessions of a ChatGPT Novice

Video Module

This 3-minute video presents the story of a software developer who accidentally caused a data breach using ChatGPT.

Your employees will learn:

- What harm can come with inappropriate use of AI
- Why generative AI tools should be used with caution



Remember: Consider fitting in a few of the supporting training modules this week to run parallel to the next installments of The Inside Man series. Variety is the spice of life! - AJ

Generative AI: Intelligent and Dangerous?

Interactive Training Module



This 5-minute module, designed for use on a mobile device, gives a high-level overview of how cybercriminals can use artificial intelligence (AI) to power cyber attacks and how users can take steps to prevent becoming a victim.

Your employees will learn:

- Warning signs of AI-generated social engineering attacks
- How to stay secure while using AI programs

3 Downloadable Assets/Digital Signage

- *Security Doc: How to Spot a Deepfake* - Newsletter-style asset that presents the basics of deepfakes and teaches how to spot them
- *AI and Cybercrime* - Poster-style reminder of the benefits and risks of generative AI
- *Using Artificial Intelligence Safely and Securely* - Newsletter-style asset that summarizes the main rules of behavior to ensure protection against new threats presented by the use of AI

Week 3 Campaign - Mobile Device, Travel Security Remote Workers

The third week's suggested campaign theme focuses on mobile device security and staying cyber aware when traveling or working remotely. Alternatively, we suggest sharing the **How Secure is Your Mobile Device?** message this week.

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

Security Snapshots: "Travel Travails"

Video Module

This 2-minute video highlights the importance of planning for security when planning to travel.

Your employees will learn:

- The many distractions that come with traveling, for work or fun
- Steps to take to travel securely with mobile devices and laptops

Cyber Essentials Series: Working Remotely

Video Module

This 7-minute training module explores how to work securely whether users are traveling or working from home.

Your employees will learn:

- Cyber risks inherent to working away from the office
- How to stay safe while working remotely by avoiding scams, spotting phishing securing home WiFi

3 Downloadable Assets/Digital Signage

- *Data Privacy at Work and at Home* - Newsletter-style asset that provides a quick refresher of what data privacy is, why it's so important and how to achieve it
- *Mobile Experts Series* - Poster-style reminder for how to set up mobile devices, what to do in case of loss or theft and how to recognize mobile device scams
- *Taking Home Security Awareness* - Newsletter-style asset with tips on how to maintain cybersecurity while working remotely full time, part time or hybrid

Week 4 Campaign - Incident Response

The fourth and final week's suggested campaign theme is the concept of incident response. For your employees this often means knowing to report something suspicious when they see something, whether a suspected phishing email or unsecure sensitive information. Everyone is a part of the team when it comes to cybersecurity. Alternatively, we suggest using the **How to Handle Suspicious Emails** message this week.

See a full list of this week's content below.

Incident Response: First Steps

Video Module



This 2-minute video explains why incident response is critical to an organization's health.

Your employees will learn:

- The importance of saying something when they see something suspicious
- How to confirm if a suspected incident is legitimate or not

Reporting Security Incidents

Mobile-First Module



This 7-minute training module, designed for use on a mobile device, discusses the importance of every user reporting incidents when they see them. Your employees will learn:

- What a security incident is and how they occur
- How to spot situations or events that might be incidents
- Why it's so important to report immediately and how to do it

3 Downloadable Assets/Digital Signage

- *Following Policy and Reporting Incidents* - Newsletter-style asset that reminds users of their role in reporting cyber incidents per organizational policy
- *First Steps Series* - Poster-style reminder of every user's role in maintaining a strong security culture
- *Security Doc: Cyber Heroes Series - Tailgating - Stranger Danger* - Infographic-style asset highlighting the importance of physical security, the potential threat of tailgating and why access control mechanisms for guests are so important

Remember: Keep Cybersecurity in Mind!

Thanks for reading this handbook, and I hope you've found it useful. Cybersecurity Awareness Month is a great reason to shine a spotlight on cybersecurity, but it's important to make sure that your teams keep doing their part all year round, not just this month. We know bad actors don't take breaks so neither can we! But by staying vigilant, remembering our training and working together, every one of us can help keep our company and our data safe.

Cheers,

Mark Shepherd

IT Security Manager
Khromacom

Khromacom, Mark and AJ may be fictional, but the cyber threats they're up against are all too real.

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 **#SecureOurWorld** 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 empowers your workforce to make smarter security decisions every day. Tens of thousands of organizations worldwide trust the KnowBe4 platform to strengthen their security culture and reduce human risk. KnowBe4 builds a human layer of defense so organizations can fortify user behavior with new-school security awareness and compliance training.

Deploying KnowBe4 results in users that are alert and care about the damage that phishing, ransomware and other social engineering threats pose. The platform includes a comprehensive suite of awareness and compliance training, real-time user coaching, AI-powered simulated social engineering, and crowdsourced anti-phishing defense.

With content in 35+ languages, KnowBe4 provides the world's largest, always-fresh library of engaging content to strengthen your human firewall.

For more information, please visit www.KnowBe4.com