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.

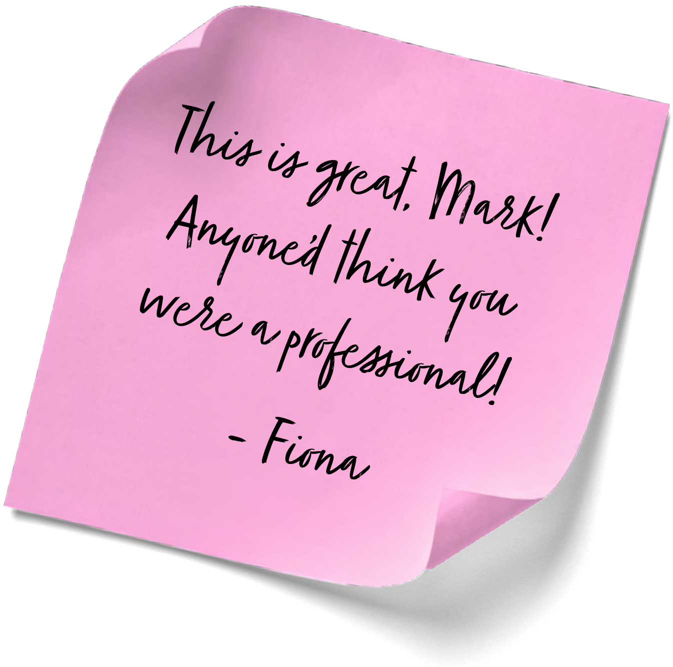
I know from personal experience how many major incidents have been narrowly avoided in the past, and I can say from personal experience that even the smallest of actions can have huge and far reaching consequences. Security awareness should be an integral part of every work day, of course, but October 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



This is great, Mark!
Anyone'd think you
were a professional!
- Fiona

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: https://info.knowbe4.com/resources/free-cybersecurity-resource-kits/cybersecurity-awareness-month-kit-weekly-training-planner-c
- 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

Access all courses and content via the links provided until October 31, 2024.

- 2 video modules
  - *QR Codes: Safe Scanning (Available in 36 languages)*
  - *Understanding URLs (Available in 35 languages)*
- 7 free interactive training modules
  - *The Inside Man: New Recruits* game
  - *Safe Web Surfing Game (Available in 25 languages)*
  - *An Overview of BEC and CEO Fraud (Available in 10 languages)*
  - *AI, Phishing, and Cybersafety (Available in 33 languages)*
  - *Links and Attachments: Think Before You Click (Available in 12 languages)*
  - *Mobile Device Security (Available in 9 languages)*
  - *Make it a Habit... PAB it! (Available in 34 languages)*

- Watch the full first season (12 episodes) of *The Inside Man*, a streaming-quality educational drama series offered by our partners at KnowBe4. Typically available only to Diamond subscription customers.
- 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: https://info.knowbe4.com/resources/free-cybersecurity-resource-kits/cybersecurity-awareness-month-kit-weekly-training-planner-c 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

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

Printed posters are great for around the office or used as trading cards. Gotta collect them all!
- AJ

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 newsletters 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 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.

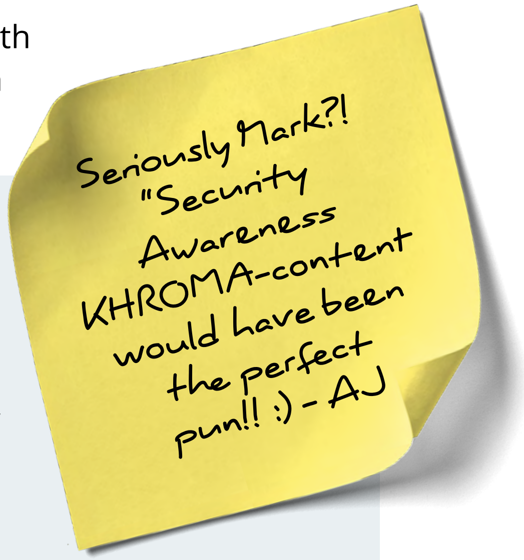
Some fantastic tips in here, Mark!

- 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:



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

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!

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-Optional-Learning-Guide

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 plus suggested content to feature.

Week 1 Campaign - Understanding Cyber Threats and Their Impact

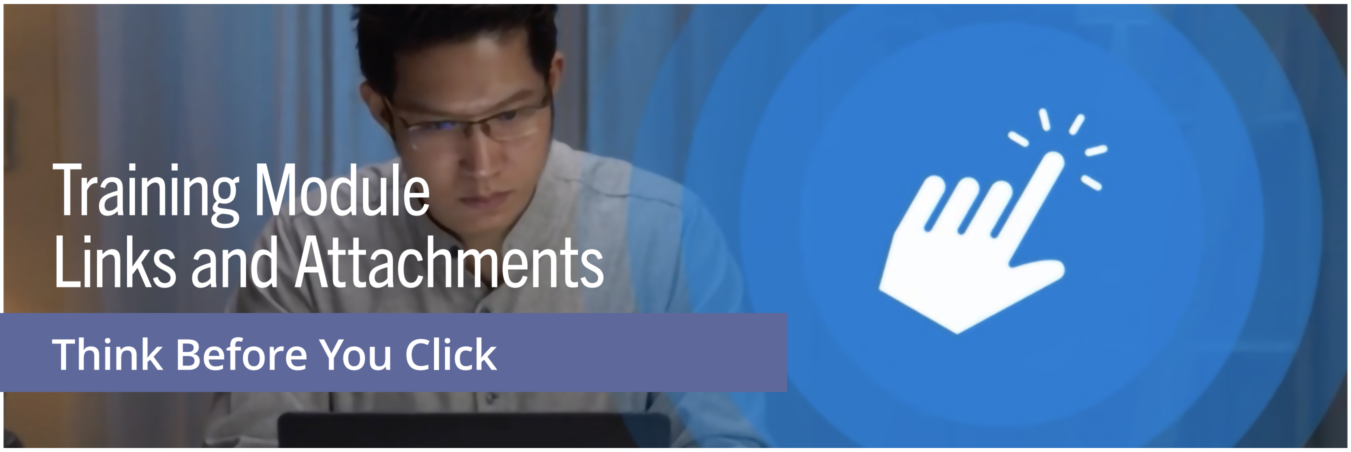
The first suggested campaign theme is all about the variety of cyber threats out there and why employee knowledge of them must be as varied as the content in this kit.

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

Season 1; Episodes 1-3

Something about these feels familiar...I know! We watched these during a lunch-and-learn. So much fun! - Fiona

In the premiere of this educational cyber-thriller, hacker-for-hire Mark, code name "Romulus," infiltrates a major tech company by scoring a job on their IT security team. Mark's shadowy handler tasks him with tightening security while uncovering details about a huge merger deal. Even before his first day, he's already gathered intelligence on his new colleagues through their overshared social media. Just when you think you know which side he's on, Mark gets caught attempting corporate espionage—but will that stop him from downloading massive troves of confidential data?



Training Module
Links and Attachments

Think Before You Click

This 10-minute module explains how cybercriminals use links and attachments to target you, what can happen if you click on them, and how you should handle any links or attachments you receive.

Your employees will learn:

- Warning signs of malicious links
- What to do with suspected suspicious emails

Safe Web Surfing

Interactive Mini-Game

In this game, your users will learn how to differentiate between malicious links and legitimate ones. Then, you will use what you've learned to help your surfer make it safely to shore while dodging common website clones.

Your employees will learn:

- How to tell a good site from bad
- Tricks bad actors use to fool users

3 Downloadable Assets/Digital Signage

Multi-Stage Vishing - Infographic that explains how multi-stage vishing attacks work, the red flags to look out for and what you can do if you receive a suspicious email

Be An Email Superhero - Poster-style reminder about the importance of email security

You Are A Target - Infographic that reminds users of the three types of social engineering: digital, in-person and phone attacks

Sharing the Content

Here's some sample email copy to use when sharing our suggested featured content for week 1: the first three episodes of *The Inside Man*. Alternatively, we suggest using the **How to Keep Your Organization Safe in and Out of the Office** newsletter this week.

Suggested Subject Line: *Our Story Begins: Jump Into The Inside Man!*

We're kicking off the first week of Cybersecurity Awareness Month with something you might not expect: Let's watch TV at work!

In the premiere of this educational cyber-thriller, hacker-for-hire Mark, code name "Romulus," infiltrates a major tech company by scoring a job on their IT security team.

Mark's shadowy handler tasks him with tightening security while uncovering details about a huge merger deal. Just when you think you know which side he's on, Mark gets caught attempting corporate espionage — but will that stop him from downloading massive troves of confidential data?

Be on the lookout for email instructions from our learning console on how to watch these episodes.

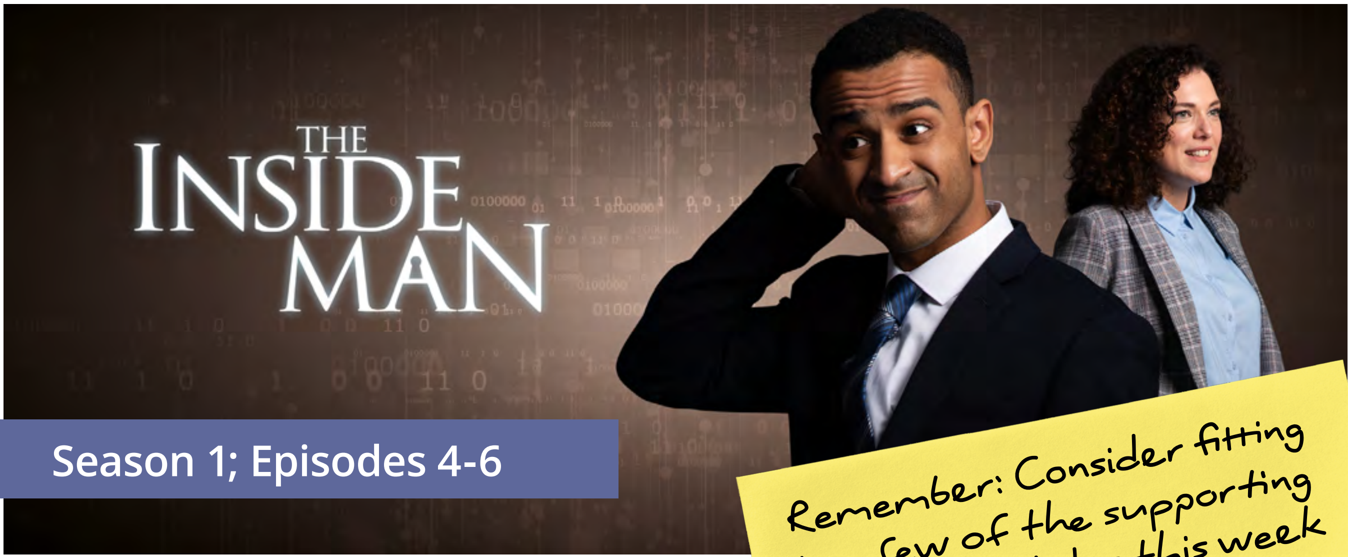
Stay tuned next week for the next episodes in our evolving cyber-adventure!

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

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.

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



Season 1; Episodes 4-6

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

Just when Mark thinks he's hit a brick wall hacking Khromacom's network security, a surprise party thrown by his new colleagues completely throws him off his game. Desperate for a breakthrough, he enlists an old pal to dumpster dive for confidential intel. After stealing a top employee's notebook during a late-night cleaning crew disguise, Mark faces an awkward encounter trying to sneak it back unnoticed. As Mark's handler piles on the pressure about the high-stakes sting operation, Mark starts questioning the endgame. He's ready to make his big move and upload the data, only to get halted by a very human moment when his boss offers him a full-time job. How will Mark respond with his two worlds colliding?

AI, Phishing, and Cybersafety

Mobile-First 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 say secure while using AI programs

An Overview of BEC and CEO Fraud

Mobile-First Module

This 5-minute module, designed for use on a mobile device, provides an overview of how these attacks work and includes tips to ensure your organization and users are prepared to handle a BEC or CEO fraud attack.

Your employees will learn:

- How BEC and CEO fraud attacks work
- The steps your organization has in place to combat these attack

3 Downloadable Assets/Digital Signage

- **Cybersmart Safety Tips** - Infographic that provides a quick overview of some common cybersecurity threats including phishing and artificial intelligence (AI) chatbots
- **Poster: Deepfakes** - Poster-style reminder that draws attention to the cyber threat of deepfakes
- **What Are AI Chatbots** - Infographic-style asset that provides an understanding of what AI chatbots are, tips for how to interact with them and how people can safeguard their data as well as their organization's data

Sharing the Content

Here's some sample email copy to use when sharing our suggested featured asset for this week: the next three episodes of *The Inside Man*. Alternatively, we suggest using the **The Dangers of AI Art and Deepfakes** newsletter this week.

> ***Suggested Subject Line:*** *Inside Man Part 2: Dumpster Diving and Deception*
>
> *When we last left our hero (villain?) Mark, he's hit a brick wall hacking Khromacom's network security.*
>
> *Desperate for a breakthrough, he enlists an old pal to dumpster dive for confidential intel. As Mark's handler piles on the pressure about the high-stakes sting operation, Mark starts questioning the endgame. He's ready to make his big move, only to get halted by a very human moment with his boss. How will Mark respond with his two worlds colliding?*
>
> *Be on the lookout for email instructions from our learning console on how to watch these episodes.*
>
> *Stay tuned next week for the next episodes in our evolving cyber-adventure!*
>
> *If you have any questions, feel free to reach out to* ***[insert contact person]****.*

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.

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

Season 1; Episodes 7-10

With his new permanent position at Khromacom, Mark faces a crisis of conscience as coworkers like Fiona awkwardly try to welcome him into the work “family.” Just as he’s warming up, a coworker named Erica falls victim to a ransomware attack that puts Mark’s loyalties to the test. Sensing Erica will be targeted at a finance conference, Mark gets assigned as her security detail, only for his handler to shockingly resurface posing as a charming businessman keen on manipulating Erica into divulging sensitive information. Mark attempts a counter sting against his handler with coworker and emerging best friend AJ. With the lines between good and evil blurring, who will Mark ultimately be loyal to?

QR Codes: Safe Scanning

Video Module

This 4-minute video module discusses the threats associated with scanning QR codes, along with security tips to help you users scan them safely.

Your employees will learn:

- How cybercriminals can take over public QR codes for their own uses
- Things to consider before engaging with any QR code

Mobile Device Security

Interactive Training Module

This 12-minute module will take users on a comprehensive learning journey about mobile device security.

Your employees will learn:

- How social engineering can play out on mobile devices
- Signs of a compromised mobile device
- Steps to secure a mobile device

3 Downloadable Assets/Digital Signage

- **How to Block Mobile Attacks** - Infographic that provides a quick way to help your users remember how to keep their mobile devices secure
- **Ahhh, Secure at Home!** - Poster-style asset with simple reminders on how your users can work from home securely
- **QR Codes: Enjoy Safe Scanning** - Infographic-style poster that provides best practice security tips so users can scan QR codes safely

Sharing the Content

Here's some sample email copy to use when sharing the suggested featured asset for this week, the next four episodes of *The Inside Man*. Alternatively, we suggest sharing the **How Secure is Your Mobile Device?** newsletter this week.

Suggested Subject Line: *The Inside Man Part 3: Double, Double, Toil and Travel*

Another week, another set of twists and turns for our Khromacom team!

Just as Mark's warming up to his new Khromacom "family," a coworker named Erica falls victim to a ransomware attack that puts Mark's loyalties to the test.

Sensing coworker Erica will be targeted at a finance conference, Mark gets assigned as her security detail, only for his handler to shockingly resurface posing as a charming businessman keen on manipulating Erica into divulging sensitive information.

With the lines between good and evil blurring, who will Mark ultimately be loyal to?

Be on the lookout for email instructions from our learning console on how to watch these episodes.

Stay tuned next week for the next episodes in our evolving cyber-adventure!

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

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.

We want you to be able to go out with a bang for the last week of Cybersecurity Awareness Month! So not only are we providing the thrilling conclusion to the first season of The Inside Man, we're offering a free mini-game that invites your employees to be part of the Khromacom cybersecurity team! See a full list of this week's content below.

Interactive Mini-Game

"The Inside Man: New Recruits Game" 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 medial looks like
- Common phishing email warning signs

Season 1; Episodes 11-12

Even after averting disaster by recruiting AJ, Mark and his new partner make a chilling discovery that could extract all the confidential merger intel straight into the enemy's hands! In a shocking climax, the handler's identity and connection to Mark's past is revealed, testing whether the former hacker's redemption is sincere. With AJ emerging as Khromacom's newest security hero, it seems the saga is reaching its climax...or is it?

Understanding URLs

Video Module

This 2-minute video describes what a user can look for to help them determine if a URL has been edited, providing best practices and tips they can follow to help keep their organization and themselves safe.

Your employees will learn:

- How hackers can manipulate URLs
- What warning signs to look for

Make It a Habit…PAB It!

Interactive Training Module

This 3-minute module is designed for organizations that have implemented KnowBe4's Phish Alert Button (PAB). It will explain how the PAB protects the organization from phishing attacks and why it is so important to make reporting suspicious emails a security habit.

Your employees will learn:

- The basics of phishing tactics
- How the PAB works
- Why reporting phishing is important

3 Downloadable Assets/Digital Signage

- **Security Doc: Cybercrime Happens Way More Than You Think!** - Infographic-style asset that shares facts and figures on the global prevalence of cyber crime.
- **Stop! Look! Think!** - Poster-style asset that reminds employees to think twice when presented with suspicious emails or other risky circumstances
- **Be On The Lookout! Phishing Red Flags** - Infographic-style poster that provides a quick refresher on how to spot the signs of a phishing attack

Sharing the Content

Here's some sample email copy to share the mini-game and last two episodes of season one of *The Inside Man*. Alternatively, we suggest using the **How to Handle Suspicious Emails** newsletter this week.

Suggested Subject Line: *Inside Man Part 4… and a Mini-Game!*

You read that correctly! The fourth and final part of the epic Inside Man saga this month comes with the opportunity to play the role of a Khromacom cybersecurity team member!

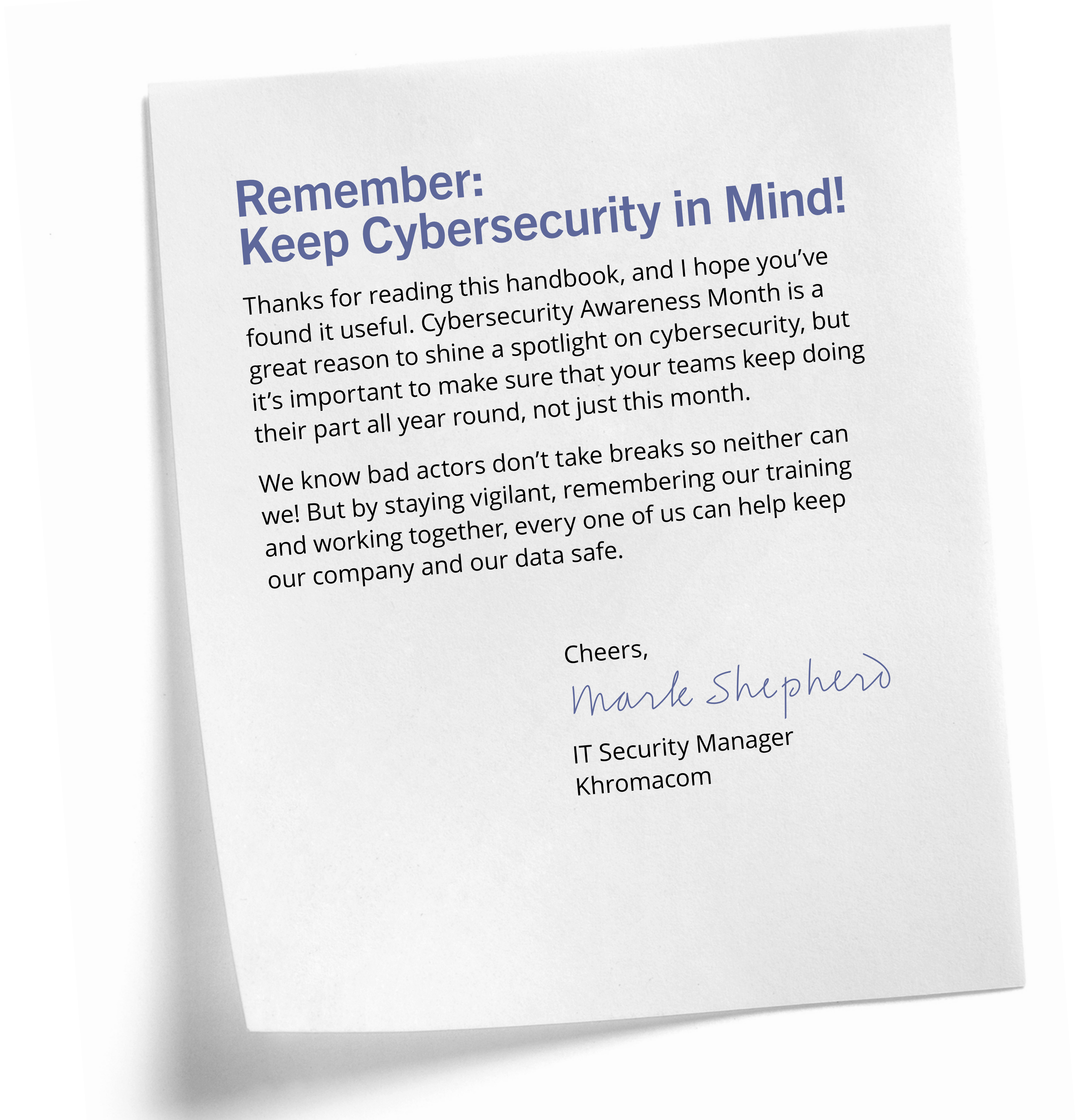
After you binge the last two episodes, check out the "The Inside Man: New Recruits" mini-game! Become part of the series as you help protect the Khromacom corporation from possible hackers and complete challenges related to password security, document handling, physical security, social media sharing, phishing and more.

You'll learn:

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

Be on the lookout for email instructions from our learning console on how to watch the thrill finale and access the mini-game!

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



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

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com