knowbe4

CYBERSECURITY

AWARENESS MONTH 2025

CUSTOMER RESOURCE KIT STRATEGY GUIDE

Table of Contents

03 Welcome

04 Your Gear

05 The Tutorial Level: Making the Most of the Content

06 Arcade Villain Cards

07 Arcade Villain Tips and Tricks

08 Know Before You Go: Campaign Techniques

09 Pressing Start in Your KnowBe4 Console

10 Level-by-Level Breakdown

11 Level 1 – General Cybersecurity

12 Summary of Assets For Week 1

14 Level 2 – AI Threats

15 Summary of Assets For Week 2

17 Level 3 – Ransomware

18 Summary of Assets For Week 3

20 Level 4 – Incident Reporting

21 Summary of Assets For Week 4

23 Bonus Level – Keeping Cybersecurity-Top-of-Mind

Welcome to the Official Strategy Guide for Cybersecurity Awareness Month 2025!

In the never-ending battle against cyber villains, your users are on the front lines. Only the most-experienced and well-equipped can stand up against the threats lurking behind every corner of cyberspace.

It's dangerous out there, so you shouldn't go alone. Take this strategy guide and treasure chest of resources to help walk you and your users through Cybersecurity Awareness Month 2025 and beyond.

Read this guide for a level-by-level walkthrough of the free security awareness content themed for each of the four weeks of Cybersecurity Awareness Month. Help your users conquer any cyber villain they come across with curated content, suggested email text for sharing those assets, user engagement ideas and more!

Pack your gear, plan your strategy and let the games begin!

Your Gear

There are no inventory limits here. Here's what you get:

For You

- **On-Demand Webinar:** FAIK Everything: The Deepfake Playbook, Unleashed
- **Whitepaper:** 7 Best Practices For Implementing Human Risk Management
- **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://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: Password Alert (Link) (Spoofs Domain)
  - Phishing Template: ChatGPT: Your Custom ChatGPT AI Portal is Now Live (Link)
  - Phishing Template: Ransomware Scan (Link) (Spoofs Domain)
  - Phishing Template: Microsoft 365: Your incident has been opened (Link)
  - Landing Page: Could This Be Game Over? (Browser-language Detecting)
  - Landing Page: Welcome to the Awareness Arcade (Browser-language Detecting)

For Your Users

Access all courses and content in your KSAT console:

- **4 free interactive training modules**
  - Double Trouble Trivia: Social Engineering Game (Available in 36 languages)
  - New Tools: Artificial Intelligence Scams (Available in 35 languages)
  - Ransonware: Blackmail Using Encrypted Data (Available in 35 languages)
  - Join the Security Team (Available in 35 languages)
- **4 video modules**
  - Defining Human Firewalls (Available in 35 languages)
  - Generative AI: Seeing Through the Deception (Available in 35 languages)
  - Security Snapshots - "Hungry" (Ransomware) (Available in 35 languages)
  - Incident Response: First Steps (Available in 35 languages)
- **4 Arcade Villain character cards and posters**
- **4 cybersecurity and security awareness tip sheets**
- **4 posters and digital signage assets perfect for reminders on key concepts**

The Tutorial Level: Making the Most of the Content

Let's start with the basics. We'll dive into detailed content walkthroughs later. To start, each piece of content is aligned to a general theme to focus on for each of the four weeks in October. Each week, consider sharing one or more of these content types:

- **Video or interactive training module**
- **Infographic**
- **Poster**
- **Arcade Villain character card**

We'll walk you through each week/level's theme in more detail later in the guide, but here's the summary:

- **Level 1:** General Cybersecurity
- **Level 2:** AI Threats
- **Level 3:** Ransomware
- **Level 4:** Incident Reporting

For help visualizing how it all fits together, check out our **Security Awareness Planner**, available at this link: https://info.knowbe4.com/resources/free-cybersecurity-resource-kits/cybersecurity-awareness-month-kit-weekly-training-planner-d. There you can access all content included in our Cybersecurity Awareness Month Kit all in one place!

Arcade Villain Cards

Let's take a closer look at each of the villains. Remember to download each card and/or poster from the same web page where you got this guide:

Download All Villain Cards

The Cyberpunks

At the core of many of the most pernicious threats across the cyber landscape sit The Cyberpunks. Calculating and cunning, The Cyberpunks know just the right tactics to convince users to download malware, click suspicious links or share confidential information.

Dr. Deepfake

From her "office" hidden away in the darkest alley of the deep web, Dr. Deepfake crafts some of the trickiest fakes and frauds known to cyber-dom. Her clients: Cybercriminals looking for everything from faked faces to voice simulators targeting the c-suite. Beware her techno-treachery!

Enkryptor

With Ran-staff in hand, Enkryptor threatens networks of all sorts with his dastardly brand of malware. His mission: lock up treasured information and data for his own uses; or just because he doesn't want you to have it!

The Doppelgänger

The Doppelgänger takes on the form of users just like yours in an attempt to keep the actions of their cybercriminal comrades hidden. With a smile and a wave of their hand, Doppelgänger will tell you phishing emails and malware infections are "no big deal." Don't fall for it!

TIP

Arcade Villain Tips and Tricks

The training content for each week is full of information on how your users can defeat each threat whenever they might encounter them in the wild. To take your user engagement to the next level, here are some ideas to make the most out of the Arcade Villain cards and posters:

Cyber Sleuths:
Organize a scavenger hunt around your office (or internal shared drive or intranet) to find the hidden Arcade Villain cards.
The employee who finds them all first wins!

AI vs. AI:
Sure Dr. Deepfake uses the power of AI for her own nefarious purposes, but it's also a valuable tool in your toolbox. Encourage your users to use a generative AI tool to come up with their own Arcade Villain personifying a specific cyber threat and share/ discuss during a lunch and learn.

Guess That Villain:
Use Google Forms or other online survey tools to build an educational quiz based on the Arcade Villain traits. Offer incentives, like small prizes or recognition, for those who score well to encourage participation.

Know Before You Go: Campaign Techniques

Planning a month-long campaign can be daunting, but you don't have to try to reinvent the wheel. The creative minds behind this content have seen these core campaign techniques work for organizations of all sizes:

Think Like a Marketer, Deploy Like a Cyber Hero

Your goal should be changing employee behavior rather than just telling your people what you'd like them to know. Think about any major advertising campaign you've seen. You'll see ads for new cars, tech and so much more across streaming platforms, social media and on TV. This varied approach helps cement the core message and influence behavior. That's why we've equipped you with enough assets to deploy multiple resources per week throughout October. This helps you give your users the critical information they need while conditioning their security reflexes so they become an effective last line of defense.

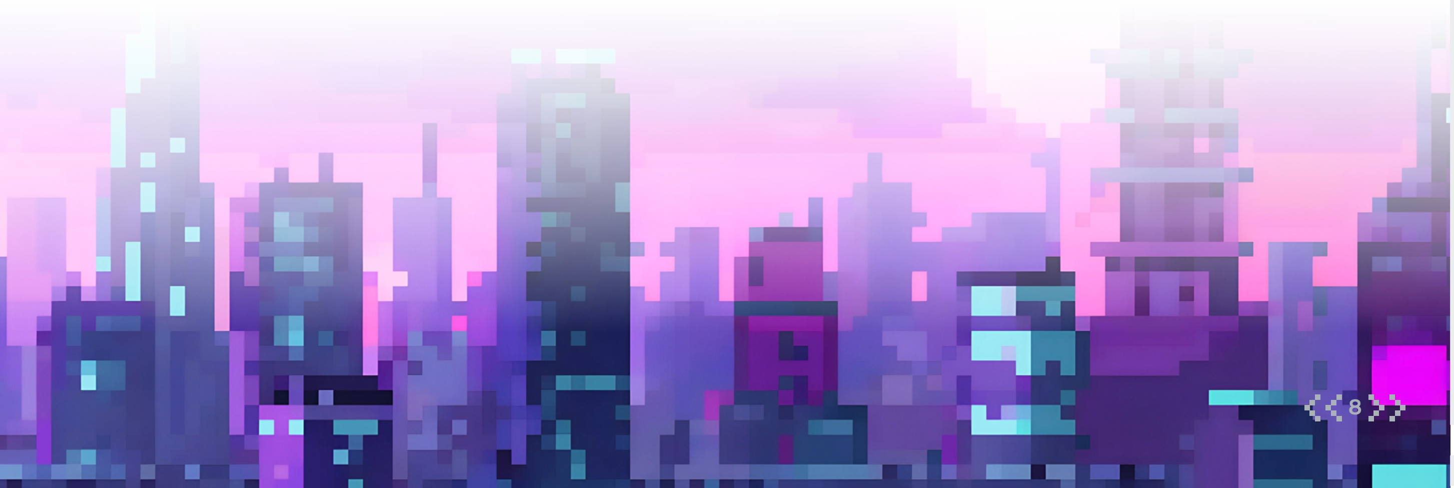
Gather Party Members from Across Your Organization

Going multiplayer can be a key to success when it comes to cybersecurity education. Use October 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.

Aim for Well-Rounded User Stats

Don't overwhelm your users with too much content at one time. At a certain point this runs the risk of them simply clicking through without learning anything. Decide what behaviors you want to shape and then prioritize the top two or three. The themes we've developed per week in October 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.



Pressing Start 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-Training-Campaigns-Guide#iv_01H84ZMYTY0NFK6REANVA7KDS2

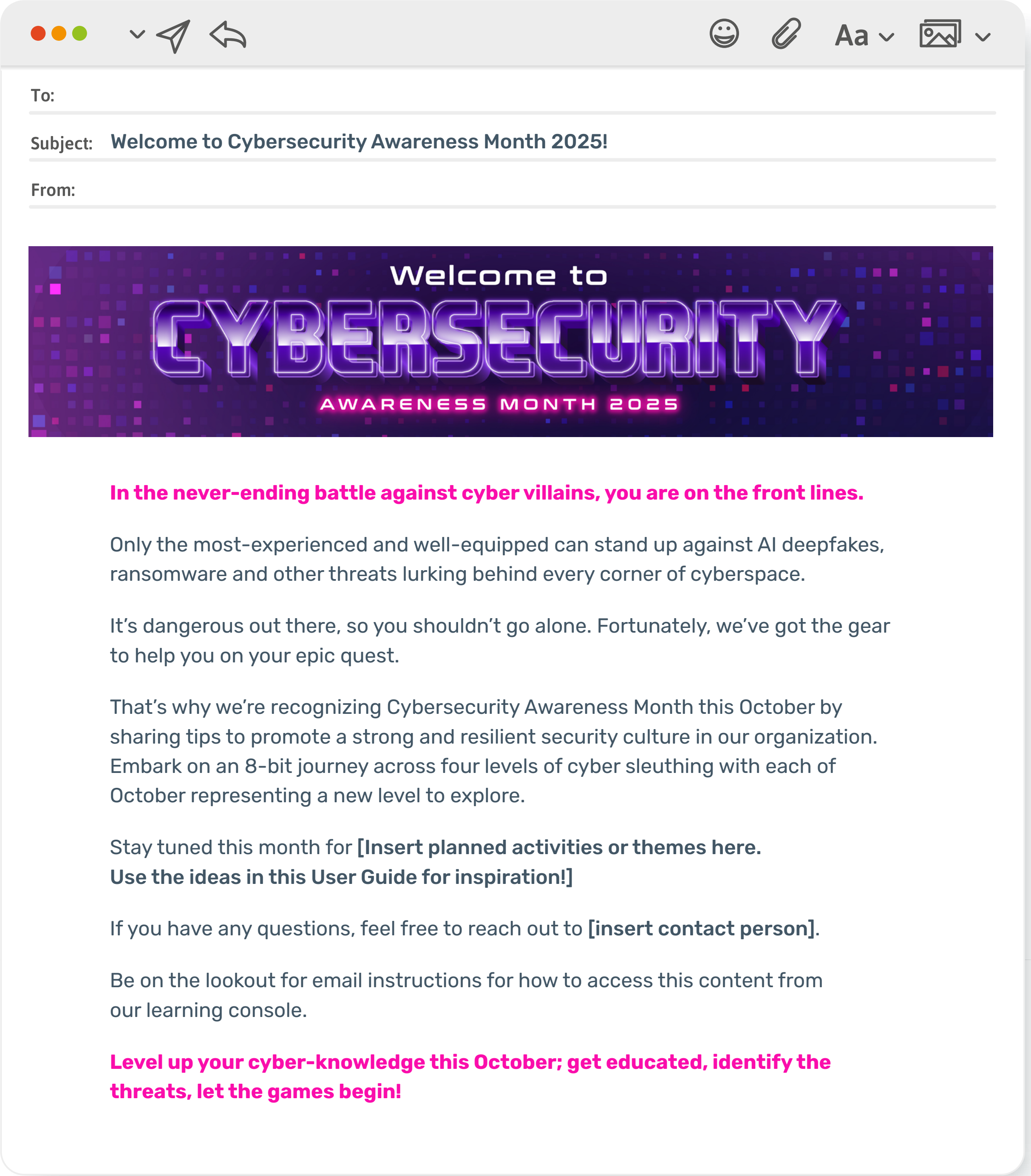
With the **Optional Learning** feature, you can allow your users to self-select which courses to take. Find out more about this process in this Knowledge Base article: https://support.knowbe4.com/hc/en-us/articles/1500002656002

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.

Level-by-Level Breakdown

Now it's time for the details. Below you'll find content broken out by week with suggested content to feature plus associated email text.

By now you'll hopefully have some ideas or strategies in mind for how you want to tackle the 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:



To:

Subject: Welcome to Cybersecurity Awareness Month 2025!

From:

In the never-ending battle against cyber villains, you are on the front lines.

Only the most-experienced and well-equipped can stand up against AI deepfakes, ransomware and other threats lurking behind every corner of cyberspace.

It's dangerous out there, so you shouldn't go alone. Fortunately, we've got the gear to help you on your epic quest.

That's why we're recognizing Cybersecurity Awareness Month this October by sharing tips to promote a strong and resilient security culture in our organization. Embark on an 8-bit journey across four levels of cyber sleuthing with each of October representing a new level to explore.

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]**.

Be on the lookout for email instructions for how to access this content from our learning console.

Level up your cyber-knowledge this October; get educated, identify the threats, let the games begin!

WEEK 1

LEVEL 1

GENERAL CYBERSECURITY

The most basic and prevalent cyberthreats are no excuse for your users to keep their guard down. The goal of the first week is an introductory level to a variety of common cyberthreats that continue to take a toll on organizations of all sizes.

At the core of many of the most pernicious threats across the cyber landscape sit The Cyberpunks. Calculating and cunning, The Cyberpunks know just the right tactics to convince users to download malware, click suspicious links or share confidential information.

ATTACKS:

Convince 25 HP

Impersonate 35 HP

Summary of Assets For Week 1

Interactive Training Module: Double Trouble Trivia: Social Engineering Game

In this interactive trivia game, users learn all about social engineering and phishing in a Jeopardy-style quiz format. Users compete against a computer-controlled component; the most points wins!

Your employees will learn:

- **The damage caused by social engineering**
- **Common attack methods**
- **Tactics scammers use to gain access to systems and devices**

Video Module – Defining Human Firewall

This two-minute video discussed the idea of the “human firewall" and reminds users that security technologies, like firewalls and email filters, can’t catch every malicious attack.

Your employees will learn:

- **Why cybercriminals target employees specifically**
- **The vital role they play in keeping your organization secure**

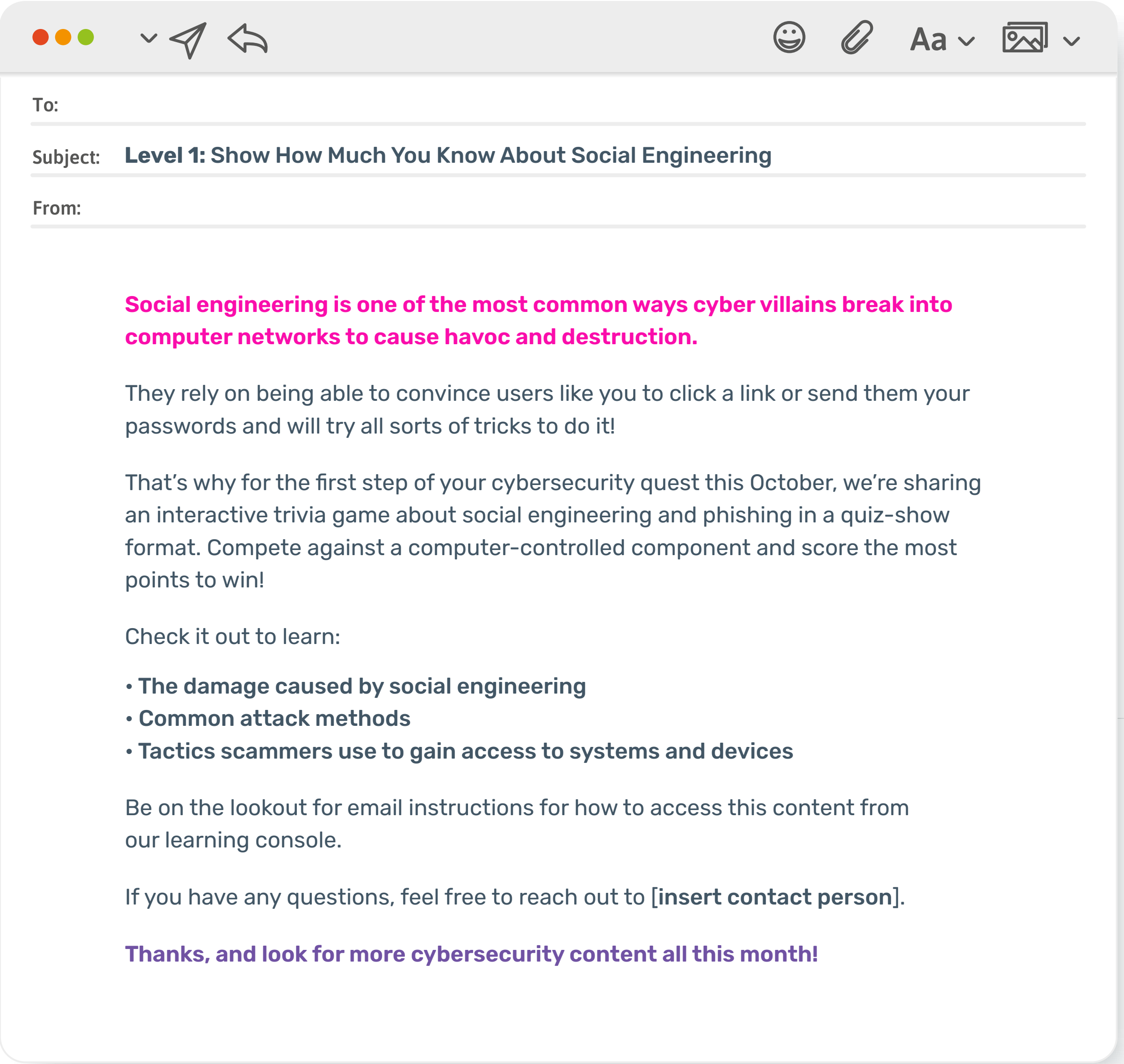
3 Downloadable Assets/Digital Signage

- **Power Up Your Password Security -** Arcade-themed infographic that explains password best practices **(with complementary poster)**
- **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

Summary of Assets For Week 1 (continued)

Sharing the Content

Here’s some sample email copy to use when sharing our suggested featured asset for this week: the **Double Trouble Trivia social engineering game.**



To:

Subject: **Level 1:** Show How Much You Know About Social Engineering

From:

Social engineering is one of the most common ways cyber villains break into computer networks to cause havoc and destruction.

They rely on being able to convince users like you to click a link or send them your passwords and will try all sorts of tricks to do it!

That’s why for the first step of your cybersecurity quest this October, we’re sharing an interactive trivia game about social engineering and phishing in a quiz-show format. Compete against a computer-controlled component and score the most points to win!

Check it out to learn:

- **The damage caused by social engineering**
- **Common attack methods**
- **Tactics scammers use to gain access to systems and devices**

Be on the lookout for email instructions for how to access this content from our learning console.

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

Thanks, and look for more cybersecurity content all this month!

WEEK 2

LEVEL 2

AI THREATS

Few threats have rocketed to the top of the infosec world's worry list like AI-powered phishing emails, scams and deepfakes. The goal of the second level and the associated focus content is to ensure your users are well-versed in these threats both as they go about their work life and explore the internet in their down time.

DR DEEPFAKE

From her "office" hidden away in the darkest alley of the deep web, Dr. Deepfake crafts some of the trickiest fakes and frauds known to cyber-dom. Her clients: Cybercriminals looking for everything from faked faces to voice simulators targeting the c-suite. Beware her techno-treachery!

ATTACKS:

Deep Hurting 15 HP

Large Language Monstrosity 70 HP

Summary of Assets For Week 2

Interactive Training Module - New Tools: Artificial Intelligence Scams

This 10-minute module uses video and realistic scenarios to teach learners at all career levels about the dangers. Users will also take a short quiz to reinforce what they've learned.

Your employees will learn:

- **What new scam possibilities the rise of AI technology brings**
- **How to look out for AI-based scams and what to do about them**

Video Module – Generative AI: Seeing Through the Deception

This four-minute video module informs users how cybercriminals use generative AI in their attacks and the warning signs that can help them identify deepfake images, videos and voice calls.

Your employees will learn:

- **How cybercriminals are using AI technology for their own ends**
- **Common AI-based scams and tactics to look out for**

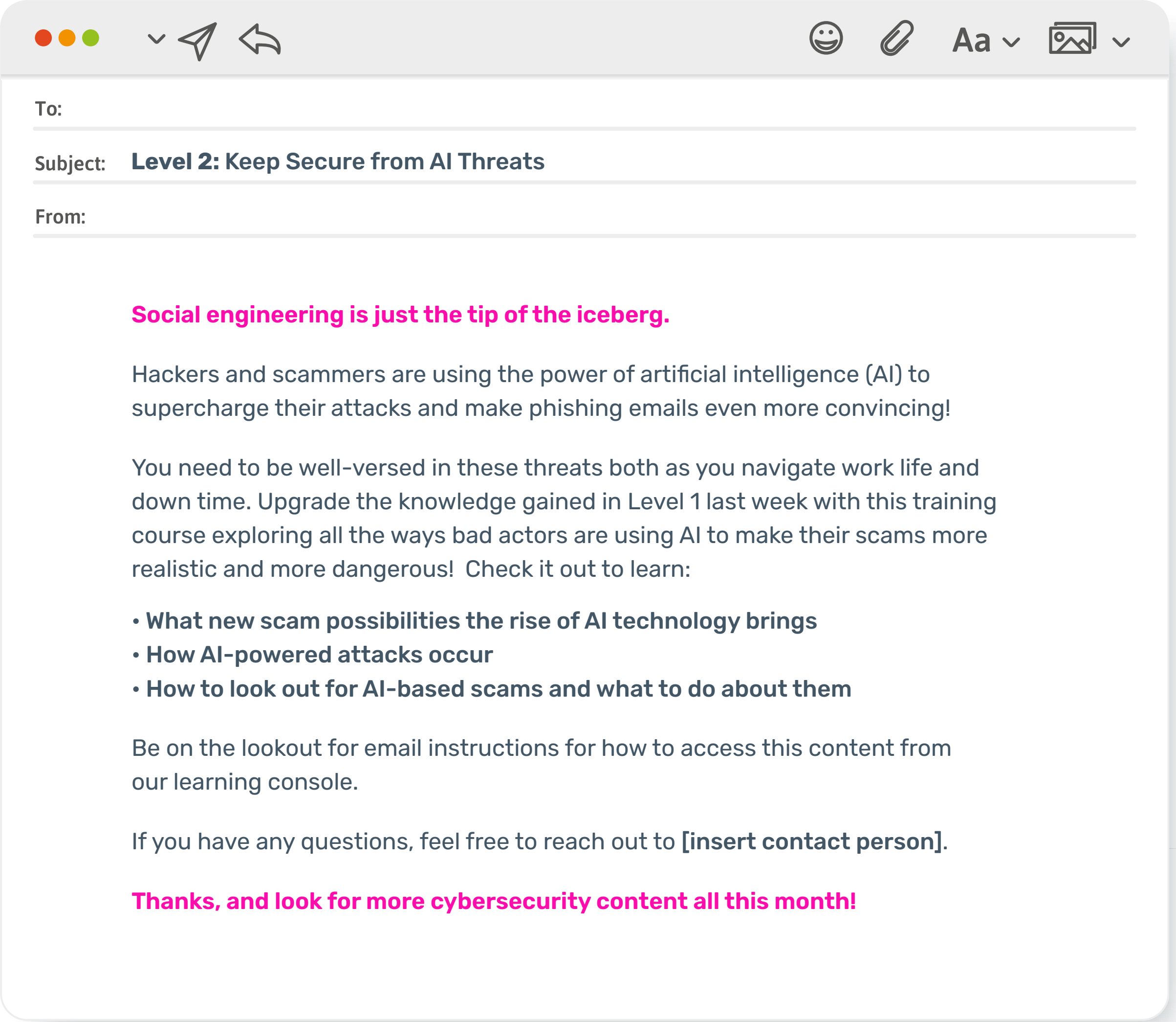
3 Downloadable Assets/Digital Signage

- **Using Artificial Intelligence Safely and Securely -** Infographic that provides a summary of safe use cases for generative AI and how cybercriminals can exploit these tools
- **AI and Cybercrime -** Poster-style reminder that the benefits of AI technology come with cybersecurity threats
- **Artificial Intelligence, Security, and You -** Infographic-style summary of how AI can be used for nefarious purposes

Summary of Assets For Week 2 (continued)

Sharing the Content

Here's some sample email copy to use when sharing our suggested featured asset for this week: the **New Tools: Artificial Intelligence Scams** module.



To:

Subject: **Level 2:** Keep Secure from AI Threats

From:

Social engineering is just the tip of the iceberg.

Hackers and scammers are using the power of artificial intelligence (AI) to supercharge their attacks and make phishing emails even more convincing!

You need to be well-versed in these threats both as you navigate work life and down time. Upgrade the knowledge gained in Level 1 last week with this training course exploring all the ways bad actors are using AI to make their scams more realistic and more dangerous! Check it out to learn:

- **What new scam possibilities the rise of AI technology brings**
- **How AI-powered attacks occur**
- **How to look out for AI-based scams and what to do about them**

Be on the lookout for email instructions for how to access this content from our learning console.

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

Thanks, and look for more cybersecurity content all this month!

WEEK 3

LEVEL 3

RANSOMWARE

A threat cybercriminals keep shelling out the coin for, ransomware threatens all corners of the cyberworld. Help your users navigate the third level of Cybersecurity Awareness Month with the equipment and know-how they'll need to be ransomware-ready.

With Ran-staff in hand, Enkryptor threatens networks of all sorts with his dastardly brand of malware.

His mission: lock up treasured information and data for his own uses; or just because he doesn't want you to have it!

ATTACKS:

KryptoLock 15 HP

MakeYouWannaCry 80 HP

Summary of Assets For Week 3

Interactive Training Module - Ransomware: Blackmail Using Encrypted Data

In this seven-minute module, employees will learn what to do in case of an malware-related emergency and what options are available to protect themselves against a ransomware attack and its consequences. Users will also take a short quiz at the end.

Your employees will learn:

- **The most common methods of ransomware attack**
- **What to do in case of a ransomware emergency**
- **How to prevent a ransomware infection**

Video Module – Security Snapshots - "Hungry" (Ransomware)

This two-minute module shows how even a momentary lack of attention can lead to clicking on the wrong link and letting ransomware in.

Your employees will learn:

- **Why it's important to stop, look and think before clicking on emails**
- **What to do in the face of a suspected ransomware infection**

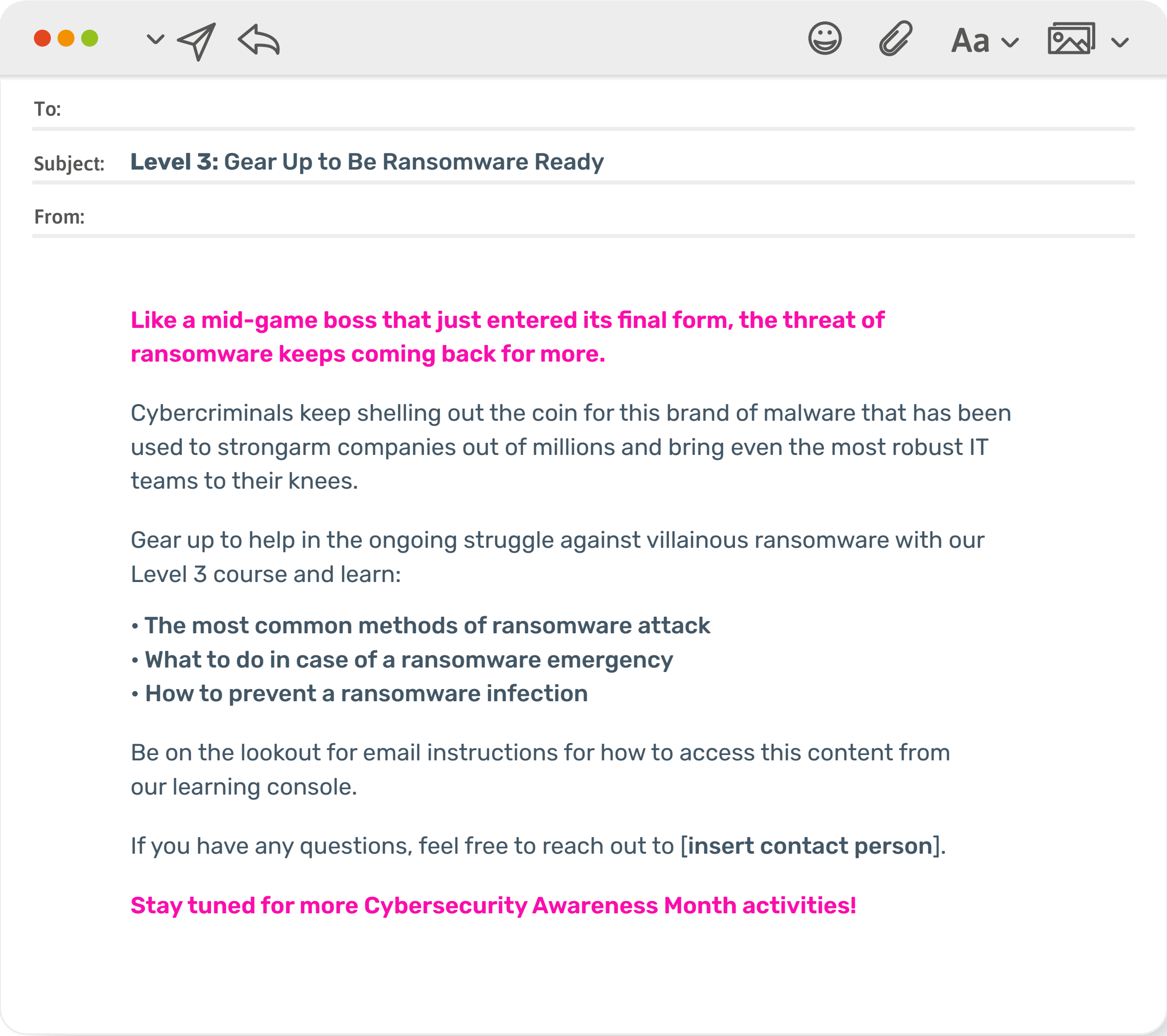
3 Downloadable Assets/Digital Signage

- **Criminal Minds - Ransomware** - Infographic that summarizes ways to prevent ransomware infection
- **Jaws: Don't Be a Victim** - Movie poster-style asset reminding users to think before they click
- **Ransomware Basics -** Infographic-style reminder of what ransomware is and how it works to infect and compromise computer systems

Summary of Assets For Week 3 (continued)

Sharing the Content

Here's some sample email copy to use when sharing the suggested featured asset for this week, the interactive training module: **Ransomware: Blackmail Using Encrypted Data.**



To:

Subject: **Level 3:** Gear Up to Be Ransomware Ready

From:

Like a mid-game boss that just entered its final form, the threat of ransomware keeps coming back for more.

Cybercriminals keep shelling out the coin for this brand of malware that has been used to strongarm companies out of millions and bring even the most robust IT teams to their knees.

Gear up to help in the ongoing struggle against villainous ransomware with our Level 3 course and learn:

- **The most common methods of ransomware attack**
- **What to do in case of a ransomware emergency**
- **How to prevent a ransomware infection**

Be on the lookout for email instructions for how to access this content from our learning console.

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

Stay tuned for more Cybersecurity Awareness Month activities!

WEEK 4

LEVEL 4

INCIDENT REPORTING

Combining all your users have learned throughout the month, the fourth and final level is all about making sure they know what to do when they see something. From reporting phishing emails to seeking help from IT, sharing when something seems not right is one of the most important steps in helping to keep your organization cybersecure.

THE DOPPELGÄNGER

The Doppelganger takes on the form of users just like you in an attempt to keep the actions of their cybercriminal comrades hidden. With a smile and a wave of their hand, Doppelganger will tell you phishing emails and malware infections are "no big deal." Don't fall for it!

ATTACKS:

Ambivalence Ray 35 HP

Procrastinate 10 HP

Summary of Assets For Week 4

Mobile-First Training Module - Join the Security Team

This four-minute module, designed for use on a mobile device, teaches how security incidents impact your entire organization and how every employee has a role to play in managing risk.

Your employees will learn:

- **Misconceptions about data security**
- **Common causes of security incidents**
- **How to make security-conscious decisions**

Video Module – Incident Response: First Steps

This two-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**

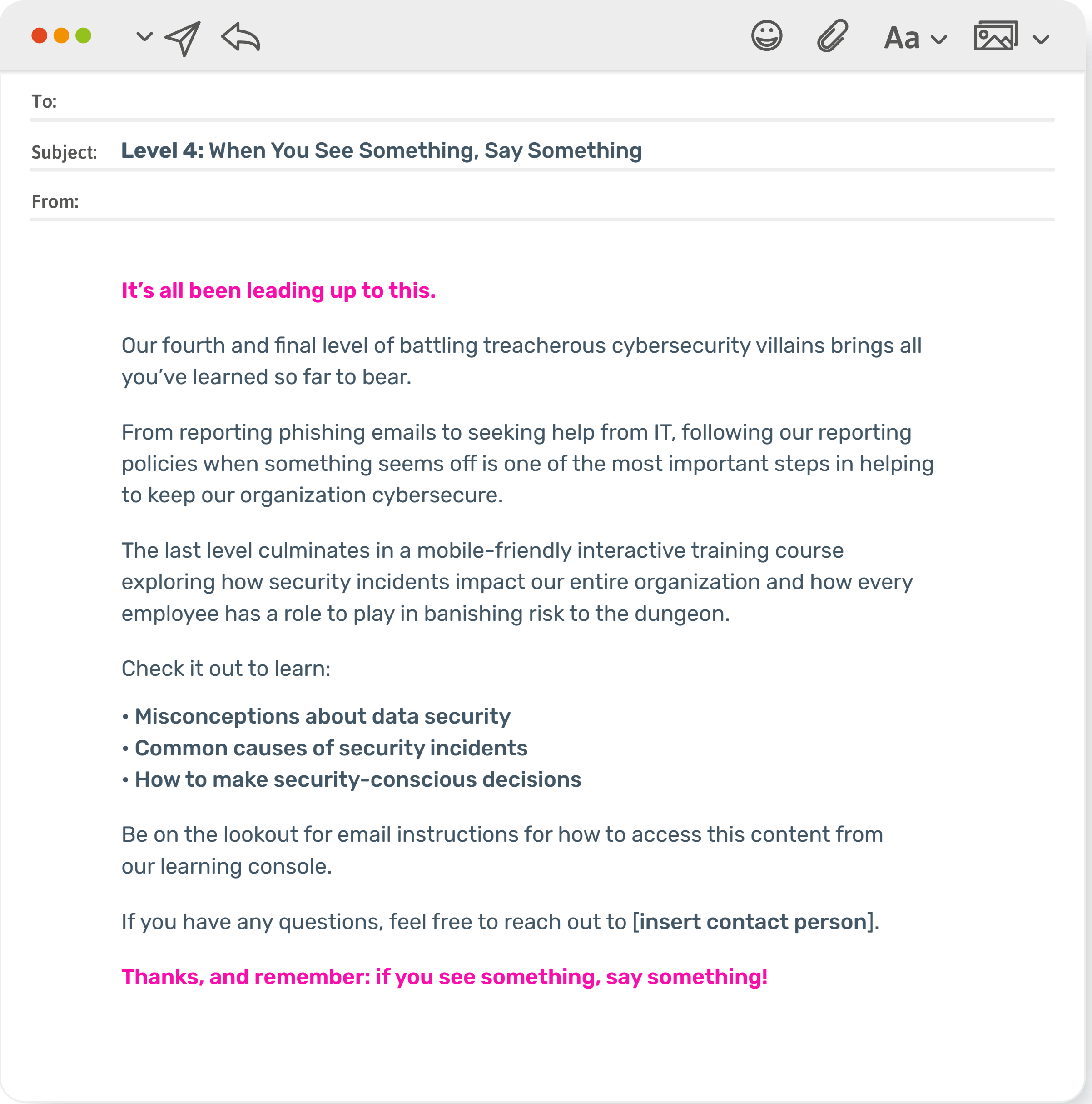
3 Downloadable Assets/Digital Signage

- **Types of Incidents to Report** - Infographic-style asset summarizing common security incidents that should be reported immediately
- **Incident Response -** Poster-style asset that reminds employees that timely reporting of suspicious activity is a vital part of security
- **Following Policy and Reporting Incidents -** Article-style asset that provides a quick refresher on the importance of following the organization's incident reporting policies and procedures

Summary of Assets For Week 4 (continued)

Sharing the Content

Here’s some sample email copy to use when sharing our suggested featured asset for this week: the mobile-first module **Join the Security Team.**



To:

Subject: **Level 4: When You See Something, Say Something**

From:

It’s all been leading up to this.

Our fourth and final level of battling treacherous cybersecurity villains brings all you’ve learned so far to bear.

From reporting phishing emails to seeking help from IT, following our reporting policies when something seems off is one of the most important steps in helping to keep our organization cybersecure.

The last level culminates in a mobile-friendly interactive training course exploring how security incidents impact our entire organization and how every employee has a role to play in banishing risk to the dungeon.

Check it out to learn:

- **Misconceptions about data security**
- **Common causes of security incidents**
- **How to make security-conscious decisions**

Be on the lookout for email instructions for how to access this content from our learning console.

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

Thanks, and remember: if you see something, say something!

BONUS

LEVEL

KEEPING CYBERSECURITY TOP-OF-MIND

We hope this strategy guide and associated resources will help you level-up your users' knowledge of cyberthreats of all types.

Unlike some video games, there are no cheat codes to a strong security culture. Real behavior change for the better means a strategy that turns your largest attack surface — your workforce — into your biggest asset, thereby reducing human risk.

Think of this kit as a complement to a maxed-out approach to human risk management (HRM). 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 #CyberAware to stay in the loop throughout Cybersecurity Awareness Month!

knowbe4

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