Table of Contents

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. Our kit web page provides you:

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://www.knowbe4.com/resources/free-cybersecurity-resource-kits/cybersecurity-awareness-month-kit-weekly-training-planner-p

For Your Users

Access all courses and content via the links provided until October 31, 2025.

- **4 free interactive training modules**
  - Insights From a Hacker: Social Engineering Red Flags (Available in 36 languages)
  - AI, Phishing, and Cybersafety (Available in 35 languages)
  - Ransomware Ready (Available in 35 languages)
  - Links and Attachments: Think Before You Click (Available in 12 languages)

- **4 video modules**
  - Security Culture and You (Available in 35 languages)
  - AI and Sensitive Info Don't Mix (Available in 12 languages)
  - Cloud Ransomware Demo (Available in 36 languages)
  - QR Codes: Safe Scanning (Available in 36 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://www.knowbe4.com/resources/free-cybersecurity-resource-kits/cybersecurity-awareness-month-kit-weekly-training-planner-p. 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:

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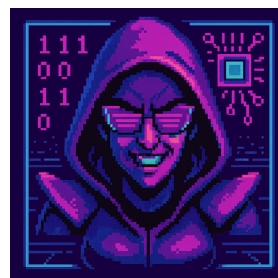
Guess that Villain: Use Google Forms or other online survey tools to build an educational quiz based on the Arcade Villain traits. Offer incentives, like small prizes or recognition, for those who score well to encourage participation.

Know Before You Go: Campaign Techniques

With so much training content in your inventory, you could be worried about trying to put it all together in a way that really speaks to your users. We totally get it; 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.

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]**.

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

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.

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.

ATTACKS:

Convince 25 HP   Impersonate 35 HP

Summary of Assets For Week 1

Interactive Training Module: Insights from a Hacker: Social Engineering Red Flags

Social engineering is one of the main tricks cybercriminals use to get people to take actions that go against their or their organization's best interests. To stay safe online and protect yourself and your organization, it is vital that you don't fall for these tricks. In this 10-minute module, you will meet a social engineer and learn how to spot the red flags and signs of danger associated with common social engineering methods.

Your employees will learn:

- **What motivates hackers**

- **The different varieties of phishing attacks**

- **How to spot the red flags of social engineering**

ACCESS NOW

Video Module – Security Culture and You

This four-minute video explores how building a strong security culture can help protect both organizations and employees' homes from cyber attacks.

Your employees will learn:

- **What security culture is and why it's important**

- **What a strong security culture looks like in practice**

- **Their role in building a strong security culture**

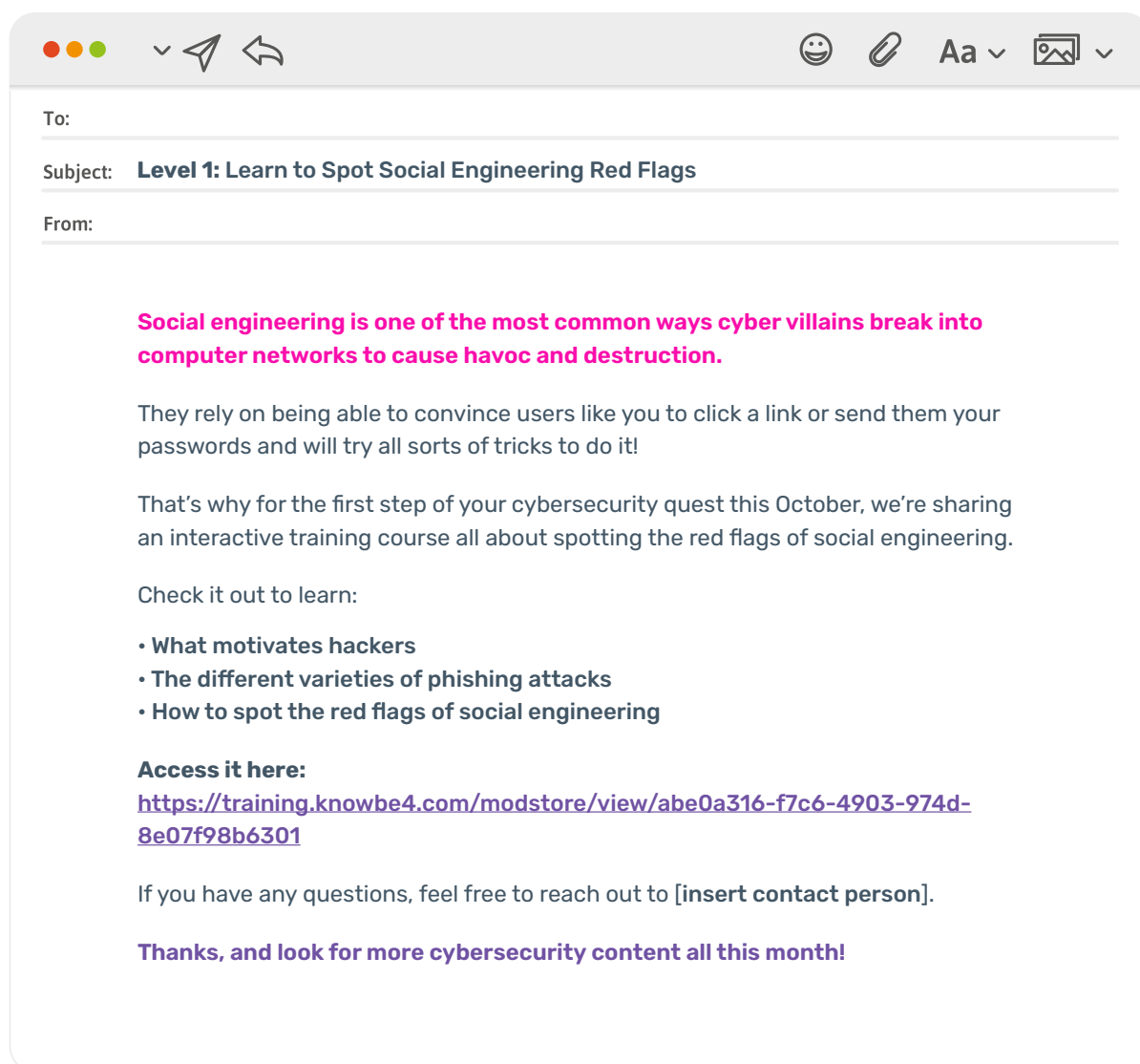**ACCESS NOW**

3 Downloadable Assets/Digital Signage

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

- **Stay Alert for Messaging Scams -** Infographic-style reminder of ways to protect against scams on messaging apps

DOWNLOAD

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 **Insights from a Hacker: Social Engineering Red Flags** training module.

To:

Subject: **Level 1:** Learn to Spot Social Engineering Red Flags

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 training course all about spotting the red flags of social engineering.

Check it out to learn:

• **What motivates hackers**
• **The different varieties of phishing attacks**
• **How to spot the red flags of social engineering**

Access it here:
https://training.knowbe4.com/modstore/view/abe0a316-f7c6-4903-974d-8e07f98b6301

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

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

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 78 HP

Summary of Assets For Week 2

Mobile-First Module - AI, Phishing, And Cybersafety

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

Your employees will learn:

- **Why AI-powered phishing is on the rise**

- **Warning signs of AI-generated social engineering attacks**

- **How to stay secure while using AI programs**

ACCESS NOW

Video Module – AI and Sensitive Info Don't Mix

This two-minute video module explores the critical importance of protecting sensitive information from AI systems and provides practical guidance on mitigating these risks.

Your employees will learn:

- **Why sensitive information should not be shared with AI tools or large language models**

- **Best practices for keeping sensitive information separate from AI instances**

ACCESS NOW

3 Downloadable Assets/Digital Signage
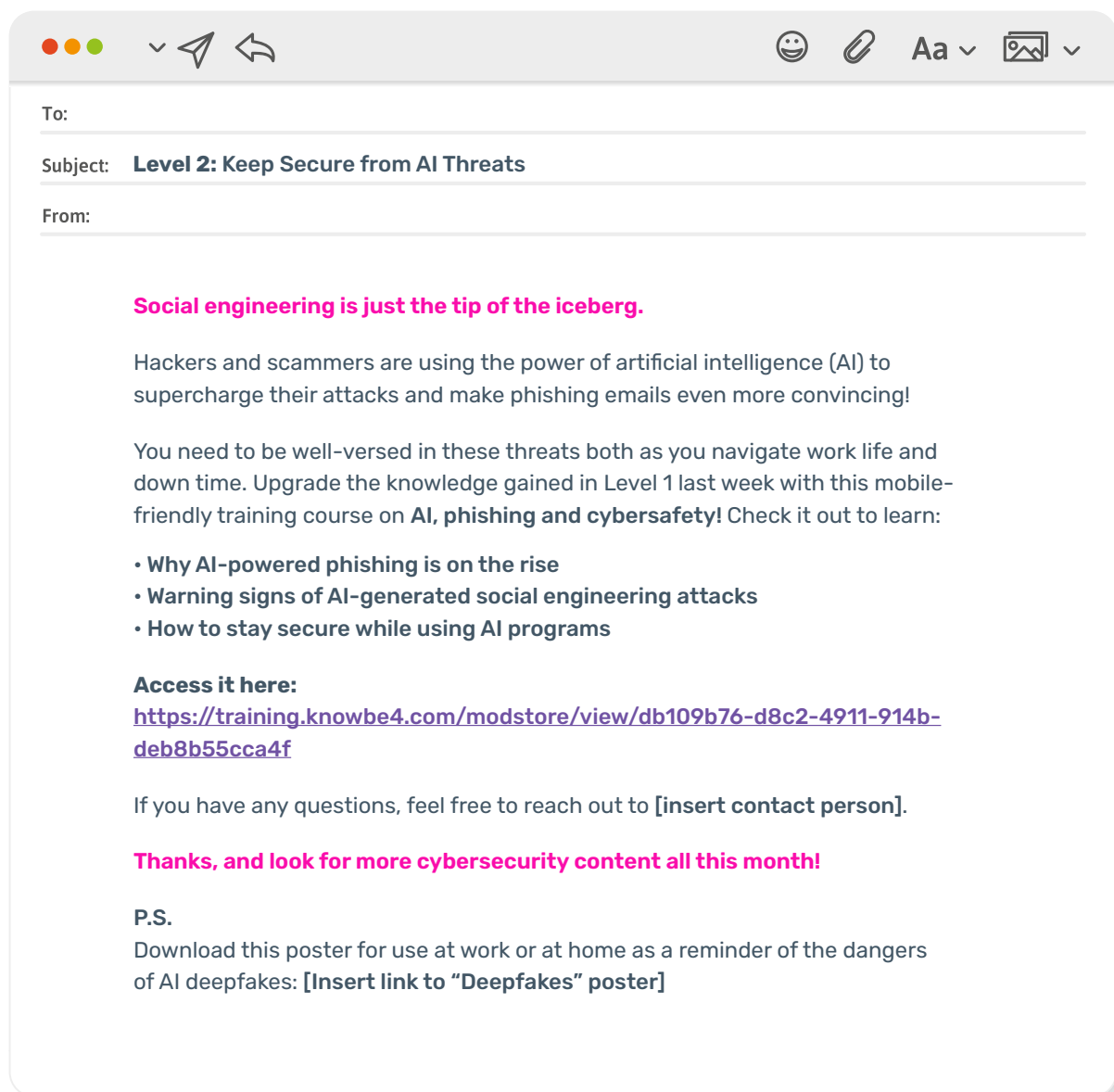
- **Cybersmart Safety Tips -** Infographic that provides a quick overview of some common cybersecurity threats including phishing and artificial intelligence AI chatbots

- **Deepfakes -** Poster-style reminder that draws attention to the cyber threat of deepfakes

- **Protect Your Digital Data -** Infographic-style summary of how AI use can impact digital identity and data privacy

DOWNLOAD

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 **AI, Phishing, And Cybersafety** 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 mobile-friendly training course on **AI, phishing and cybersafety!** Check it out to learn:

• **Why AI-powered phishing is on the rise**
• **Warning signs of AI-generated social engineering attacks**
• **How to stay secure while using AI programs**

Access it here:
https://training.knowbe4.com/modstore/view/db109b76-d8c2-4911-914b-deb8b55cca4f

If you have any questions, feel free to reach out to **[insert contact person]**.
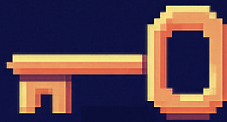
Thanks, and look for more cybersecurity content all this month!

P.S.
Download this poster for use at work or at home as a reminder of the dangers of AI deepfakes: **[Insert link to "Deepfakes" poster]**

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.

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!

ATTACKS:

KryptoLock **15 HP**   MakeYouWannaCry **80 HP**

Summary of Assets For Week 3

Interactive Training Module - Ransomware Ready

This five-minute module will empower employees to make smart security decisions to protect against ransomware attacks.

Your employees will learn:

• **Ransomware impacts**

• **How to spot an attack**

• **How to prevent a ransomware infection**

ACCESS NOW

Video Module – Cloud Ransomware Demo

In this seven-minute demonstration, a team of KnowBe4 experts shows how using cloud-based systems doesn't always protect users from things like ransomware, which can be installed even when using cloud devices. Everyone is a critical part of their organization's defense, even in the cloud.

Your employees will learn:

• **The role they play in keeping their organization's cloud environment secure from ransomware**

• **How to have a healthy suspicion when asked to take an unusual action**

ACCESS NOW

3 Downloadable Assets/Digital Signage
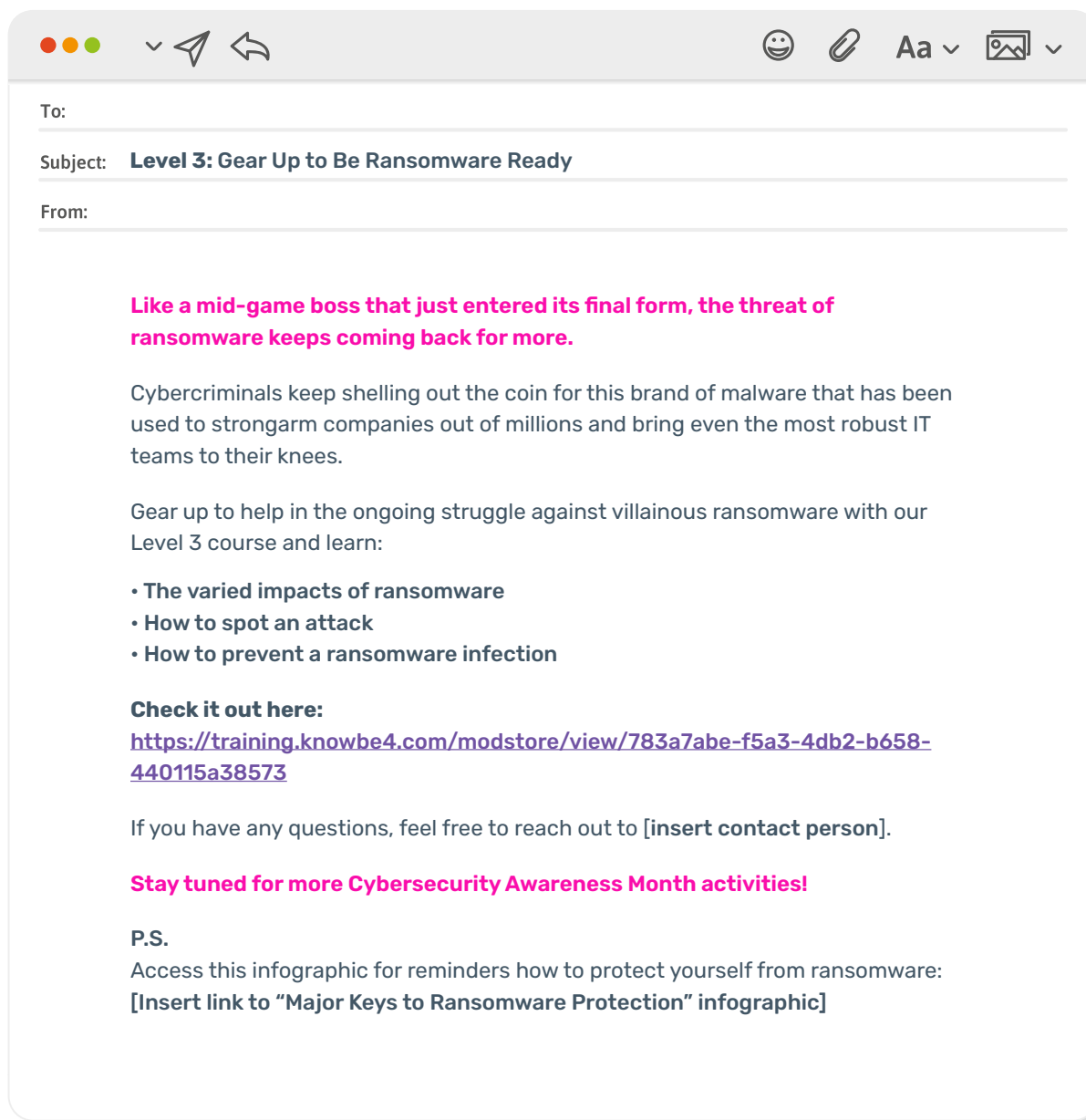
• **Major Keys to Ransomware Protection -** Infographic that discusses key steps to take to prevent ransomware infection

• **Jaws: Don't Be a Victim -** Movie poster-style asset reminding users to think before they click

• **Security Doc: Your Role -** Infographic-style asset that reminds users of their role in defending your organization from cyber attacks

DOWNLOAD

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 Ready**.

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 varied impacts of ransomware**
• **How to spot an attack**
• **How to prevent a ransomware infection**

Check it out here:
https://training.knowbe4.com/modstore/view/783a7abe-f5a3-4db2-b658-440115a38573

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

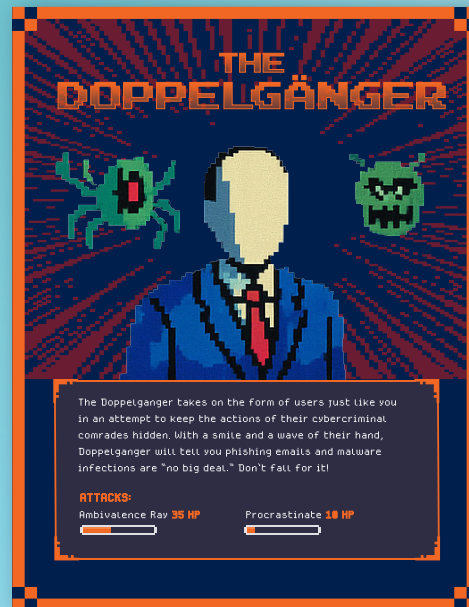**Stay tuned for more Cybersecurity Awareness Month activities!**

P.S.
Access this infographic for reminders how to protect yourself from ransomware:
[Insert link to "Major Keys to Ransomware Protection" infographic]

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 **18 HP**

Summary of Assets For Week 4

Interactive Training Module Links and Attachments: Think Before You Click

This 10-minute module explains how cybercriminals use links and attachments to target users and what users can do about it.

Your employees will learn:

- • **The dangers behind suspicious links**

- **How to handle any unexpected links or attachments they receive**

- **Why reporting suspected phishing attacks is important**

ACCESS NOW

Video Module – QR Codes: Safe Scanning

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

Your employees will learn:

- **What QR codes are and what they're designed for**

- **How cybercriminals take advantage of them**

ACCESS NOW

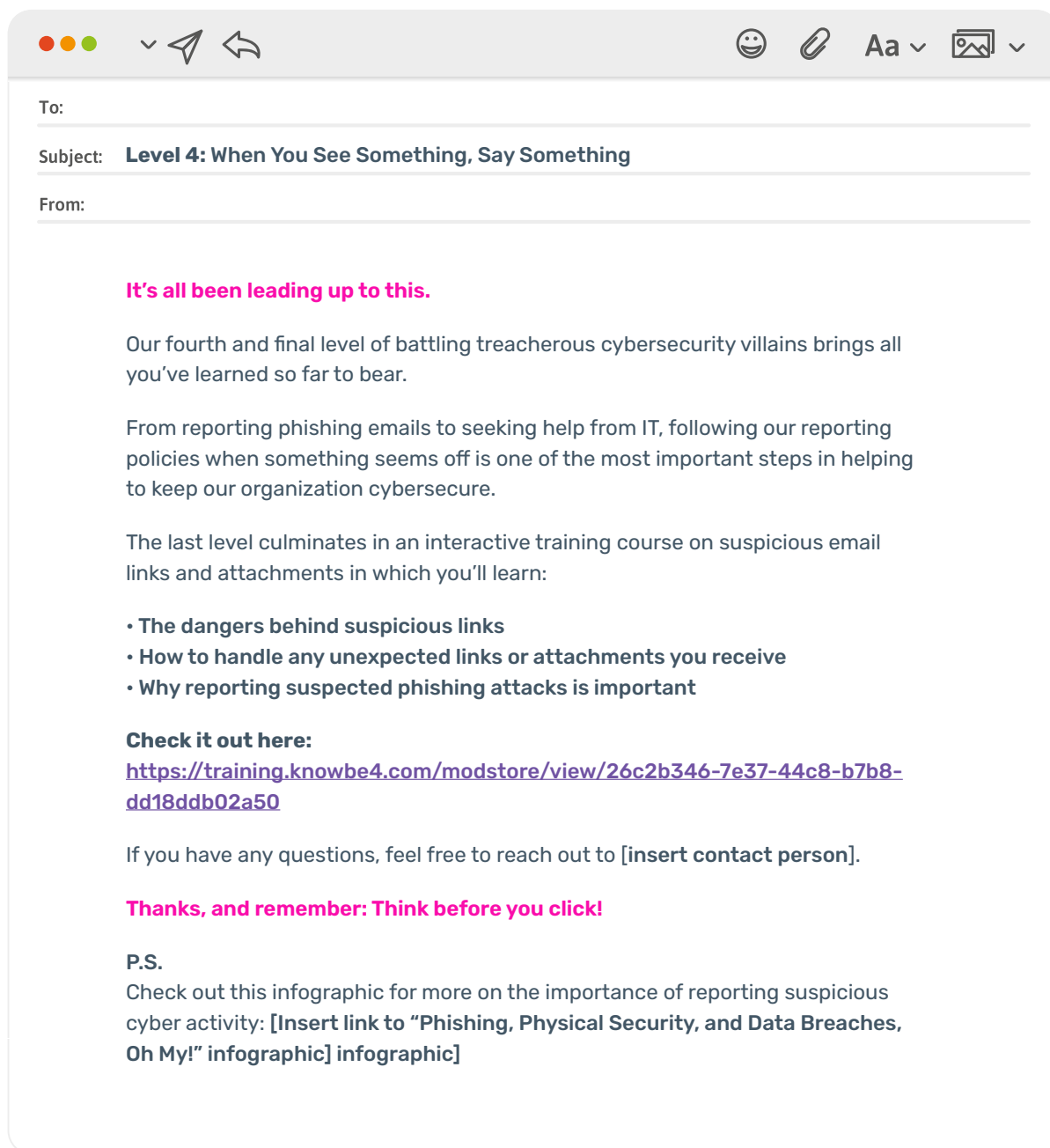## 3 Downloadable Assets/Digital Signage

- **Don't Get Hooked: Report Every Phishing Attempt -** Infographic-style asset that reminds users of the importance of reporting phishing emails per organizational policy

- **Catch Sight of a Concern? Help Others Learn! -** Poster-style asset reinforcing the importance of prompt reporting when it comes to potential security incidents

- **Phishing, Physical Security, and Data Breaches, Oh My! -** Infographic-style asset that explains why immediately reporting security concerns can help stop small issues from becoming major incidents

DOWNLOAD

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 interactive module **Links and Attachments: Think Before You Click**.

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 an interactive training course on suspicious email links and attachments in which you'll learn:

• **The dangers behind suspicious links**
• **How to handle any unexpected links or attachments you receive**
• **Why reporting suspected phishing attacks is important**

Check it out here:
https://training.knowbe4.com/modstore/view/26c2b346-7e37-44c8-b7b8-dd18ddb02a50

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

Thanks, and remember: Think before you click!

P.S.
Check out this infographic for more on the importance of reporting suspicious cyber activity: [**Insert link to "Phishing, Physical Security, and Data Breaches, Oh My!" infographic] infographic**]

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 take the next step in your approach to HRM, 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!

knowbe4