

# 2024 Cybersecurity Awareness Month Kit: The Cybersecurity Reporter

A month-long curated guide about the importance of reporting suspicious emails in the age of AI.

Every October, Cybersecurity Awareness Month is dedicated to talking with your employees and customers about staying safe, both at work and at home. At Proofpoint, we know your planning must happen early. Get started quickly with this complimentary campaign and content about the best practices to identify and report phishing emails.



## About our theme

Cyber criminals continually develop new attack methods. One tactic remains consistent: phishing emails. Especially now, with the use of generative AI, phishing can be even more difficult to identify.

Your employees will receive suspicious emails that ask them to take an action, such as click a link or open an attachment. It's important for them recognize the warning signs, and just as critical for them to know how to report the email.

We created the "The Cybersecurity Reporter" theme specifically for this campaign. Together, we will explain best practices for identifying suspicious messages and reporting them to your organization. It's an ideal choice for Cybersecurity Awareness Month, but you can use it any time of year.

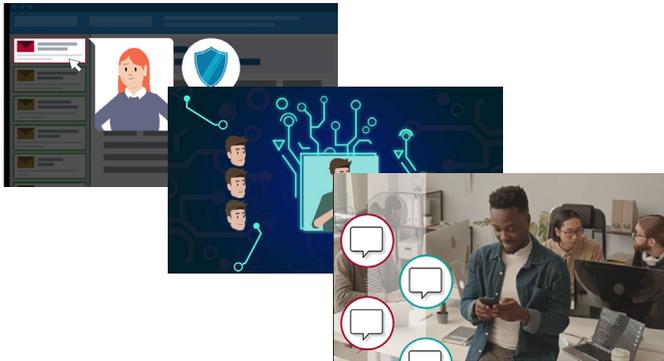
## How to use this kit

Proofpoint has curated a selection of free learning resources from our Proofpoint Security Awareness content library. This material will help you raise awareness of how to handle phishing attacks, especially AI-generated phishing. The kit has messaging for easy communications, and a cadence for launching the campaign. We encourage you to review our suggested resources, campaign messaging, and timeline before finalizing your campaign approach.

## Suggested resources

### Videos

We've selected key pieces of campaign content that explain different phishing threats and the ways that people can defend themselves. Videos create great engagement so this year's kit has three video modules, all handpicked from the timely content that Proofpoint releases based on our industry-leading threat intelligence.



- **“Cybersecurity Reporter: Reporting Suspicious Emails”** – a 2-minute reporter-themed overview of the phishing basics, and how to spot and protect against them
- **“Understanding Deepfakes”** – a 3-minute overview of what AI-generated deepfakes are, and how to spot and protect against them
- **“Attack Spotlight: Conversational Scams”** – a 3-minute overview of what AI-generated conversation scams are, and how to spot and protect against them

### Images

We've also created images that you can add to emails, chat channels, virtual meetings, and other communications to reinforce our Cybersecurity Reporter theme.

- One infographic **“Reporting Suspicious Emails”** – Offer this reporter-themed infographic for deeper-dive information about malicious messages
- One animated GIF **“Cybersecurity Reporter”** – Share these reporter-themed animations across your digital channels
- Four images **“Cybersecurity Reporter Awareness”** – Use these reporter-themed images to add reinforcement to the educational topics
- Five virtual backgrounds **“Cybersecurity Reporter”** – Add flair to virtual meetings and video conferences with this reporter theme

All content pieces are available in 13 languages:

- English, USA
- Arabic, Egypt
- French, Canada
- French, France
- German, Germany
- Italian, Italy
- Japanese, Japan
- Korean, Korea
- Portuguese, Brazil
- Spanish, Spain
- Spanish, Latin America
- Chinese Simple
- Chinese Traditional

You have access to the design files and image files for all artwork. This gives you flexibility to modify these elements to reflect your organization's culture and increase engagement in the program, such as:

- Resize to different print and display sizes
- Add your organization's logo and brand elements
- Edit the text and change colors



## One month before launch

### Plan your campaign

As you prepare to launch your campaign, make sure you're ready to share the news.

- **Review our suggested resources and communications** to determine what you will and won't use during your campaign.
- **Make adjustments to art files** as desired.
- **Identify your delivery methods** for content and communications (e.g., email, internal chat channels, a shared portal, and/or an internal wiki).
- **Share your plan** with key stakeholders and decision-makers—and course-correct, as needed. Use one of our Cybersecurity Reporter virtual backgrounds if your discussion happens via video conference.
- **Work to get buy-in** that's top-down and cross-functional to amplify the voice of your campaign.
- **Identify your launch date**, end date, and key milestone dates in between.



### Create a central content repository

We suggest using a central repository—like an internal wiki—for all the user-facing learning resources in the campaign. This will eliminate the need to send all your content via email or chat channels, and will give employees a single place to go to manage most of their assigned activities.

### Create an internal chat channel

If you haven't already done so, create an internal chat channel specifically for cybersecurity awareness and training. This will give you a quick, easy way to send reminders about program activities and milestone dates.

## The week before launch

### Announce the upcoming campaign

The week before your official launch, we suggest sending an organization-wide email that previews the upcoming program. If possible, the email should come from your organization's CISO or CEO. This will lend weight and credibility to the campaign, which is helpful in setting a positive tone for your efforts.



- Share the animated GIF “Cybersecurity Reporter” along with this suggested communication via email or internal chat (modify as needed):

#### **SUBJECT LINE:**

#### **Coming Soon: The Cybersecurity Reporter**

On <date>, we will kick off a new security awareness campaign called “The Cybersecurity Reporter.” During this month-long initiative, you will have access to information and educational resources that will explain the importance of reporting suspicious messages, which are a significant risk for organizations and people worldwide.

Each of us has a role to play in defending against phishing emails and other cyberattacks. This upcoming program will provide valuable resources and tips you can use to better protect yourself at work and at home.

Stay tuned! <insert virtual meeting details>

**WEEK 1**

Hot off the press!  
Report suspicious  
emails.

Launch your program



- Host a kickoff session and use a virtual background to start the theme.
- Tell attendees to expect weekly emails with links to the Cybersecurity Reporter material.
- In your content repository, add the video module “Cybersecurity Reporter: Reporting Suspicious Emails” and the image “Don’t Take the Bait.”
- Send a communication via email or internal chat using this suggested text (modify as needed):

**SUBJECT LINE:**

**Hot off the Press! Report Suspicious Emails**

Technical safeguards can’t always protect us, so it’s important to know our role in keeping everyone safe. This two-minute video about reporting suspicious emails covers the basics of phishing emails, how to spot them, and how protect against them. Remember, don’t take the bait.

Access the video through the following link at your earliest convenience. You’ll need to watch it to get the most out of the rest of the material we’ll share this week. <[insert link]>

- Later in the week, share the image as a reminder. Here is suggested messaging:

**Don’t Take the Bait.** You are the last line of defense to protect yourself and our organization from phishing emails. Remember to always report suspicious emails.

**WEEK 2**

Stop the presses!  
Look out for AI (Part 1)

Encourage participation



- Early in Week 2, add the video module “Understanding Deepfakes” and the image “Stop the Presses!”
- Send a reminder communication via email or internal chat channels using the following text (modify as needed).

**SUBJECT LINE:**

**Stop the Presses! Look Out for AI (Part 1)**

By now, you should have watched the awareness video we shared last week. (If you haven’t, please do that today.)

Today we will watch another video, this time about how generative AI makes phishing more difficult to detect. The topic is Understanding Deepfakes, and in three minutes it will reveal a new way attackers are trying to trick you. <[insert link]>.

- Later in the week, share the image as a reminder. Here is suggested messaging:

**Stop the Presses! Protect Yourself From Deepfakes.** This AI-generated phishing can mimic authority figures in videos, images, or voice clips to spread intentionally misstated information.

**WEEK 3**

**Extra! Extra!  
Read all about it!  
Applaud participation**



- Early in Week 3, add the infographic “Reporting Suspicious Emails” and the image “Extra! Extra! Quishing Alert.”
- Send a reminder communication via email or internal chat channels using the following text (modify as needed).

**SUBJECT LINE:  
Extra! Extra! Read All About It!**

Congratulations to everyone who has their reporter hat on, and is taking advantage of our Cybersecurity Reporter materials.

We’ve added a new resource to [<\[insert link\]>](#): the infographic Reporting Suspicious Emails. This will help reinforce how to spot suspicious emails and report them safely. Attackers are always thinking about new ways to trick us, such as phishing with QR codes or “quishing.”

- Later in the week, share the image as a reminder. Here is suggested messaging:

**Extra! Extra! Quishing Alert.** Avoid scanning unsolicited QR codes from unfamiliar or out-of-context sources, whether physical or electronic.

**WEEK 4**

**See, then say!  
Look out for AI (Part 2)  
Send wrap-up invitation**



- Early in this final week, add the video module “Attack Spotlight: Conversational Scams” and the image “See Something, Say Something.”
- Send a communication to remind employees to complete all activities, along with an invitation to participate in a virtual wrap-up meeting.

**SUBJECT:  
See, Then Say! Look Out for AI (Part 2).**

We hope you’ve been taking advantage of the Cybersecurity Reporter resources we’ve been sharing with you over the past few weeks. To conclude, we’ve added a final video "Attack Spotlight: Conversational Scams" here [<\[insert link\]>](#). It’s an interesting three minutes about another AI-generated kind of phishing attack.

And always remember what this image says [<\[insert link\]>](#): “If you see something, say something.” Please report security incidents promptly! Taking action can prevent further compromise.

I’d also like to invite you to a virtual wrap-up meeting where we’ll discuss success stories related to this campaign, honor our participants, and ask for your feedback. [<insert meeting details>](#)

If you have any questions or feedback, please reach out to me at [<\[email\]>](#).

## Close of your campaign

### Host wrap-up meeting

It's time to wrap up the Cybersecurity Reporter campaign. Use one of the virtual meeting backgrounds during the wrap-up meeting. And if possible, open the discussion with important points, such as the following:

- What participants liked—and didn't like—about the campaign
- Things learned that weren't known before
- Topics that people would like to learn more about



## Want even more impact?

### Become a Proofpoint customer

This Cybersecurity Awareness Month Kit is part of a larger Cybersecurity Reporter campaign that is exclusively available to Proofpoint customers. The full campaign builds on the content in this document, giving you a packed month of communication tools and awareness content that encourage active participation.

Proofpoint customers have access to extensive essential resources, such as:

- **Campaign guide** that expands this document plan with additional content and information
- **Additional modules** that dive deeper into web browsing best practices
- **Postcard** to alert users to the upcoming campaign and encourage participation
- **Activity tracker** to help users record their completed activities
- **Badges** that can be sent to users as they finish their weekly activities
- **Incentive items**, such as printable stickers that can be used to reward participation
- **Sharable content**, such as posters, animated screensavers, awareness images, and a newsletter to share tips and reminders throughout the campaign

[Contact us for a demo.](#)

For more information, visit [proofpoint.com](https://www.proofpoint.com).

#### ABOUT PROOFPOINT, INC.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 85 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at [www.proofpoint.com](https://www.proofpoint.com).

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.