proofpoint.

2025

Cybersecurity Awareness Month Kit

Human-centric threats beyond the inbox

A month-long curated guide for raising cybersecurity awareness

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 human-centric threats.

This 4-week complimentary security awareness campaign is designed to expose new human-targeted attacks. **It's meant to help your employees understand, identify and make safe decisions when they're confronted by cyberthreats.**

About this year's topic: Human-Centric Threats Beyond the Inbox

As the digital workspace expands, human-centric security challenges grow. While email remains the primary attack vector, cybercriminals are expanding their attacks into other channels, like Microsoft Teams, Slack, Zoom, LinkedIn and WhatsApp. Once cybercriminals compromise an account, they work to deepen their foothold, avoid detection and setup further stages of their attack.

This might mean data exfiltration, ransomware deployment or financial theft. While people might believe that they're engaging with a trusted entity on these platforms, they may be interacting with a threat actor unknowingly. That's why **it's important for them recognize new attack vectors and social engineering tactics—to ensure they can protect themselves and the organization.**

Our material this year details some best practices for identifying threats that target users across email and other digital channels. It also educates users on impersonation and supply chain fraud tactics as well as explains the impact of account compromise. It's an ideal choice for Cybersecurity Awareness Month, but you can use it any time of the year.

About this kit

Proofpoint has curated a selection of free learnings from Proofpoint ZenGuide Security Awareness content library. The kit contains messaging for easy communication, 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

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

1. **"Threat Overview: Phishing in Messaging Apps"**

   4-minute overview on how attackers are executing targeted phishing attacks across email as well as communication and collaboration tools, like Microsoft Teams, Slack and Google Chat

2. **"Time to Think About... The Supply Chain"**

   nano overview that raises awareness about supply chain attacks and preventing supplier fraud

3. **"60 Seconds to Better Security: What is Spoofing?"**

   1-minute overview of email spoofing, tips for identifying spoofed emails and how attackers use this impersonation tactic

4. **"Notes from an Expert: Business Email Compromise (BEC)"**

   3-minute video from a Proofpoint Threat Research expert on why attackers use BEC scams and how to recognize them

5. **"Very Attacked Persons: Protecting Accounts"**

   2-minute overview on how and why attackers target certain individuals because of their access to privileged data or network access, and how to recognize and understand the risks associated account compromise

Planning
Before launch

One month before

- Review our suggested resources and communications to determine what you will and won't use during your campaign.
- Identify your delivery methods for content and communications (for example, 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.
- 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.

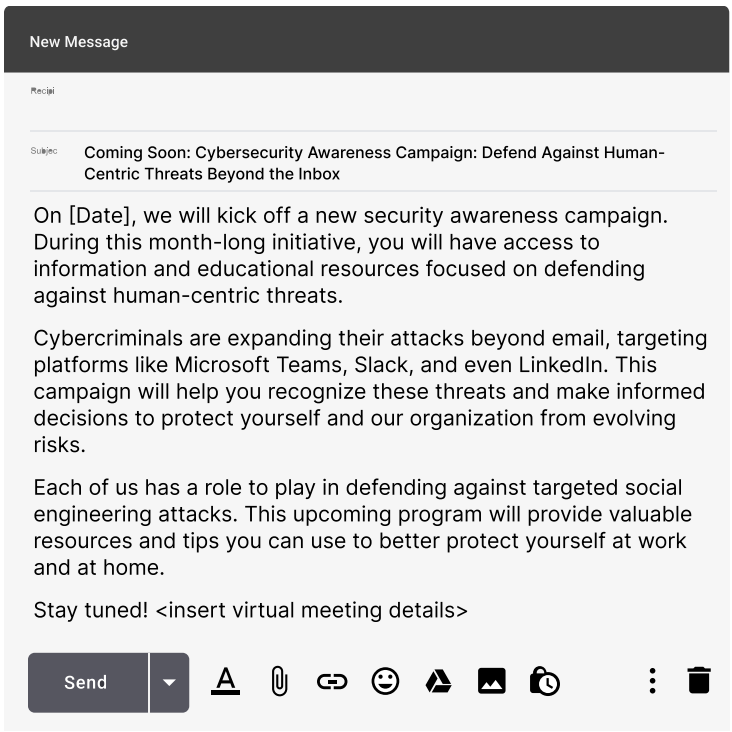
Create an internal chat channel

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

One week before

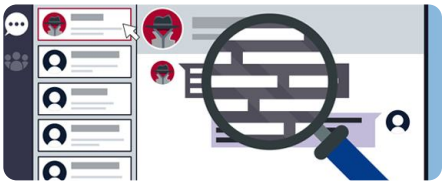
- Announce the upcoming campaign
- The week before your official launch, prepare a message for members of your organization. We suggest sending an organization-wide email that previews the upcoming program. If possible, the email should come from your organization's CISO or CEO. This will lend weight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

Send this suggested communication via email or internal chat (modify as needed).



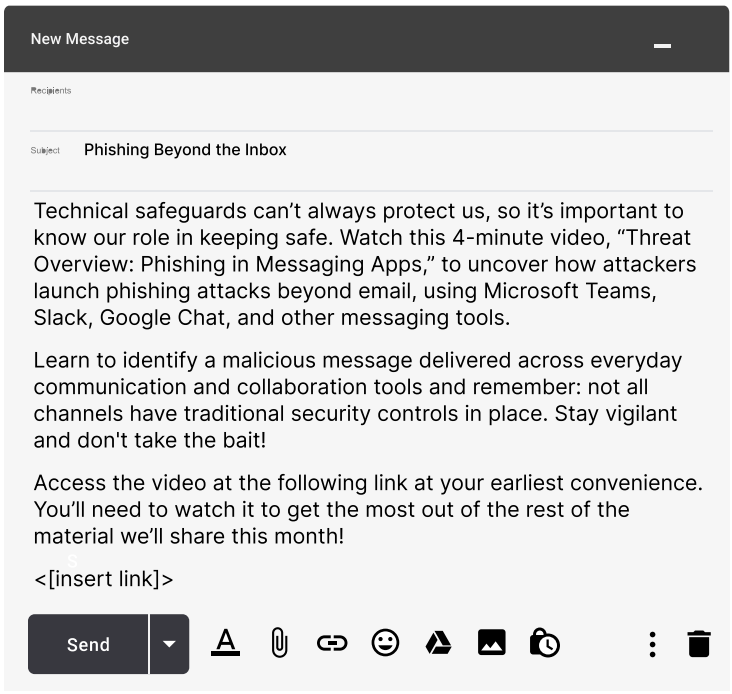
Launch: Week 1

- Host a kickoff session.
- Tell attendees to expect weekly emails with links to the security awareness learning modules.
- In your content repository, add the video module **"Threat Overview: Phishing in Messaging Apps."**



Download assets

Send a communication via email or internal chat using this suggested text (modify as needed).

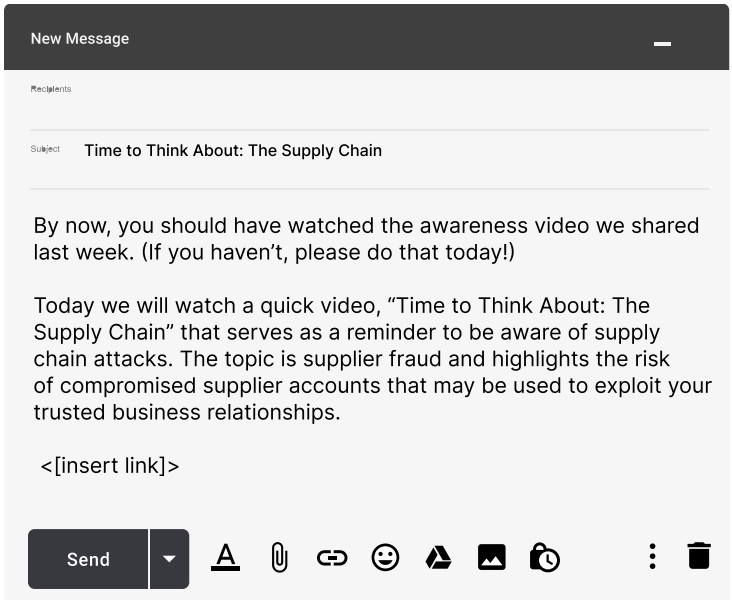


Encourage: Week 2

- Encourage participation early in Week 2
- Add the video module **"Time to Think About: The Supply Chain."**

Download assets

Send a communication via email or internal chat using this suggested text (modify as needed).



Applaud: Week 3

- Early in Week 3, add two video modules:
  - **"60 Seconds to Better Security: What is Spoofing?"** (Week 3, Part 1)
  - **"Notes from an Expert: Business Email Compromise."** (Week 3, Part 2)

Download assets

Send a communication via email or internal chat channels using the following text (modify as needed).

New Message

Recipients

Subject 60 Seconds to Better Security: What is Spoofing?

Congrats to everyone who is taking advantage of this month's cybersecurity awareness material.

We've added a new resource to <[insert link]>: "60 Seconds to Better Security: What is Spoofing?". This video provides a basic explanation of email spoofing—when an attacker forges a sending address so that a message looks like it's being sent by a legitimate company, institution or person. This is one of several impersonation tactics used by attackers to manipulate an individual into revealing credentials, financial information or personal data.

Send

- **Later in the week**, share a second video, Week 3, Part 2, **"Notes from an Expert: Business Email Compromise"** (BEC) attacks.

Download assets

Send a communication via email or internal chat channels using the following text (modify as needed).

New Message

Recipients

Subject Notes from an Expert: Business Email Compromise

Congrats your progress in week 3 of this month's cybersecurity awareness material.

We've added a new resource to <[insert link]>: "Notes from an Expert: Business Email Compromise." You will hear from a Proofpoint Threat Research expert in this video on the Business Email Compromise (BEC) attacks, that are often associated with a spoofed email and attempts to trick employees, partners or customers into transferring money or giving up sensitive data.

Send

Wrap-up: Week 4

- Early in this final week, add video module "**Very Attacked Persons: Protecting Accounts**"
- Send a communication to remind employees to complete all activities with an invitation to a virtual wrap-up meeting.

Download assets

Send a communication via email or internal chat channels using the following text (modify as needed).

New Message

Recipients

Subject Protecting Against Account Compromise

We hope you've been taking advantage of this month's security awareness resources we've been sharing with you. To conclude, we've added a final video "Very Attacked Persons: Protecting Accounts." <[insert link]> It's an interesting two minutes on how and why attackers target certain individuals because of their access to privileged data or network access, and how to recognize and understand the risks associated account 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 have any feedback, please reach out to me at <[email]>.

Send

Time to wrap up the Cybersecurity Awareness Campaign! If possible, open the discussion to important points such as the following:

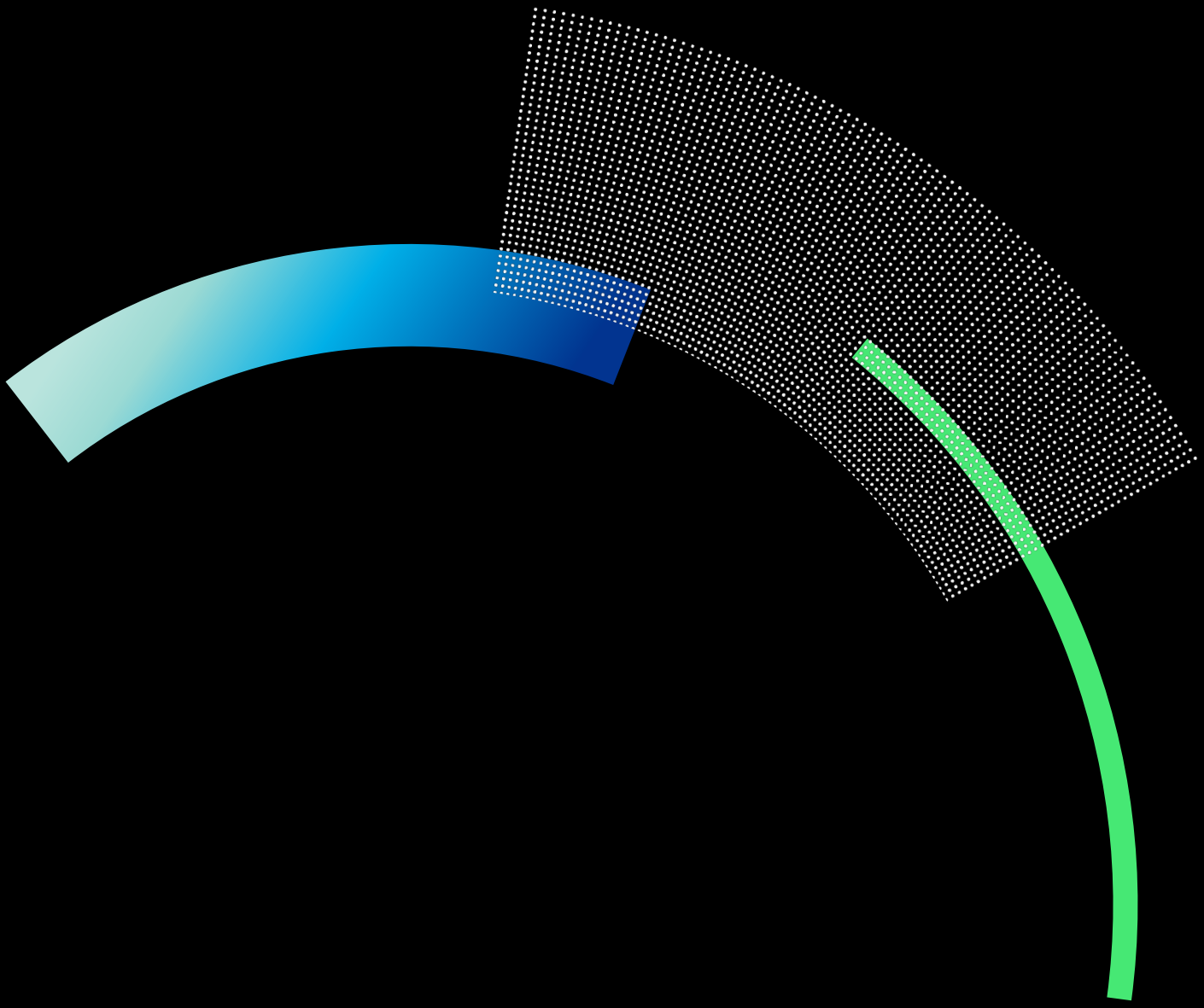
- What participants liked—and didn't like—about the campaign
- Things learned that weren't known before
- Topics that people would like to learn more about

This is a kit that will help you jumpstart your cybersecurity awareness month and empower your people to be more resilient against human-centric, multichannel and multistage attacks.

Want even more impact?

Become a Proofpoint customer and get full access to the ZenGuide™ content library. Proofpoint ZenGuide is a security awareness and behavior change solution. It's a key component of Proofpoint Prime Threat Protection—a comprehensive, integrated solution that combines technology with education to deliver threat protection and resilience against today's human-centric cyber threats.

LEARN MORE ABOUT PROOFPOINT PRIME THREAT PROTECTION →



proofpoint.

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% 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

Connect with Proofpoint: LinkedIn

DISCOVER THE PROOFPOINT PLATFORM →

[Part number and date of collateral]