How to Use Our Cybersecurity Awareness Month Resources

Raise cybersecurity awareness across your organization with the help of our free resources. This guide offers ideas about how to communicate with your end users and utilize the variety of materials available to you.

At Proofpoint, we celebrate all initiatives that highlight the importance of cybersecurity best practices and the role of end users in maintaining strong security postures. To help organizations raise awareness of the ever-present phishing threat, we've curated a selection of free resources you can use to support your Cybersecurity Awareness Month initiatives this October.

The Zip file you downloaded and the links in this document give you access to written, visual and video content that can be emailed, displayed, posted or presented throughout the month. You'll find a description of these items—including ideas on how to use the materials—in Section 1.

We've also developed a suggested Cybersecurity Awareness Month communication plan and schedule (see Section 2). Here, you'll find guidance and tips for successfully planning and executing a month-long phishing awareness campaign with the materials provided.

Section 1: Available Resources

The following phishing awareness resources are accessible via the Zip file you downloaded or via the links noted below.

Phishing Awareness Poster

This printable poster is a free sample from our library of premium Security Awareness Materials. Lighthearted and eye-catching, it's a great addition to high-traffic areas within your organization. It helps drive awareness of the phishing threat and reminds employees to beware of offers that are too good to be true, a lure commonly used by attackers.

You will find this poster in the Zip file. The ideal print size is 11x17.

Phishing Awareness Newsletter

This sample from our "Security-Minded" newsletter series—also available to those who license our Security Awareness Materials—helps explain the phishing threat, using language and terminology relatable to an end-user

audience. It also delivers actionable tips employees can use to improve their email IQ at work and at home. In addition, the newsletter includes advice users can share with family and friends, as well as a phishing-themed crossword puzzle.

You will find this newsletter in the Zip file.

Video: '60 Seconds to Better Security: What Is Phishing?'
Third-party surveys we've commissioned for our research studies have consistently revealed a lack of phishing awareness at a very fundamental level: Between 30% and 40% of working adults around the globe are unable to identify the definition of phishing in a multiple-choice array. This shows a disconnect between the language spoken by infosec teams and the language understood by end users.

Our "60 Seconds to Better Security" series of informational videos defines essential cybersecurity terminology. If you're concerned some of your end users fall in the 30-40% range from our surveys, our "What Is Phishing?" segment is an excellent resource to share.

You can find this and other "60 Seconds" videos on YouTube.

Phishing 'Decision Tree' Infographic
This printable resource offers step-by-step guidance for qualifying incoming emails. It helps users recognize the types of questions they should ask about the messages they receive, and the danger signs they should look for. Distribute to all employees as a visual reminder to keep near their computers or print and hang in common areas within your organization.

You will find this infographic in the Zip file. The ideal print size is 11x17.

'Phishing 101' Webinar
To give you increased flexibility, we've provided this resource in multiple formats: a pre-recorded MP4 with video and audio, as well as fully scripted PowerPoint slides. This gives you multiple options for utilizing this resource, including the following:

- Post the webinar file to a shared portal and allow users to watch individually at their leisure
- Set up lunch-and-learn sessions in which employees watch the webinar together
- Deliver the presentation yourself, as written
- Use the slides as a starting point and adjust the scripting as needed to address concerns specific to your organization

You will find the MP4 and PowerPoint files in the Zip file.

Article: 'Three Keys to Avoiding Phishing Emails and Ransomware Attacks'
This post from the Proofpoint Security Awareness Training blog outlines three essential best practices for identifying and avoiding malicious emails. Users will be advised about the dangers of skimming messages instead of studying them; the questions they should ask themselves before engaging with a message; and the importance of verifying requests before acting on them.

You will find this article on the Proofpoint blog.

Attack Spotlight: Raise Awareness of Trending Cybersecurity Threats
Our Attack Spotlight series provides free awareness resources you can use to alert end-users to trending cybersecurity threats. This blend of Proofpoint threat intelligence and security awareness training expertise allows you to quickly and easily arm your end users against dangerous real-world attacks.

Topics covered to date include OneDrive, DocuSign, and Microsoft Office 365 phishing campaigns. Each Attack Spotlight installment explains the threat in a brief awareness module and a "Teachable Moment" PDF. All Attack Spotlight resources are available for unlimited use.

Access our Attack Spotlight archive on the Proofpoint website (and stay tuned for future installments).

Section 2: Suggested Program Plan

Below you will find ideas for executing your Cybersecurity Awareness Month initiatives. We have included the following:

- A suggested week-by-week plan for your program, beginning in late September
- Recommended content for weekly emails
- Ideas for budget-friendly giveaways and end-user incentives

We encourage you to modify our suggested communications and adjust your plan as appropriate to reflect your company culture, organizational structure and budget.

Week of September 16: Pre-Launch Communication to End Users
We suggest sending an organization-wide email that previews your upcoming program. If possible, the email should be sent by your organization's CISO or CEO. This will lend weight and credibility to the program, which sets a great tone for your efforts.

SUBJECT: *Coming Soon: Cybersecurity Awareness Month*

October is Cybersecurity Awareness Month, and we're working with our trusted partner, Proofpoint, to bring you a phishing awareness program that will highlight and reinforce the email best practices we've been sharing here at <insert company name>.

Starting next week, you'll see posters in common areas around the building; these posters will give you a hint of the activity we have planned to formally kick off the program on October 1.

I encourage you to attend the kickoff and to fully participate in the activities that our infosec team will be sponsoring throughout October. Cybersecurity is an important initiative for our organization, and each employee is an important link in the security chain.

We are committed to providing the resources to make our security chain as strong as possible. Our forthcoming Cybersecurity Awareness Month program will provide tips and information that you can put to good use not only here at work, but also in your personal life.

Stay tuned!

Week of September 23: Preparation for Launch

On Monday and/or Tuesday, hang the Phishing Awareness Poster (see the Zip file) in common areas around your organization. Capitalize on the donut theme featured in the poster and plan to host a breakfast launch party on October 1.

On Wednesday, send a meeting invitation with the time and location of your launch party. Within larger organizations, we suggest having multiple locations to accommodate all employees; the larger the group(s), the better. When possible, ask department heads or team managers to send out the invitations; this will again show that the program has top-down support within your organization.

Here is suggested text to include with the invitation:

SUBJECT: *Join us for breakfast on October 1*

Cybersecurity skills are sweet ... and so is free breakfast! Join your coworkers for coffee and donuts as we kick off Cybersecurity Awareness Month on October 1.

October 1: Program Launch

On the morning of October 1, host end users for the launch of your Cybersecurity Awareness Month program. Get company leaders involved as much as possible; ideally, your CISO or CEO would welcome and speak to employees and let them know that, throughout the month, you will be sharing videos, posters, and articles designed to improve phishing awareness. It's a great idea to stress that the advice they will receive can used at work and at home, and that they will be able to share many of the tips and resources with family and friends.

If your budget allows, close out the meeting by distributing a cybersecurity-themed giveaway to all employees. You don't have to invest a lot of money; even bags of Goldfish Crackers or Swedish Fish will accomplish your goal: Getting employees to keep thinking about your program after they leave the room.

In the late morning or afternoon of October 1, send a kick-off email:

SUBJECT: *Security Awareness Month is here!*

We hope you were able to join us this morning as we kicked off Cybersecurity Awareness Month. Throughout October, we'll be sharing videos, articles, and other resources that will help you to better understand the

importance of email security. You'll also learn a number of valuable tips you can use both at work and at home … and even share with family and friends!

Our first awareness tool is a short video: "60 Seconds to Better Security: What Is Phishing?" If you don't know what phishing is—or if you think you know, but aren't sure—this brief YouTube video by Proofpoint, a leading provider of cybersecurity solutions, is must-see TV. You'll need to have a good sense of what phishing is to get the most out of the rest of the materials we'll share this month.

Happy watching!

Week of October 7: 'Phishing 101' Webinar

Ask department heads or team managers to get their employees together for lunch-and-learn sessions during the week to watch the "Phishing 101" webinar (found in your Zip file). Ask coordinators to write down any questions attendees might have and submit them to the infosec team. At the end of the week, post the webinar to a shared internal resource and send out an organization-wide email:

***SUBJECT:** Did you watch 'Phishing 101'?*

We hope you were able to join your fellow coworkers earlier this week to watch the "Phishing 101" webinar. If you weren't able to participate in a lunch-and-learn session this week, that's OK: We've posted the webinar to <our internal wiki>. You can find it <here [embed link]>.

For those who did attend, we thank you for taking the time out of your schedule to learn more about best practices for email security. We also thank those who submitted questions following the webinar. Here are answers to some of the most frequently asked questions:

<insert questions and answers>

Week of October 14: Phishing Infographic and Article

On Monday and/or Tuesday, distribute printouts of the Phishing 'Decision Tree' Infographic (available in the Zip file) and ask employees to display the graphic near their computers. This is a great opportunity for end users to interact with you face-to-face, and for you to let them know that the infographic can help them identify potentially dangerous emails.

On Wednesday, communicate the following:

***SUBJECT:** Stay on the lookout for phishing emails*

Earlier this week, we distributed a terrific email security resource: an infographic that gives you step-by-step advice for identifying potentially risky messages. We encourage you to follow this advice with unsolicited emails

you receive, and report any messages that seem suspicious. (If you did not receive a copy of the infographic, please reply to this email.)

We also encourage you to read this article on the Proofpoint Security Awareness Training blog: "Three Keys to Avoiding Phishing Emails and Ransomware Attacks." It provides additional context for the tips noted on the infographic and reinforces key topics covered in last week's "Phishing 101" webinar.

Week of October 21: Phishing Newsletter

Early in the week (ideally on Tuesday), send your organization the "Security-Minded" newsletter (you'll find it in the Zip file). We suggest this email text:

SUBJECT: *Phishing prevention is about being security-minded*

We hope you've been taking advantage of the phishing awareness resources we've been sharing with you this month. This week, we're bringing you Proofpoint's "Security-Minded" newsletter, which offers a mix of information, advice, and even a fun (and potentially rewarding) activity.

Download and print the attached PDF. Read through the newsletter, which will help you complete the crossword puzzle on the second page. Once you've completed the puzzle, put your name on the page and drop it off <with a member of the infosec team>.

All those who ***turn in a completed puzzle by October 31 will be eligible to win*** *<one of five $20 Dunkin' gift cards>. (Winners will be announced during the week of November 4.)*

P.S. Don't be shy about sharing the tips in this newsletter with your family and friends!

Week of October 28: Attack Spotlight

Take a look through our Attack Spotlight archive and share the awareness materials associated with a threat that your organization is most likely to experience (or perhaps has already experienced).

You will find suggested text for your email on the same page as the Attack Spotlight awareness tools. In that email, add a reminder for users to turn in their completed crossword puzzles by October 31 in order to be eligible for the prize drawing.

Week of November 4: Program Wrap-Up Email

SUBJECT: *Cybersecurity Awareness Month winners are …*

Cybersecurity Awareness Month has come to a close, and we hope you took advantage of the tools and tips we shared with you last month.

We thank all those who completed and submitted the crossword puzzle from the "Security-Minded" newsletter. ***The winners of the <five $20 Dunkin' gift cards> are:***

<insert names>

The calendar page may have turned, but our cybersecurity efforts shouldn't end. The advice and resources you gained last month can be used year-round to improve cybersecurity here in the office and at home.

We thank you for your efforts to become a strong link in our security chain!