STAYING SECURE IN CYBER FALLS

Security Awareness Campaign Kit

A campaign-in-a-box to support and promote National Cybersecurity Awareness Month (NCSAM)

MediaPRO
Cybersecurity & Privacy Education

MediaPRO
Cybersecurity & Privacy Education

WELCOME TO YOUR STAYING SECURE IN CYBER FALLS SECURITY AWARENESS KIT

We've put together a collection of interactive resources and content to help you make the most of National Cybersecurity Awareness Month (NCSAM) this October. The bundle includes a communications plan for running this month-long security awareness campaign.

The InfoSec community agrees that addressing the human side of cybersecurity through security awareness and training is vital. The discussion now rests on how to deliver training content in a way that permeates through an entire company and leads to changes in risky employee behavior.

Such changes are not achieved overnight, nor are they earned through one-off employee awareness training. Employee education is best achieved through varied content and delivery methods, deployed on a recurring basis.

That's why this campaign kit gives you enough educational content on a variety of topics to send two-to-three resources per week throughout the month. And they're not just about phishing!

This kit covers the following key cyber-risk areas:

- **Incident Reporting**
- **Cloud Computing**
- **Physical Security**
- **Working/Computing Remotely**
- **Identifying Personal Information**
- **Phishing**
- **Safe Use of Social Media**
- **Identifying Malware**

Welcome to Cyber Falls

The theme of this campaign kit is an interactive learning experience called “Cyber Falls,” accessed via: https://cyberfalls.io. Cyber Falls, an “Everytown USA,” utilizes interactive content and a touch of humor to illustrate the many ways cyberthreats reach into the lives of your colleagues, family, and friends.

In Cyber Falls, visitors can learn valuable tips through a series of animations, games, comic strips, and more, that they can use in day-to-day life.

By interacting with this content, we hope your employees will learn about the eight key risk areas, and maybe even have a little fun! The more engaging a security awareness initiative is, the more effective it will be.

What You Get

In addition to this communications plan, you’ll find the following content contained in the ZIP file:

- A link to a “Security Checkup” interactive assessment for employees to test their cybersecurity and data privacy know-how quickly and easily
- Access to five video links accessed via Cyber Falls
- A link to a gamified activity focusing on protecting personal information
- Two educational infographics
- Seven printable posters covering a variety of cybersecurity topics
- Six sample emails for sharing the resources in this kit with your employees throughout the campaign

Staying Secure in Cyber Falls

Five Week Communication Calendar

Week 1: Oct 1-4 — Introduction to Campaign

- Link to "Security Checkup" knowledge assessment
- *8 Ways to Stay Secure for National Cybersecurity Awareness Month* Infographic
- Introductory Email

Week 2: Oct 7-11 — Incident Reporting and Physical Security

- Link to Incident Reporting educational video
- Link to Physical Security educational video
- Printable Secure Facilities poster
- Sample email to share content with employees

Week 3: Oct 14-18 — Personal Information and Social Media

- Link to a gamified activity focusing on protecting personal information
- Printable Social Media Mishaps poster
- Sample email to share content with employees

Week 4: Oct 21-25 — Cloud Computing and Working Remotely

- Link to Wi-Fi Drifter educational video
- Link to Cloud Computing educational video
- Printable Wi-Fi Dangers poster
- Sample email to share content with employees

Week 5: Oct 28-31 — Phishing Awareness and Identifying Malware

- Link to Security Zombie educational video
- Four Malware Monster posters
- *How to Spot a Phishing Email* infographic
- Sample email to share content with employees

How You Know It's Working

One of the benefits of a multi-topic awareness campaign is the opportunities it creates for tracking progress. The more topics you educate on, the more data points you can collect and analyze to see the impact of your awareness initiative.

Though this campaign only lasts a month, collecting baseline data and observations before you begin can still prove useful. At the end of the month, you can check in across these same variables to measure the impact of your campaign and the behavior change it inspired.

Here are some ideas for data points and observations to track:

Incident Reporting

Communicate with your IT team to see how often your employees report potential incidents involving cybersecurity or sensitive information. Track this number for changes throughout the campaign and compare at the end of the month.

Network Event and Data Loss Prevention Logs

Work with your IT team to set a baseline on the number of automated reports created for things like unsecured login attempts and suspicious data transmission events.

Reported Phishing Emails

If your IT staff has an established way of logging suspected phishing emails reported by employees, keep an eye on those numbers throughout the campaign.

Word of Mouth

How often do you hear employees talking about cybersecurity or data privacy topics in common areas around your office? Keep an ear open to these sorts of discussions before, during, and after the campaign to see what interested in these topics the campaign has generated.

STAYING SECURE IN CYBER FALLS COMMUNICATIONS PLAN

This plan explains how to deploy the five-week Staying Secure in Cyber Falls security awareness campaign.

Week 1: Introductory Email and Assessment

Instructions

Send the introductory email on Monday of this week. This email explains the campaign and contains a link to the "Security Checkup." The email will invite your learners to take the assessment and download their results for review at the end of the campaign.

Consider sending a secondary email this week with your own results from the checkup to show you're taking part in the campaign, too!

Part of Week 1 is the introductory infographic *8 Ways to Stay Secure for National Cybersecurity Awareness Month*. This infographic lays out the eight key risk areas addressed in the checkup and focused on in the communications during the month.

Resources

- Link to "Security Checkup" knowledge assessment
- *8 Ways to Stay Secure for National Cybersecurity Awareness Month* Infographic
- Introductory Email

Include the infographic directly with the Introductory Email as an attachment or, if your IT rules forbid this, as a link to download from a company-run file-sharing tool.

Tip: Don't stop at email! So many organizations have instant messaging tools, such as Slack or Microsoft Teams, that are the perfect medium to share quick-hit content like infographics.

Access Security Checkup

Week 2: Incident Reporting and Physical Security

Instructions

Send the Week 2 email at the beginning of the week to kick off this week's theme, which focuses on the importance of employees reporting potential cyber incidents and the risks associated with poor physical security practices.

Resources

- Link to Incident Reporting educational video
- Link to Physical Security educational video
- Printable Secure Facilities poster
- Sample email to share content with employees

The links in this week's email send users to the "Cyber Falls Cinema" to watch two videos, each less than two minutes. Both videos are animated and convey their messages with a mix of humor and scenarios likely to resonate with your employees.

Week 2 also includes a poster focusing on the physical security risk area perfect for printing out and displaying in common areas or as a digital element of a rotating screen saver on communal monitors.

Tip: These videos, like all the videos included in this campaign kit, come with closed captioning, so consider displaying them this week on any communal TV screens or monitors you may have around your office.

Watch Incident Reporting Video

Watch Physical Security Video

Week 3: Personal Information and Social Media

Instructions

On Monday, send this week's email to introduce the Week 3 theme: identifying and protecting personal information and secure use of social media.

This week takes your learners into the Cyber Falls Mall for a exploration of what personal information can safely be shared and what types of information shouldn't be. The mini-game invites the learner to choose what types of information are appropriate to share when entering a sweepstakes encountered in a shopping mall environment.

Week 3 also includes a printable poster advising caution in sharing work-related information on personal social media channels.

Resources

- Link to a mini-game activity focusing on protecting personal information
- Printable *Social Media Mishaps* poster
- Sample email to share content with employees

Tip: Display or share this week's poster alongside the others that are part of this campaign to help employees connect the variety of ways personal information can be compromised.

Access Mini-Game

Week 4: Cloud Computing and Working Remotely

Instructions

Send the Week 4 email to share the contented related to this week's theme: cloud computing and working remotely.

Resources

- Link to Wi-Fi Drifter educational video
- Link to Cloud Computing educational video
- Printable *Wi-Fi Dangers* poster
- Sample email to share content with employees

Week 4 brings your learners back to the Cyber Falls Cinema for two more videos. One focusing on using Wi-Fi securely, the other explaining the risks inherent in using cloud storage tools.

Week 4 also includes a shareable and printable poster cautioning against the use of unsecured networks. Consider rotating out the campaign's posters throughout the month to encourage employee interest in what might be coming next.

Tip: Consider having a "movie lunch" with either of these two videos and lead a discussion after about the threats discussed.

Watch Wi-Fi Drifter Video

Watch Cloud Computing Video

Week 5: Phishing Awareness and Identifying Malware

Instructions

Happy Halloween! The wrap-up week resources for NCSAM take learners to the cinema one more time for a horror movie! This brief video shows how "security zombies" in the form of untrained employees can put your organization at risk by mindlessly clicking on phishing emails and letting in malware.

Send the Week 5 email early in the week to give your employees access to this video and attach the included infographic on the five common ways to spot a phishing email.

Week 5 also includes a variety of printable and shareable posters featuring different types of malware personified as monsters. If your organization has any Halloween events, consider incorporating these posters (remember, Halloween is Thursday, Oct 31!).

Resources

- Security Zombies educational video
- Four *Malware Monster* posters
- *How to Spot a Phishing Email* infographic
- Sample emails to share content with employees

We've also included a sample email to wrap up the campaign and drive home the importance of every employee's role in cybersecurity.

Tip: Is your office hosting Halloween festivities? Work with your office administrator to print the Malware Monster posters as small cards and hide them throughout the office. Whoever collects all four before Halloween gets a prize!

Watch Video

Measuring Campaign Results

If you gathered some baseline observations based on our suggestions in the *How You Know It's Working* section, now is the time to review the campaign's impact. Continue collecting these observations over the next two weeks following campaign's end.

Some possible questions to answer

- Did the number of reported potential cyber incidents go up or down?
- Did reported phishing emails increase?
- Has your IT department seen a change in things like unsecured login attempts and suspicious data transmission events?

Beyond these numbers-based metrics, consider assessing your employees from a softer point of view. This means doing the legwork to see if the seeds of a risk-aware culture have been planted.

These signs may be subtle. But you may notice, as you come into the office kitchen to get a cup of coffee, that your employees are talking about one of the videos you shared during this campaign. Or maybe they're discussing that particularly tricky phishing email that made its way to your marketing department.

When your employees happily joke about data classifications, when they brag about the difficulty of their passwords, and when they argue about the right answer on the latest quiz you sent out, you will know that you have started to make real progress in creating a risk-aware culture.

Cybersecurity Awareness Month and Beyond

This campaign kit will help you take advantage of National Cybersecurity Awareness Month and start a drum beat of security awareness in your organization. But NCSAM is only one month.

To achieve a risk-aware culture, security awareness cannot be relegated to one-twelfth of the year. The best results are obtained from a comprehensive campaign that includes these elements:

- An initial knowledge assessment to gauge existing employee know-how and set a baseline to judge training effectiveness
- A primary training event (such as a training courses employees work through for a set 20-30 minutes)
- Supporting training events (knowledge days, lunch and learns, etc.)
- Training materials to reinforce key training topics (educational videos, posters, mini-games, etc.)
- Simulated phishing campaigns to further test employee knowledge and training effectiveness
- Periodic knowledge assessments to see what employees have learned

Think of this campaign kit as a starter pack for a full-fledged awareness initiative. Many of these resources can be used outside of NCSAM, but they cannot take the place of a focused awareness program incorporating many, if not all, the elements listed above.

MediaPRO's Approach to Security and Privacy Awareness

A focused, campaign-based approach to security and privacy awareness forms the bedrock of MediaPRO's TrainingPacks. TrainingPacks combine engaging, flexible, out-of-the box courses with reinforcement materials, impact reports, an optional phishing simulator and great customer support. You can license TrainingPacks separately or bundled, based on what makes the most sense for your organization. You can run courses on our LMS or yours. All TrainingPack content is designed to build competency across the eight core behavior risks covered in this campaign kit, and more.

Learn More About MediaPRO