INFOSEC

Marine Lowlifes

SECURITY AWARENESS CAMPAIGN KIT

Everything you need to get your coworkers to (really) care about security.

Table of Contents

CAMPAIGN KIT

Marine Lowlifes

Security Awareness like a (Marketing) Boss: Running a Layered Campaign

Mandatory security training is a reality for many organizations, but training compliance alone will not prevent a security incident. Looking to really engage your workforce and drive behavioral change? We recommend borrowing a concept from Marketing 101: run a layered security awareness campaign.

What is a Layered Campaign & Why Should You Care?

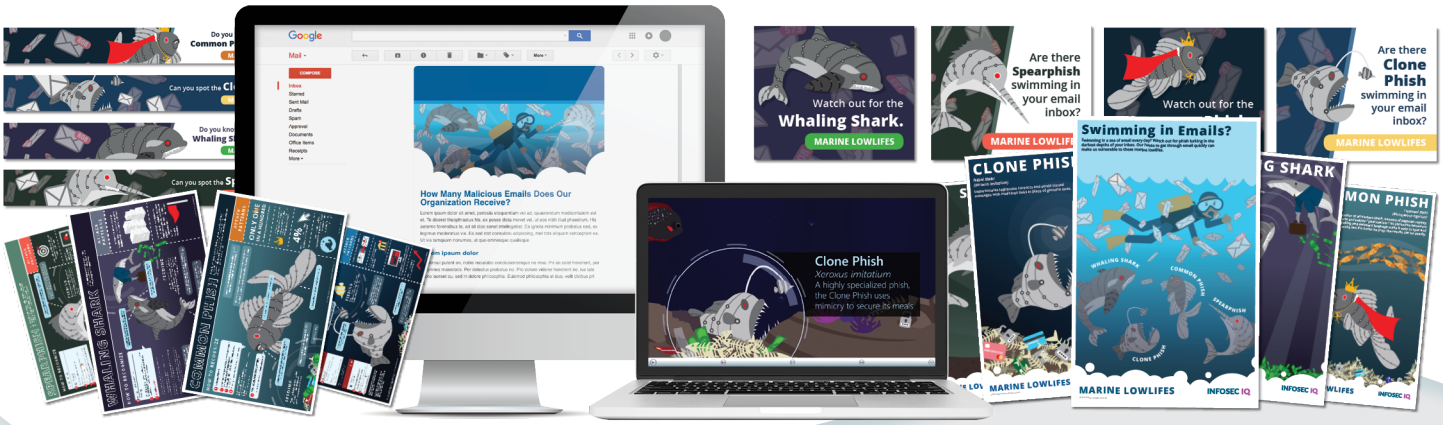
A "campaign" goes beyond a set of training modules and the email you use to deliver them. It's an entire package of communications and content built around a single, repeatable, recognizable theme. Effective campaigns are designed to connect with your audience, deliver your message and drive action. While marketers rely on layered campaigns to promote brand awareness and drive sales, security awareness practitioners like you can use these same principles to deliver a security awareness program that engages your workforce and drives behavioral change.

The Infosec Security Awareness Campaign Kit

If you're like most IT and security practitioners, you love the idea of making security awareness and training more engaging and, ultimately, more effective. What you don't like is the time-consuming work to get there. We get it. That's why we've put together this campaign kit with instructions and content to run your own layered security awareness campaign.

Introducing the Marine Lowlifes

Our campaign theme is, "Marine Lowlifes" — a series of modules, posters and other content that teach your audience about the most dangerous phish lurking in their inboxes. This campaign focuses on the dangers of phishing emails and what your employees can do to identify and avoid these attacks. Along with a full suite of training resources, we've included a communication plan to assist you in executing every step of your campaign.



Download Resource Library

GETTING STARTED

Measure Your Baseline

Before launching your campaign, it's important to record as much baseline data and observations as possible. This gives you the opportunity to measure the impact of your campaign and the behavioral change it inspires.

Quantitative Metrics

Your pre-campaign security awareness metrics depend on your technical security infrastructure and your existing security awareness efforts. Some useful baseline quantitative metrics to consider are:

- Phishing click rate (both real and simulated)
- Phishing report rate (both real and simulated)
- Previous training completion rates
- Security assessment scores
- Number of employee-reported suspicious emails
- Number of employee-reported security incidents
- Number of employee-triggered security incidents (blocked by endpoint protection or security services)

Qualitative Observations

Data-driven metrics are vital to measure the success of your program, but qualitative observations are a valuable resource for evaluating and refining your ongoing efforts. Before launching your campaign, ask yourself:

- What kind of feedback, if any, do you receive about your current security awareness efforts?
- Is cybersecurity a common topic of discussion between employees?
- Do employees feel comfortable asking your team security-related questions or reporting suspicious activity? Do employees know how to report anything suspicious?

Record all of your findings with the intention of measuring and comparing their respective values after the completion of your campaign.

Marine Lowlifes Communication Plan

The following communication plan provides instructions for assembling the 10-week Marine Lowlifes Campaign Kit. This includes download links for all Marine Lowlifes security training and awareness content as well as explicit instructions for how to communicate your message and manage the campaign.

Week 1: Campaign Teaser

Resources

Contest

How Many Malicious Emails Does Our Organization Receive?

Instructions

Running a simple, topical contest is a great way to draw attention to your security awareness initiative, but it also brings the topic of phishing and email security front and center. This contest invites employees to guess the total number of potentially malicious emails your team blocks every month with a prize promised to the employee with the closest guess.

Launching your campaign with a phishing-themed contest provides a jumpstart to employee engagement. However it also presents an approachable way to introduce email security as an individual responsibility and the threat of phishing attacks at your organization.

Utilize Email 1 to launch your contest and Email 2 to announce the winner.

What you need:

- Find the average number of emails flagged as malicious by your email servers each month
- Prize for the winner(s) who comes closest to the actual number

Quick Tip!

Incentives drive engagement. Gift cards and vacation time are always great contest prizes, but even simple prizes like Goldfish crackers or Swedish Fish help improve engagement while reinforcing the campaign's Marine Lowlifes theme.

Email 1

Subject Line: How many phish are in the sea of email?

Instructions

Send Email 1 at the beginning of the week to launch the contest.

Download Email

Poster: Swimming In Emails

Instructions

Identify one or more locations to hang your entire poster series throughout the length of the campaign. Start by hanging the Swimming In Emails poster with the intention of hanging each additional poster beside it as the campaign progresses.

Download Poster

Email 2

Subject Line: [Winners announced] And the winner is...

Instructions

Send Email 2 at the end of the week to announce the contest winner and provide a teaser for your campaign.

Download Email

Week 2: Common Phish (Part 1)

Resources

Email

Subject Line: You've seen it before and you'll see it again

Instructions
Send the Week 2 Email to formally introduce the Marine Lowlifes campaign, the Common Phish and related training resources.

Download Email

Training Module: Common Phish

Instructions
Assign the Common Phish training module in the Week 2 Email.

Download Module

Poster: Common Phish

Instructions
Hang the Common Phish poster by your Swimming In Emails poster in high-traffic areas.

Download Poster

Digital Banner: Common Phish

Instructions
Add the Common Phish digital banner to your Intranet homepage, newsletter or any internal messaging resource.

Download Banner

Quick Tip!

It's important to drive curiosity from the very start of your campaign. Adding a layer of mystery can help. This campaign kit includes new content every week, giving you the chance to tease the following week's topic and keep your employees attention. After hanging the Swimming In Emails poster in week 1, tease the reveal of each subsequent poster with an empty frame or silhouette to build anticipation each week.

Week 3: Common Phish (Part 2)

Resources

Email

Subject Line: What Common Phish wish you didn't know

Instructions
Send the Week 3 Email to provide additional information and tips regarding common phishing attacks and deliver the Common Phish infographic.

Download Email

Infographic: Common Phish

Instructions
In addition to delivering the Common Phish infographic in the Week 3 Email, share it using all of your organization's available internal communication channels.

Download Infographic

Quick Tip!

Don't run your campaign from the outside looking in. While your campaign is running, be sure to track participation, invite feedback and monitor results. Don't be afraid to pivot mid campaign and emphasize the strategies or communication channels driving the most engagement.

Week 4: Spearphish (Part 1)

Resources

Email
Subject Line: It picked you for a reason

Instructions
Send the Week 4 Email to introduce the Spearphish and related training resources.

Download Email

Poster: Spearphish

Instructions
Hang the Spearphish poster by your existing Marine Lowlifes posters in high-traffic areas.

Download Poster

Training Module: Spearphish

Instructions
Assign the Spearphish training module in the Week 4 Email.

Module only available in Infosec IQ

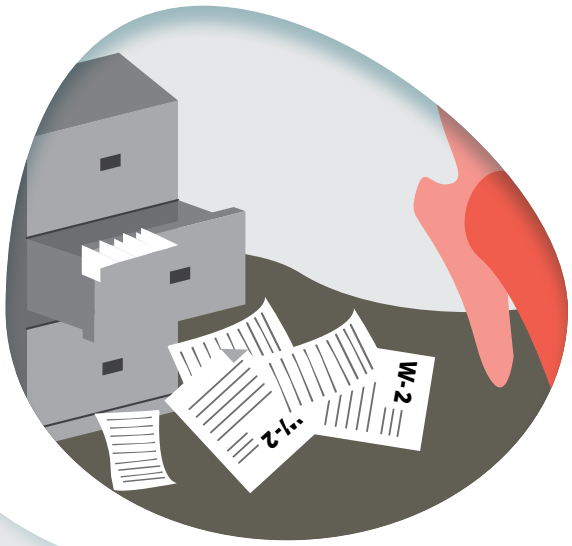
Digital Banner: Spearphish

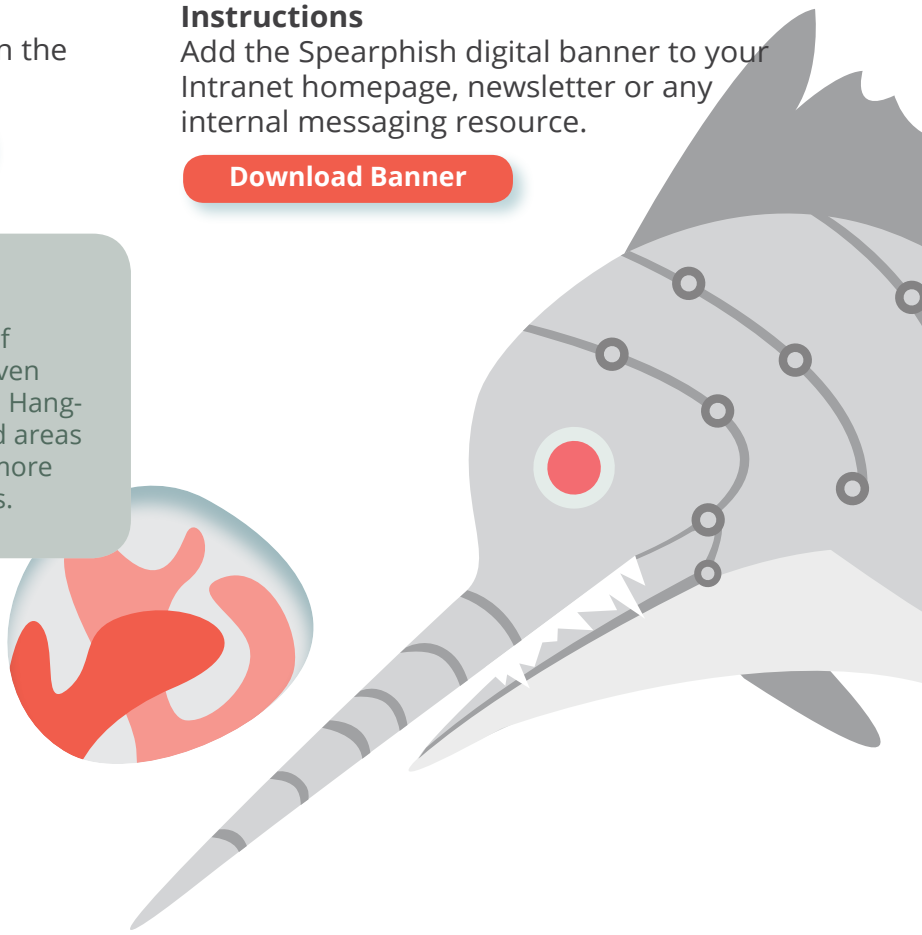
Instructions
Add the Spearphish digital banner to your Intranet homepage, newsletter or any internal messaging resource.

Download Banner

Quick Tip!

Location, location, location. Take advantage of break rooms, common spaces, elevators or even bathrooms to draw attention to your posters. Hanging your posters in the right, heavily trafficked areas or presenting them in a creative way can be more effective than printing out hundreds of copies.





Week 5: Spearphish (Part 2)

Resources

Email
Subject Line: Don't get speared

Instructions
Send the Week 5 Email to provide additional information and tips regarding spearphishing attacks and deliver the Spearphish infographic.

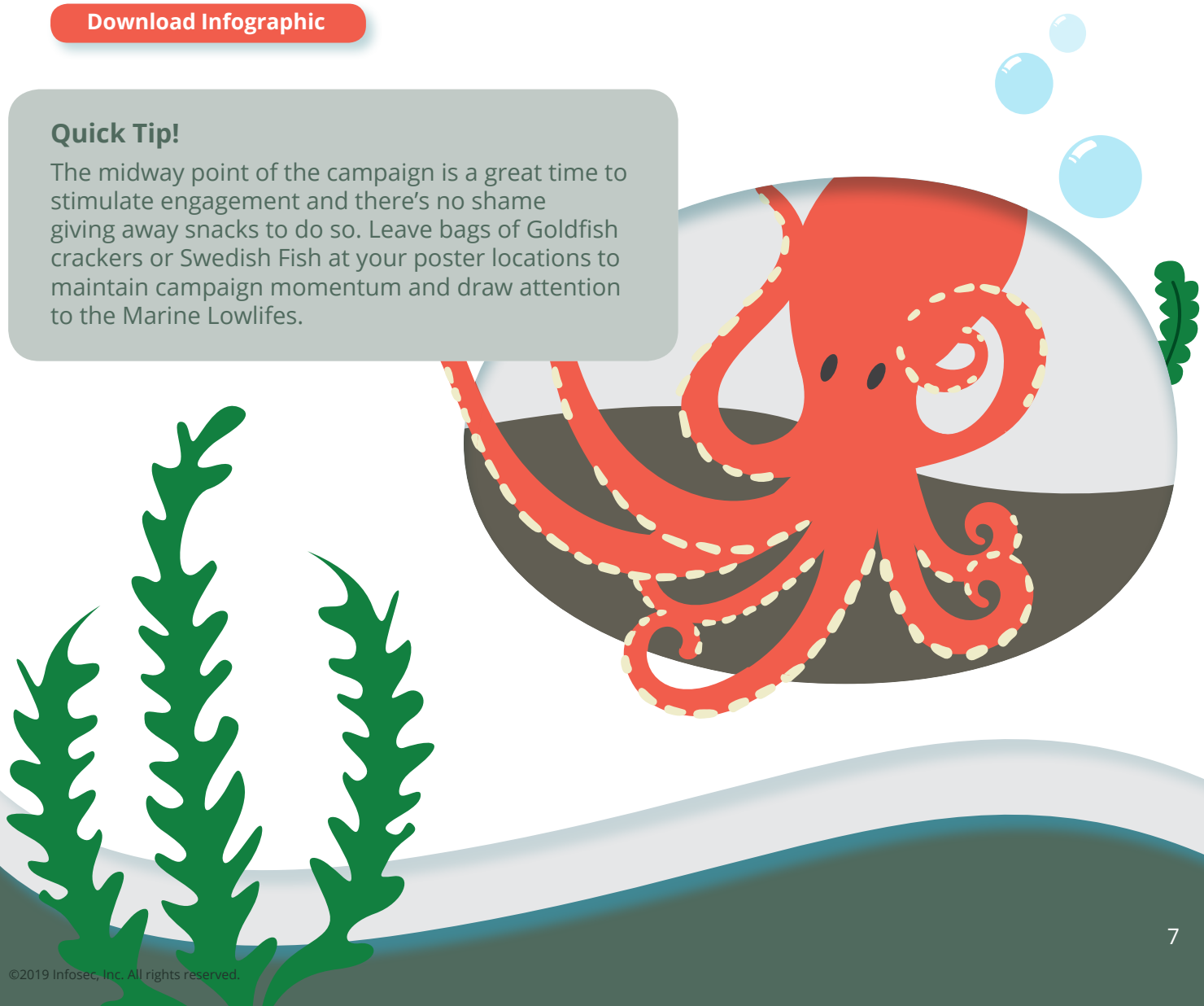
Download Email

Infographic: Spearphish

Instructions
In addition to delivering the Spearphish infographic in the Week 5 Email, share it through your organization's instant messaging app or any other internal communication channels.

Download Infographic

Quick Tip!
The midway point of the campaign is a great time to stimulate engagement and there's no shame giving away snacks to do so. Leave bags of Goldfish crackers or Swedish Fish at your poster locations to maintain campaign momentum and draw attention to the Marine Lowlifes.



Week 6: Whaling Shark (Part 1)

Resources

Email
Subject Line: When a phish becomes a shark

Instructions
Send the Week 6 Email to introduce the Whaling Shark and related training resources.

Download Email

Training Module: Whaling Shark

Instructions
Assign the the Whaling Shark training module in the Week 6 Email.

Module only available in Infosec IQ

Poster: Whaling Shark

Instructions
Hang the Whaling Shark poster by your existing Marine Lowlifes posters in high-traffic areas.

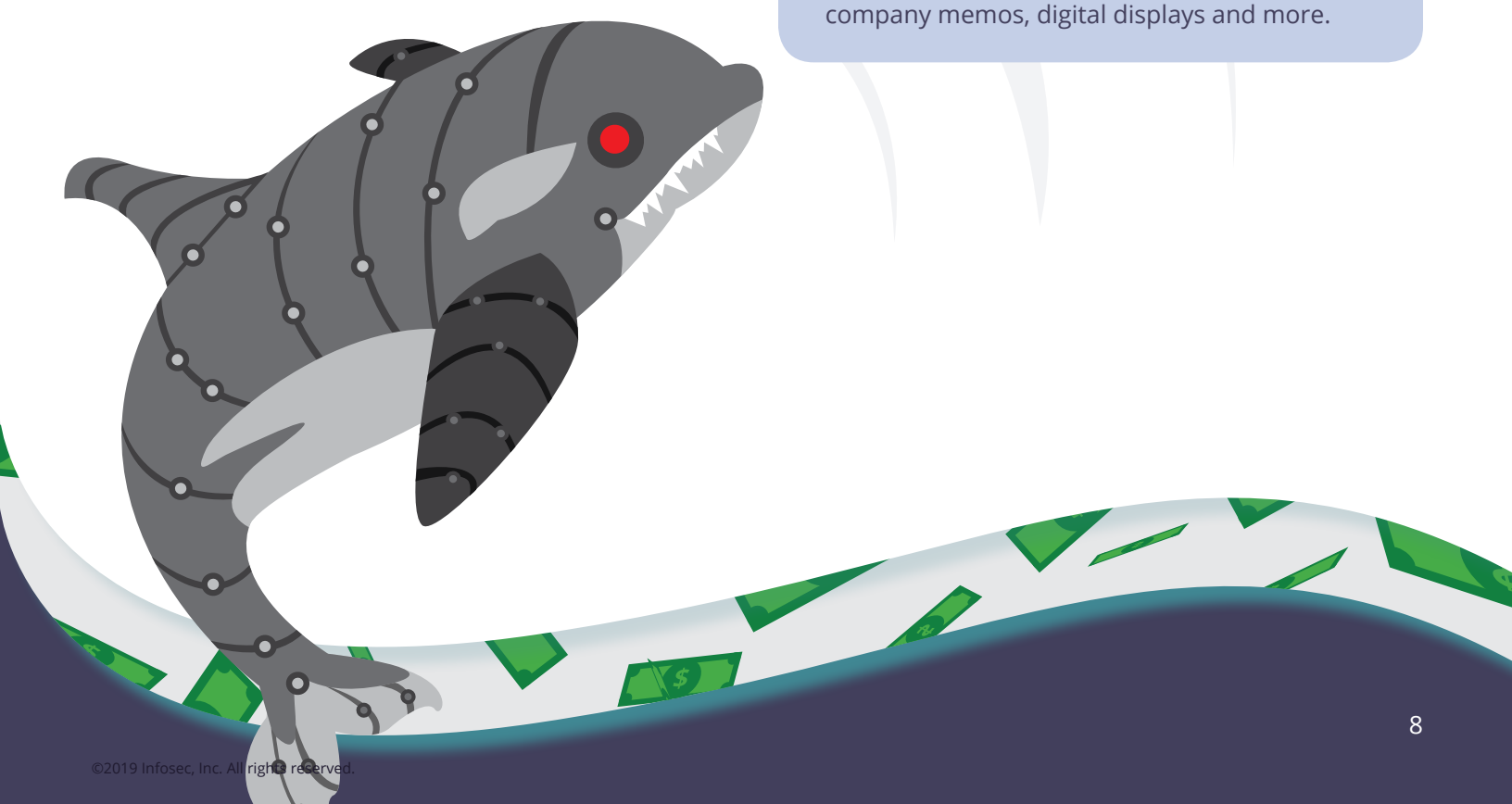
Download Poster

Digital Banner: Whaling Shark

Instructions
Add the Whaling Shark digital banner to your Intranet homepage, newsletter or any internal messaging resource.

Download Banner

Quick Tip!
Successful campaigns utilize every communication channel available to keep a consistent message in front of the audience. Marine Lowlifes-themed digital banners give you the flexibility to add visual reinforcement to internal pages, company memos, digital displays and more.



Week 7: Whaling Shark (Part 2)

Resources

Email

Subject Line: What the Whaling Shark wants

Instructions
Send the Week 7 Email to provide additional information and tips regarding C-Suite phishing attacks and deliver the Whaling Shark infographic.

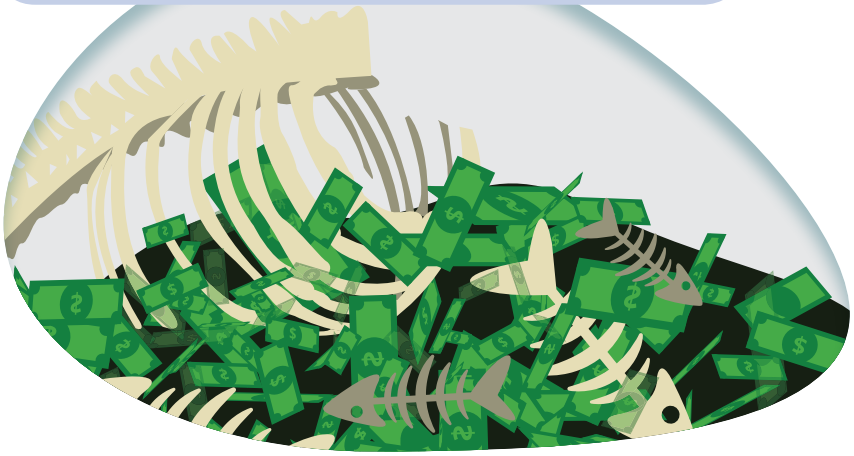
Download Email

Infographic: Whaling Shark

Instructions
In addition to delivering the Whaling Shark infographic in the Week 7 Email, share it through your organization's instant messaging app or any other internal communication channels.

Download Infographic

Quick Tip!
Does your organization use Slack, Microsoft Teams or any other internal chat app? If so, use it to share the infographics. Infographics are the perfect blend of visuals and informative content for group messaging channels.



Week 8: Clone Phish (Part 1)

Resources

Email
Subject Line: The master of disguise

Instructions
Send the Week 8 Email to introduce the Clone Phish and related training resources.

Download Email

Training Module: Clone Phish

Instructions
Assign the Clone Phish training module in the Week 8 Email.

Module only available in Infosec IQ

Poster: Clone Phish

Instructions
Hang the Clone Phish poster by your existing Marine Lowlifes posters in high-traffic areas.

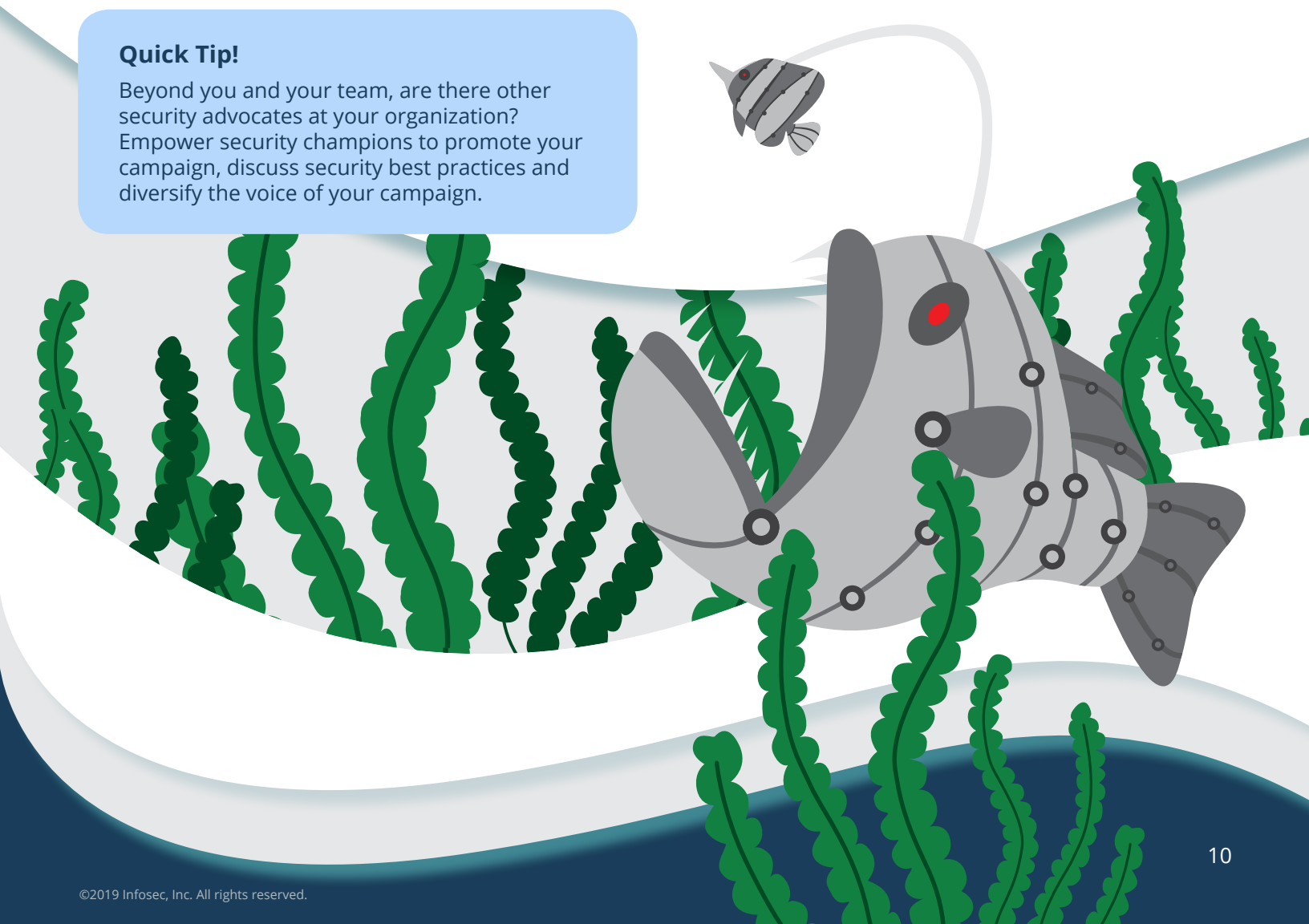
Download Poster

Digital Banner: Clone Phish

Instructions
Add the Clone Phish digital banner to your Intranet homepage, newsletter or any internal messaging resource.

Download Banner

Quick Tip!
Beyond you and your team, are there other security advocates at your organization? Empower security champions to promote your campaign, discuss security best practices and diversify the voice of your campaign.



Week 9: Clone Phish (Part 2)

Resources

Email

Subject Line: Tricks to spot the clever Clone Phish

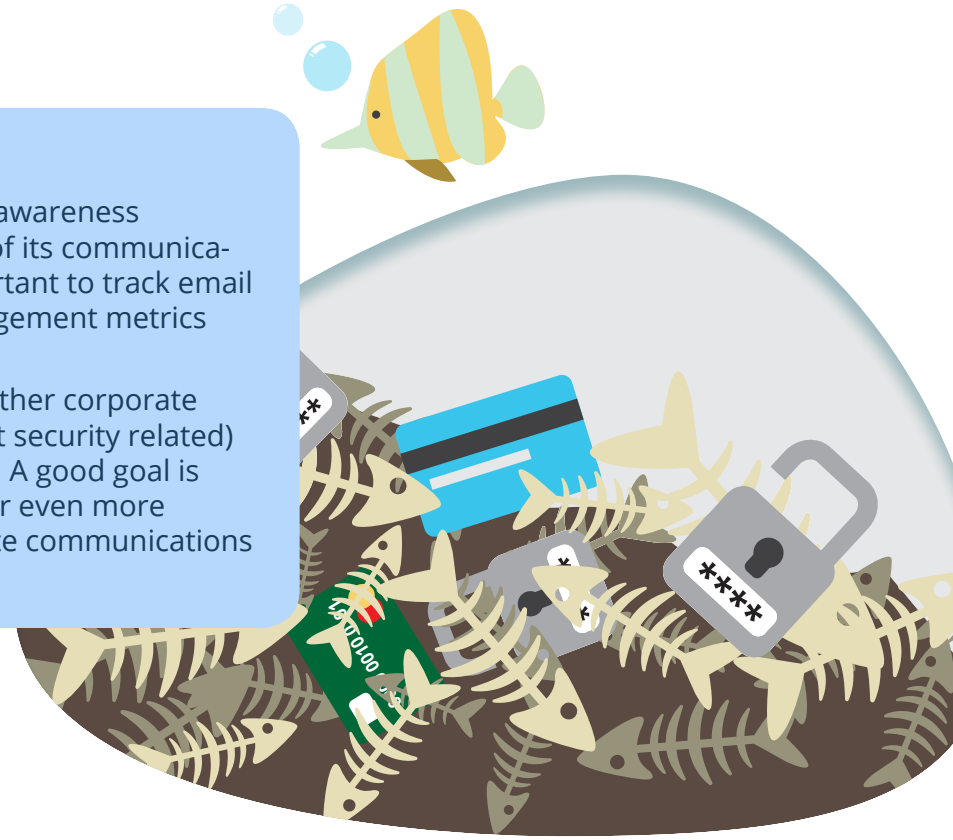
Instructions
Send the Week 9 Email to provide additional information and tips regarding the most well-disguised phishing attacks and deliver the Clone Phish infographic.

Download Email

Infographic: Clone Phish

Instructions
In addition to delivering the Clone Phish infographic in the Week 9 Email, share it through your organization's instant messaging app or any other internal communication channels.

Download Infographic

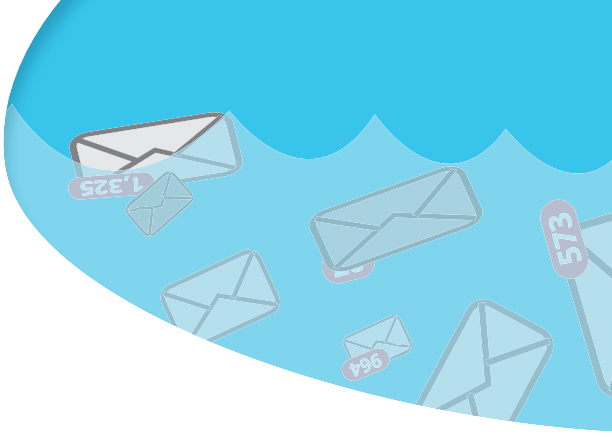


Quick Tip!

The effectiveness of a layered security awareness campaign hinges on the effectiveness of its communication strategy. For that reason, it's important to track email opens, email clicks and any other engagement metrics you have access to.

Comparing those to the metrics from other corporate communications campaigns (that aren't security related) can help you gauge your effectiveness. A good goal is to run a campaign that's as engaging, or even more engaging, than other previous corporate communications campaigns.

Week 10: Campaign Conclusion



Resources

Email

Subject Line: You've conquered the sea of emails!

Instructions

Send the Week 10 Email to emphasize the ongoing need to stay vigilant to spot phishing emails and conclude the campaign.

Download Email

10-Week Communication Calendar

1. **Week 1 Email 1**
   Contest: How Many Malicious Emails Does Our Organization Receive?
   Poster: Swimming in Emails
   Week 1 Email 2
2. **Week 2 Email**
   Training Module: Common Phish
   Poster: Common Phish
   Digital Banner: Common Phish
3. **Week 3 Email**
   Infographic: Common Phish
4. **Week 4 Email**
   Training Module: Spearphish
   Poster: Spearphish
   Digital Banner: Spearphish
5. **Week 5 Email**
   Infographic: Spearphish
6. **Week 6 Email**
   Training Module: Whaling Shark
   Poster: Whaling Shark
   Digital Banner: Whaling shark
7. **Week 7 Email**
   Infographic: Whaling Shark
8. **Week 8 Email**
   Training Module: Clone Phish
   Poster: Clone Phish
   Digital Banner: Clone Phish
9. **Week 9 Email**
   Infographic: Clone Phish
10. **Week 10 Email**

Measuring Campaign Success

After your campaign is complete, it's time to look at the results.

Quantitative Metrics

To start, review all baseline metrics you recorded before launching your campaign.
Your baseline metrics may include:

- Phishing click rate (both real and simulated)
- Phishing report rate (both real and simulated)
- Previous training completion rates
- Security assessment scores
- Number of employee-reported suspicious emails
- Number of employee-reported security incidents
- Number of employee-triggered security incidents (blocked by endpoint protection or security services)

Next, measure these results again to establish the immediate impact of your campaign. This may include running a phishing simulation campaign or distributing a follow-up security awareness assessment.

Even after measuring the immediate results of your campaign, it is important to understand its impact over time. Tracking the same metrics over the long term can show trends and highlight areas for specific improvement with your next simulated phish or future training assignments.

Qualitative Observations

Everybody, including your leadership, loves a good story. Data is important, but having qualitative observations and anecdotes can be really helpful to report alongside your metrics. They help your metrics come to life. After completing your campaign, ask yourself the following questions:

- What feedback or "buzz" did you hear about the campaign?
- What was the most successful aspect of this campaign? Is there some part of the campaign people really enjoyed or engaged with more?
- What would you improve in your next campaign?
- How did this campaign impact the leadership team's opinion on security awareness?

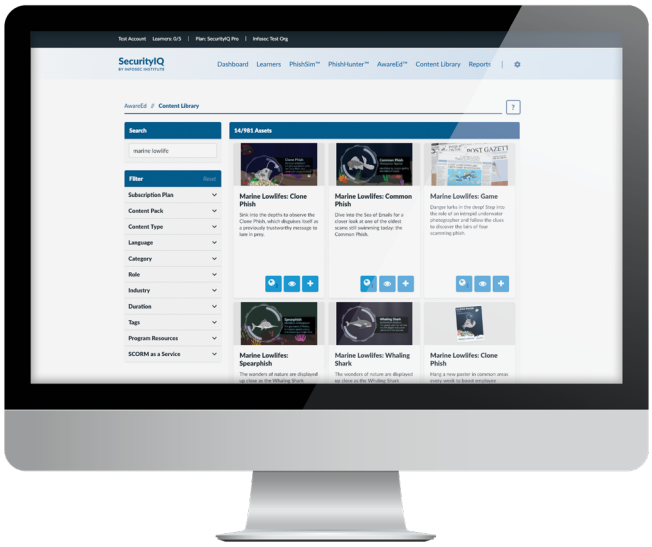
Keeping the Momentum

This campaign kit was designed to help you run a layered security awareness campaign from start to finish, but the job of security awareness and training is never truly finished. New employees join your organization, security threats change and some employees revert to bad security habits. Even after the campaign is complete, keep your security awareness momentum going with new security awareness materials and training exercises. And remember, by providing security awareness resources that your workforce wants to engage with, you can begin to influence the security culture of your organization.

Infosec IQ Security Awareness & Anti-Phishing Training

As security threats continue to evolve, so should your approach to security awareness and training. To spread security awareness and drive employee behavioral change, it takes an integrated approach to engage your workforce.

Infosec IQ is an integrated security training program offering awareness training and phishing simulations with a security awareness content library of 900+ training modules, assessments and reinforcement tools. With a focus on truly engaging content and an integrated, campaign-based approach to security awareness, Infosec IQ isn't just a training delivery platform or a tick for your compliance checkbox. It's an active driver of security awareness and behavioral change designed to help you keep your workforce and organization secure.



Demo Infosec IQ

INFOSEC IQ