Anti-Phishing & Security Awareness Training

SECURITYIQ PROGRAM PLAN

A 12-MONTH PLAN FOR CREATING A CULTURE OF SECURITY AWARENESS.

SecurityIQ
BY INFOSEC INSTITUTE

What's Inside:

Month 0: Establishing Baselines	1
Month 1: Phishing Foundations	3
Month 2: Diving Deeper into Phishing	5
Month 3: Password Security	7
Month 4: Malware	9
Month 5: Social Engineering	11
Month 6: Internet Security	13
Month 7: Phishing Review	15
Month 8: Privacy & Data Security	17
Month 9: Removable Media	19
Month 10: Mobile, Wireless & Remote Access	21
Month 11: Security Awareness Review	23
Month 12: Advanced Security Awareness	25

The SecurityIQ 12-Month Plan is an off-the-shelf solution to comprehensive security awareness training. Developed by InfoSec Institute's team of experienced security education professionals, it will help you achieve program success and phish rates as low as just 1%.

This detailed plan outlines suggested simulations, modules and resources from PhishSim, AwareEd and Security Excellence to grow your team's security awareness. Use the plan as is, or amend it to match your team's individual needs.

INFOSEC
INSTITUTE

866.471.0059 | securityiq@infosecinstitute.com

Month 0: Establishing Baselines

Prior to program launch, we'll establish your team's security awareness baseline using PhishSim, SecurityIQ's phishing simulator. This important indicator is based on your team's phish rate and will be used to track progress overtime.

PhishSim

Your Client Success Manager (CSM) will help you select the right phishing templates for your team and execute the baseline simulation. They'll help you interpret results and make recommendations for next steps based on your organization's level of security awareness. Here's how it works:

1. Create a baseline phishing campaign and enroll all users.
2. Working with your CSM, select phishing templates for your baseline campaign.
3. Review and prepare for campaign launch. We recommend running the baseline campaign unannounced for best accuracy.
4. Run the baseline campaign for all learners. Your CSM will show you how to review results and let you know how your organization's phish rate compares to others in your industry.

AwareEd

After completion of the baseline phishing campaign, we recommend reviewing your 12-month awareness plan with your CSM to confirm selected modules match your team's level of security education.

Security Excellence

Reporting & Client Support

Now that your baseline phishing campaign is complete, we recommend officially announcing the 12-month program to your team. Your Security Excellence Resource Kit is available to assist with team communication.

Internal Communication Resources

- Program Launch Email, Management
- Program Launch Email, General Workforce
- Program Launch Presentation, Management
- Program Launch Presentation, General Workforce

Month 1: Phishing Foundation

In Month 1, we'll introduce foundational security concepts to help learners identify phishing attempts. Phishing campaigns will continue to build overall security awareness, and tools from the Security Excellence Resource Kit may be deployed to reinforce lessons from the modules.

PhishSim

Phishing campaigns will continue in Month 1. Templates may be adjusted for increased difficulty based on results from the baseline campaign.

AwareEd

Foundational Campaign 1

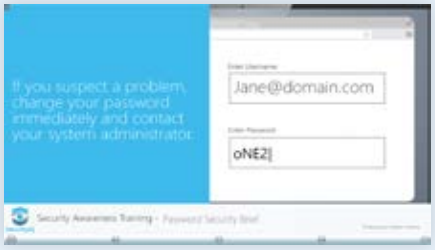
We recommend assigning modules immediately following the baseline phishing campaign. Suggested modules include:

- Program Introduction (5:13 Minutes)
- Phishing Brief, especially for learners phished in the baseline campaign (3:06 Minutes)
- Social Engineering Brief (4:11 Minutes)
- Password Security Brief (4:37 Minutes)

Foundational Campaign 2

The second foundational campaign is an extension of the first. It introduces additional security topics for improved security awareness. Suggested modules include:

- Malware Brief (3:37 Minutes)
- Removable Media Brief (3:20 Minutes)
- Privacy and PII Brief (11:31 Minutes)



Password Security Brief

Removable Media Brief

Security Excellence

Reporting & Client Support

We recommend evaluating the following reports for program assessment:

- PhishSim campaign summary report
- Phished learners report
- Awareness campaign results (participation & completion)

Internal Communication Resources

- Performance Email, Executive
- Performance Email, General Workforce
- Security Awareness Poster: Phishing Attacks
- What's your SecurityIQ? Monthly Newsletter: Phishing Foundations

Month 2: Diving Deeper into Phishing

In Month 2, we'll dive deeper into phishing, introduce new tools like the PhishNotify button and discuss advanced phishing tactics such as spearfishing.

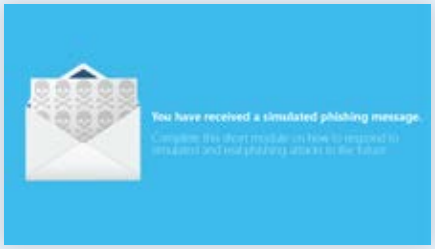
PhishSim

Phishing simulations in Month 2 will increase in difficulty. We'll use personalized templates targeted at specific groups of learners. These templates will closely resemble actual email communications that learners see on a daily basis. The PhishNotify button may also be introduced at this time.

AwareEd

AwareEd modules in Month 2 will build on and reinforce anti-phishing lessons introduced in Month 1. All content will be new for learners who did not get phished during the baseline campaign. Suggested modules include:

- Phishing (20:50 Minutes)
- Suspicious Hosts (3:50 Minutes)
- Spearphishing (2:40 Minutes)
- Reporting Phishing Emails (1:10 Minutes)
- Password Security Brief (4:37 Minutes)



Reporting Phishing Emails

Security Excellence

Reporting & Client Support

We recommend evaluating the following reports for program assessment:

- Custom template phish rates
- Phish rates from Month 1 vs. Month 2
- Number of learners who ran the macro
- Awareness campaign results (participation & completion)

Internal Communication Resources

- Performance Email, Executive
- Performance Email, General Workforce
- Security Awareness Poster: Spearphishing Attacks
- What's your SecurityIQ? Monthly Newsletter: Diving Deeper into Phishing

Month 3: Password Security

In Month 3, we'll introduce password security best practices and test learners' abilities to create strong passwords and keep them secure.

PhishSim

Phishing simulations in Month 3 will include several types of phishing attacks designed to collect user passwords. These include "drive-by" attack emails with links prompting password reset, and data-entry attack emails directing learners to websites requiring password entry. The Password Security Static Education may be used in Month 3.

AwareEd

AwareEd content in Month 3 will show learners how to create complex passwords following best practices for password creation. The module also explains how weak or shared passwords can compromise security. Suggested modules include:

» Password Security (21:16 Minutes)

Password Security

Security Excellence

Reporting & Client Support

We recommend evaluating the following reports for program assessment:

- Custom template phish rates
- Month-over-month phish rates
- Awareness campaign results (participation & completion)

Internal Communication Resources

- Performance Email, Executive
- Performance Email, General Workforce
- Security Awareness Poster: Password Security
- What's your SecurityIQ? Monthly Newsletter: Password Security

Month 4: Malware

In Month 4, we'll discuss malware and ransomware and show learners how hackers can use seemingly harmless email attachments to install malicious software.

PhishSim

Phishing simulations in Month 4 will focus on attachment attacks and "drive-by" attacks that invite learners to download files.

AwareEd

Modules in Month 4 will focus on malware and ransomware to build on lessons learned from earlier phishing simulations. Suggested modules include:

- Malware (17:01 Minutes)
- Ransomware (4:38 Minutes)

Malware

Security Excellence

Reporting & Client Support

We recommend evaluating the following reports for program assessment:

- Training completion vs. phished learners
- Month-over-month phish rates
- Awareness campaign results (participation & completion)
- Individual phish rates (for identifying learners with additional training needs)

Internal Communication Resources

- Performance Email, Executive
- Performance Email, General Workforce
- Security Awareness Poster: Malware
- What's your SecurityIQ? Monthly Newsletter: Malware

Month 5: Social Engineering

Month 5 introduces learners to the concept of social engineering. We'll discuss how social engineering works, how to spot it and what learners can do to prevent social engineering attacks.

PhishSim

In Month 5, learners will receive highly personalized and targeted phishing emails. Simulations will be ran by group type for maximum effectiveness and proper difficulty. Imitating internal communication (or communication with trusted parties) is suggested, as well as using templates that are based on internal and external current events.

AwareEd

AwareEd modules for the fifth month will focus on social engineering techniques. We'll review related risks such as physical security and help desks, a common avenue for social engineering, to teach learners how to prevent hacking attempts. Suggested modules include:

- Social Engineering (12:54 Minutes)
- Physical Security (13:00 Minutes)
- Help Desk (5:00 Minutes)

Social Engineering

Security Excellence

Reporting & Client Support

We recommend evaluating the following reports for program assessment:

- Current template phish rates
- Month-over-month phish rates
- Awareness campaign results (participation & completion)

Internal Communication Resources

- Performance Email, Executive
- Performance Email, General Workforce
- Security Awareness Poster: Social Engineering
- What's your SecurityIQ? Monthly Newsletter: Social Engineering

Month 6: Internet Security

In Month 6, we explore best practices for Internet security and share how safe browsing can help prevent cyberattacks. Risks associated with social media and cloud services will also be introduced.

PhishSim

Phishing simulations in Month 6 will include data-entry attacks using templates mimicking social media and cloud service communications.

AwareEd

AwareEd modules in Month 6 will walk learners through safe web browsing and review the security risks associated with social media and cloud services. Suggested modules include:

- Safe Browsing (10:58 Minutes)
- Social Media (6:14 Minutes)
- Cloud Services (6:53 Minutes)

Safe Browsing

Security Excellence

Reporting & Client Support

We recommend evaluating the following reports for program assessment:

- Current template phish rates
- Month-over-month phish rates
- Awareness campaign results (participation & completion)

Internal Communication Resources

- Performance Email, Executive
- Performance Email, General Workforce
- Security Awareness Poster: Internet Security
- What's your SecurityIQ? Monthly Newsletter: Internet Security

Month 7: Phishing Review

Month 7 will review core phishing content and reinforce key messaging to learners. We'll collect a new organization-wide phish rate to assess progress from the first six months. This month may be modified to include compliance training if required; ask your Client Success Manager for recommended phishing campaigns and modules.

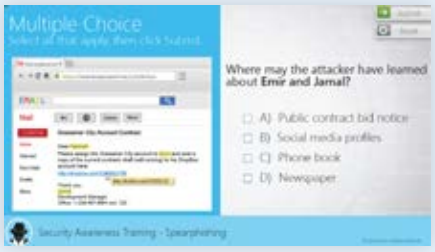
PhishSim

Phishing simulations in Month 7 are designed to reassess phishing awareness across the organization. The original baseline phishing campaign may be rerun, or program administrators can create a new campaign featuring various templates and attack types.

AwareEd

Modules for Month 7 will reinforce key anti-phishing messages with brief phishing-related modules, followed by an assessment module. Suggested modules include:

- Phishing Brief (3:06 Minutes)
- Suspicious Hosts (3:50 Minutes)
- Spearphishing (2:40 Minutes)
- Reporting Phishing Emails* (1:10 Minutes)
- Phishing Assessment - LinkedIn, Capital One (30 Seconds Each)



Spearphishing

* If PhishNotify plugin is used

Security Excellence

Reporting & Client Support

We recommend evaluating the following reports for program assessment:

- Current template phish rates
- Month-over-month phish rates
- Awareness campaign results (participation & completion)

Internal Communication Resources

- Performance Email, Executive
- Performance Email, General Workforce
- Security Awareness Poster: Ransomware Attacks
- What's your SecurityIQ? Monthly Newsletter: Phishing Review

Month 8: Privacy & Data Security

Month 8 focuses on the importance of privacy and data security. Personally identifiable information (PII) will be defined and discussed, and best practices for handling PII in the workplace will be outlined in detail.

PhishSim

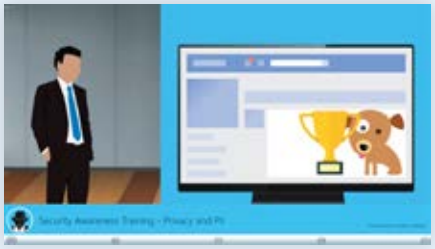
In Month 8, we'll launch targeted data-entry attack campaigns containing suspicious requests for personal information.

AwareEd

This month's modules will contain in-depth review of privacy and data security policies. Topics include best practices for collecting, storing, using, sharing and disposing of personal information. Suggested modules include:

- Privacy and PII (11:31 Minutes)
- Data Security (9:51 Minutes)

Data Retention and Data Destruction modules may be also included (or added as a follow-up or a group-specific campaign) if data security is a key area of focus.



Privacy and PII

Security Excellence

Reporting & Client Support

We recommend evaluating the following reports for program assessment:

- Current template phish rates
- Month-over-month phish rates
- Awareness campaign results (participation & completion)

Internal Communication Resources

- Performance Email, Executive
- Performance Email, General Workforce
- Security Awareness Poster: Privacy & Data Security
- What's your SecurityIQ? Monthly Newsletter: Privacy & Data Security

Month 9: Removable Media

In Month 9, we take an in-depth review of the security risks associated with removable devices. Best practices for device encryption and backup will also be introduced.

PhishSim

This month's phishing campaign will feature templates designed to mimic internal communications. Emails will prompt learners to respond with requests related to backups and file sharing.

AwareEd

Modules in Month 9 will explain the risks associated with removable media, as well as secure use of removable media for backup and sharing. Malware awareness is reinforced in a short module. Suggested modules include:

- Removable Media (10:47 Minutes)
- Malware Brief (3:37 Minutes)

Removable Media

Security Excellence

Reporting & Client Support

We recommend evaluating the following reports for program assessment:

- Current template phish rates
- Month-over-month phish rates
- Awareness campaign results (participation & completion)

Internal Communication Resources

- Performance Email, Executive
- Performance Email, General Workforce
- Security Awareness Poster: Removable Media
- What's your SecurityIQ? Monthly Newsletter: Removable Media

Month 10: Mobile, Wireless & Remote Access

In Month 10, we'll review best practices for working remotely on wireless and mobile networks, and discuss common security threats in mobile and wireless environments.

PhishSim

Phishing simulations in Month 10 will include several targeted campaigns using templates related to mobile devices, wireless networks and remote access security.

AwareEd

Modules in Month 10 discuss security threats in mobile and remote environments. Modules may be adjusted based on organizational needs and policies. Suggested modules include:

- Mobile Security (10:31 Minutes)
- Working Remotely (12:23 Minutes)

Mobile Security

Security Excellence

Reporting & Client Support

We recommend evaluating the following reports for program assessment:

- Current template phish rates
- Month-over-month phish rates
- Awareness campaign results (participation & completion)

Internal Communication Resources

- Performance Email, Executive
- Performance Email, General Workforce
- Security Awareness Poster: Working Remotely
- What's your SecurityIQ? Monthly Newsletter: Mobile, Wireless & Remote Access

Month 11: Security Awareness Review

Month 11 is dedicated to program review. Critical lessons from the program will be reinforced, and phish rates will be reassessed for all learners.

PhishSim

The baseline phish rate will be reestablished in Month 11 for overall program evaluation. This may be accomplished through one campaign for all learners, or through several targeted campaigns featuring all attack types and various template categories.

AwareEd

In Month 11, we'll review key security awareness topics from earlier in the year to optimize retention and create lasting security awareness.

Security Awareness Review Campaign 1

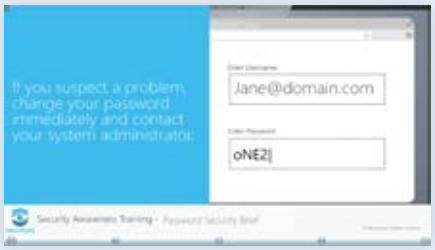
Suggested modules include:

- Phishing Brief (3:06 Minutes)
- Password Security Brief (4:37 Minutes)
- Safe Web Browsing Brief (5:03 Minutes)

Security Awareness Review Campaign 2

Suggested modules include:

- Physical Security Brief (6:06 Minutes)
- Social Engineering Brief (4:11 Minutes)
- Ransomware (4:38 Minutes)



Password Security Brief

Social Engineering Brief

Security Excellence

Reporting & Client Support

We recommend evaluating the following reports for program assessment:

- Current template phish rates
- Month-over-month phish rates
- Awareness campaign results (participation & completion)

Internal Communication Resources

- Performance Email, Executive
- Performance Email, General Workforce
- Security Awareness Poster: Security Incident Reporting
- What's your SecurityIQ? Monthly Newsletter: Security Awareness Review

Month 12: Advanced Security Awareness

Month 12 covers advanced security topics like advanced persistent threats (APTs), insider threats and encryption. Learners will be tested using sophisticated phishing techniques for final evaluation of program impact.

PhishSim

In Month 12, we'll attempt to phish learners using highly sophisticated phishing templates focusing on internal communication.

AwareEd

Modules in Month 12 will include advanced cybersecurity concepts. Role-based security education will be a key area of focus for optimal relevancy and lesson retention. Suggested modules include:

- Advanced Persistent Threat (7:22 Minutes)
- Insider Threats (3:46 Minutes)
- Intelligent Personal Assistant (8:14 Minutes)
- Encryption (5:22 Minutes)

For different roles in the organization, the following modules could be also introduced as additional campaigns:

- Avoiding Cybersecurity Risks for Executives (9:45 Minutes)
- Security Awareness for IT Professionals (10:37 Minutes)
- International Travel Security (7:38 Minutes)

Advanced Persistent Threat

International Travel Security

Security Excellence

Reporting & Client Support

We recommend evaluating the following reports for program assessment:

- Current template phish rates
- Month-over-month phish rates
- Awareness campaign results (participation & completion)

Internal Communication Resources

- Performance Email, Executive
- Performance Email, General Workforce
- Security Awareness Poster: Insider Threats
- What's your SecurityIQ? Monthly Newsletter: Advanced Security Awareness