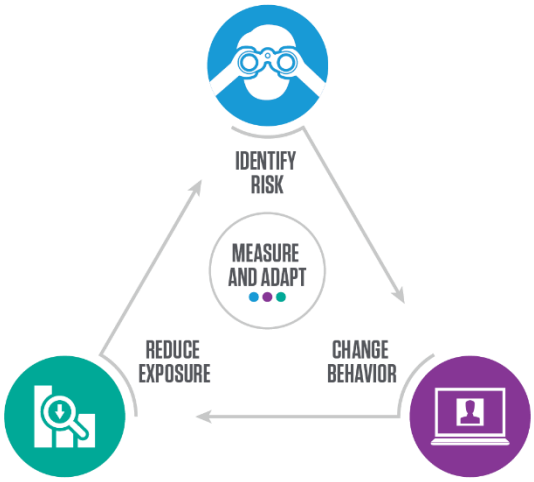
Best Practices for Proofpoint Essentials – Security Awareness

Advice for running your cybersecurity education program

This document provides advice and guidance for using Proofpoint Essentials – Security Awareness to execute a new (or revamped) security awareness training program.

We highlight components and activities related to four key actions:

- Identifying risk
- Changing behavior
- Reducing exposure
- Measuring and adapting



Following, we highlight suggested products and activities within each of the four action categories. These products and actions are then showcased within a recommend two-year calendar that you can use in your planning efforts.

The recommendations you will find in this document are intended to assist your organization with planning, scheduling, and communicating about a new or relaunched security awareness training program. The primary focus is around baseline measurements, fundamental cybersecurity topics, and key learning objectives for users who have had limited or infrequent education about best practices and essential security behaviors.

Identify Risk: ThreatSim Phishing Simulations

Email remains one of attackers' favorite tools for targeting users and infiltrating organizations. **ThreatSim® Phishing Simulations** allow you to gauge your employees' vulnerability to three key threats:

- Embedded links
- Malicious attachments
- Requests for sensitive data

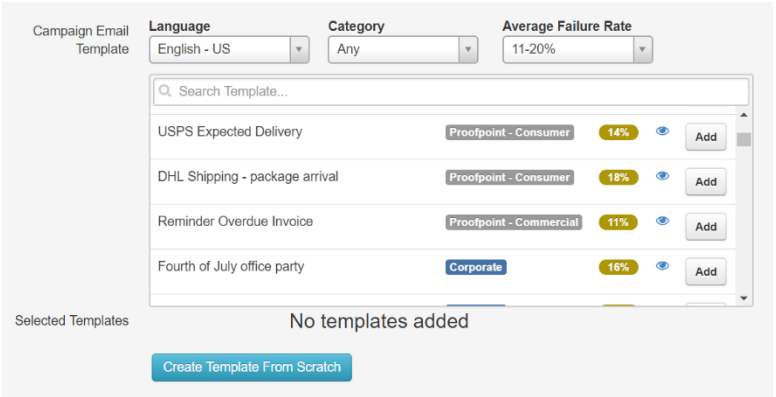
The ThreatSim library includes thousands of customizable templates across more than 35 languages. You can:

- Test employee responses to a variety of lures, including industry-specific communications and perennial threats (like tax and shipping scams).
- Use our Dynamic Threat Simulation phishing templates to send simulated attacks that reflect current lures spotted in the wild by Proofpoint threat intelligence.
- Present a "Teachable Moment" to anyone who falls for one of your tests. These brief, action-oriented landing pages can be delivered to users who engage with simulated phishing attacks. This allows you to provide context for users and raise awareness of anti-phishing behaviors.
- Take advantage of our Auto-Enrollment feature to automatically assign targeted, follow-up training to anyone who falls for a simulated phishing email. Use this feature about once a quarter to deliver appropriate education modules to employees who perform poorly on phishing simulations. (See our recommendations for Auto-Enrollment in the suggested schedule later in this document.)

How to Use Phishing Simulations

Before you formally launch your phishing assessments, send a test simulation to a small group of "in-the-know" members of your organization. This will help you identify any potential technical hurdles before sending a broader test.

When you're ready to launch, we recommend sending a "blind" phishing simulation to establish a baseline vulnerability measurement. What we mean by "blind" is that no "obvious" Teachable Moment or training assignment is attached to the phishing simulation, so the user doesn't know they've been sent a test. Instead, opt for an "Error Message" Teachable Moment, which resolves to a browser error window. Blind phishing tests help to eliminate crosstalk (or the so-called "prairie dog effect") among users, giving you the best opportunity for a reliable measurement.



A portion of the ThreatSim administrator interface

Your baseline test should be of moderate difficulty; essentially, you want to send a simulated attack that you believe a trained user would recognize to be dangerous. Following that, we recommend that you:

- Run phishing simulations every four to six weeks, and mix it up: use different threats, themes, and lures. Collaborate with email and messaging teams so you can identify templates that correspond to the threats your organization is facing.
- Start with relatively "easy" tests and progress to more difficult tests as your users' abilities improve. Refer to the following section to learn more about average failure rates (AFRs), and look for those details within the ThreatSim interface to help you choose the right tests at the right time.
- Use Auto-Enrollment on three or four tests a year. Choose training that aligns with the test you sent (for example, if you sent a link-based simulated attack, assign our Avoiding Dangerous Links module).
- Require users to complete follow-up training assignments within one week. This ensures that users will connect the dots between the simulated attack, the mistake they made, and the actions that will help them avoid real phishing messages.
- Let end users know that they may see brands from well-known companies in your phishing exercises in order to effectively simulate real-world attacks. Instruct users to report suspicious messages to your IT security team rather than reaching out directly to external companies and brand owners.

Examples of Simulated Phishing Templates

Template AFRs can help you determine the relative difficulty rating of individual phishing tests. These pieces of information, along with previous results, can help guide you as you plan and execute your program.

For your reference, Table 1 highlights a small selection of templates available within the ThreatSim platform. We generally gauge difficulty ratings based on the following percentages:

- Easy: 0-10% AFR
- Medium: 11-20% AFR
- Hard: 21% and higher AFR

Template Name	Description	Difficulty Rating	AFR[1]
Benefits Enrollment Update	Asks recipient to log into account to accept new privacy policies (credential phishing/data entry template)	Easy	7%
Jump in This Quick Meeting	Requests that employee join a call using the provided link (link-based template)	Easy	9%
DocuSign Document	Presents a document to electronically review and sign (credential phishing/data entry template)	Medium	13%
Voicemail Alert	Prompts recipient to click a link to listen to a new voicemail message (link-based template)	Medium	18%
Xerox Scanned Document	Prompts recipient to download a scanned document sent from a Xerox printer (attachment-based template)	Medium	19%
Code of Conduct – Reported Incident	Claims a code of conduct incident has led to terminations and asks employees to click to review the incident report and company code of conduct (link-based template)	Hard	22%
ADPayroll Invoice	Prompts the recipient to review a payroll invoice for the prior week and to call the number on the invoice with any questions (attachment-based template)	Hard	41%

Table 1: Examples of ThreatSim phishing templates

Change Behavior: End-User Training

Don't mistake it: behavior change should be the primary goal for your security awareness training program. You want users to break bad habits and learn new skills (and how to apply them) in general. But you also want to address risky behaviors that are most likely to impact your organization's mission.

It's why education activities logically follow the vulnerability assessments outlined in the "Identify Risk" section. Awareness and training are two different things: knowing that a threat exists is not the same as knowing how to detect and deal with the threat when it presents itself. Education leads to behavior change—and a stronger last line of defense. Training will help your organization reduce its exposure to user-driven cybersecurity threats.

To effectively and efficiently change employee behaviors, our Essentials bundle allows you to deliver a combination of:

- Broad, organization-wide training
- Targeted, threat-based training

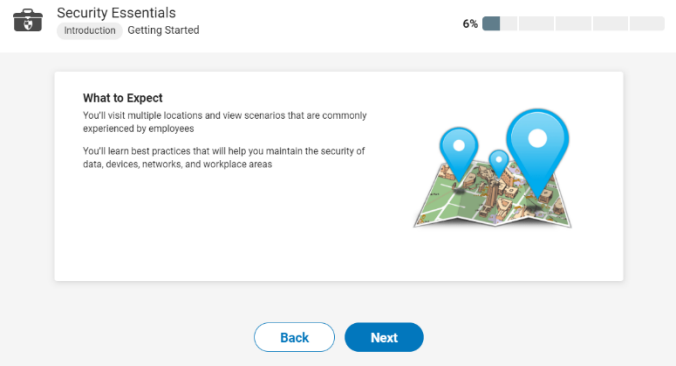
[1] AFRs can fluctuate over time based on frequency and volume of usage among our customers. The AFRs noted in the table were based on data available in February 2020. Your organization's AFRs may vary from those identified within ThreatSim, depending upon the education level of the end users being tested and any edits made to a template prior to its use.

Broad, Organization-Wide Training

The Proofpoint training approach is rooted in learning science, applying key principles that facilitate adult learning and knowledge retention. Our tools can help you build a strong cybersecurity foundation across your organization—and build on that foundation over time. We offer localized content in more than 35 languages and help you deliver training across a range of cybersecurity topics.

In the suggested schedule later in this document, you will see recommended organization-wide training assignments for the following courses:

- Security Essentials
- Email Security
- Introduction to Phishing
- Mobile Device Security
- Password Protection Series (4 modules)
  - Beyond Passwords
  - Multi-Factor Authentication (MFA)
  - Password Management
  - Password Policy
- Safe Social Networking
- Safer Web Browsing
- Social Engineering



A portion of our Security Essentials training

Threat-Based Training

With the changing threat landscape—and the variety of ways threat actors target individual organizations—it's critical to keep users in tune with emerging threats. The vulnerabilities you identify during phishing simulations and the review of threat reports should guide your threat-based training choices.

In the suggested program schedule later in this document, you will see recommendations for using our Auto-Enrollment feature within ThreatSim to automatically assign the following mini-modules from our "Securing Your Email – Fundamental" series to individuals who fall for email-based phishing tests:

- Avoiding Dangerous Attachments
- Avoiding Dangerous Links
- Data Entry Phishing

Reduce Exposure: End-User Reporting and Verification

You cannot stop all cybersecurity attacks and issues from reaching your employees' inboxes and devices. But developing a "see something, say something" policy within your organization can help reduce your exposure to active attacks. We recommend taking the following key actions within your organization:

- Work with your organization's IT resources to develop procedures users can follow to report suspicious emails, websites, on-site activities, and other physical and cybersecurity risks.
- Institute a verification procedure for all payment requests (including wire transfers) and transfers of sensitive data.
- Clearly communicate policies and procedures to users, and provide written/visual references for them when possible. And regularly remind users about the importance of reporting suspicious activities and following verification procedures.

Measure and Adapt: Business Intelligence

Measurement should be an ongoing component of your security awareness training program, and it should happen regularly. In the schedule below, you will see suggestions for using the reports within your Essentials toolkit to share your findings with key stakeholders in your organization (including your end users). Use the reports within your Essentials toolkit to:

- Evaluate progress
- Gauge ROI
- Benchmark, track, and trend user knowledge

Suggested Schedule

Following is a suggested schedule for implementing a security awareness training program using the Essentials toolkit. Though we offer specific advice on which training modules to deliver and when, we expect you will adjust this schedule based on your risk analysis and available resources.

2 months before program officially launches to end users	• Send a test phishing simulation to a small group of "in-the-know" members of your organization to identify any potential technical hurdles before sending a broader test. • Send your baseline phishing test. – This test should be "blind" — no "obvious" Teachable Moment or training assignment should be attached to the test. Instead, opt for a browser error Teachable Moment. – Your goal: users should not know they've been sent a test so you can get a "pure" baseline vulnerability measurement. – Choose a simulated attack that is of moderate difficulty (essentially, a message you believe a trained user would recognize to be dangerous).

1 month before program launches to users	*First week*
	• Announce your forthcoming cybersecurity awareness training program to end users.
	  – If possible, host a formal kick-off event within your organization, like a pizza lunch or coffee-and-donuts breakfast get-together.
	  – Note that your initiative will officially launch the following month.
	  – Explain that you'll be using a mix of phishing tests and training sessions.
	  – Let end users know that they will see brands from well-known companies in your phishing exercises in order to effectively simulate real-world attacks. Instruct users to report suspicious messages to your IT security team rather than reaching out directly to external companies and brand owners.
	Week 2-4
	• Share your policies and procedures for reporting suspicious activities and verifying payment/data requests.
	• Post copies of new policies and procedures in common areas or individual users' workspaces.
	• Consider using a "test" message (sent via ThreatSim) to help users practice your procedures for reporting suspicious emails.

Month 1	**Month 2**	**Month 3**	**Month 4**
Day 1 Send a welcome email to all users and include a link to their first training assignment: **"Security Essentials" and "Introduction to Phishing"** (to be completed in 30 days)	Send a **link-based phishing test** Auto-enroll vulnerable users in the "**Avoiding Dangerous Links" training** (to be completed in one week)	Send a **data entry/credential phishing test**	Assign **"Email Security" training** to all users (to be completed in 30-60 days)
Month 5	**Month 6**	**Month 7**	**Month 8**
Send an **attachment phishing test** Host cyber Q&A and/or lunch-and-learn sessions (if resources allow)	Send a **data entry/credential phishing test** Auto-enroll vulnerable users in **"Data Entry Phishing" training** (to be completed in one week)	Assign **"Password Policy" and "Multi-Factor Authentication (MFA)" training** (to be completed in 30-60 days) Provide a **status update** to management and end users	Send a **link-based phishing test**

Month 9	Month 10	Month 11	Month 12
Send an **attachment phishing test** Auto-enroll vulnerable users in **"Avoiding Dangerous Attachments"** training (to be completed in one week)	Assign **"Mobile Device Security" training** (to be completed in 30-60 days)	Send a **link-based phishing test**	Send an **attachment-phishing test** Host cyber Q&A and/or lunch-and-learn sessions (if resources allow)
Month 13	**Month 14**	**Month 15**	**Month 16**
Early in the month, repeat a blind phishing test to gauge overall progress Late in the month, assign **"Safer Web Browsing" training** (to be completed in 30-60 days)	Send a **data entry/credential phishing test** Provide a **status update** to management and end users	Send a **link-based phishing test** Auto-enroll vulnerable users in **"Avoiding Dangerous Links" training** (to be completed in one week)	Assign **"Social Engineering" training** to all users (to be completed in 30-60 days)
Month 17	**Month 18**	**Month 19**	**Month 20**
Send an **attachment phishing test**	Send a **link-based phishing test** Host cyber Q&A and/or lunch-and-learn sessions (if resources allow)	Assign **"Beyond Passwords" and "Password Management" training** to all users (to be completed in 30-60 days)	Send a **data entry/credential phishing test** Auto-enroll vulnerable users in **"Data Entry Phishing" training** (to be completed in one week)
Month 21	**Month 22**	**Month 23**	**Month 24**
Send a **link-based phishing test**	Assign **"Safe Social Networking" training** to all users (to be completed in 30-60 days Provide a **status update** to management and end users	Send a **link-based phishing test** Host cyber Q&A and/or lunch-and-learn sessions (if resources allow)	Send an **attachment phishing test** Auto-enroll vulnerable users in **"Avoiding Dangerous Attachments"** training (to be completed in one week)

Points to Keep in Mind

- Though we have been prescriptive in our advice, your assessments and your organization's experiences and resources should guide your training choices and program cadence. For example, if you uncover a widespread cybersecurity issue within your organization, prioritize organization-wide training about that issue over the training assignments we've recommended in the schedule.
- We recommend organizing cybersecurity activities during Security Awareness Month each October. Be creative in your planning. You can find additional free resources and advice at Proofpoint.com.
- For an adjustable, color-coded schedule that coincides with the above schedule, look for the scheduling tool PowerPoint file in the Essentials portal.