Getting Started

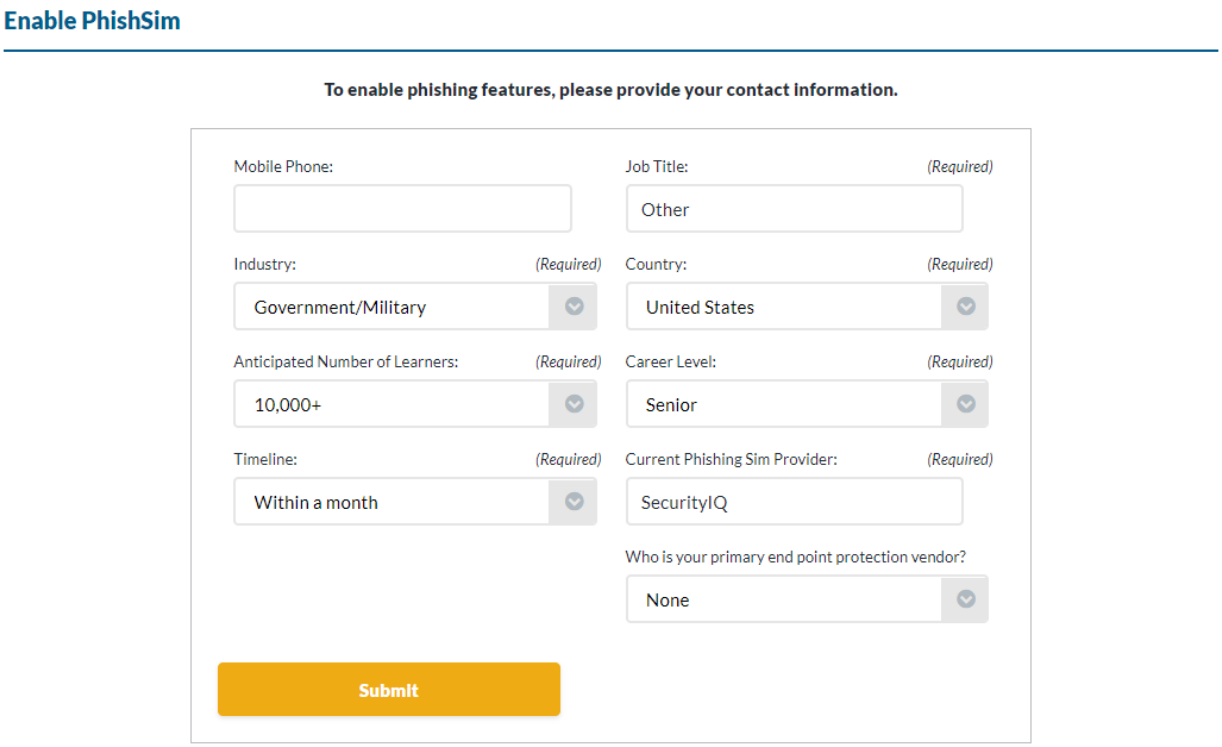
TABLE OF CONTENTS

INITIAL SET-UP

BECOMING AN ACCOUNT ADMINISTRATOR

In order to get access to the Infosec IQ platform, one must be set-up as an Account Administrator. If you haven't already, you should be receiving an email from: no-reply@securityiq-notifications.com (see image below)

Upon receiving the email, please select "Create Your SecurityIQ Account" and complete the required fields to get your username and password set up. Please note that your username must be your work email. Once registered, you will be taken to an "Enable PhishSim" page where it will ask you for additional information to gain access to the platform. Please complete the form as followed:



ADDING AND MANAGING LEARNERS

To enroll employees in different simulated phishing and interactive training campaigns, they must become a learner in the platform. There are three ways to upload learners into the platform:

- Syncing with Active Directory
- Uploading a CSV File
- Manually adding the learner(s)

ACTIVE DIRECTORY

To download and configure your Active Directory/Infosec IQ sync, navigate to **Active Directory Synchronizer** under the **Learners** tab.

Once on that page:

1) Copy the **Secret Key** that is specific to your account.
2) **Download** the compressed zip-file that contains all the tools needed to complete the synchronization.
3) Check the **Override safety switch on next sync** box and hit **save.**

Complete step-by-step instructions: https://infosec.force.com/ISIcommunity/s/article/learners-ad-sync#learner-adsync-intro

CSV UPLOAD

To import new learners or update existing learners utilizing a CSV file, navigate to **Import** under the **Learners** tab.

On this page, download the "Sample CSV File" and enter in all the information needed in the Required Columns:

- First Name
- Last Name
- Email

You can also include additional information in the optional columns. We recommend adding as much information for the learner as possible, as this will help build out different groups and pull reports in the future. In addition, all of the headers must remain in place for the upload to be successful.

GROUPS

An Account Administrator can organize learners into groups to schedule them in campaigns and to pull reports. There are two different types of groups that are available in the Infosec IQ platform: **Static** and **Dynamic**. Groups can get created when uploading learners, or they can be created and managed by navigating to **Groups** under the **Learners** tab.

STATIC GROUPS

Static Groups in Infosec IQ can manually be updated by adding and removing learners to that group. They can also get created during the Active Directory Synchronization or CSV process. An Account Administrator can create static groups by selecting **Static** under **New Learner Group.**

DYNAMIC GROUPS

Dynamic Groups will automatically add/remove learners to and from the group based on a set of criteria selected. Account Administrators can select different fields based off attributes and/or actions that they would like the group to be populated with.

Use the link below to view a collection of dynamic groups that other Infosec IQ customers have found useful: https://infosec.force.com/ISIcommunity/s/article/Useful-groups

WHITELISTING

Whitelisting is required to ensure that our PhishSim phishing simulation emails are successfully delivered to your learners' inbox. Our IP addresses and domains are not published anywhere in our public documentation. You must first log in to your Infosec IQ account and go to the account settings to view the list of available IP addresses and domains required. The whitelisting must be done on your email server and any other security appliance you may have in front of the email server.

Use the link below to view full step-by-step instructions:
https://infosec.force.com/ISIcommunity/s/article/settings-whitelisting

UPDATING AND MANAGING YOUR ACCOUNT SETTINGS

CUSTOMER NAME AND EMAIL

This section allows you to change your customer name and email as it will appear across the Infosec IQ platform and within notifications sent to your learners. These fields can be used as variables using the {{customer email}} and {{customer name}} within email and notification templates.

ADDING STATE SEAL LOGO OR DEPARTMENT LOGO

You can use your company logo to customize your Infosec IQ platform. Learners will see your company logo when they receive a notification, are in a learning module, or on a landing page.

Use the link below for step-by-step instructions:
https://infosec.force.com/ISIcommunity/s/article/settings-branding

ADDING ADDITIONAL ACCOUNT ADMINISTRATORS

You can add more Account Administrators to your Infosec IQ account using the **Account Administrators** section.

Use the link below for step-by-step instructions:
https://infosec.force.com/ISIcommunity/s/article/settings-administrators

ADDING REPORT RECIPIENTS

Adding a Report Recipient will allow you to send reports and analytics to emails that you have specified. People listed as a Report Recipient will not have administrative access to the platform.

SUPPRESSING THE FOOTER

The footer is included in every email template as the {{footer}} variable and includes text which indicates that the email is a simulation and comes from Infosec IQ. If the footer is not suppressed, it will look like the image below.

To suppress the footer, please follow the steps listed in the link below in the **Add Your Organization's Domain** section:

https://infosec.force.com/ISIcommunity/s/article/phishsim-settings

CAMPAIGN CREATION

PHISHSIM

PhishSim campaigns allow you to schedule and send phishing emails to Infosec IQ learners. You can control who receives the emails, the specific emails that are sent and how the campaign will behave.

EMAIL TEMPLATE CREATION

To access a complete list of our customizable email templates, navigate to **Email Templates** located under **PhishSim**. Once on the email template page, you can preview and modify existing email templates. You can also build email templates from scratch or using the source code from an email in your inbox. To learn more about our WYSIWYG template editor, visit:

https://infosec.force.com/ISIcommunity/s/article/Email-Templates-Editor

BATTERIES

Batteries are collections of email templates that are used to charge your PhishSim campaign. There are several default batteries included with your Infosec IQ platform. To view and create new batteries, navigate to **Batteries** under **PhishSim**. To learn more about batteries, and how to build them, visit:

https://infosec.force.com/ISIcommunity/s/article/phishsim-batteries#phishsim-batteries-intro

SCHEDULING CAMPAIGNS

To begin creating a campaign, navigate to **Campaigns** under the **PhishSim** tab and follow the instructions provided in the link below:

https://infosec.force.com/ISIcommunity/s/article/phishsim-campaigns#phishsim-campaign-intro

AWAREED

AwareEd campaigns allow you to schedule awareness training for your organization by combining courses and notifications. You can customize campaigns to change the type, topic and duration of trainings your learners participate in.

NAVIGATING THE CONTENT LIBRARY

Our Content Library contains all the interactive modules and assessments that are available. On this page you can filter on Language, Content Type, Category, Role, Industry, Duration, Tags, Program Resources, and those that are available in SCORM.

COURSES

Courses allow you to create different collections of training assets which can then be assigned to different groups of learners using campaigns.

To view existing courses, navigate to **Courses** under the **AwareEd** tab. You can create a new course in our Content Library by following the instructions provided in the link below:
https://infosec.force.com/ISIcommunity/s/article/awareed-courses#awareed-courses-intro

---

SCHEDULING CAMPAIGNS

To view and modify existing campaigns, as well as customize your own, navigate to **Campaigns** under the **AwareEd** tab. Use the link below to walk you through how to launch a campaign:
https://infosec.force.com/ISIcommunity/s/article/awareed-campaigns#awareed-campaigns-intro

REPORTING

The Infosec IQ Analytics component provides you with the ability to pull and combine specific data points from your Infosec IQ platform.

TYPES OF REPORTS

CAMPAIGN REPORTS

After you have launched the campaign, you can get real-time campaign information by selecting the **Details** option when hovering over the campaign name. From there, select the bar graph on the right-hand side for the campaign run you are interested in. On this page, you will get an overview of who has been phished, who reported the attack using the PhishNotify plugin, etc. To download the information on this page, simply select the **download** button next to the **Phish Rate** percentage:

Campaign Run Details

Run	Status	Start	End	Length	Learners	Templates	Open Rate	Phish Rate	
1	Complete	05/18/2018	05/18/2018	0 Days	1	3	100%	100%	

AUTO REPORTS

Auto Reports are automatically generated for all AwareEd and PhishSim campaigns that are created in Infosec IQ. These reports will provide you with detailed information about the campaigns which you have scheduled/run. Auto Reports will be automatically removed upon the deletion of a corresponding campaign.

Navigate to **Auto Reports** under the **Reports** tab to see a list of the existing Auto Reports.

DATA BROWSER

The Infosec IQ platform provides the ability to create custom reports through the Data Browser page. The Data Browser functionality can be used to present filtered data points (for Learners, Groups, Timeline or Phishing Attempts) in a spreadsheet format to make reports to meet your specific needs. To create a Data Browser Report, navigate to **Data Browser** under the **Reports** tab. For more information on Data Browser Reports, follow the link provided below:
https://infosec.force.com/ISIcommunity/s/article/analytics-data-browser#analytics-databrowser-intro

HELPFUL RESOURCES AND TOOLS

User Manual: https://infosec.force.com/ISIcommunity/s/
How-to Videos: https://infosecinstitute.wistia.com/projects/nze2trlncp