SecurityIQ Implementation

Part 1

SecurityIQ
BY INFOSEC INSTITUTE

Agenda

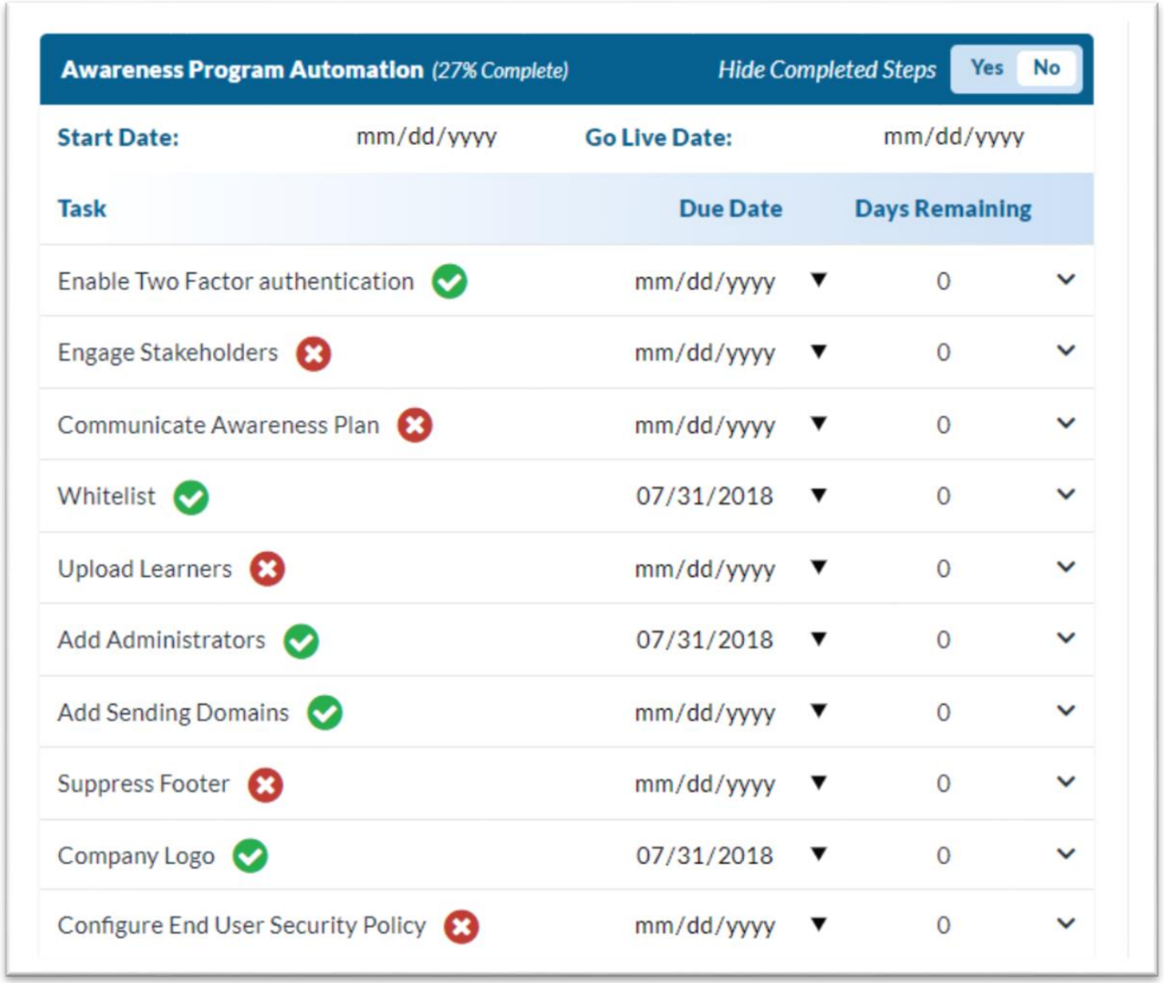
Thank you for your recent investment in our SecurityIQ Program. Before rolling out your first campaign, you will need to:

- ❑ Add learners into the platform
- ❑ Whitelist Email Stack
- ❑ Customize Account Settings
  - Update User Information
  - Add Logo
  - Add Account Administrators
- ❑ Add Domains and Suppress Footer
- ❑ Deploying PhishNotify

Awareness Program Automation

Once you have created your account in SecurityIQ and login, you will first see your account's Dashboard. The "Awareness Program Automation" section will assist you not only during your implementation, but throughout your lifespan with SecurityIQ.

For each of these tasks listed, you are able to drill down for more information as well as mark them as complete. There are a couple items that will automatically be marked as complete, as you start completing different actions in the platform.



Awareness Program Automation *(27% Complete)* *Hide Completed Steps* Yes No

Start Date: mm/dd/yyyy **Go Live Date:** mm/dd/yyyy

Task	Due Date	Days Remaining	
Enable Two Factor authentication ✓	mm/dd/yyyy ▼	0	⌄
Engage Stakeholders ✗	mm/dd/yyyy ▼	0	⌄
Communicate Awareness Plan ✗	mm/dd/yyyy ▼	0	⌄
Whitelist ✓	07/31/2018 ▼	0	⌄
Upload Learners ✗	mm/dd/yyyy ▼	0	⌄
Add Administrators ✓	07/31/2018 ▼	0	⌄
Add Sending Domains ✓	mm/dd/yyyy ▼	0	⌄
Suppress Footer ✗	mm/dd/yyyy ▼	0	⌄
Company Logo ✓	07/31/2018 ▼	0	⌄
Configure End User Security Policy ✗	mm/dd/yyyy ▼	0	⌄

Adding Learners

- Active Directory Sync: This is the recommended way to upload leaners into the SecurityIQ platform. To access our Active Directory tool:
  - Login to SecurityIQ
  - Hover over Learners and select “Active Directory Synchronizer”
  - Download the Compressed Zip file to access the Import Tools and Instructions
  - To access instructions with screen shots follow link below: https://resources.infosecinstitute.com/securityiq-awareed-and-phishsim-users-manual-pt-3-learners-groups/#LearnersandGroups_ActiveDirectorySynchronizer_ActiveDirectorySynchronizer

- CSV file: This is recommended if you are unable to use our Active Directory tool. Please use the sample CSV file found under Learners > Import to ensure that all of the columns and data are formatted correctly for the import.

Whitelisting

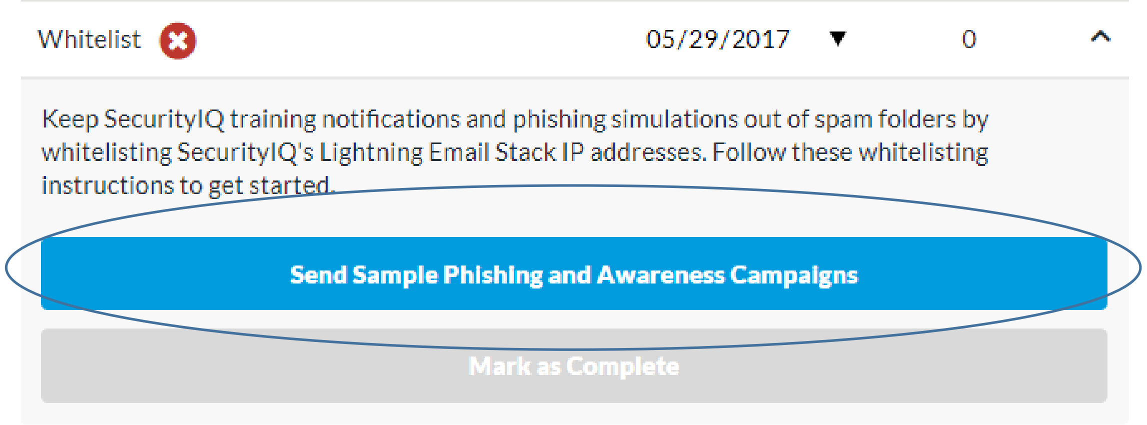
In order to prevent our PhishSim and AwareEd emails, including Training Notifications, from being blocked or filtered into your spam folder you will need to whitelist our Email Stack.

To access the IPs/Domains/Headers:

1. Login to SecurityIQ
2. Access your Account Settings by clicking the settings gear in the top right corner
3. Once in your Account Settings, scroll down to the bottom and locate the Email Stack section on the left-hand side - *Please make sure that "lightning stack" is selected and saved*
4. Once the Whitelisting is Complete, we will need to run a quick campaign to test that the emails will arrive in the inbox. Please see slide 6 for instructions on how to set this up

Whitelisting Test

For this, you will need to navigate to your SecurityIQ Dashboard. On the Dashboard, please locate the “Whitelist” task under the Awareness Program Automation Section and drill down:



Keep SecurityIQ training notifications and phishing simulations out of spam folders by whitelisting SecurityIQ's Lightning Email Stack IP addresses. Follow these whitelisting instructions to get started.

In this section, you are able to send out a sample phishing and awareness training campaign to yourself. You will receive the default enrollment notification for AwareEd and three different PhishSim Email templates: Amazon, Dropbox, and LinkedIn.

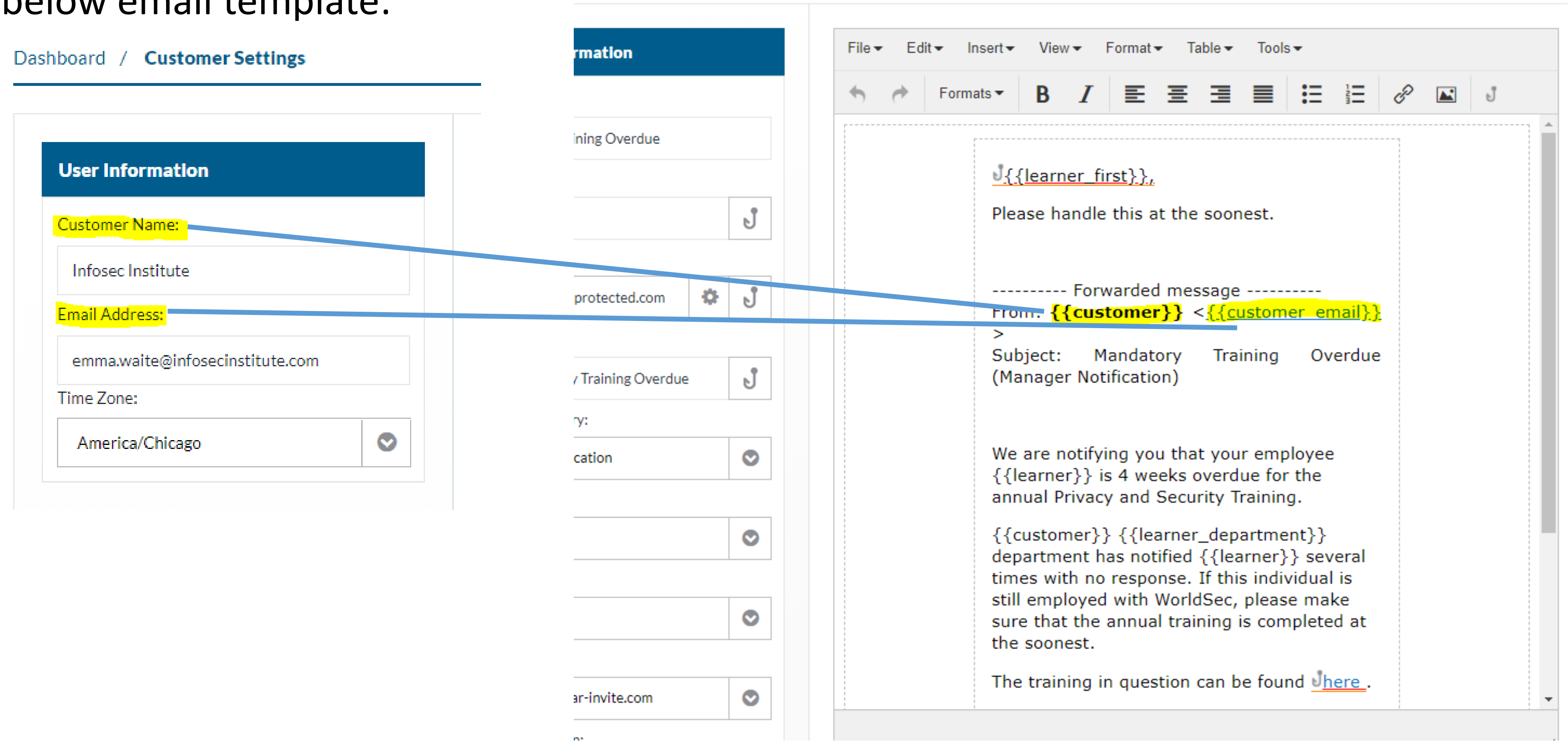
Customize Account Settings

- Adding Logo: Your company logo is used to customize your SecurityIQ platform. Learners will be able to see your company logo when they are in a learning module, receive a notification, or on a landing page.
  - Dimensions: The logo dimensions must be larger than 420x420 and smaller than 1280x1280 (both horizontally and vertically).
  - Background: We also recommend finding a logo with a transparent background as it will provide better branding for your company

- Adding Administrators: You can add more Account Administrators to your SecurityIQ Account by selecting "New Administrators". From there enter the email address of the person and select "add". The new admin should expect to receive a verification email for them to get their account set up.

Customize Account Settings - Continued

- Updating User Information: The information listed in the section, may be used in phishing simulated emails and notifications if the template makes use of variables. Please see an example of what variables are in the below email template:



Dashboard / **Customer Settings**

User Information

Customer Name:

Infosec Institute

Email Address:

emma.waite@infosecinstitute.com

Time Zone:

America/Chicago

{{learner_first}},

Please handle this at the soonest.

---------- Forwarded message ----------
From: **{{customer}}** <{{customer_email}}>
>
Subject: Mandatory Training Overdue (Manager Notification)

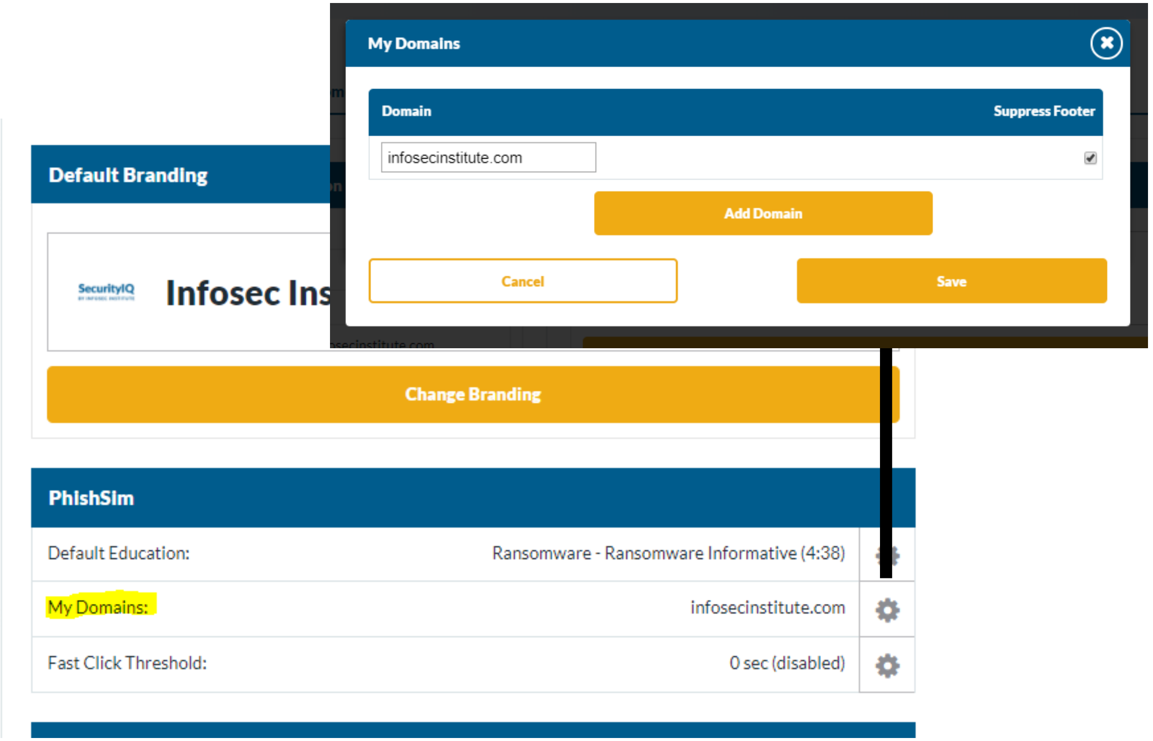
We are notifying you that your employee {{learner}} is 4 weeks overdue for the annual Privacy and Security Training.

{{customer}} {{learner_department}} department has notified {{learner}} several times with no response. If this individual is still employed with WorldSec, please make sure that the annual training is completed at the soonest.

The training in question can be found here.

Adding Domains and Suppress Footer

In your SecurityIQ Account Settings, you can add a list of all the learners' email domains in the "My Domains" section under PhishSim by selecting the settings gear.



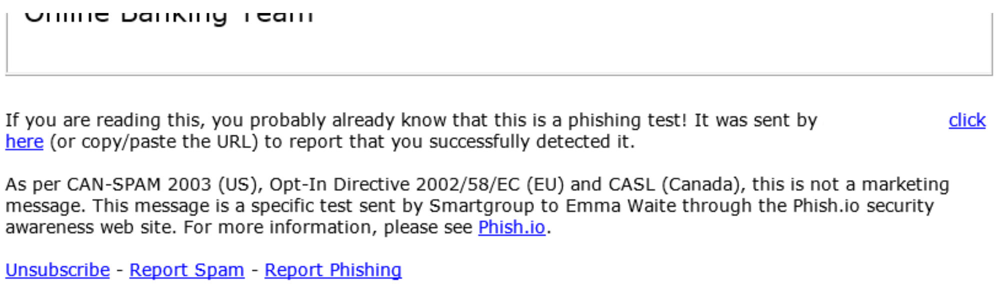
My Domains

Domain	Suppress Footer
infosecinstitute.com	☑

PhishSim

Default Education:	Ransomware - Ransomware Informative (4:38)
My Domains:	infosecinstitute.com
Fast Click Threshold:	0 sec (disabled)

In this pop-up window, you can also select to suppress the footer. The footer contains verbiage found at the bottom of an email (see below) that gets sent out through a PhishSim Campaign:



Online Banking Team

If you are reading this, you probably already know that this is a phishing test! It was sent by click here (or copy/paste the URL) to report that you successfully detected it.

As per CAN-SPAM 2003 (US), Opt-In Directive 2002/58/EC (EU) and CASL (Canada), this is not a marketing message. This message is a specific test sent by Smartgroup to Emma Waite through the Phish.io security awareness web site. For more information, please see Phish.io.

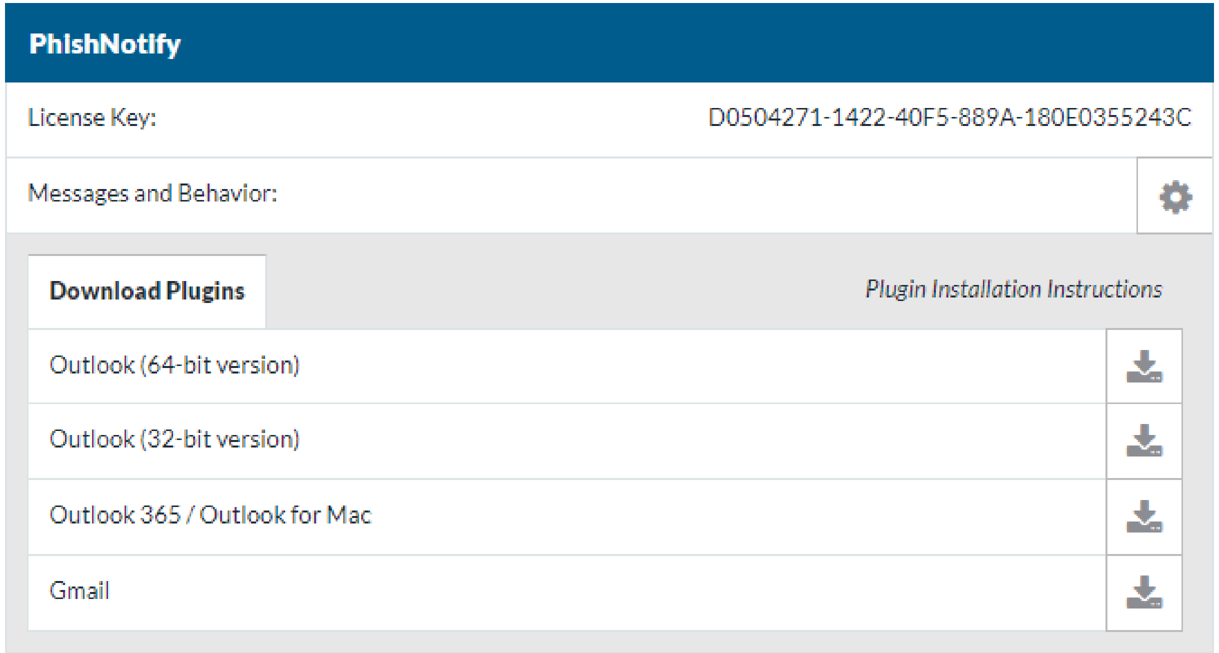
Unsubscribe - Report Spam - Report Phishing

PhishNotify

SecurityIQ
BY INFOSEC INSTITUTE

What is PhishNotify?

PhishNotify is a great tool for identifying potentially malicious emails that come into your learner's inbox, as well as simulated phishing emails sent out through SecurityIQ. This tool is available on Outlook, Office365, and Gmail as a Chrome Extension. You can access the different tools, as well as the Plugin Installation Instructions, in your Account Settings under the PhishNotify Section:



PhishNotify

License Key: D0504271-1422-40F5-889A-180E0355243C

Messages and Behavior:

Download Plugins

Plugin Installation Instructions

Outlook (64-bit version)

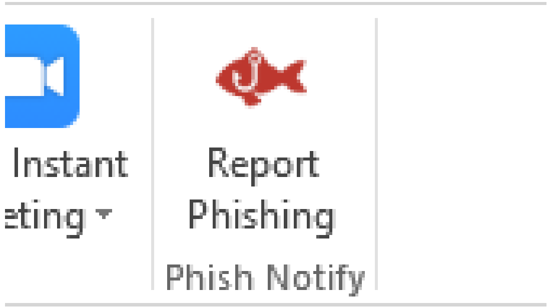
Outlook (32-bit version)

Outlook 365 / Outlook for Mac

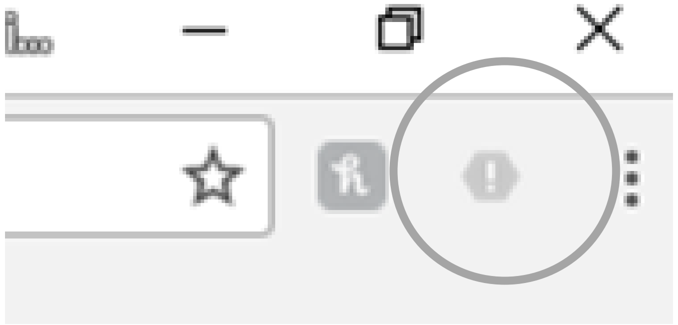
Gmail

What does PhishNotify look like?

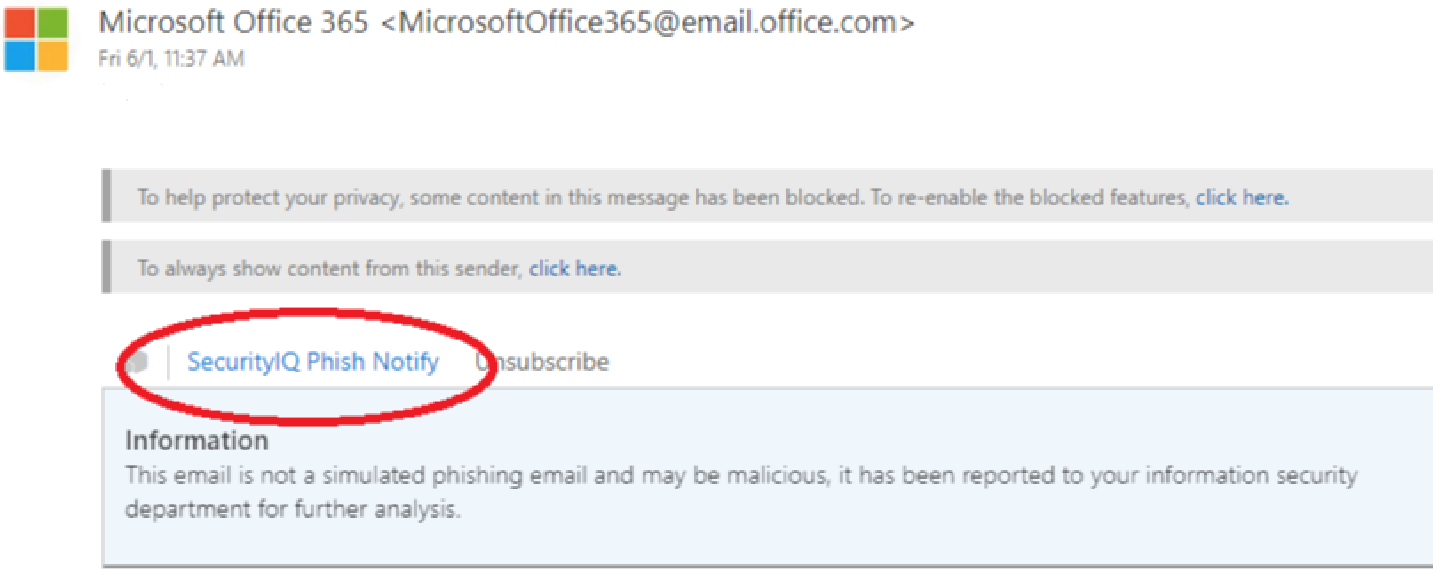
Outlook



Chrome Extension



Office365



Microsoft Office 365 <MicrosoftOffice365@email.office.com>
Fri 6/1, 11:37 AM

To help protect your privacy, some content in this message has been blocked. To re-enable the blocked features, click here.

To always show content from this sender, click here.

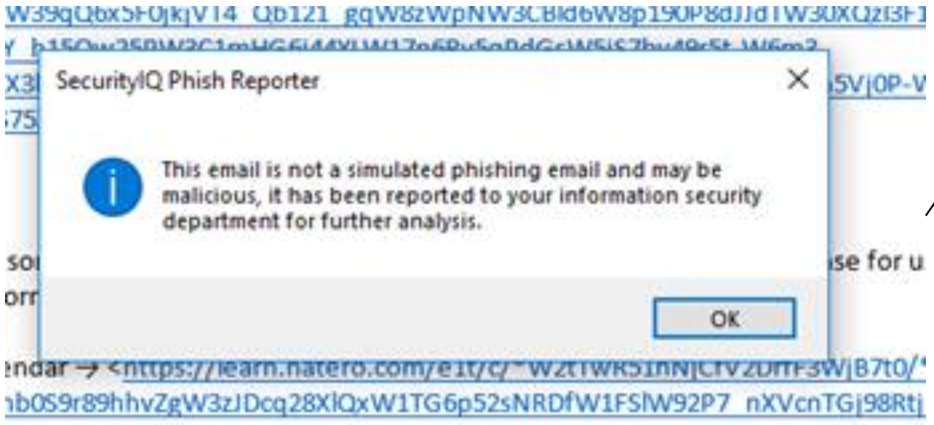
SecurityIQ Phish Notify | Unsubscribe

Information
This email is not a simulated phishing email and may be malicious, it has been reported to your information security department for further analysis.

Messaging and Behavior

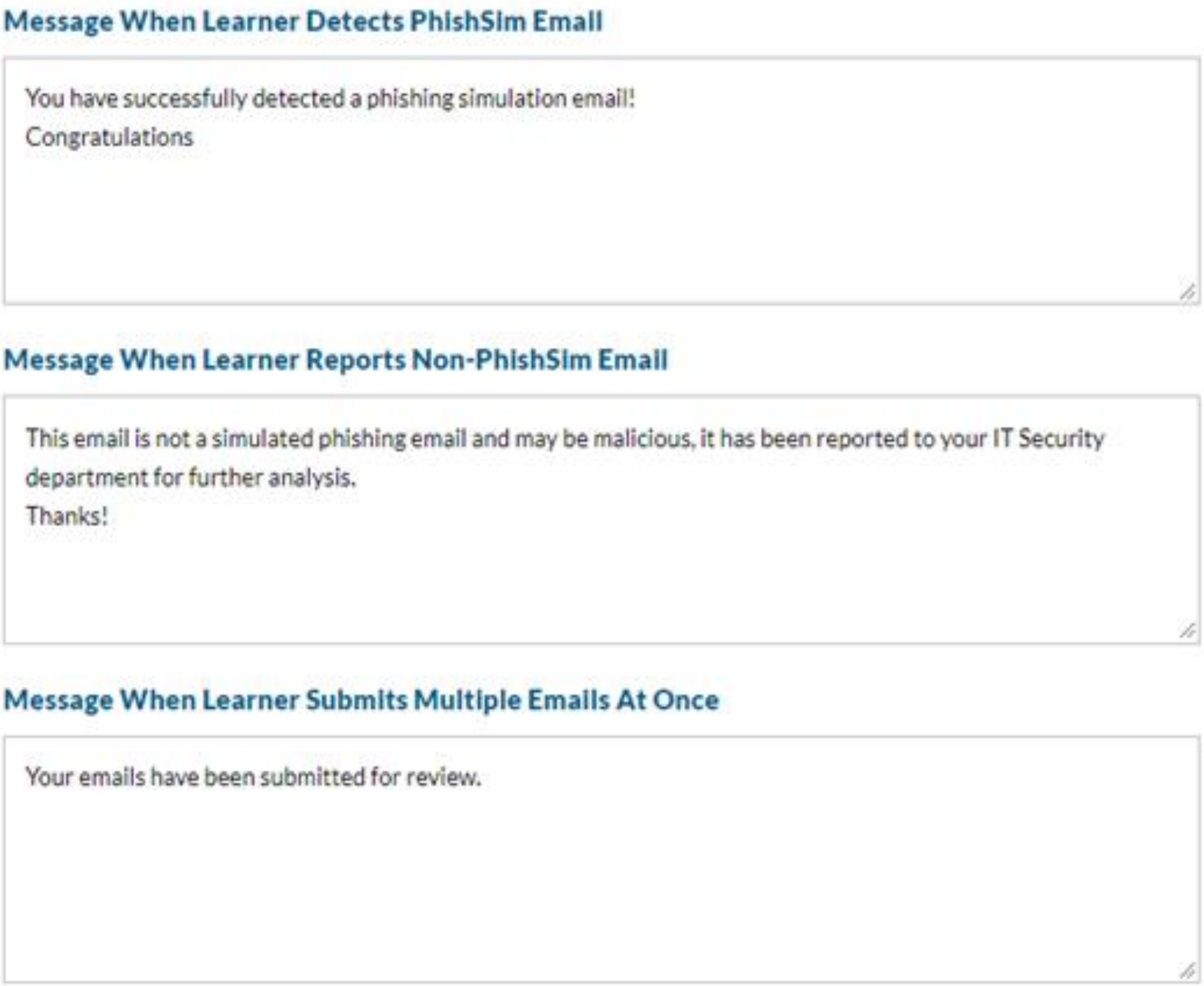
When a learner clicks on the PhishNotify plugin, a message will appear.

As an Administrator, you have the ability to customize the message



SecurityIQ Phish Reporter

This email is not a simulated phishing email and may be malicious, it has been reported to your information security department for further analysis.



Message When Learner Detects PhishSim Email

You have successfully detected a phishing simulation email!
Congratulations

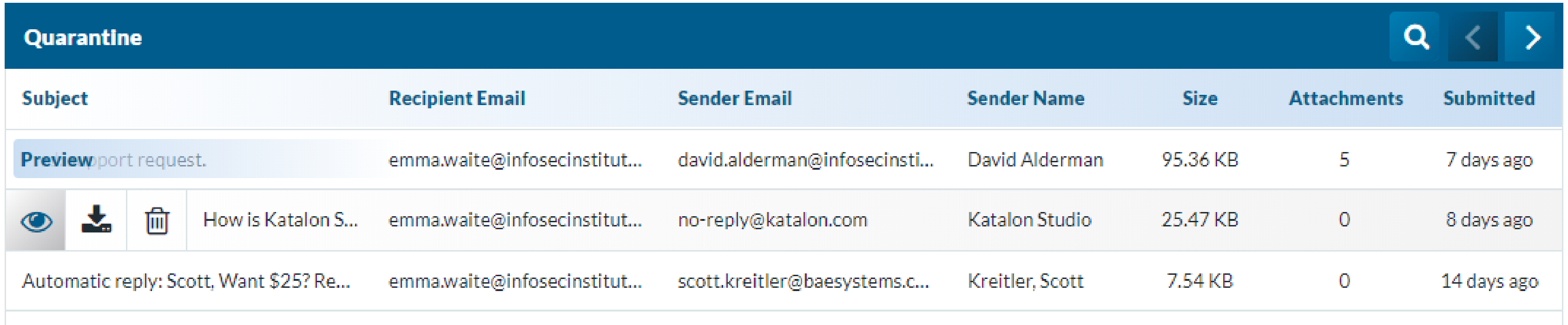
Message When Learner Reports Non-PhishSim Email

This email is not a simulated phishing email and may be malicious, it has been reported to your IT Security department for further analysis.
Thanks!

Message When Learner Submits Multiple Emails At Once

Your emails have been submitted for review.

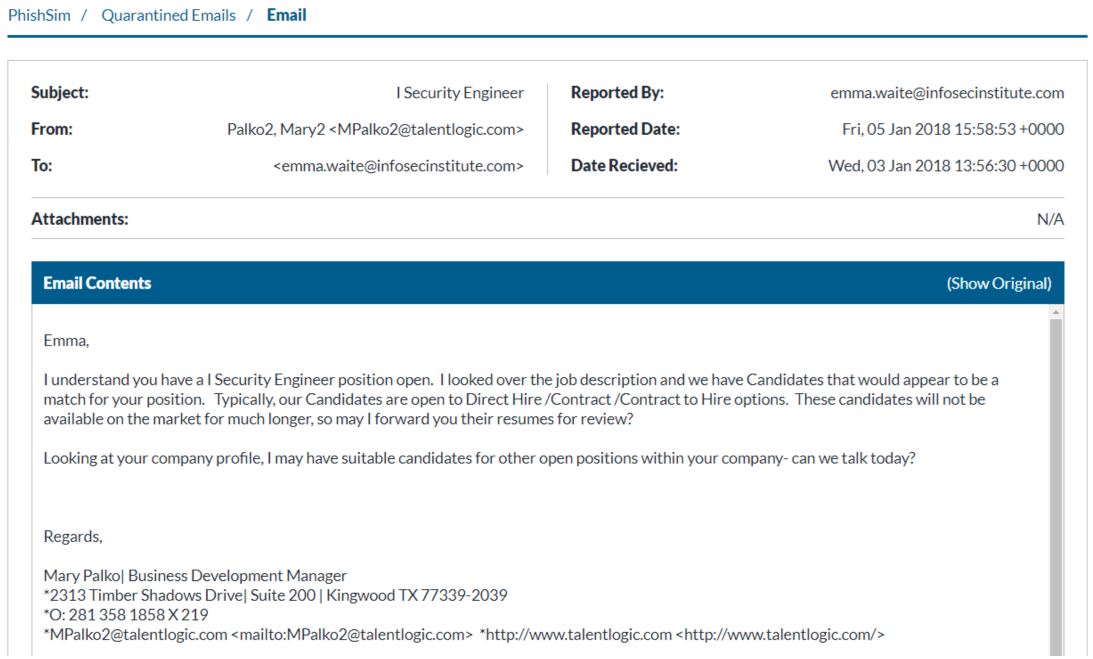
Quarantined Emails



Quarantine

Subject	Recipient Email	Sender Email	Sender Name	Size	Attachments	Submitted
Preview port request.	emma.waite@infosecinstitut...	david.alderman@infosecinsti...	David Alderman	95.36 KB	5	7 days ago
How is Katalon S...	emma.waite@infosecinstitut...	no-reply@katalon.com	Katalon Studio	25.47 KB	0	8 days ago
Automatic reply: Scott, Want $25? Re...	emma.waite@infosecinstitut...	scott.kreitler@baesystems.c...	Kreitler, Scott	7.54 KB	0	14 days ago

As an Administrator you can analyze any non-PhishSim email that is reported inside your SecurityIQ account. You can see what the email looked like in the person's inbox as well as view the source code of that email safely.



PhishSim / Quarantined Emails / **Email**

Subject:	I Security Engineer	**Reported By:**	emma.waite@infosecinstitute.com
From:	Palko2, Mary2 <MPalko2@talentlogic.com>	**Reported Date:**	Fri, 05 Jan 2018 15:58:53 +0000
To:	<emma.waite@infosecinstitute.com>	**Date Recieved:**	Wed, 03 Jan 2018 13:56:30 +0000

Attachments: N/A

Email Contents (Show Original)

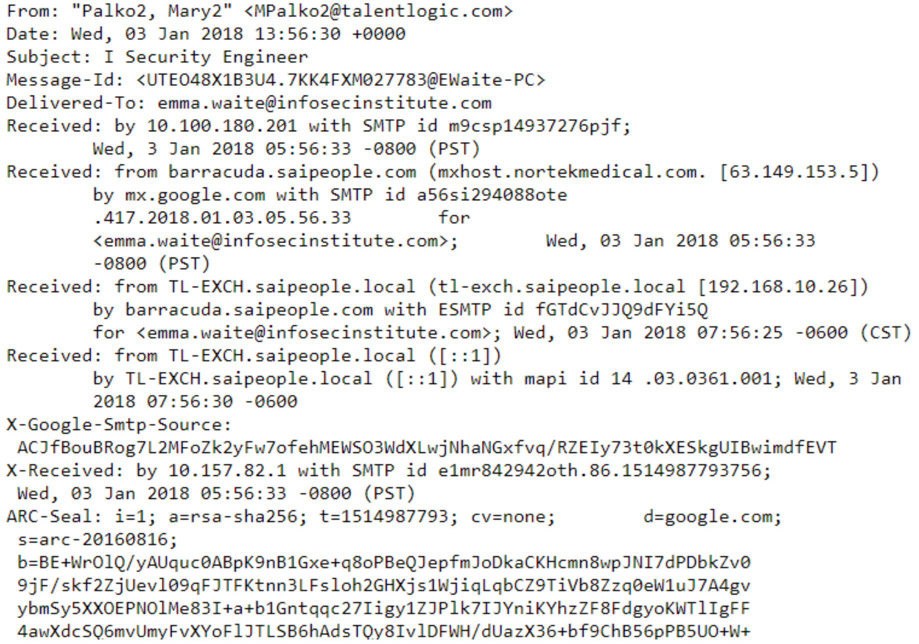
Emma,

I understand you have a I Security Engineer position open. I looked over the job description and we have Candidates that would appear to be a match for your position. Typically, our Candidates are open to Direct Hire /Contract /Contract to Hire options. These candidates will not be available on the market for much longer, so may I forward you their resumes for review?

Looking at your company profile, I may have suitable candidates for other open positions within your company- can we talk today?

Regards,

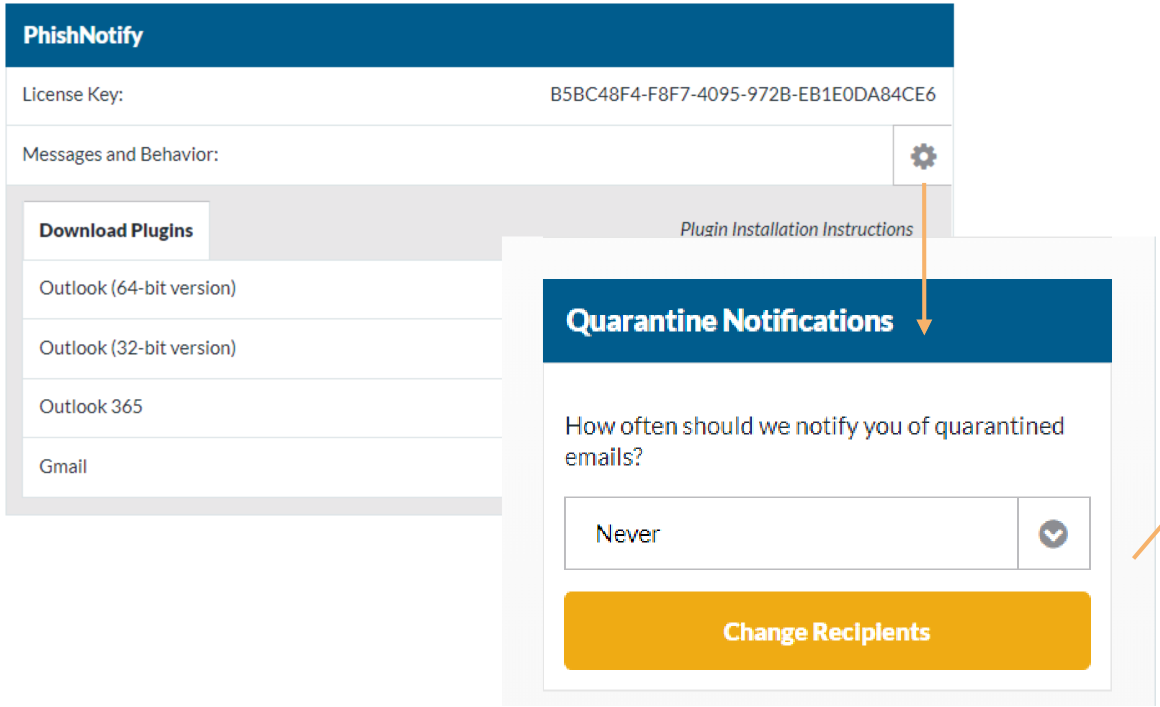
Mary Palko| Business Development Manager
*2313 Timber Shadows Drive| Suite 200 | Kingwood TX 77339-2039
*O: 281 358 1858 X 219
*MPalko2@talentlogic.com <mailto:MPalko2@talentlogic.com> *http://www.talentlogic.com <http://www.talentlogic.com/>



```
From: "Palko2, Mary2" <MPalko2@talentlogic.com>
Date: Wed, 03 Jan 2018 13:56:30 +0000
Subject: I Security Engineer
Message-Id: <UTEO48X1B3U4.7KK4FXM027783@EWaite-PC>
Delivered-To: emma.waite@infosecinstitute.com
Received: by 10.100.180.201 with SMTP id m9csp14937276pjf;
        Wed, 3 Jan 2018 05:56:33 -0800 (PST)
Received: from barracuda.saipeople.com (mxhost.nortekmedical.com. [63.149.153.5])
        by mx.google.com with SMTP id a56si294088ote
        .417.2018.01.03.05.56.33        for
        <emma.waite@infosecinstitute.com>;        Wed, 03 Jan 2018 05:56:33
        -0800 (PST)
Received: from TL-EXCH.saipeople.local (tl-exch.saipeople.local [192.168.10.26])
        by barracuda.saipeople.com with ESMTP id fGTdCvJJQ9dFYi5Q
        for <emma.waite@infosecinstitute.com>; Wed, 03 Jan 2018 07:56:25 -0600 (CST)
Received: from TL-EXCH.saipeople.local ([::1])
        by TL-EXCH.saipeople.local ([::1]) with mapi id 14 .03.0361.001; Wed, 3 Jan
        2018 07:56:30 -0600
X-Google-Smtp-Source:
 ACJfBouBRog7L2MFoZk2yFw7ofehMEWSO3WdXLwjNhaNGxfvq/RZEIy73t0kXESkgUIBwimdfEVT
X-Received: by 10.157.82.1 with SMTP id e1mr842942oth.86.1514987793756;
 Wed, 03 Jan 2018 05:56:33 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1514987793; cv=none;        d=google.com;
 s=arc-20160816;
 b=BE+WrOlQ/yAUquc0ABpK9nB1Gxe+q8oPBeQJepfmJoDkaCKHcmn8wpJNI7dPDbkZv0
 9jF/skf2ZjUevl09qFJTFKtnn3LFsloh2GHXjs1WjiqLqbCZ9TiVb8Zzq0eW1uJ7A4gv
 ybmSy5XXOEPNOlMe83I+a+b1Gntqqc27Iigy1ZJPlk7IJYniKYhzZF8FdgyoKWTlIgFF
 4awXdcSQ6mvUmyFvXYoFlJTLSB6hAdsTQy8IvlDFWH/dUazX36+bf9ChB56pPB5UO+W+
```

Quarantined Email Notifications

As an Account Administrator you can also choose to be notified whenever someone submits a potentially malicious email to SecurityIQ's Quarantine section. To do this, locate the PhishNotify section in your Account Settings and select the settings gear (see image below)



PhishNotify

License Key: B5BC48F4-F8F7-4095-972B-EB1E0DA84CE6

Messages and Behavior:

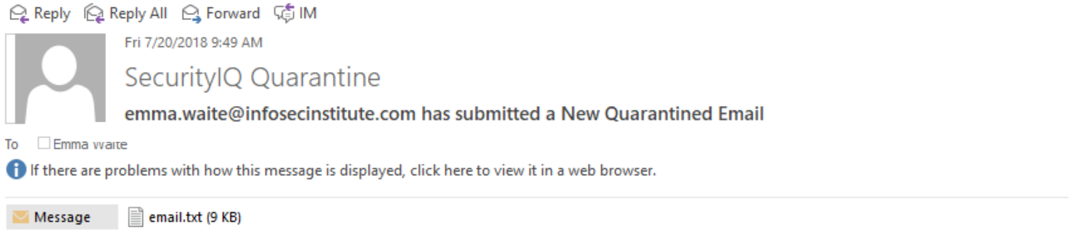
Download Plugins — *Plugin Installation Instructions*

- Outlook (64-bit version)
- Outlook (32-bit version)
- Outlook 365
- Gmail

Quarantine Notifications

How often should we notify you of quarantined emails?

Never



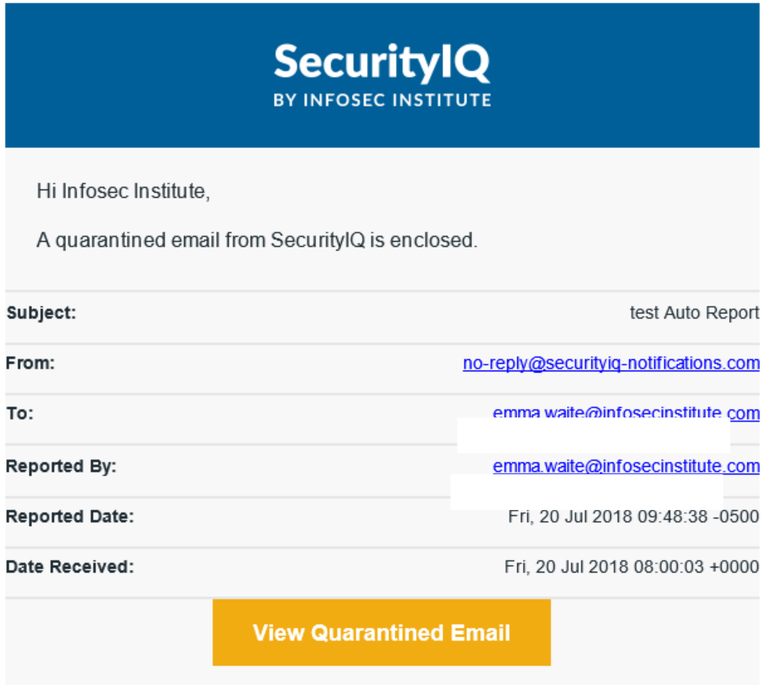
Fri 7/20/2018 9:49 AM

SecurityIQ Quarantine

emma.waite@infosecinstitute.com has submitted a New Quarantined Email

To ☐ Emma Waite

If there are problems with how this message is displayed, click here to view it in a web browser.



Hi Infosec Institute,

A quarantined email from SecurityIQ is enclosed.

Subject:	test Auto Report
From:	no-reply@securityiq-notifications.com
To:	emma.waite@infosecinstitute.com
Reported By:	emma.waite@infosecinstitute.com
Reported Date:	Fri, 20 Jul 2018 09:48:38 -0500
Date Received:	Fri, 20 Jul 2018 08:00:03 +0000