Security Awareness Training

SECURITY AWARENESS TRAINING

Safelisting Guide

April 2021

Table of Contents

OVERVIEW

Proofpoint Security Awareness Training uses a variety of systems to communicate to devices within your network and deliver email messages to your end users. This guide documents the IP addresses, domains, and URLs used per licensed product per hosted environment to deliver this information, so please refer to the appropriate sections below depending on your hosted environment. This document should be provided to your email or security administrators to ensure reliable communications.

> **Notes:**
>
> - Only perform safelisting for your licensed Proofpoint Security Awareness Training products.
> - Only safelist the IPs for your hosted location (North America, Europe, and Asia Pacific). If you aren't sure of your hosted location, please click your **name** in the upper right corner of Community, and then click **My Account** > **Related** > **Provisioning Object** link. Or, contact wst-support@proofpoint.com or your assigned Customer Success Manager.

Tips:

- For the most current safelisting information, please access Community and click the **Safelisting** link on the Home page or use the **Search** textbox to search for "Safelisting Guide." Also consult the Safelisting Guide for information on safelisting mail gateways (Exchange/Office 365 and Google Apps) and additional mail filters (such as, Proofpoint Protection Services, Symantec, Mimecast).
- To view the change log for the "Safelisting Guide," please access Community and search for "Safelisting Guide Change Log."

NORTH AMERICA ENVIRONMENT

Use the following safelisting information if your hosted location is North America (NA).

> **Note:** If you have multiple mail filters, you may have to insert a custom mail header to safelist instead of safelisting via IP address.

End-User Sync

Ensure that the following URLs for NA-hosted environments are safelisted in your organization's firewall to ensure that End-User Sync for Active Directory can communicate with our servers:

- https://rolodex-us.securityeducation.com/api/sign_in
- https://rolodex-us.securityeducation.com/api/users
- https://rolodex-us.securityeducation.com/api/authenticated_hello
- https://rolodex-us.securityeducation.com/api/hello

PhishAlarm

PhishAlarm connects to the Training Platform with a secured web connection on port 443 (TLS 1.2 or higher). Ensure that the appropriate URLs below for NA-hosted environments are safelisted in your organization's firewall and proxy server to allow PhishAlarm to communicate securely with the Training Platform.

PhishAlarm For Outlook URLs (North America)

- https://phishalarm-us-east-1-v2.securityeducation.com/api/v1/
- https://phishalarm-us.securityeducation.com
- https://analyzer-api.securityeducation.com

PhishAlarm For Exchange URL (North America)

- https://addin-us.securityeducation.com

PhishAlarm For Exchange will also make calls to the following URLs:

- https://d2wy8f7a9ursnm.cloudfront.net/
- https://notify.bugsnag.com/
- https://code.jquery.com/
- https://appsforoffice.microsoft.com/
- https://outlook.office365.com/EWS/Exchange.asmx
- https://outlook.office.com/api/
- https://polyfill.io

> **Note:** Exchange Web Services (EWS) must be externally available for on-premise Exchange. In addition, OAUTH is required in order to use the PhishAlarm Add-in. The IP address, **52.1.14.157** (for North America), is for the resources that will be accessing your EWS for your on-premise Exchange Server. You must safelist **52.1.14.157** to allow the email from the EWS to reach our PhishAlarm server.

Analyzer

Ensure that the following information for NA-hosted environments is safelisted in your organization's mail filter or firewall to ensure that you can receive the email from Analyzer:

Mail Sender Name:	outgoing.analyzer.securityeducation.com
Mail Sender IP:	34.192.109.34; 52.207.139.168
Sender Email Address*:	analyzer@analyzer.securityeducation.com

When the Analyzer Setting for Forward using original end-user email address is OFF, then the TRO reports are sent with these Sender email addresses. If this option is toggled ON, then the Sender email address will be that of the end-user who reported the email with PhishAlarm.

Phishing Simulation

This section contains the phishing domains and IPs used in Phishing Simulation campaigns for NA-hosted environments.

Phishing Simulation Domains

Below is a list of phishing domains you may utilize in your Phishing Simulation campaigns for NA-hosted environments. We recommend that you provide this list to your IT or security administrators to ensure that your users will be able to access the Teachable Moment seamlessly from within your organization's network.

> **Note:** Many default Phishing Simulation phishing templates include a subdomain. Therefore, if you are safelisting by domain, you may wish to wildcard it. For example, you would safelist "*.proofpoint.com" instead of safelisting "proofpoint.com" to ensure that all subdomains are included.

Phishing Simulation Teachable Moments will also make calls to the following URLs:

- https://tslp.s3.amazonaws.com
- https://java.com
- https://ajax.googleapis.com
- https://fonts.googleapis.com
- https://tscontent.s3.amazonaws.com
- https://d2wy8f7a9ursnm.cloudfront.net
- https://dp4eiskq7iesj.cloudfront.net

Phishing Simulation (North America)

4ooi.co	enegry.org	password-update.net
4ooi.com	entwurf-laden.de	payablaccounts.com
4ooi.in	eservce.com	paypol-login.com
4ooi.info	event-planer.net	pharmamedsonline.com
account-maintenance.com	exch01-corp.com	pharmlink.in
accounts-receivable.co	facbook-login.com	phishingtraining.com
ackisses53.com	firstfedtrust.com	pipelinenews.net
acxx53.com	flightstatalert.com	postcardfast.com
acxx53.de	freeenergypress.com	prnewsnet.us
admissionshelpu.org	fundingsource.services	publicemailservice.com
adobe-0nline.com	goggl.cc	qqoffi55.cc
adobecloudservices.com	gotwebinar.online	qqoffi55.com
aibabba-deals.com	gov-online.net	qquio.com
amazoon.online	gov-services.com	ransomware.site
annualenroll.com	greetingsweb.com	register-now.world

avoidphishing.securityeducation.com
[Note: This domain is for Phishing Simulation Attachment Campaigns only]

breaking-news-network.net

breaking-news-now.com

business-services.org

byt.im

cadeauavant.fr

cardservices.online

cloud-store.services

combase.co

committee4strongleadership.com

concur-s0lutions.com

contract-sign.online

corpbenefitplan.com

corp-hr.com

corp-internal.co.uk

corp-internal.com

corp-internal.net

corp-internal.us

corpoutlook.com

corp-proxy.com

creditmass.ru

cyber-sale.net

dcscanscation.com

decision2016.win

detailswire.com

docsign-online.com

dropboxlink.com

dynssi.com

ee77red.ru

egencia-online.com

electioninfo.online

emailquarantine.com

grnail.world

hpdocument.com

informedvoterleague.com

info-week.net

info-week.us

instagrarn.net

internalitsupport.com

investmentsecureportal.com

itnues.net

lesportsacxx53.com

link91.in

linkedincdn.com

loan-payments.com

localhostlocaldomain.com

luk66.cn

mailcenter-alert.com

mail-delivery-system.com

maildeliverysystem.net

maliciousfile.online

matchesonline.net

meeting-reminder.com

metflix.us

micrasoft-office365.com

microsoftsql.net

myensurance.co

nationalcouncil4not-for-profits.com

netbenefits-access.com

office3889.com

olympicresults.online

onedrive-micrasoft.com

onlinedocshare.com

password-update.com

rwebfix.com

saleslinkforce.com

salesteamlink.com

scandeviceservices.com

sec-10k.com

securebankingsevices.com

securelogin-wallet.com

securityeducation.com

self-serve.co

seriouslydonotclickthis.com

sharepoint-docshare.com

shipment-confirm.com

shippingupdate.net

sn84229.co

sphotos-fbcdn.com

sportstoday.biz

stubclub.co

techsupport-corp.com

thisisaphishingattack.com

trackingupdate.net

tradeinternationai.com

travelresinfo.com

updamicrosoft.com

updatracking.com

user-account.online

user-account-maintenance.com

vobamobile.net

voicemailaccess.net

webfilteralert.com

www01-local.com

The following DMARC (Policy Reject) domains are available by request for NA-hosted environments. Please contact your Customer Success Manager or Customer Support for assistance.

- mail-center-alert.com
- e-servce.com
- corpinternal.us

Phishing Simulation Assessment IPs

Phishing Simulation will send simulated phishing attacks to your end users. To ensure users are provided a realistic phishing simulation assessment, we recommend safelisting the following IP addresses for NA-hosted environments:

- 107.23.16.222
- 54.173.83.138

Phishing Simulation stock images are embedded in attachments and Teachable Moments. Safelisting this domain in your firewall or proxy server will ensure these images are displayed to your end users:

- tslp.s3.amazonaws.com

Custom images are images that the Phishing Admin has uploaded to personalize their Phishing campaign and are stored at the following domain to safelist:

- ts-uploads.s3.amazonaws.com

> **Note:** Phishing Simulation emails will come from whatever **“from address”** you chose when creating a campaign. You can add the **“from address”** to your safe sender list to ensure that the message arrives to the end user's inbox and the tracking pixel is downloaded without having to click **download images**. Clicking on **download images** prevents proper tracking of email opens. This will also prevent the message from ending up in the junk folder. You can add the address to the end user's safe sender list via GPO or PowerShell.

Training Notifications

Proofpoint recommends that Training Notifications are sent with a “From:” address that uses your organization’s domain name, since this email address will be more familiar to the user and allow the user to easily reply to the message should they have questions. Contact your mail administrator beforehand, though, as most email systems restrict email using your organization’s domain name to authorized mail servers.

To allow email from our servers using your organization’s domain name, we recommend asking your email administrator to make the following changes:

- Add the appropriate IP addresses to your SPF records and your email filter safelist.
- **securityeducation.com** and **ws01.securityeducation.com** are domains that can also be safelisted for web filtering for NA-hosted environments.

Training Platform

The following are Proofpoint Security Awareness Training Platform IPs for NA-hosted environments to safelist:

- 107.20.210.250
- 52.1.14.157

In order to have the uploaded images from the Training Platform automatically downloaded within Outlook, we recommend safelisting the following domain and adding it to the Trusted Sites:

- platform.securityeducation.com

The following URL can be safelisted to ensure proper delivery of all assets, including text content, graphics, photographs, videos, audio files, and databases:

- d1fbefs0dyob6i.cloudfront.net

EUROPE ENVIRONMENT

Use the following safelisting information if your hosted location is Europe (EU).

> **Note:** If you have multiple mail filters, you may have to insert a custom mail header to safelist instead of safelisting via IP address.

End-User Sync

Ensure that the following URLs for EU-hosted environments are safelisted in your organization's firewall to ensure that End-User Sync for Active Directory can communicate with our servers.

- https://rolodex-eu.securityeducation.com/api/sign_in
- https://rolodex-eu.securityeducation.com/api/users
- https://rolodex-eu.securityeducation.com/api/authenticated_hello
- https://rolodex-eu.securityeducation.com/api/hello

PhishAlarm

PhishAlarm connects to the Training Platform with a secured web connection on port 443 (TLS 1.2 or higher). Ensure that the appropriate URLs below for EU-hosted environments are safelisted in your organization's firewall and proxy server to allow PhishAlarm to communicate securely with the Training Platform.

PhishAlarm For Outlook URLs (Europe)

- https://phishalarm-eu-west-1-v2.securityeducation.com/api/v1/
- https://phishalarm-eu.securityeducation.com
- https://analyzer-api.eu.securityeducation.com

PhishAlarm For Exchange URL (Europe)

- https://addin-eu.securityeducation.com

PhishAlarm For Exchange will also make calls to the following URLs:

- https://d2wy8f7a9ursnm.cloudfront.net/
- https://notify.bugsnag.com/
- https://code.jquery.com/
- https://appsforoffice.microsoft.com/
- https://outlook.office365.com/EWS/Exchange.asmx
- https://outlook.office.com/api/
- https://polyfill.io

> **Note:** Exchange Web Services (EWS) must be externally available for on-premise Exchange. In addition, OAUTH is required in order to use the PhishAlarm Add-in. The IP address, **52.30.130.201** (for Europe), is for the resources that will be accessing your EWS for your on-premise Exchange Server. You must safelist **52.30.130.201** to allow the email from the EWS to reach our PhishAlarm server.

Analyzer

Ensure that the following information for Europe hosted environments is safelisted in your organization's mail filter or firewall to ensure that you can receive the email from Analyzer.

Mail Sender Name:	outgoing.analyzer.eu.securityeducation.com
Mail Sender IP:	34.252.12.130; 52.30.8.165
Sender Email Address*:	analyzer@analyzer.eu.securityeducation.com

***When the Analyzer Setting for Forward using original end-user email address is OFF then the TRO reports are sent with these Sender email addresses. If this option is toggled ON, then the Sender email address will be that of the end-user who reported the email with PhishAlarm.*

Phishing Simulation

This section contains the phishing domains and IPs used in Phishing Simulation campaigns for EU-hosted environments.

Phishing Simulation Domains

Below is a list of phishing domains you may utilize in your Phishing Simulation campaigns for EU-hosted environments. We recommend that you provide this list to your IT or security administrators to ensure that your users will be able to access the Teachable Moment seamlessly from within your organization’s network.

> **Note:** Many default Phishing Simulation phishing templates include a subdomain. Therefore, if you are safelisting by domain, you may wish to wildcard it. For example, you would safelist “*.proofpoint.com” instead of safelisting “proofpoint.com” to ensure that all subdomains are included.

Phishing Simulation Teachable Moments will also make calls to the following URLs:

- https://tslp.s3.amazonaws.com
- https://java.com
- https://ajax.googleapis.com
- https://fonts.googleapis.com
- https://tscontent.s3.amazonaws.com
- https://d2wy8f7a9ursnm.cloudfront.net

- https://dp4eiskq7iesj.cloudfront.net

Phishing Simulation (Europe)

4ooi.co.uk
4ooi.net
accounts-receivable.online
admissionshelpu.com
adobe-0nline.net
adobedocuments.com
aibaba-deals.com
amazoon.site
annualenroll.net
avoidphishing.eu.securityeducation.com
[Note: This domain is for Phishing Simulation Attachment Campaigns only]
bancaire.co.uk
bancaire.org
beingthebestU.com
bizsolutions-int.co.uk
bizsolutions-int.com
breaking-news-network.co.uk
breaking-news-now.net
c0ncursolutions.com
cardservices.vip
citydiscounts.org
cloud-store.space
coffeetooyourdesk.com
combase.io
committee4strongleadership.org
contract-sign.site
corpbenefitplan.net
corp-internal.co
corp-internal.org
corpoutlook.co.uk
corp-password-mangemet.com
corp-password-mangemet.fr
corp-password-mangemet.us
electioninfo.news
emaildistro.net
emailquarantine.net
enegry.info
entwurf-laden.com
epayroll.solutions
eservce.biz
eservce.co.uk
eservce.fr
eservce.net
event-planer.com
exch01-corp.net
facbooklogin.co.uk
firstfedtrust.us
flightstatalert.net
flight-status-alert.com
flight-status-alert.me
freeenergypress.org
fundingsource.world
giftgreeting.com
global-bancaire.com
gotwebinar.org
gov-services.net
grnail.online
hpdocument.net
hr-internal.co
hrmc.me.uk
ibwalletsecurelogin.com
informedvoterleague.org
info-week.biz
instagrarn.org
internalitsupport.net
investmentsecuresite.com
matchesonline.org
meeting-reminder.net
metflix.pw
micrasoft-395office.com
micrasoft-onedrive.com
myensurance.services
Mypayrollservice.net
nationalcouncil4not-for-profits.org
olympicresults.site
onlinebankingsevices.com
online-docshare.com
p183321.net
package-track.com
package-track.info
password-update.me
payqal-login.com
phishingtraining.eu
ransomware.website
recruitpros.co
register-now.net
rnetflix.io
scandoc-center.com
securityeducation.com
security-education.net
self-serve.ltd
shipping-notification.info
shoppingbuyrewards.com
sportstoday.life
sso-local.net
stubclub.net
swift-track.co.uk
swift-track.info

cyber-sale.com	k-trafficxmj.co	techsupport-corp.net
dcscanscation.net	k-trafficxmj.co.uk	therecruitpro.net
decision2016.online	k-trafficxmj.com	uscis-gov.net
detailswire.net	linkedincdn.co.uk	user-account.net
docsign-online.net	linkedincdn.net	verifier-sure.com
docs-sharepoint.com	linkedincdn.us	vobamobile.co
dodgylink.co.uk	loanpaymentservices.com	xerox-scandevice.com
domainte.com	localhostlocaldomain.net	yggui.de
dropboxlink.net	mailcenter-alert.net	yggui.li
dynssi.net	mail-delivery-system.info	youarebeingphished.com
Eatandreward.com	maliciousfile.com	Yourexpo.co.uk
egencia-website.com	maliciousfile.download	

The following DMARC (Policy Reject) domains are available by request for EU-hosted environments. Please contact your Customer Success Manager or Customer Support for assistance.

- mail-center-alert.net
- e-servce.biz
- corpinternal.org

Phishing Simulation Assessment IPs

Phishing Simulation will send simulated phishing attacks to your end users. To ensure users are provided a realistic phishing simulation assessment, we recommend safelisting the following IP addresses for EU-hosted environments.

- 52.17.45.98
- 52.16.190.81

Phishing Simulation stock images are embedded in attachments and Teachable Moments. Safelisting this domain in your firewall or proxy server will ensure these images are displayed to your end users:

- tslp.s3.amazonaws.com

Custom images are images that the Phishing Admin has uploaded to personalize their Phishing campaign and are stored at the following domain to safelist:

- ts-eu-uploads.s3.amazonaws.com

> **Note:** Phishing Simulation emails will come from whatever **“from address”** you chose when creating a campaign. You can add the **“from address”** to your safe sender list to ensure that the message arrives to the end user's inbox and the tracking pixel is downloaded without having to click **download images**. Clicking on **download images** prevents proper tracking of email opens. This will also prevent the message from ending up in the junk folder. You can add the address to the end user's safe sender list via GPO or PowerShell.

Training Notifications

Proofpoint recommends that Training Notifications are sent with a "From:" address that uses your organization's domain name, since this email address will be more familiar to the user and allow the user to easily reply to the message should they have questions. Contact your mail administrator beforehand, though, as most email systems restrict email using your organization's domain name to authorized mail servers.

To allow email from our servers using your organization's domain name, we recommend asking your email administrator to make the following changes:

- Add the appropriate IP addresses to your SPF records and your email filter safelist.
- **securityeducation.com** and **ws02.securityeducation.com** are domains that can also be safelisted for web filtering for EU-hosted environments.

Training Platform

The following are Proofpoint Security Awareness Training Platform IPs for EU-hosted environments to safelist:

- 54.229.2.165
- 52.30.130.201

In order to have the uploaded images from the Training Platform automatically downloaded within Outlook, we recommend safelisting the following domain and adding it to the Trusted Sites:

- platform-web-eu.securityeducation.com

The following URL can be safelisted to ensure proper delivery of all assets, including text content, graphics, photographs, videos, audio files, and databases:

- d2k53c71t1ovai.cloudfront.net

ASIA PACIFIC ENVIRONMENT

Use the following safelisting information if your hosted location is Asia Pacific (AP).

> **Note:** If you have multiple mail filters, you may have to insert a custom mail header to safelist instead of safelisting via IP address.

End-User Sync

Ensure that the following URLs for AP-hosted environments are safelisted in your organization's firewall to ensure that End-User Sync for Active Directory can communicate with our servers.

- https://rolodex-oz.securityeducation.com/api/sign_in
- https://rolodex-oz.securityeducation.com/api/users
- https://rolodex-oz.securityeducation.com/api/authenticated_hello
- https://rolodex-oz.securityeducation.com/api/hello

PhishAlarm

PhishAlarm connects to the Training Platform with a secured web connection on port 443 (TLS 1.2 or higher). Ensure that the appropriate URLs below for AP-hosted environments are safelisted in your organization's firewall and proxy server to allow PhishAlarm to communicate securely with the Training Platform.

PhishAlarm For Outlook URLs (Asia Pacific)

- https://phishalarm-ap-southeast-2.securityeducation.com/api/v1/
- https://phishalarm-ap.securityeducation.com
- https://analyzer-api.ap.securityeducation.com

PhishAlarm For Exchange URL (Asia Pacific)

- https://addin-oz.securityeducation.com

PhishAlarm For Exchange will also make calls to the following URLs:

- https://d2wy8f7a9ursnm.cloudfront.net/
- https://notify.bugsnag.com/
- https://code.jquery.com/
- https://appsforoffice.microsoft.com/
- https://outlook.office365.com/EWS/Exchange.asmx
- https://outlook.office.com/api/
- https://polyfill.io

> **Note:** Exchange Web Services (EWS) must be externally available for on premise Exchange. In addition, OAUTH is required in order to use the PhishAlarm Add-in. The IP address, **54.66.252.242** (for Asia Pacific), is for the resources that will be accessing your EWS for your on-premise Exchange Server. You must safelist **54.66.252.242** to allow the email from the EWS to reach our PhishAlarm server.

Analyzer

Ensure that the following information for AP-hosted environments is safelisted in your organization's mail filter or firewall to ensure that you can receive the email from Analyzer.

Mail Sender Name:	outgoing.analyzer.ap.securityeducation.com
Mail Sender IP:	13.210.197.63; 13.55.113.235
Sender Email Address*:	analyzer@analyzer.ap.securityeducation.com

***When the Analyzer Setting for Forward using original end-user email address is OFF then the TRO reports are sent with these Sender email addresses. If this option is toggled ON, then the Sender email address will be that of the end-user who reported the email with PhishAlarm.*

Phishing Simulation

This section contains the phishing domains and IPs used in Phishing Simulation campaigns for AP-hosted environments

Phishing Simulation Domains

Below is a list of phishing domains you may utilize in your Phishing Simulation campaigns for AP-hosted environments. We recommend that you provide this list to your IT or security administrators to ensure that your users will be able to access the Teachable Moment seamlessly from within your organization's network.

> **Note:** Many default Phishing Simulation phishing templates include a subdomain. Therefore, if you are safelisting by domain, you may wish to wildcard it. For example, you would safelist "*.proofpoint.com" instead of safelisting "proofpoint.com" to ensure that all subdomains are included.

Phishing Simulation Teachable Moments will also make calls to the following URLs:

- https://tslp.s3.amazonaws.com
- https://java.com
- https://ajax.googleapis.com
- https://fonts.googleapis.com
- https://tscontent.s3.amazonaws.com
- https://d2wy8f7a9ursnm.cloudfront.net
- https://dp4eiskq7iesj.cloudfront.net

Phishing Simulation (Asia Pacific)

accounts-receivable.ltd
admissionshelpu.net
adobe0nline.com
adobe-cloudservices.com
aibabadeals.com
amaznlogin.com
amazoon.cc
avoidphishing.ap.securityeducation.com
[Note: This domain is for Phishing Simulation Attachment Campaigns only]
bankaccount-login.info
barterbox-payments.info
biz-assistant.net
c0ncurso1utions.com
cardservices.world
cloud-store.online
club-chatter.net
event-planer.co
facbook-login.net
freephoneupgrade.net
fundingsource.network
gigarnartonline.com
gov-services.online
greetingstech.com
grnail.services
hr-internal.online
ibwallet-securelogin.com
informedvoterleague.net
instagrarn.ai
investmentsecureportal.net
kompu82.com
loan-payments.online
macrosoft-onedrive.com
nationalcouncil4not-for-profits.net
one-drive-micrasoft.com
online-docshare.net
paypol-login.net
perchaseonline-2016.net
register-now.co
rnetflix.net
securebankingsevices.net
self-serve.group
sharepoint-onlinedocs.com
shorehaminsurance.com
sportstoday.tech
stubclub.org
techsupport-corp.online
tilburybank.com

combase.online committee4strongleadership.net cybersales-direct.com doc-sign.services egenciaonline.com electioninfo.co emeraldquestlogin.info epayroll.ltd essexhealthsystern.com	mailcenter-alerts.com marigoldbank-payments.com matchesonline.ai mawern.com micrasoft-office365.online myensurance.net my-wombank-online.com	uinvest.pro uq39.download uscis-gov.site user-account.co vobamobile.com wombank-rewards.com wombonk.com worryfreeonlineauctions.com yourdailyupload.net

The following DMARC (Policy Reject) domains are available by request for AP-hosted environments. Please contact your Customer Success Manager or Customer Support for assistance.

- mail-center-alerts.com
- e-servce.net
- corpinternal.co

Phishing Simulation Assessment IPs

Phishing Simulation will send simulated phishing attacks to your end users. To ensure users are provided a realistic phishing simulation assessment, we recommend safelisting the following IP addresses for AP-hosted environments.

- 13.55.65.8
- 13.55.54.143

Phishing Simulation stock images are embedded in attachments and Teachable Moments. Safelisting this domain in your firewall or proxy server will ensure these images are displayed to your end users:

- tslp.s3.amazonaws.com

Custom images are images that the Phishing Admin has uploaded to personalize their Phishing campaign and are stored at the following domain to safelist:

- ts-ap-uploads.s3.amazonaws.com

> **Note:** Phishing Simulation emails will come from whatever **“from address”** you chose when creating a campaign. You can add the **“from address”** to your safe sender list to ensure that the message arrives to the end user's inbox and the tracking pixel is downloaded without having to click **download images**. Clicking on **download images** prevents proper tracking of email opens. This will also prevent the message from ending up in the junk folder. You can add the address to the end user's safe sender list via GPO or PowerShell.

Training Notifications

Proofpoint recommends that Training Notifications are sent with a “From:” address that uses your organization’s domain name, since this email address will be more familiar to the user and allow the user to easily reply to the message should they have questions. Contact your mail administrator beforehand, though, as most email systems restrict email using your organization’s domain name to authorized mail servers.

To allow email from our servers using your organization’s domain name, we recommend asking your email administrator to make the following changes:

- Add the appropriate IP addresses to your SPF records and your email filter safelist.
- **securityeducation.com** and **ws03.securityeducation.com** are domains that can also be safelisted for web filtering for AP-hosted environments.

Training Platform

The following are Proofpoint Security Awareness Training Platform IPs for AP-hosted environments to safelist:

- 54.153.131.110
- 54.66.252.242

In order to have the uploaded images from the Training Platform automatically downloaded within Outlook, we recommend safelisting the following domain and adding it to the Trusted Sites:

- platform-web-oz.securityeducation.com

The following URL can be safelisted to ensure proper delivery of all assets, including text content, graphics, photographs, videos, audio files, and databases:

- d1skokb0xwm98g.cloudfront.net.

ACCESSING SUPPORT AND HELPFUL RESOURCES

You can contact Customer Support for assistance from within the Wisdom Community or by email. Within the Wisdom Community, you can live chat with a Support Representative, create a new support case, ask a question of the entire user community forum, and view support documentation and Knowledgebase articles for immediate answers to your questions.

Contacting Customer Support

Through Wisdom Community

From within the Wisdom Community, you can live chat with a Support Representative or create a new support case.

1. Sign into the Security Education Platform.
2. Click the **Community** link in the upper right corner of the platform.
3. From the Wisdom Community home page, click the **Chat and Support** link, or click your username in the upper right corner of the page and select **Contact Support** from the drop-down menu. Use any of the following options on the Help Finder page.

Chat Now	Connect with our support team on Live Chat from 2 a.m. to 9 p.m. ET Monday through Friday. Click the **Chat Now** button, fill out the form, and click the **Request a Chat** button.
Create A New Support Case	Fill out the fields under **Create A New Support Case**, add an attachment (optional), and click **Submit**.

By Email

You can open a support ticket with Customer Support by email at wst-support@proofpoint.com. Be sure to include a brief description of your issue in the Subject line of the email. You will immediately receive a confirmation email with your Case Number.

Viewing Documentation and Knowledgebase Articles

Before contacting Customer Support, you can access the Wisdom Community to view support documentation and Knowledgebase articles, which may be a more immediate resource for the answer to your question.

1. Sign into the Security Education Platform.
2. Click the **Community** link in the upper right corner of the platform.
3. Click on any of the tabs or links or enter criteria into the **Search** textbox to locate helpful information.

Asking A Community Question

You can post a question for others in the Community to answer.

1. Sign into the Security Education Platform.
2. Click the **Community** link in the upper right corner of the platform.
3. Scroll down to the bottom of the Home page and click the **Ask A Community Question** button.
4. Fill out the online form and click **Ask**.