Whitelisting Instructions

To ensure that all emails from the platform will be successfully delivered to your customers, you'll need to ensure you have properly whitelisted the below IP Addresses and Domains. We've also included our phishing header below, as some partners wish to whitelist that as well.

Important: If you are using Office 365, you will need to configure Advanced Delivery for SecOps Mailboxes and Third-Party Phishing Simulations. See page 2 for details.

IP Addresses

Welcome, Weekly Micro Training, Monthly Newsletter & Push Notification Emails

- 149.72.184.111
- 168.245.40.98

Phishing Emails

- 168.245.68.173
- 149.72.207.249
- 168.245.34.162
- 168.245.30.20
- 18.209.119.19
- 34.231.173.178
- 54.209.51.230
- 157.230.65.76

Domains

Welcome, Weekly Micro Training, Monthly Newsletter & Push Notification Emails

- security-reminders.com
- pii-protect.com

Phishing Emails

- it-support.care
- customer-portal.info
- member-services.info
- bankonlinesupport.com
- secureaccess.biz
- logineverification.com
- logmein.com
- mlcrosoft.live
- cloud-service-care.com
- packagetrackingportal.com

Phishing Email Header

This is the Phishing Email Header we use; you can choose to whitelist these as well but not required:

- X-SN-EMAIL-PHISHING

Sender Emails

Whitelist these for the Welcome, Weekly Security Tip & Push Notifications emails:

- No-reply@security-reminders.com
- no-reply@pii-protect.com

Whitelisting for Various Platforms

The methods to do this will depend on the spam filter you are using. Some common filters are listed below along with directions on how to whitelist.

Microsoft 365

Use one of the following methods to whitelist:

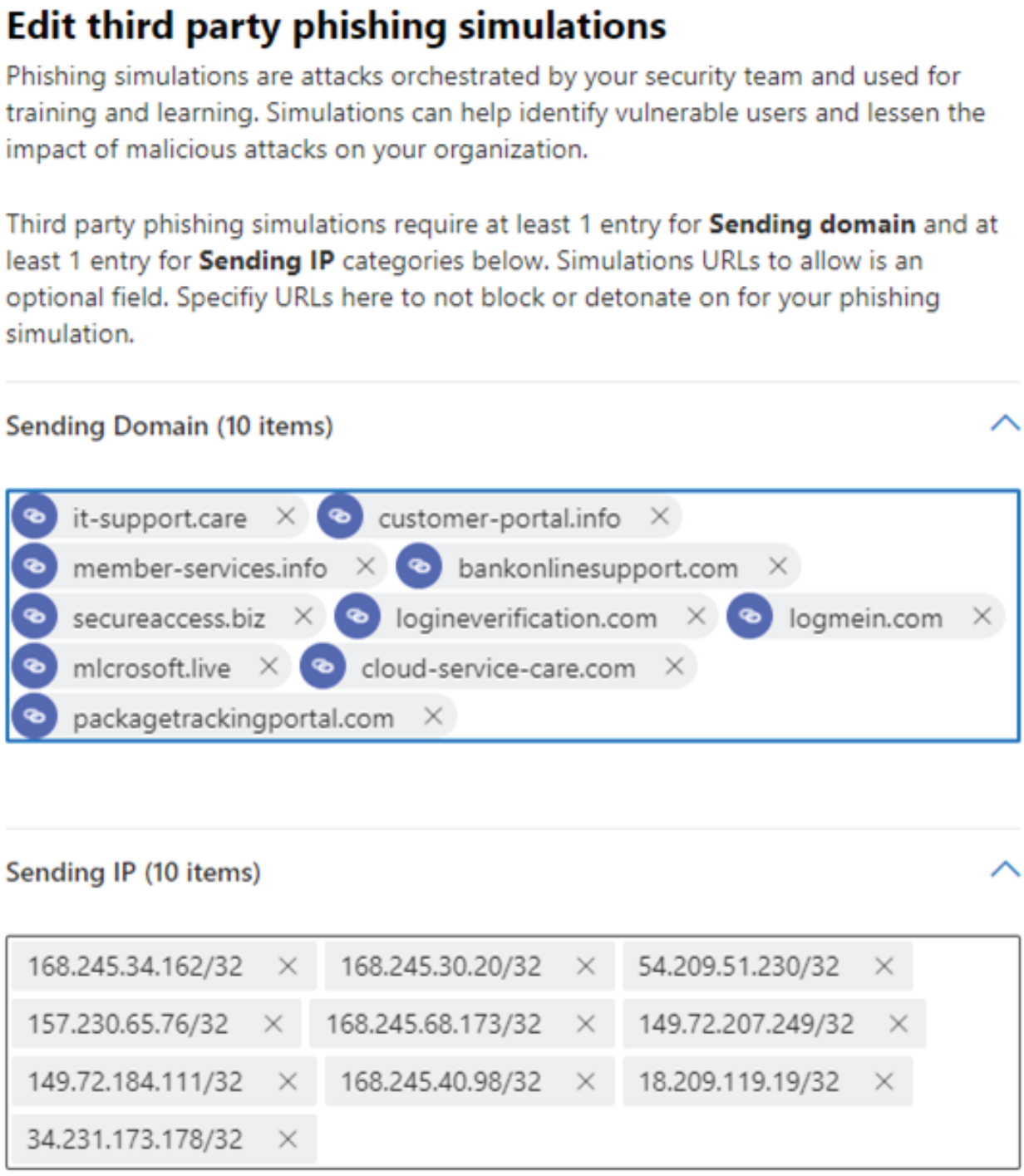
- Powershell Script
- Manually Set Up Advanced Delivery for Third-Party Phishing Simulations

Powershell Script

```
#Requires -Modules ExchangeOnlineManagement
Connect-IPPSSession
$ips = "168.245.34.162/32",
"168.245.30.20/32",
"54.209.51.230/32",
"157.230.65.76/32",
"168.245.68.173/32",
"149.72.207.249/32",
"149.72.184.111/32",
"168.245.40.98/32",
"18.209.119.19/32",
"34.231.173.178/32"

$domainlist = "it-support.care",
"customer-portal.info",
"member-services.info",
"bankonlinesupport.com",
"secureaccess.biz",
"logineverification.com",
"logmein.com",
"mlcrosoft.live",
"cloud-service-care.com",
"packagetrackingportal.com"

$phishRuleName = "BSNPhishSimOverrideRule"

New-PhishSimOverridePolicy -Name PhishSimOverridePolicy
New-PhishSimOverrideRule -Name $phishRuleName -Policy PhishSimOverridePolicy -SenderDomainIs
$domainlist -SenderIpRanges $ips
```

Manually Set Up Advanced Delivery for Third-Party Phishing Simulations

- Log into your Office 365 portal and go into the Admin Center. The 3rd party phishing simulator is under Policies & Procedures > Threat Policies > Advanced Delivery. Add the 8 IP addresses and 10 domains from the lists above.
- Direct Link: https://security.microsoft.com/advanceddelivery?viewid=PhishingSimulation_



Important!

If using the Report Message add-in, a user will receive false positive readings of clicking on links if the tool is used.

- https://support.microsoft.com/en-us/office/use-the-report-message-add-in-b5caa9f1-cdf3-4443-af8c-ff724ea719d2

If You Are Using Microsoft Advanced Threat Protection in Office 365:

Use the following document to set up "do not rewrite" lists:

- https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-a-custom-do-not-rewrite-urls-list-with-atp?view=o365-worldwide

G Suite

Find support for G Suite whitelisting:

- https://support.google.com/a/answer/2368132?hl=en

Other Platforms

Find support for whitelisting other platforms:

- **Exchange 2007:** http://exchangepedia.com/2007/01/exchange-2007-content-filter-the-whitelist-is-here.html
- **Exchange 2010:** https://technet.microsoft.com/en-us/library/bb125225(v=exchg.141).aspx
- **Barracuda Block and Accept Policies:** https://campus.barracuda.com/product/emailsecuritygateway/article/BSF/IPAnalysisInbound/?welcome-to-campus=techlibrary
- **Barracuda Intent Analysis Instructions:** https://campus.barracuda.com/product/emailsecurityservice/article/BESS/IntentInbound/?welcome-to-campus=techlibrary
- **Websense:** http://www.websense.com/content/support/library/web/v76/filter_faqs/filter_faq_whitelist.aspx
- **Trend Micro:** http://esupport.trendmicro.com/solution/en-US/1056393.aspx
- **Forefront Protection for Exchange:** https://technet.microsoft.com/en-us/library/cc483077.aspx