Email Allow List and Best Practices

https://campus.barracuda.com/doc/78153005/

Allow List for Campaign Emails

When you run a Security Awareness Training email campaign, emails are sent to your domain. These emails might be classified as suspicious by email security systems. To ensure that Security Awareness Training campaign emails reach their intended recipients, you *may* need to add Security Awareness Training campaign email domains to the allow lists in your email security systems.

> **Important**! If you are using Barracuda Email Gateway Defense, or are otherwise setting up Microsoft Office 365, you are instructed to create a mail flow rule that bypasses the additional spam filtering that O365 performs. As long as that rule is in place, these emails will flow directly to the users' inbox and the Allow List instructions here *do not* apply.

If you are not setting up with O365 or using Barracuda Email Gateway Defense, meet with your email security system vendor or administrator to have them allow the Security Awareness Training campaign email domains or the IP addresses for the Security Awareness Training mail servers. If you decide to allow by domain, include the *email server* domain you select when you configure the domain.

Emails coming from standard Security Awareness Training servers to your organization will originate from one or more of these IP addresses. Allow these IP addresses for the Security Awareness Training email servers on your email security system or service:

- `64.132.201.82`
- `64.132.201.93`
- `74.203.211.2`
- `74.203.211.13`
- `207.67.44.178`
- `207.67.44.189`

All SMTP servers sending emails for Barracuda-supplied domains identify themselves in the Received header as `mail.spearphish.com`. Barracuda recommends that you check only the `spearphish.com` domain if you are allow listing by the Received header. The `spearphish.com` domain should only be in the two oldest Received headers. Here is an example of Received headers:

```
Received: from mail.spearphish.com (207.67.44.189) by xxx.xxx.xxx
(NNN.NNN.NNN.NNN) …; Wed, 3 Feb 2022 11:15:05 +0000
```

```
Received: from localhost (localhost [127.0.0.1]) by mail.spearphish.com
(Postfix) with ESMTP id NNNNNNNNNN for <xxxx@example.com>; Wed, 3 Feb 2022
05:15:05 -0600 (CST)
```

`xxx.xxx.xxx.xxx (NNN.NNN.NNN.NNN)` is the host name and IP address of the receiving mail server. `NNNNNNNNN` is a numeric ESMTP id.

The message Return-Path header will be set to `reply_xxxxxxxxxx@[from domain]`, where `xxxxxxxxx` is replaced with a random identifier and the `From domain` will be replaced with one of the domains specified in the campaign's email accounts. Note that some mail gateways and mail servers might strip the Return-Path header before it reaches the user's mailbox. If you plan to use the Return-Path header, you must confirm that the header is not stripped before it reaches the user's mailbox.

The Envelope Sender Address is not the same as the From header and will not match. The Envelope Sender Address matches the Return-Path. The From header matches one of the Email Accounts specified in the campaign.

Changes in the Google and Outlook mail clients that now expose that the Return-Path is set to `[mailbox]@spearphish.com` required an update to the way return mail is routed. The Envelope Sender Address and the Return-Path header are now set to an email address with the same domain as specified in the Security Awareness Training email account.

- If you are using the Envelope Sender Address or the Return-Path header to allow email messages from the Barracuda system, you must allow based on the campaign's email account From email address or From email domain.
- If you are using an email-only domain that you own, the Return-Path will still be set to `reply_xxxxxxxxx@spearphish.com`.

The SMTP domains are configured with both the Sender ID Framework (SPF) and the DomainKeys Identified Mail (DKIM) DNS TXT record types. The Barracuda inbound SMTP servers identified by DNS MX records are used for receiving replies, delivery notifications, and out-of-office messages from your email system to Barracuda.

- 10 mail.spearphish.com (IP will be set to be identical to one of the IPs used below for mail1, mail2, or mail3)
- 20 mail1.spearphish.com 64.132.201.93
- 30 mail2.spearphish.com 74.203.211.13
- 40 mail3.spearphish.com 207.67.44.189

Note: You can also configure the system to use third-party SMTP email servers for some campaigns. This is a non-standard option that requires additional allow list details.

Preventing Emails from Going to Junk Email

Office 365

To prevent emails from going to the junk email in Office 365:

1. In Office 365, open the Exchange Online Admin Center. Navigate to **Protection > Spam Filter**.
2. Create a new spam filter. Name it something like *Allow <campaign_name> domain email*.
3. In the **Allow Lists** area, locate the **Allowed Sender** area. Enter the From email address(es) that you use in each of your campaigns (e.g., `noreply@endtrust.net`).
4. In the **Applied to** area, add your domain information.
5. Save this filter and make it a higher priority than the default spam filter provided with Office 365.

Note that you must perform these steps again for future campaigns that use different emails and domains.

Office 2013

There are two ways to prevent emails from going to the junk email in Office 2013.

Method 1: Safe Sender

Create a Safe Sender list and deploy it using Group Policy. Refer to the Microsoft documentation on safe senders for details.

Method 2: Completely Disable the Junk Email Folder

Use a Group Policy to set the following registry settings to completely disable the Junk email folder in each user's Outlook client:

- HKEY_CURRENT_USER\Software\Policies\Microsoft\office\14.0\outlook
- DWORD: Disable Antispam
- Value of 1 disables the junk filter

The Outlook Email client determines which content goes into the Junk email folder, and it is not controlled by Exchange.

Note that the Group Policy setting does not apply if your users use web mail to check their email. Refer to the next section, **Disabling the Junk Email Folder in Office 365**, for more information.

Disabling the Junk Email Folder in Office 365

You can disable the Junk email folder for all mailboxes by using PowerShell.

> This technique is provided as an alternative method for handling junk and spam emails. Your organization must determine if it is appropriate to remove Junk folders for all inboxes.

To disable the Junk email folder:

1. Connect to your Office 365 instance with PowerShell.
2. Run this command to get the current setting for all users:
   `Get-Mailbox | get-mailboxjunkemailconfiguration`
   When you initially run this script, the **Enabled** attribute (the status of Office 365's built-in junk email processing) is reported as **True** for all users.
3. Run this command to disable junk processing on each mailbox:
   `get-mailbox|set-mailboxjunkemailconfiguration -enabled $false`
   This command sets the **Office Junk Mail** folder to **False** for all of the user mailboxes, including shared and service mailboxes.

Office 365 Partner Connector Setup

To prevent IP addresses from being waitlisted during campaigns, all clients using Office 365 must create a partner connector that includes IP addresses from the Security Awareness Training allow list document.

> Refer to Microsoft's documentation on Office 365 Partner Connectors for detailed instructions.

For your Office 365 partner connector:

1. Select **Use the sender's IP address** and enter the following IPs:
   - `64.132.201.82`
   - `64.132.201.93`
   - `74.203.211.2`
   - `74.203.211.13`
   - `207.67.44.178`
   - `207.67.44.189`
2. Ensure that **Reject email messages if they aren't sent over TLS** is selected.
3. Save the partner connector.

Allowing by IP Address in Office 365

Set Up your IP Allow List

1. Log into your Office 365 Admin Portal. Under **Apps**, go to **Admin**.
2. Under **Admin Centers**, select **Exchange**.
3. In the **Protection** section, click **Connection Filter**.
4. Click the pencil icon to edit the default Connection Filter policy.
5. In the IP Allow List, click the plus sign to add an IP address.
6. Enter the IP addresses listed at the beginning of this article.
7. Click **OK**, then click **Save**.
   Continue with the next section below.

Bypass Spam Filtering and the Clutter Folder

1. Navigate to **Admin > Mail > Mail Flow**.
2. Under **Mail Flow > Rules**, click the plus button and select **Create a new rule...**
3. Provide a name for the rule.
4. Click **More Options**.
5. Make selections to create this logical statement: **Apply this rule if... The Sender... IP address is in any of these ranges or exactly matches**.
6. Specify the IP addresses listed at the beginning of this article, then click **OK**.
7. On the **Modifying the message properties** page, under **Do the following**, click **Modify the message properties**, then **Set a Message Header**.
8. Set the message header **X-MS-Exchange-Organization-BypassClutter** to the value **true**. Click **OK**.
   Note that both of these values are case-sensitive.
9. Back under **Do the following**, select **Modify the message properties**.
10. Select **Set the spam confidence level (SCL) to**, then select **Bypass Spam Filtering**.
11. Click **Save**.

Microsoft 365 Defender and ZAP

Microsoft 365 Defender with Microsoft ZAP (Zero-hour purge) blocks phishing messages, including legitimate, *simulated* phishing attacks used for training from Barracuda.

If you use Microsoft 365 Defender to protect your email, configure it to allow campaign emails and avoid machine clicks on links within campaign emails.

For additional information and full instructions, refer to Using Microsoft 365 Defender with Security Awareness Training.

Google Safe Browsing Initiative

This Google policy might block Security Awareness Training phishing domains that you want to use in your campaigns.

To remove this Google block on one or more Barracuda phishing domains, add the blocked domains to the SafeBrowsingAllowlistDomains parameter of Chrome's Enterprise Policy configuration.

For full instructions, refer to Disabling Google Safe Browsing Warning Message Using Group Policy.

Additional Best Practices

The following sections describe additional methods of optimizing your setup of Security Awareness Training, but they are not required.

Landing Page Server Allow List

When users click a link within a campaign message, they are directed to an HTTP or HTTPS Landing Page server. The IP addresses of the Landing Page servers include:

- 64.132.201.82
- 64.132.201.92
- 74.203.211.2
- 74.203.211.12
- 207.67.44.178
- 207.67.44.188

You can also allow based on the domain name used for each campaign.

Administrative Web Application Allow List

Administrative functions are available using encrypted SSL/TLS at https://phishline.com hosted at one of the following IP addresses:

- 64.132.201.82
- 74.203.211.2
- 207.67.44.178

We strongly recommend you use Barracuda's multifactor authentication (MFA) option for all administrative users.

Educational Content and Survey / Content Delivery Network Allow List

Barracuda's Security Awareness Training servers are located in the Midwest region of the United States. With our worldwide customers, there is always a concern about reducing latency and bandwidth delays when showing educational videos. To solve that, Barracuda can distribute the read-only multimedia content using a reputable Content Delivery Network (CDN). For security reasons, training content is only delivered via HTTPS.
To create an allow list for educational content and surveys, use the following:

- `https://phishline.com`
- `https://*.phishline.com`
- `https://fonts.googleapis.com`
- `https://fonts.gstatic.com`
  Note: The CDN option is only used to distribute the **Image Gallery** components including MP4, WEBM, JPG, GIF, and similar file types. Barracuda recommends you allow list requests and responses for static multimedia content only. The web application and data collection are exclusively performed on the Security Awareness Training servers even with the CDN option.

Important

Using web proxies or content caching interferes with the normal communication between the user and the LMS (Learning Management System) and can result in data inaccuracies.

To avoid this issue, add the entries in this section to the allow list for the web proxy and exclude them from caching. Add *either one* of the following lists of entries:

• `https://phishline.com` • `https://*.phishline.com`	• `https://phishline.com` • `https://lmscs.phishline.com` • `https://lmsjs.phishline.com` • `https://lmsps.phishline.com`

Landing Page “Enable Local IP Detection”

There are two methods to enable detection of the local/non?natted IP address of a browser.

Enable Local IP Detection

To enable JavaScript/Java Local IP Detection Logic, navigate to **Campaigns > Landing Pages > Landing Page Manager**, and select the **Enable Local IP Detection** check box. Note that this setting is *disabled* by default to minimize the chances that users would receive JavaScript, Java, or other errors/warnings on landing pages.

When you enable local IP detection, each web page might attempt to create a WebRTC connection using stun:stun.services.mozilla.com. Be advised that Barracuda does not control this server. Upon

request, Barracuda can provide firewalled access to our hosted stun/RFC 3489 service. If you choose to block access to any/all stun services, the other techniques will be attempted, such as using a custom Java applet. This technique can help augment the data collected for Portable Media Campaigns, where no user information can be associated with the Smart Attachment.

X_FORWARDED_FOR Headers

If you do not want to Enable Local IP Detection on a landing page, you can use industry-standard X_FORWARDED_FOR headers. Configure your proxy/NAT firewall to provide these headers. Depending on your network and risk environment, you might be able to configure it to selectively send those headers to the Barracuda web servers rather than sharing with all sites.

Mail Transport Routing

Barracuda strongly recommends a direct mail connection to your email server. This eliminates issues with antivirus/antispam filtering services. These filtering services can cause false clicks or block mock phishing emails entirely if they are not configured properly to allow the emails coming from the Barracuda email servers. Using a mail transport to directly route emails from the PhishLine email servers to your mail server eliminates these issues. To implement mail transport routing, Barracuda needs direct access to TCP port 25 on your email server's external IP. This usually requires a new firewall rule on your company firewall that allows this direct connection. The only other requirement is to provide Barracuda with your mail server’s public host name or public IP address.

Email Address Allow List

You might also combine the above allow list techniques with email account-specific rules based on the addresses used to send out each campaign. For example, you might choose to add `noreply@neverclick.net` to your safe senders list using Group Policy to facilitate delivery of campaign emails directly to user inboxes. Be sure to combine this type of allow listing with IP/DKIM/SPF allow listing. You do not want to allow list a domain or account only to open the door to real attackers. It is also a best practice to disable all allow list settings upon campaign completion.

Gmail Customers

Refer to this support link.

- https://support.google.com/a/answer/60751?hl=en

As a G Suite administrator, you can help ensure that messages received from specific sending IP addresses do not get marked as spam. Do this by adding the addresses to an email allow list in your Google Admin console. When you create an email allow list for your G Suite account, it affects your entire domain. You cannot create email allow lists that apply to specific organizational units. See other settings you might use instead.

Other Usage Considerations

- **Malicious Code**: Barracuda will never intentionally send you malware. Therefore, there is no reason to ever allow list antivirus or other malicious code filters. It is an important layer of protection you should keep in place.
- **Timing**: If you are using domain-based or email-account-based allow listing, you will likely want to limit those to the duration of your campaign. Otherwise, you could enable real attackers to misuse your allow list in the future.
- **Domain Name**: Each campaign lists the domain names that will be used to deliver your campaign content. Some administrators prefer to allow list by domain instead of IP. Be sure to take measures to prevent real attackers from exploiting those allow listed domain names for real attacks.
- **Email Accounts**: Each campaign lists all of the email accounts that will be used to deliver your campaign content.
- **Web Pages**: Each campaign lists the web page servers. If you choose to use the Content Delivery Network acceleration for Multimedia Content, you must add `media.phishline.com` as a domain name.
- **Message Content**: Many filters examine actual message content. Within the message template editor, Security Awareness Training also provides a spam filtering score based on a popular antispam solution. To ensure delivery of messages, each campaign allows you to send test emails, so you can test the delivery of the messages and replies, while also confirming that the landing page links work.

Additional Help

If you have any questions about using allow lists, contact Barracuda Technical Support.

You can also allow list Security Awareness Training for Barracuda Email Security Gateway.

Figures