Whitelisting Barracuda PhishLine

https://campus.barracuda.com/doc/75170371/

For additional Barracuda product whitelisting, see:

- Barracuda Web Security Gateway – Creating Block and Accept Policies
- Barracuda NextGen Firewall F – How to Create a URL Filter Policy Object

For additional information on whitelisting, contact your Barracuda product vendor.

Barracuda PhishLine uses advanced training and simulation to measure your organization's vulnerability to phishing emails and teach your users how to avoid becoming victims of data theft, malware, and ransomware. To deploy PhishLine in your organization, you must first whitelist PhishLine's IP address ranges and domains.

Message Content
Many filters examine actual message content. Within the message template editor, PhishLine provides a spam filtering score based on a popular anti-spam solution. To ensure message delivery, each campaign allows you to send test emails to test the delivery of messages and replies while confirming the landing page links work.

Best Practice

Once the PhishLine campaign is complete, you can disable the whitelisting settings.

Whitelist PhishLine IP Addresses

Barracuda recommends whitelisting IP addresses instead of whitelisting domains. This is because spammers can use an exempt email address to bypass filtering; as such, **IP whitelisting is a more reliable way to identify trusted domains and is recommended over whitelisting domains**.

To implement your PhishLine campaign, you must first whitelist the following IP addresses:

- 64.132.201.82
- 64.132.201.92
- 64.132.201.93

- 74.203.211.2
- 74.203.211.12
- 74.203.211.13
- 207.67.44.178
- 207.67.44.188
- 207.67.44.189

To whitelist these IP addresses:

1. Log in to your Barracuda Email Security Gateway web interface.
2. Go to the **BLOCK/ACCEPT > IP Filters** page.
3. In the **Allowed IP/Range** section, enter the first PhishLine Server in the **IP/Network Address** field.
4. In the **Netmask** field, type `255.255.255.255`.
5. Optionally, add a note in the **Comment** field. For example, type: `PhishLine IP Address`
6. Click **Add** to whitelist the entered IP address.
7. Complete steps 2 through 6 for each of the PhishLine IP addresses.

Whitelist Campaign Email

If the email sender and recipient addresses are the same, the Barracuda Email Security Gateway disregards any whitelisting and processes the mail normally. This is done because spammers know that users tend to whitelist their own email address.

In addition to whitelisting the PhishLine IP addresses, you can set specific rules on email addresses used to send out the PhishLine campaign to your users.

1. Log in to your Barracuda Email Security Gateway web interface.
2. Go to the **BLOCK/ACCEPT > Sender Filters** page.
3. In the **Allowed Email Addresses and Domains** section, enter the first recipient email address you want to always exempt (whitelist) in the **Email Address/Domain** field.
4. Optionally, add a note in the **Comment** field. For example, type: `PhishLine Campaign Email`
5. Click **Add** to whitelist the entered address.
6. Complete steps 2 through 5 for any additional email addresses you want to whitelist.

Whitelist by Domain

Each campaign lists the domain names used to deliver your campaign content. You can whitelist a domain on the **Inbound Settings > Sender Policies** page. Adding a domain, subdomain, or email

sender and selecting **Exempt** always accepts, or "whitelists" messages, meaning that:

- Messages from whitelisted senders bypass spam scoring, Intent Analysis, content filters, and Sender Policy Framework (SPF)
- Virus scanning and rate control are still applied

  Spammers can use an exempt email address to bypass filtering; as such, **IP whitelisting is a more reliable way to identify trusted domains and is recommended over whitelisting domains.**

  To whitelist email addresses and.or domains:

1. Log in to your Email Security Gateway web interface.
2. Go to the **BLOCK/ACCEPT > Sender Filters** page.
3. In the **Allowed Email Addresses and Domains** section, enter the domain name you want to whitelist.
4. Optionally, add a note in the **Comment** field, for example, type: `PhishLine Domain`
5. Click **Add** to whitelist the entered domain.
6. Complete steps 2 through 5 for any additional domains you want to whitelist.