Anti-Fraud and Anti-Phishing Protection

https://campus.barracuda.com/doc/96023011/

If you make setting changes, allow a few minutes for the changes to take effect.

Phishing scams are typically fraudulent email messages that appear to come from legitimate senders, for example, a university, an Internet service provider, or a financial institution. These messages usually contain a URL that, when clicked, directs the user to a spoofed website or otherwise tricks the user to reveal private information such as login, password, or other sensitive data. This information is then used to commit identity and/or monetary theft.

You can configure Email Gateway Defense to evaluate and rewrite fraudulent URLs so that, when clicked, the user is safely redirected to a valid domain or to a Barracuda Networks domain warning of the fraud.

To configure, log into Email Gateway Defense, and go to the **Inbound Settings > Anti-Phishing** page:

- **Anti-Fraud Intelligence** – This Barracuda Networks anti-phishing detection feature uses a special Bayesian database for detecting Phishing scams.
- **External Sender Warning** – When set to **On**, adds a banner to the top of all inbound emails that originate from outside your organization, cautioning your users about opening attachments and clicking links.

  If the email body does not contain any text or html, the external warning will not be added.
- **Email warning banners** – Notification banners will display if there are any potential threats identified in the email. For more information, see Email Warning Banner Messages. **Note** that this feature is currently available as a beta release and will be gradually rolled out to customers.
  - **On** – Notification banners are turned on for all users.
  - **Trial Mode** – Notification banners are turned on only for a select set of users. Enter the desired user email addresses separated by commas.
  - **Off** – Notification banners are turned off for all users.
- **Intent Analysis** – When set to **On**, Email Gateway Defense scans for links inside documents sent as attachments in email. Scanning occurs when the message is processed and delivered. This process checks the links inside attachments for malicious content. If malicious content is detected in the message, the **Content Intent** action is performed on the message:
  - **Content Analysis** – Select whether to **Block**, **Quarantine**, or **Defer** messages detected by **Intent Analysis** to contain malicious content. Set to **Off** to take no action.
- **Link Protection** – When set to **Yes**, the service automatically rewrites a deceptive URL in an email message to a safe Barracuda Networks URL, and delivers that message to the user. The following are exempt from Link Protection:
  - Sender email addresses added under **Inbound Settings > Sender Policies**

- URLs/domains under **Intent Domain Policies** set as **Ignore**
- URLs/domains that are trusted by Barracuda Networks

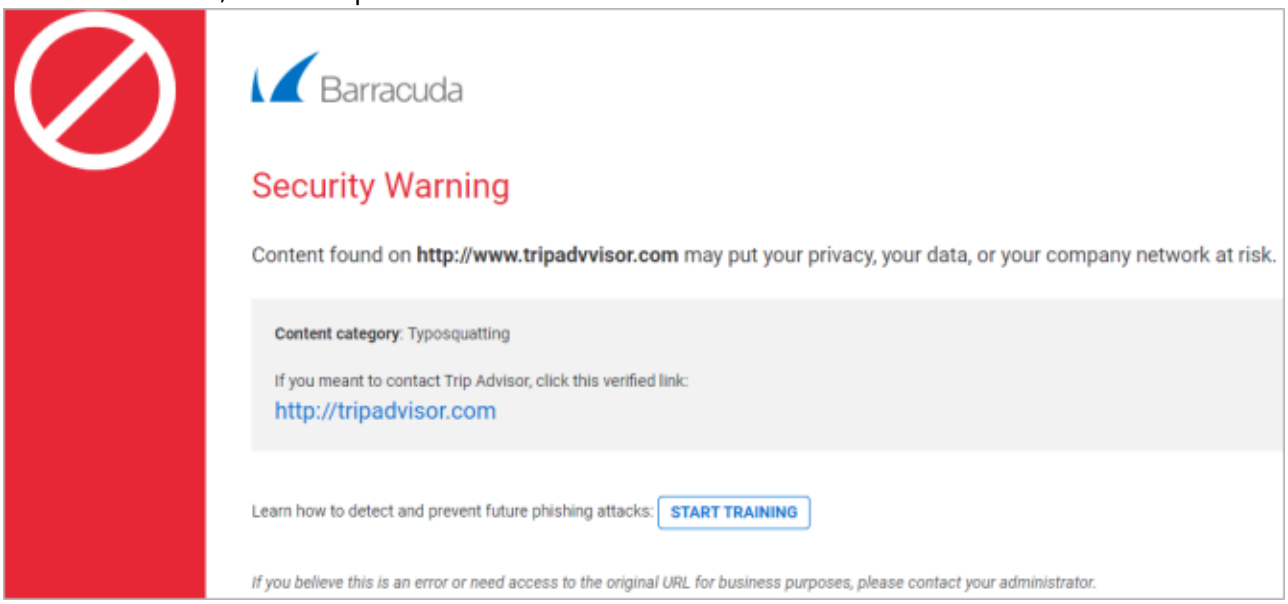
When Link Protection is enabled, URLs are *not* rewritten if:

- The URL is exempt
- The URL is contained in an encrypted message
- The URL is within an attachment

Note that Email Gateway Defense maintains a list of exempted domains for Link Protection.

Link protection employs the Advanced Threat Protection (ATP) service when evaluating URLs that could lead the user to open a bad file. To disable ATP for links, you must disable Link Protection.

When the user clicks the URL, the service evaluates it for validity and reputation. If the domain is determined to be valid, the user is directed to that website. If the URL is suspicious, the user is directed to the Barracuda Link Protection Service warning page which displays details about the blocked URL, for example:



To minimize false positives and page load delays, Barracuda Networks maintains a list of domains considered safe. Because of this, some links detected in messages are wrapped while others are not. For example, Barracuda Networks does not currently wrap google.com, but does wrap googlegroups.com because it provides user-generated content.

- **Typosquatting Protection** – Typosquatting is a common trick used by hackers to fool users into thinking they are visiting a valid domain but the domain name is misspelled. Typosquatting is detected only if the URL is rewritten, that is, if it is not exempt. When clicked, the user is taken to a different domain that may be spoofing the expected domain. The **Typosquatting Protection** feature checks for common typos in the URL domain name and, if found, rewrites the URL to the correct domain name so that the user visits the intended website. For example, if the URL **https://www.tripadivsor.com** (where the 'i' and 'v' positions are switched in the domain name) appears in an email message, the service detects the typo and rewrites the URL to the valid domain **https://www.tripadvisor.com**. Note that **Link Protection** must be set to

Yes before you can enable **Typosquatting Protection**.

Figures

1. linkprotect_example1.png