Anti-Fraud and Anti-Phishing Protection

https://campus.barracuda.com/doc/54267210/

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.

Using the features described in this article require that you first set up the Cloud Protection Layer (CPL) service with your Barracuda Email Security Gateway. You can configure the Cloud Protection Layer to evaluate and rewrite fraudulent URLs so that, when clicked, the user is safely redirected to a valid domain or to a Barracuda domain warning of the fraud.

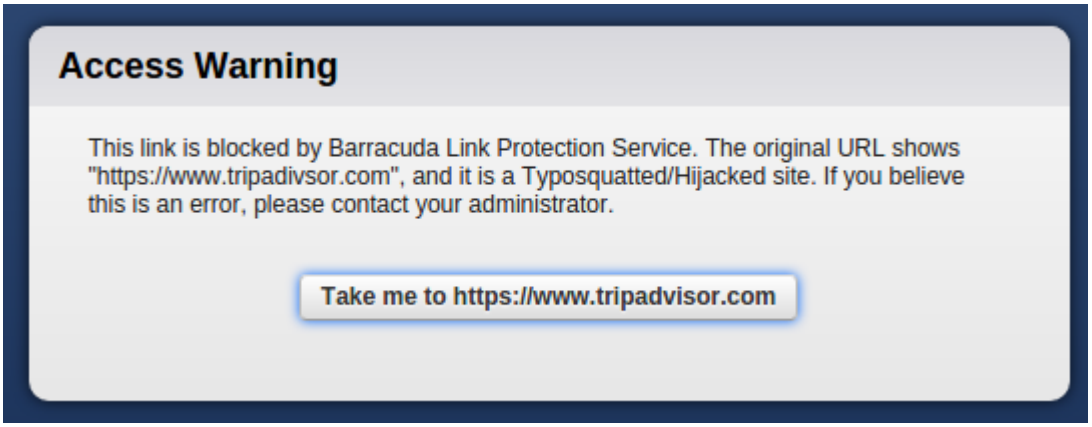
The Barracuda Cloud Protection Layer is available with a current Advanced Threat Protection (ATP) subscription. See setup instructions in the article Cloud Protection Layer.

To configure, log in to the Cloud Protection Layer, 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.
- **Intent Analysis** – When set to **On**, the Cloud Protection Layer 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** 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 URL, and delivers that message to the user.

  When Link Protection is enabled, URLs are not rewritten if:
  - The URL is exempt
  - The URL is contained in an encrypted or protected message
  - The URL is within an attachment

  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 maintains a list of domains considered safe. Because of this, some links detected in messages are wrapped while others are not. For example, Barracuda 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.tripadivsor.com**. Note that **Link Protection** must be set to **Yes** before you can enable **Typosquatting Protection**.

  Barracuda typosquatting works with tools such as Desvio to determine misspelled domain names. To protect your misspelled domains, contact providers such as Desvio to add your misspelled domain name variations to their list.

Figures