Intent Analysis - Inbound Mail

https://campus.barracuda.com/doc/96023008/

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

The intent of spam messages is to get a user to reply to an email, to visit a web site, or to call a phone number. Intent analysis involves researching email addresses, web links (URLs), and phone numbers embedded in email messages to determine whether they are associated with legitimate entities. Phishing emails are examples of Intent.

Frequently, Intent Analysis is the defense layer that catches phishing attacks. Intent Analysis can be enabled or disabled on the **Inbound Settings > Anti-Phishing** page. Domains found in the body of email messages can also be blocked based on or exempt from Intent Analysis on that page. See also Anti-Fraud and Anti-Phishing Protection.

Email Gateway Defense applies the following forms of Intent Analysis to inbound mail, including real-time and multi-level intent analysis.

Full URL Classifier

At the time of email processing, the classifier will trigger a virtual scan of any unknown URLs and save the verdict in Barracuda Real-Time System (BRTS). The next time an email is seen with the same normalized URL again, BRTS intent analysis will trigger a block on malicious URLs. The URL classifier uses machine learning and variety of threat intelligence data to identify malicious URLs that have never been seen before. This helps to identify new malware or phishing URLs, feed this intelligence to BRTS, and block these attacks in the future.

Intent Analysis

Markers of intent, such as URLs, are extracted and compared against a database maintained by Barracuda Central.

Real-Time Intent Analysis

For new domain names that may come into use, Real-Time Intent Analysis involves performing DNS lookups against known URL block lists.

Multilevel intent analysis

Use of free websites to redirect to known spammer websites is a growing practice used by spammers to hide or obfuscate their identity from mail scanning techniques such as Intent Analysis. Multilevel Intent Analysis involves inspecting the results of Web queries to URLs of well-known free websites for

redirections to known spammer sites.