Link Protection (URL/Link re-writing and analysis)

Included in Zix Email Threat Protection, Advanced Email Threat Protection, and select Email Security and/or Compliance Bundles.

Link Protection

Malicious links are a common theme in today's modern malware and phishing campaigns. Popular website development tools (WordPress, Drupal, etc.) are providing a back door for attackers to host their malicious content on legitimate websites without the owner's knowledge. Zix Email Threat Protection's Link Protection service addresses these, and attacks from linked malware and phishing attacks.

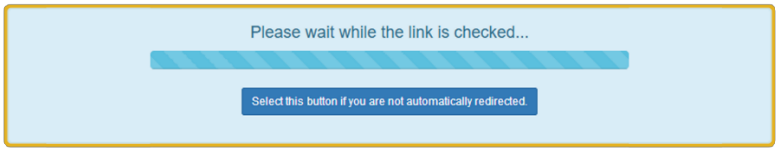
Link Protection replaces all full, shortened, or obfuscated links in an email message with "wrapped" equivalents before the recipient receives the message, delivering an additional layer of protection against possible threats. When a "wrapped" link is clicked, it's redirected to our sandbox system which immediately examines the destination for suspicious behavior or known malicious content. Based on testing, the user is either automatically redirected to the site, or is provided a warning with details of the tests performed.

Policies are configurable for each domain, with scoping flexibility to activate it for all users of a domain, all users of a domain with specific per-user exclusions, or active for only specific users.

Policy options include Trusted Domains and Links, which include both full domains and sub-domains. Domains can be entered using wildcards to match variations. Links matching one of the Trusted Domains and Links are not replaced.

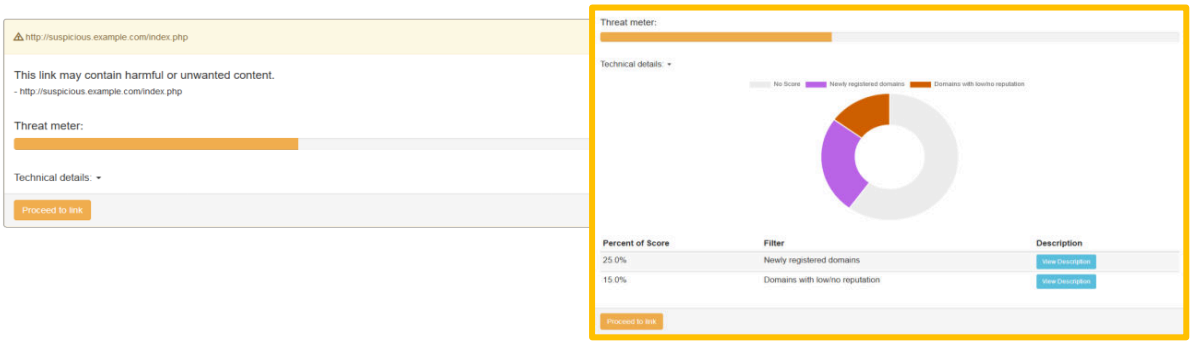
Additional options include appending an email footer indicating links have been replaced. The system provides default text, which can be customized to meet the customer's desired wording/phrasing and security policies.

User experience involves the following pop-up window while links are being tested.

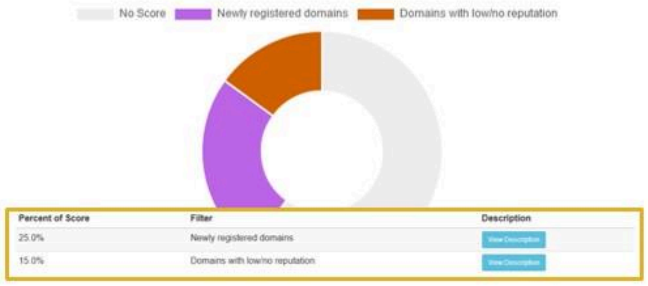


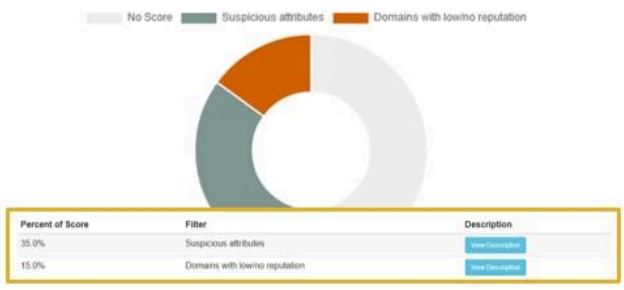
If the original link does not match any filters, once analysis completes, the user is automatically redirected to the destination.

If the original link is found to be suspicious, the user is warned and provided a threat meter and an analysis report with additional technical details. Users have the option to proceed to the link.

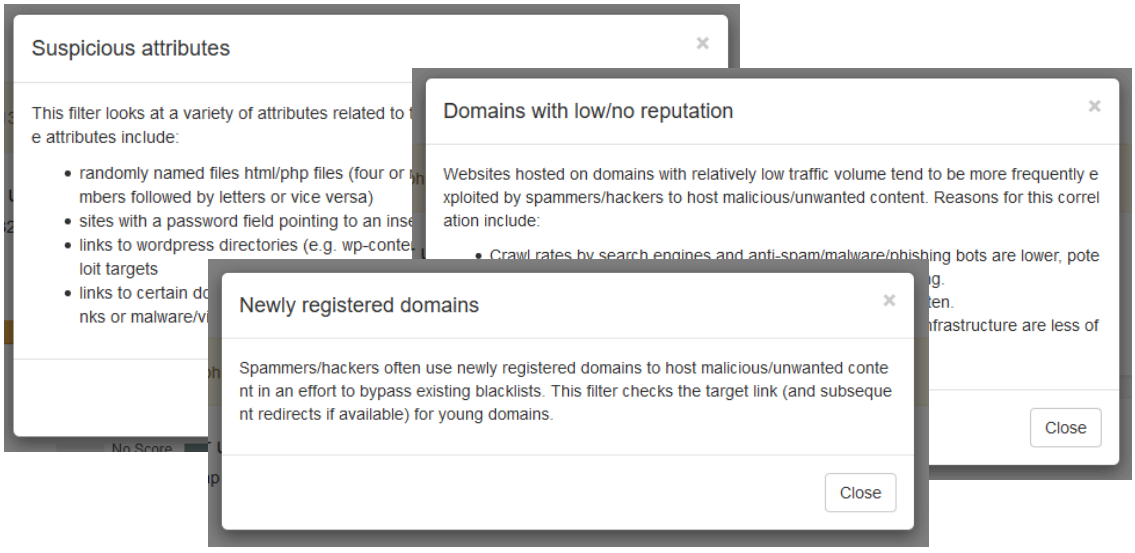


Users can view Technical Details, providing a breakdown on why a link received a warning. This consists of a Percent of Score for a filter and more information about the filters.





To learn more about why a filter matched the link, the "View Description" provides a pop-up with in-depth information about the filter and attributes that lead to its scoring. With this information, users can better determine if they should turn back or proceed.



If the original link is found to have harmful or unwanted content, the user is given a warning with technical details. Blocked links do not have an option for the user to proceed. The "View Description" link provides a pop-up containing an in-depth explanation about the filter and reason for blocking.