

CLAIMS

What is claimed is:

1. A method for providing pre-emptive intercept warning for online privacy or security, comprising:
 - at a privacy security appliance comprising at least one computer processor:
 - establishing a virtual private network (VPN) connection with a computer application executed by a client device;
 - receiving, over the VPN connection, an internet protocol request for a website host;
 - communicating the internet protocol request to the website host;
 - receiving a response to the internet protocol request from the website host;
 - inspecting the response for privacy or security issues with embedded links in the response;
 - scoring the embedded links based on the inspection;
 - generating a mock webpage based on the response comprising the scoring for the embedded links; and
 - delivering the mock webpage with the scoring to the application over the VPN;
 - wherein the mock webpage comprises links to the embedded links.
2. The method of claim 1, wherein the privacy security appliance obfuscates identifying information for the application and the client device before communicating the internet protocol request to the website host.

3. The method of claim 1, wherein the application comprises a web browser.

4. The method of claim 1, further comprising:
retrieving, from a database, a privacy policy associated with one of the embedded links, wherein the embedded link is scored based on the privacy policy.

5. The method of claim 1, further comprising:
determining that the embedded link is on a blacklist of websites, wherein the embedded link is scored based on its presence on the blacklist.

6. The method of claim 1, further comprising:
determining that the embedded link is on a blacklist of websites, wherein the embedded link is scored based on its presence on the blacklist.

7. A method for providing pre-emptive intercept warning for online privacy or security, comprising:
at a privacy security appliance comprising at least one computer processor:

receiving, from a plug-in for an application executed by a client device, a response to an internet protocol request from a website host, the internet protocol request submitted by the application;

inspecting the response for privacy or security issues with embedded links in the response;

scoring the embedded links based on the inspection;

generating a mock webpage based on the response comprising the scoring for the embedded links; and

delivering the mock webpage with the scoring;
wherein the mock webpage comprises links to the embedded links.

8. The method of claim 7, wherein the application comprises a web browser.

9. The method of claim 7, further comprising:
retrieving, from a database, a privacy policy associated with one of the embedded links, wherein the embedded link is scored based on the privacy policy.

10. The method of claim 7, further comprising:
determining that the embedded link is on a blacklist of websites,
wherein the embedded link is scored based on its presence on the blacklist.

11. The method of claim 7, further comprising:
determining that the embedded link is on a blacklist of websites,
wherein the embedded link is scored based on its presence on the blacklist.

12. A method for providing pre-emptive intercept warning for online privacy or security, comprising:

at a privacy security appliance comprising at least one computer processor:

establishing a virtual private network (VPN) connection with a computer application executed by a client device;

receiving, over the VPN connection, an internet protocol request for a website host;

communicating the internet protocol request to the website host;
receiving a response to the internet protocol request from the website host;
inspecting the response for privacy or security issues with embedded links in the response;
scoring the embedded links based on the inspection;
associating the scores with each embedded link; and
delivering the response with the scoring to the application over the VPN as a mock webpage;
wherein the mock webpage comprises links to the embedded links.

13. The method of claim 12, wherein the embedded scoring is not presented until activated.

14. The method of claim 13, wherein the embedded scoring is activated by hovering over the embedded link or selecting the embedded link.

15. The method of claim 12, further comprising:
modifying HTML in the response to display the score for each embedded link.

16. The method of claim 12, wherein the privacy security appliance obfuscates identifying information for the application and the client device before communicating the internet protocol request to the website host.

17. The method of claim 12, wherein the application comprises a web browser.

18. The method of claim 12, further comprising:
retrieving, from a database, a privacy policy associated with one of the embedded links, wherein the embedded link is scored based on the privacy policy.

19. The method of claim 12, further comprising:
determining that the embedded link is on a blacklist of websites, wherein the embedded link is scored based on its presence on the blacklist.

20. The method of claim 12, further comprising:
determining that the embedded link is on a blacklist of websites, wherein the embedded link is scored based on its presence on the blacklist.