

CLAIMS

~~What is claimed is:~~

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

~~———at establishing, by 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, by the privacy security appliance and from the computer application over the VPN connection, an ~~internet protocol~~Internet Protocol (IP) request for a website host; communicating the ~~internet protocol~~, by the privacy security appliance, the IP request to the website host; receiving, by the privacy security appliance, a response to the ~~internet protocol~~IP request from the website host;~~

~~, the response including a webpage comprising a plurality of embedded links; inspecting, by the privacy security appliance, the response for privacy or security issues with the embedded links in the response;~~

~~———; scoring, by the privacy security appliance, each of the embedded links based on the inspection; generating, by the privacy security appliance, a mock webpage based on the response comprising, wherein the mock webpage does not include integrated elements to be stored or executed by a browser of the client device and represents a visual appearance of the webpage, wherein the embedded links are replaced with links to the embedded links, and wherein code in the mock webpage includes the scoring for each of the embedded links for display on the client device; and delivering, by the privacy security appliance, the mock webpage with the scoring to the computer 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 computer application and the client device before communicating the ~~internet protocol~~IP request to the website host.

3. The method of claim 1, wherein the computer 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: receiving, by a privacy security appliance and from a plug-in for a computer application executed by a client device, a response to an Internet Protocol (IP) request from a website host, wherein: the IP request is submitted by the computer application without use of the plug in, and the response is intercepted by the plug-in and is re-routed to the privacy security appliance, the response including a webpage comprising a plurality of embedded links; inspecting, by the privacy security appliance, the response for privacy or security issues with the embedded links in the response; scoring, by the privacy security appliance, the embedded links based on the inspection; generating, by the privacy security appliance, a mock webpage based on the response, wherein the mock webpage does not include integrated elements to be stored or executed by a browser of the client device and represents a visual appearance of the webpage, and wherein the embedded links are replaced with links to the embedded links; and delivering, by the privacy security appliance, the mock webpage with the scoring to the plug-in, wherein the plug-in provides the mock webpage to the computer application for display with the plug-in causing information associated with the scoring to be displayed over the mock webpage.

8. The method of claim 7, wherein the computer 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.

~~5. 10. The method of claim 47, 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 establishing, by 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, by the privacy security appliance and from the computer application over the VPN connection, an internet protocol~~Internet Protocol (IP) request for a website host; communicating the internet protocol,~~ by the privacy security appliance, the IP request to the website host; receiving, by the privacy security appliance, a response to the internet protocol~~IP request from the website host;~~

, the response including a webpage comprising a plurality of embedded links; inspecting, by the privacy security appliance, the response for privacy or security issues with the embedded links in the response;

—— ; scoring, by the privacy security appliance, each of the embedded links based on the inspection;

~~—— associating the scores~~ generating, by the privacy security appliance, a mock webpage based on the response, wherein the mock webpage does not include integrated elements to be stored or executed by a browser of the client device and represents a visual appearance of the webpage, and wherein the embedded links are replaced with each~~links to the embedded link~~links; and delivering the response, by the privacy security appliance, the mock webpage with the scoring of each of the embedded links to the computer application over the VPN as a mock webpage; wherein the browser of the client device processes the mock webpage and the scoring of each of the embedded links to present the scoring over the mock webpage in association with corresponding links of the 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 computer application and the client device before communicating the ~~internet-protocol~~IP request to the website host.

17. The method of claim 12, wherein the computer 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.