US 20110047617A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2011/0047617 A1

(43) Pub. Date: Feb. 24, 2011

Averbuch et al.

(54) **PROTECTING AGAINST NETWORK RESOURCES ASSOCIATED WITH UNDESIRABLE ACTIVITIES**

(75) Inventors: **Aaron H. Averbuch**, Seattle, WA (US); **Manav Mishra**, Kirkland, WA (US); **Roberto A. Franco**, Seattle, WA (US); **Tariq Sharif**, Redmond, WA (US)

Correspondence Address:
MICROSOFT CORPORATION
ONE MICROSOFT WAY
REDMOND, WA 98052 (US)

(73) Assignee: **Microsoft Corporation**, Redmond, WA (US)

(21) Appl. No.: **12/939,735**

(22) Filed: **Nov. 4, 2010**

Related U.S. Application Data

(63) Continuation of application No. 11/272,473, filed on Nov. 10, 2005, now Pat. No. 7,831,915.

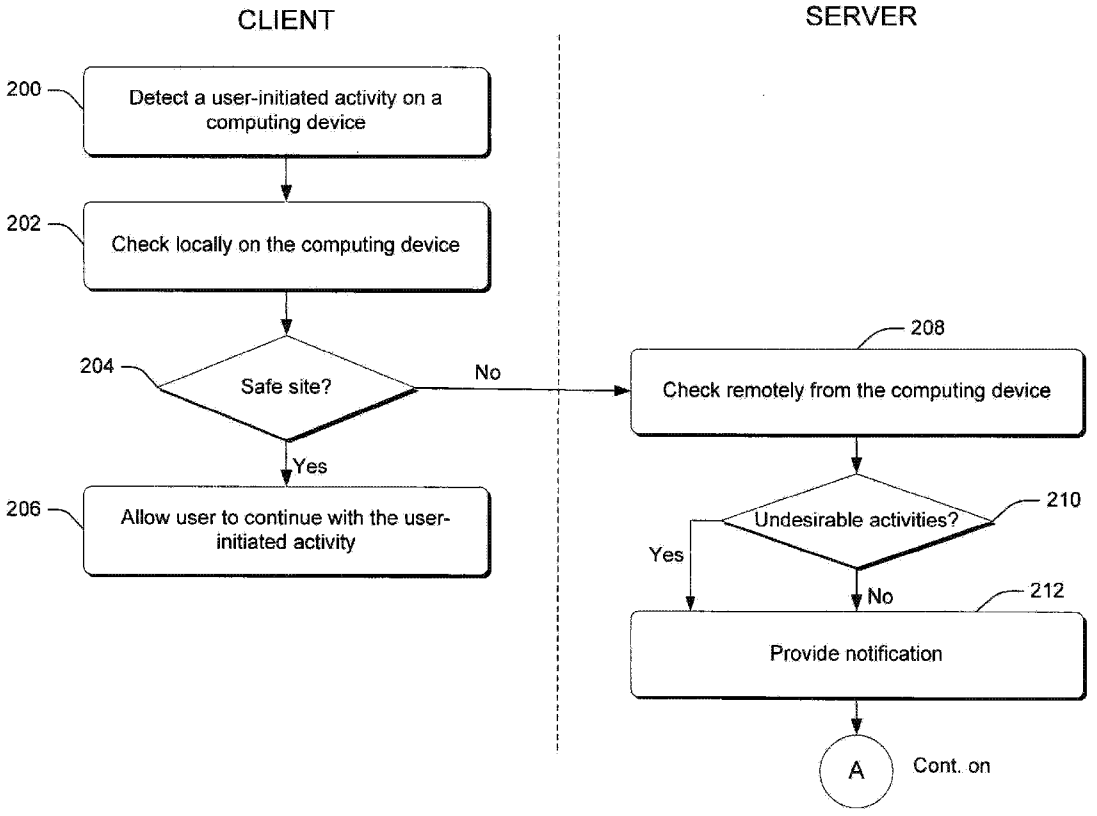
Publication Classification

(51) **Int. Cl.**
G06F 21/00 (2006.01)

(52) **U.S. Cl.** **726/22**

(57) **ABSTRACT**

Various embodiments provide protection against web resources associated with one or more undesirable activities. In at least some embodiments, a method detects and responds to a user-initiated activity on a computing device. Responding can include, by way of example and not limitation, checking locally, on the computing device, whether a web resource that is associated with the user-initiated activity has been identified as being associated with a safe site. Furthermore, in at least some embodiments, the method checks remotely, away from the computing device, whether the web resource is identified as being at least possibly associated with one or more undesirable activities.



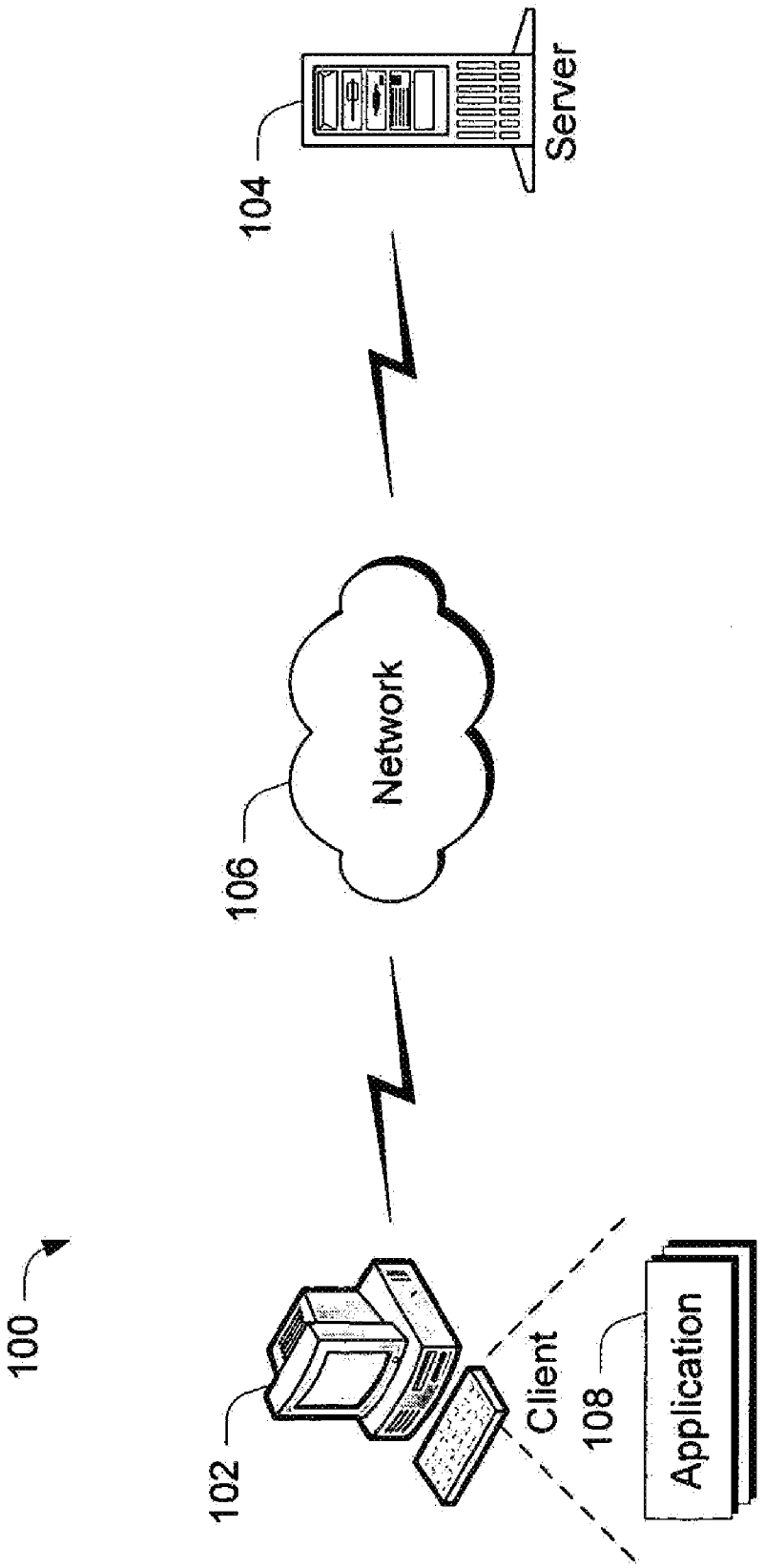


Fig. 1

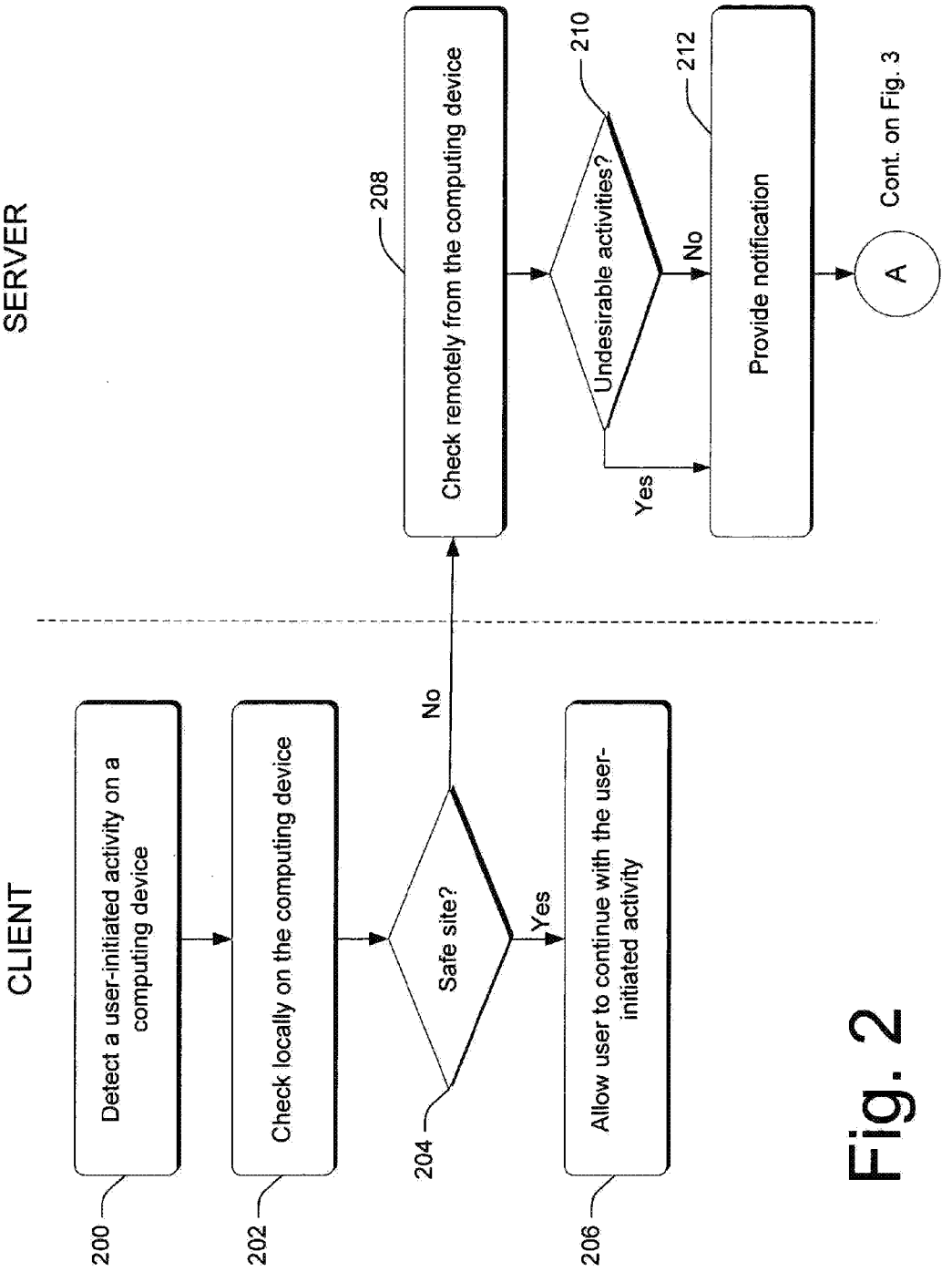

CLIENT
SERVER
Detect a user-initiated activity on a computing device
Check locally on the computing device
Safe site?
Yes
No
Allow user to continue with the user-initiated activity
Check remotely from the computing device
Undesirable activities?
Yes
No
Provide notification
A
Cont. on Fig. 3
200
202
204
206
208
210
212

Fig. 2

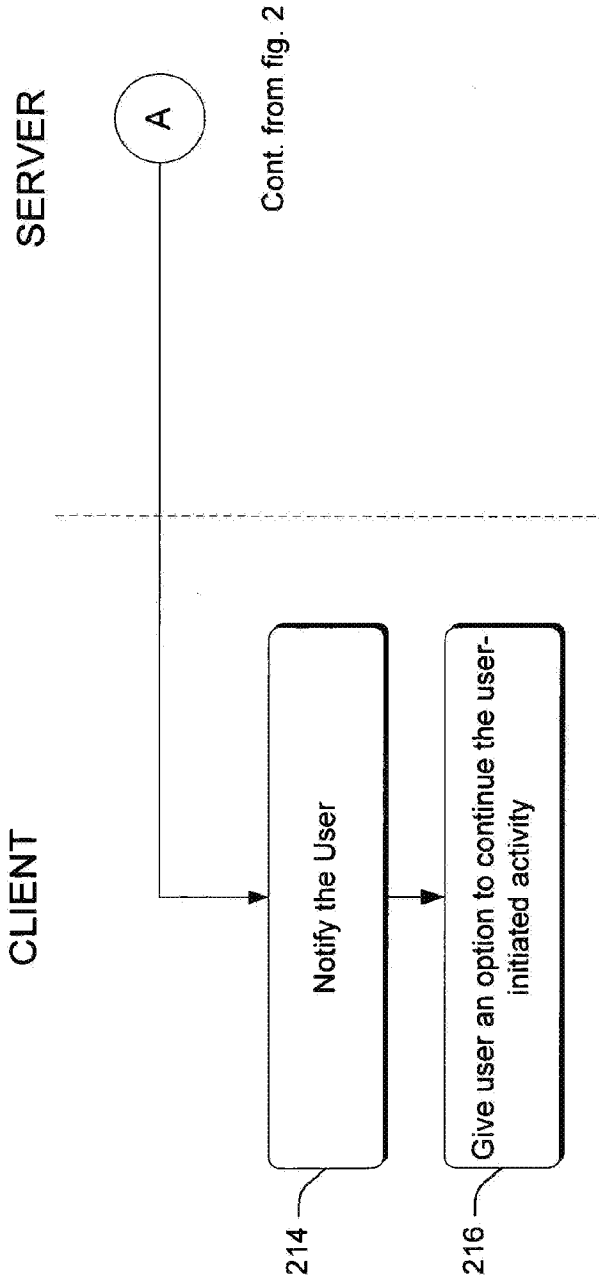

SERVER
A
Cont. from fig. 2
CLIENT
Notify the User
Give user an option to continue the user-initiated activity
214
216

Fig. 3

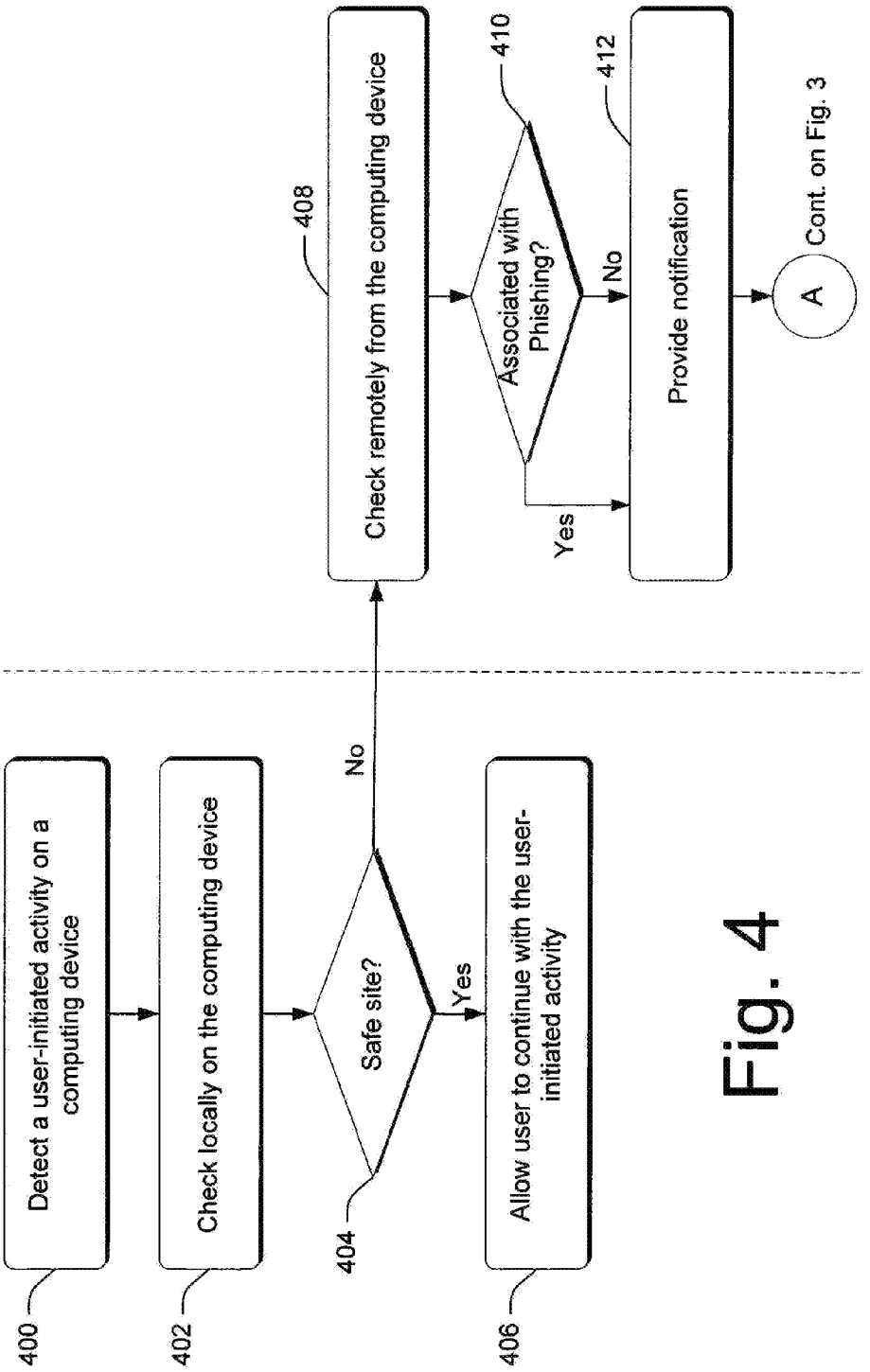

CLIENT
SERVER
Detect a user-initiated activity on a computing device
400
Check locally on the computing device
402
Safe site?
404
No
Yes
Allow user to continue with the user-initiated activity
406
Check remotely from the computing device
408
Associated with Phishing?
410
No
Yes
Provide notification
412
A
Cont. on Fig. 3

Fig. 4

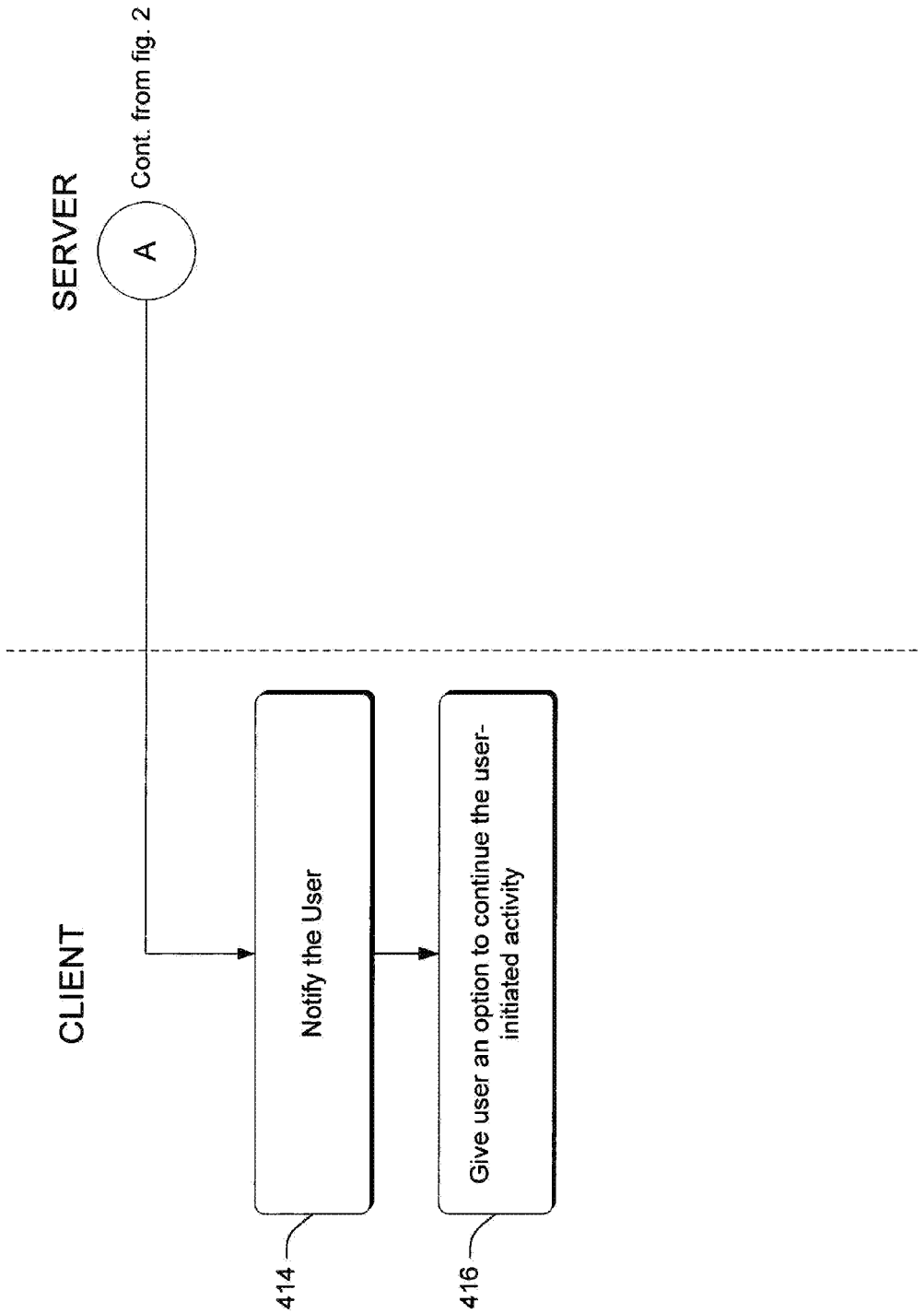
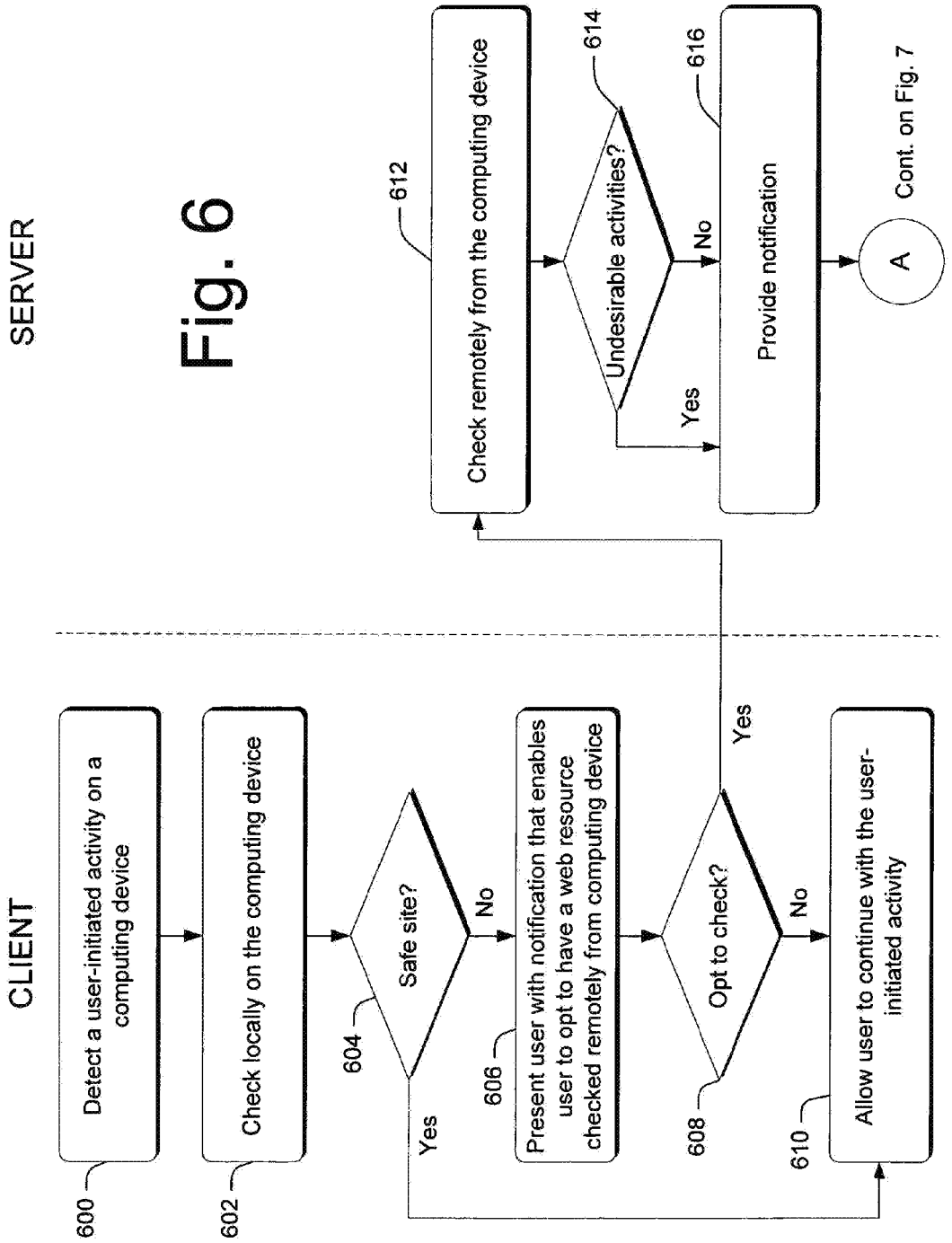

SERVER
Cont. from fig. 2
A
CLIENT
Notify the User
Give user an option to continue the user-initiated activity
414
416

Fig. 5

Fig. 6


CLIENT
SERVER
Detect a user-initiated activity on a computing device
600
Check locally on the computing device
602
Safe site?
604
Yes
No
Present user with notification that enables user to opt to have a web resource checked remotely from computing device
606
Opt to check?
608
Yes
No
Allow user to continue with the user-initiated activity
610
Check remotely from the computing device
612
Undesirable activities?
614
Yes
No
Provide notification
616
A
Cont. on Fig. 7

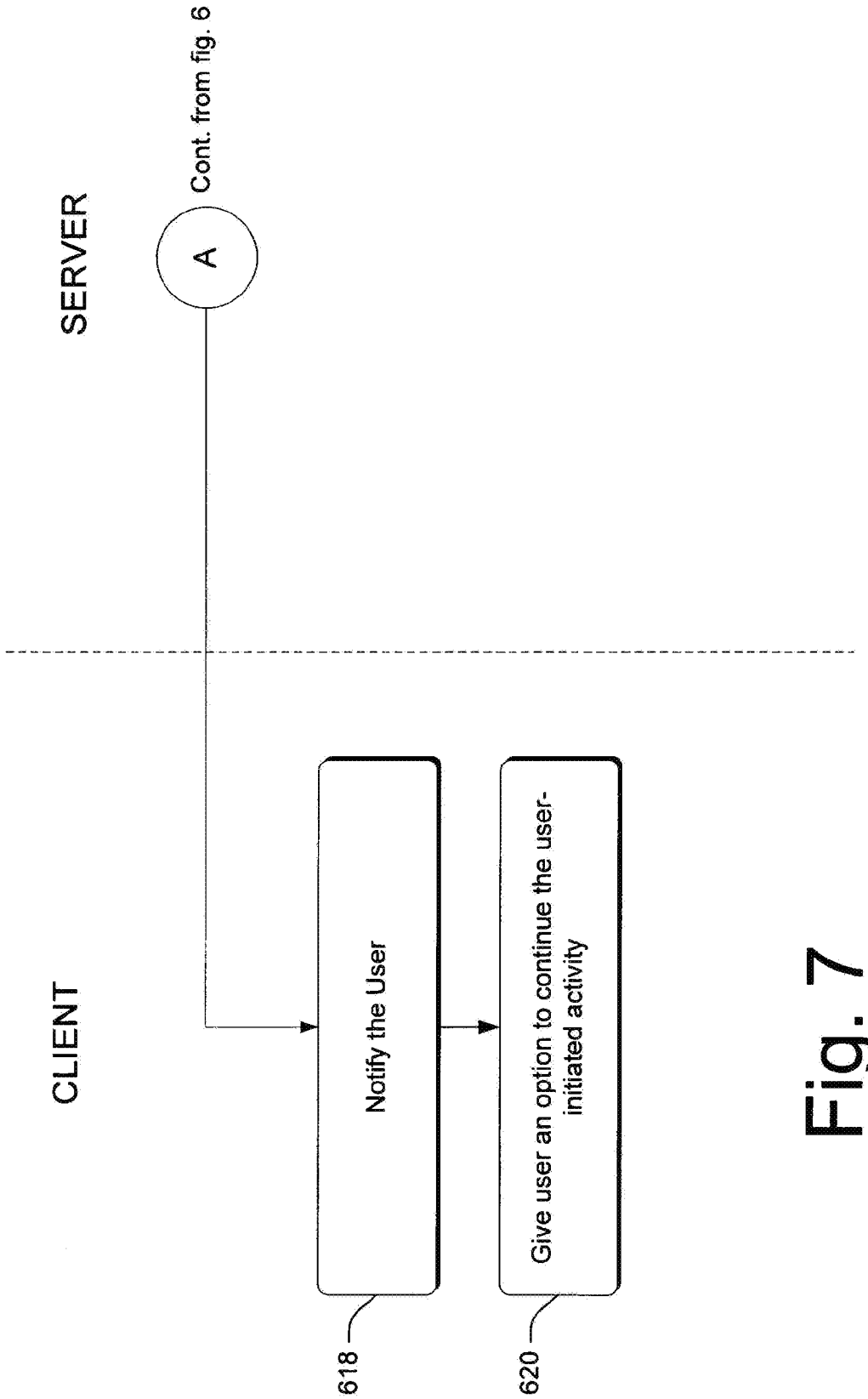

SERVER
CLIENT
Cont. from fig. 6
A
Notify the User
Give user an option to continue the user-initiated activity
618
620

Fig. 7

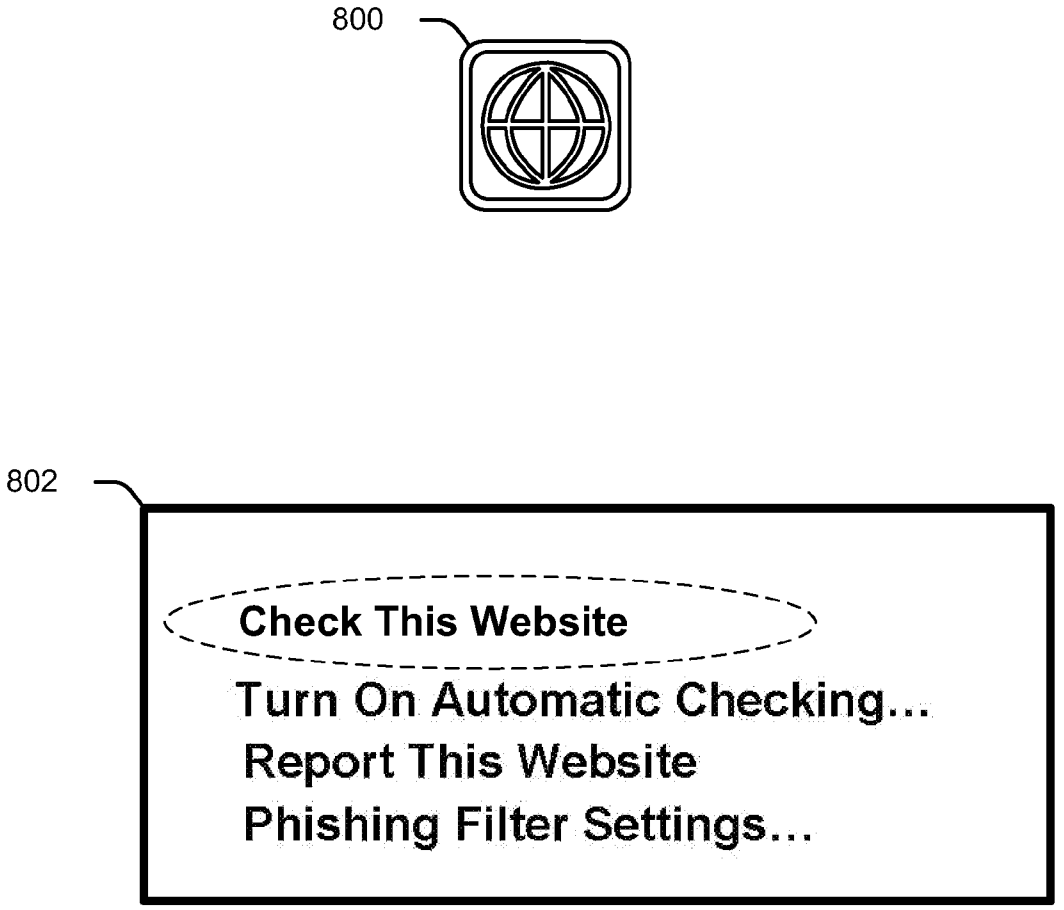

800
802
Check This Website
Turn On Automatic Checking...
Report This Website
Phishing Filter Settings...

Fig. 8

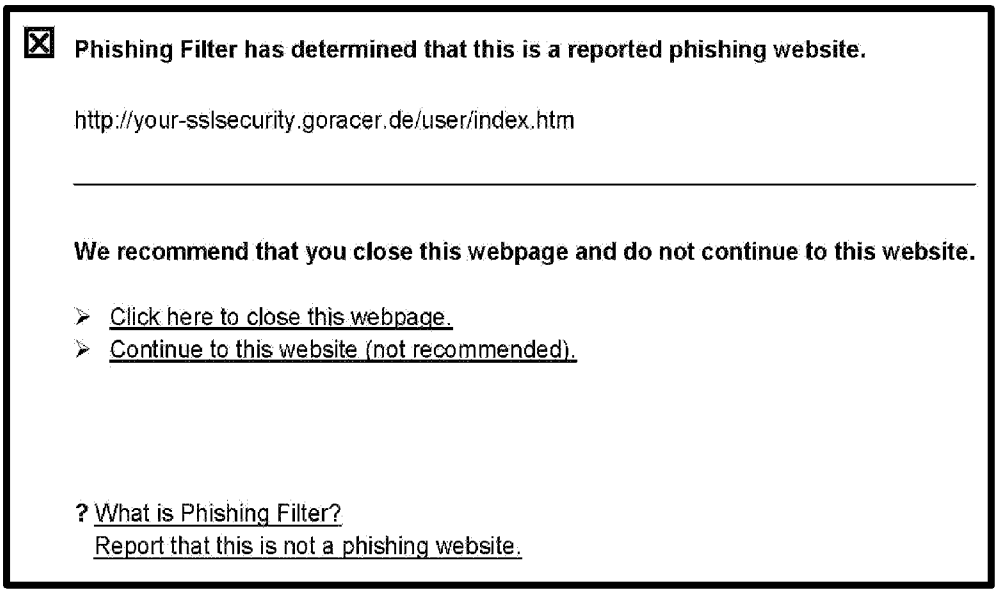

Phishing Filter has determined that this is a reported phishing website.
http://your-sslsecurity.goracer.de/user/index.htm
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
? What is Phishing Filter?
Report that this is not a phishing website.

Fig. 9

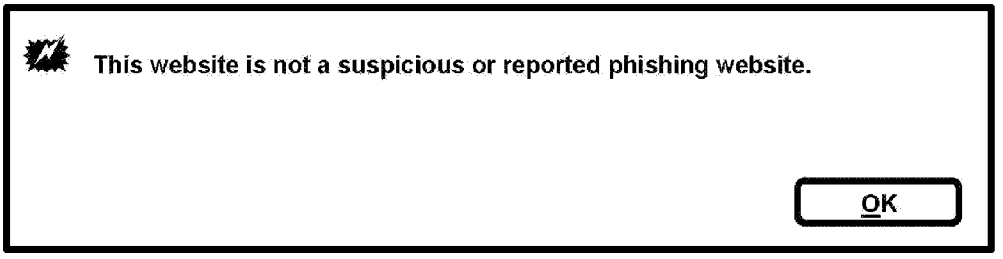

This website is not a suspicious or reported phishing website.
OK

Fig. 10

PROTECTING AGAINST NETWORK RESOURCES ASSOCIATED WITH UNDESIRABLE ACTIVITIES

RELATED APPLICATIONS

[0001] This application is a continuation of and claims priority to U.S. application Ser. No. 11/272,473, filed on Nov. 10, 2005, and entitled "Dynamically protecting against web resources associated with undesirable activities," the disclosure of which is hereby incorporated by reference herein in its entirety.

BACKGROUND

[0002] Many threats have emerged regarding online communications. Often, these threats involve web resources that can be associated with undesirable activities that can somehow impact a user and/or the user's computing device. Undesirable activities can come in many shapes and sizes. For example, phishing, where scammers or other bad actors attempt to gain illegal or unauthorized access to private information, is one example of such a threat.

[0003] Online communication can allow these scammers to reach many people easily through the use of such things as e-mail, instant messaging, or rogue web pages. Often, a user is misled into navigating to a fraudulent link that the user believes is trustworthy. As a consequence, the user may be subject to attempts to elicit private information from the user. For example, a user might type "bankoamerica.com" in an address box in an attempt to link to a Bank of America website. Once the user navigates to what appears to be, but is not, a legitimate Bank of America website, the user might inadvertently divulge private information upon request and thus be "phished".

[0004] Another way in which a user can be "phished" is by responding to an email that appears to the user to be legitimate. For example, the user may be involved in an online transaction (such as an eBay auction) and receive an email which requests that the user click a link and enter personal information in that regard.

[0005] Other examples of undesirable activities can include such things as unknowingly receiving spyware or malware.

SUMMARY

[0006] Various embodiments can protect a user against web resources associated with one or more undesirable activities. In at least some embodiments, a method detects and responds to a user-initiated activity on a computing device. Responding can include, by way of example and not limitation, checking locally, on the computing device, whether a web resource that is associated with the user-initiated activity has been identified as being associated with a safe site. After checking locally, some embodiments present the user with a notification that the web resource is not associated with a safe site. The user is then given an option to check remotely or to continue with the user-initiated activity without checking remotely. Furthermore, in at least some embodiments, if the web resource is not identified as being associated with a safe site, the method checks remotely, away from the computing device, whether the web resource is identified as being at least possibly associated with one or more undesirable activities.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] FIG. **1** illustrates an example operating environment in accordance with one or more embodiments.

[0008] FIG. **2** is a flow diagram that describes steps in a method in accordance with one or more embodiments.

[0009] FIG. **3** continues from FIG. **2** and is a flow diagram that describes steps in a method in accordance with one or more embodiments.

[0010] FIG. **4** is a flow diagram that describes steps in a method in accordance with one or more embodiments.

[0011] FIG. **5** continues from FIG. **4** and is a flow diagram that describes steps in a method in accordance with one or more embodiments.

[0012] FIG. **6** is a flow diagram that describes steps in a method in accordance with one or more embodiments.

[0013] FIG. **7** continues from FIG. **6** and is a flow diagram that describes steps in a method in accordance with one or more embodiments.

[0014] FIG. **8** illustrates a notification icon and list box presented to a user in accordance with one or more embodiments.

[0015] FIG. **9** illustrates a dialog box presented to a user in accordance with one or more embodiments.

[0016] FIG. **10** illustrates a dialog box presented to a user in accordance with one or more embodiments.

DETAILED DESCRIPTION

[0017] Various embodiments can protect a user against web resources associated with one or more undesirable activities. In at least some embodiments, a method detects and responds to a user-initiated activity on a computing device. Responding can include, by way of example and not limitation, checking locally, on the computing device, whether a web resource that is associated with the user-initiated activity has been identified as being associated with a safe site. After checking locally, some embodiments present the user with a notification that the web resource is not associated with a safe site. The user is then given an option to check remotely or to continue with the user-initiated activity without checking remotely. Furthermore, in at least some embodiments, if the web resource is not identified as being associated with a safe site, the method checks remotely, away from the computing device, whether the web resource is identified as being at least possibly associated with one or more undesirable activities.

[0018] Example Implementation

[0019] FIG. **1** illustrates an exemplary system, generally at **100**, in which various embodiments described below can be implemented in accordance with one embodiment. These various embodiments can protect against web resources that are determined or suspected of being associated with one or more undesirable activities.

[0020] There, system **100** includes a client **102** in the form of a computing device, a server **104** that is remote from the computing device, and a network **106** through which client **102** and server **104** can communicate. Client **102** can comprise any suitable computing device, such as a general purpose computer, handheld computer, and the like. In one embodiment, network **106** comprises the Internet.

[0021] In this example, client **102** embodies one or more software applications **108** through which client **102** and

server **104** can communicate. Software application(s) **108** typically reside in the form of computer-readable instructions that reside on some type of computer-readable medium. Although any suitable application can be used, in the embodiments described in this document, an application in the form of a web browser is used. It is to be appreciated and understood, however, that other types of applications can be used without departing from the spirit and scope of the claimed subject matter. For example, applications such as word processing applications, email applications, spreadsheet applications, and the like can utilize various techniques described in this document.

[0022] Various techniques may be described herein in the general context of software or program modules. Generally, software includes routines, programs, objects, components, data structures, and so forth that perform particular tasks or implement particular abstract data types. An implementation of these modules and techniques may be stored on or transmitted across some form of computer readable media. Computer readable media can be any available medium or media that can be accessed by a computing device. By way of example, and not limitation, computer readable media may comprise "computer-readable storage media".

[0023] "Computer-readable storage media" include volatile and non-volatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules, or other data. Computer-readable storage media include, but are not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can be accessed by a computer.

[0024] FIGS. **2** and **3** are flow diagrams that describe a method in accordance with one embodiment. The method can be implemented in connection with any suitable hardware, software, firmware or combination thereof. In one embodiment, the method is implemented in software in the form of computer-executable instructions, such as those defining an application that executes on a client computing device.

[0025] Step **200** detects a user-initiated activity on a client computing device. Any suitable application can be used to detect the user-initiated activity. For example, in one embodiment, an application in the form of a web browser is used to detect a user-initiated activity in the form of a navigation associated with a web resource. In addition, any suitable manner of initiating the navigation can be utilized. For example, in some embodiments, navigation can be initiated by a user clicking on a particular link that the user finds on a web page. Alternately or additionally, the navigation can be initiated by a user typing a URL in an appropriate address box that comprises part of a web page that they are browsing.

[0026] Responsive to detecting the user-initiated activity, step **202** checks locally, on the client computing device, to ascertain whether a web resource that is associated with the user-initiated activity is identified as being associated with a safe site. This step of checking locally on the client computing device can occur contemporaneously with the user-initiated activity. For example, conducting such a check can occur contemporaneously with conducting a navigation associated with a third-party web site.

[0027] In some embodiments, the local device can maintain a list of sites that have been determined as safe. For example, the microsoft.com® site might appear on such a list and be considered a safe site. More generally, a safe site can be considered as one that is not associated with activities that are considered to be undesirable. One type of undesirable activity is phishing, although other undesirable activities can be the subject of the check without departing from the spirit and scope of the claimed subject matter. These other activities can include, by way of example and not limitation, activities associated with exposing the user to malware or spyware.

[0028] In conducting the local check, step **202** can be performed in any suitable way. By way of example and not limitation, a Uniform Resource Locator (URL) associated with a user-initiated navigation can be compared to a local list of URLs which are known to be safe.

[0029] If a match occurs (the "yes" branch from step **204**), the URL associated with the navigation is identified as being associated with a safe site and step **206** allows the user to continue with the user-initiated activity.

[0030] If, on the other hand, the web resource is not identified as being associated with a safe site (i.e. the "no" branch from step **204**), then step **208** checks remotely from the computing device to ascertain whether the web resource is identified as at least possibly being associated with one or more undesirable activities.

[0031] The step of checking remotely from the computing device can also occur contemporaneously with the user-initiated activity. For example, during the remote check, a user-initiated navigation to a third party site can be allowed to continue to provide a smoothly-perceived user experience.

[0032] The remote check can be performed in any suitable way. While FIGS. **2** and **3** illustrate this step as being performed remotely from the client computing device, this is not to be construed as meaning that one or more portions of this step, as described below, cannot be performed on the local client computing device.

[0033] As an example, consider the following. In at least some embodiments, one or more remote servers can be provided with information associated with a particular web resource, such as a link or web site. This information can come from a third party service that is designed to look for and keep track of sites that are or become affiliated with undesirable activities such as phishing and the like. In some instances, this information might be utilized to develop what is referred to as reputation information which can then be used as part of a score-based system to rank the web resource, as described below. More specifically, the reputation information can be provided to the local computing device which can then compute a local score associated with the web resource. The reputation information and the local score can then be processed to derive a reputation score that is associated with the web resource. Utilizing one or more of these scores, the web resource can be ranked in categories such as: a web resource known to be associated with one or more undesirable activities, a web resource suspected of being associated with one or more undesirable activities, or a web resource that is not known or suspected of being associated with one or more undesirable activities.

[0034] Step **210** determines whether the web resource is identified as at least possibly being associated with one or more undesirable activities. This can be accomplished in any suitable way. For example, here this can be accomplished by utilizing the web resource's derived reputation score, as noted

above. Furthermore, this step can be performed completely remotely from the client computing device.

[0035] In the event that the web resource is identified as at least possibly being associated with one or more undesirable activities (i.e. the "yes" branch from step **210**), step **212** provides a notification to this effect and step **214** (FIG. **3**) notifies the user of this information. This can be performed in any suitable way. For example, the user might only be presented with an alert and/or a dialog box when the web resource has been identified as being suspected or actually being associated with undesirable activities. For example, in a score-based system, if the web resource is ranked in an appropriate category that suggests an undesirable association, then the user might be notified.

[0036] If the web resource is not identified as being associated with undesirable activities (i.e. the "no" branch from step **210**), then a similar notification can be provided to the user at step **212**.

[0037] Step **216** gives or provides the user with an option to continue the user-initiated activity. Typically this step is performed in the event that the web resource is identified as being associated with an undesirable activity, although it is illustrated slightly differently here.

[0038] Protecting Against Phishing Activities

[0039] As noted above, in at least some embodiments, techniques discussed herein can be implemented in the context of policing against phishing activities. By detecting a user-initiated activity and checking to ascertain whether an associated web resource is associated with phishing, the user can be protected from attempts by scammers or other bad actors to gain illegal or unauthorized access to private information.

[0040] As an example, consider FIGS. **4** and **5**, which illustrate a method, in accordance with one embodiment, of protecting against phishing activities. The method can be implemented in connection with any suitable hardware, software, firmware or combination thereof. In one embodiment, the method is implemented in software in the form of computer-executable instructions, such as those defining an application that executes on a client computing device.

[0041] Step **400** detects a user-initiated activity on a client computing device. Any suitable application can be used to detect the user initiated activity. For example, in one embodiment, an application in the form of a web browser is used to detect a user-initiated activity in the form of an attempted navigation associated with a web resource.

[0042] Responsive to detecting the user-initiated activity, step **402** checks locally on the client computing device to determine whether a web resource that is associated with the user-initiated activity is identified as being associated with a safe site.

[0043] This step of checking, locally on the client computing device, can occur contemporaneously with the user-initiated activity. A safe site can be any site that is not associated with phishing activities. The local check that is performed can be performed in the same or similar manner as described above.

[0044] Step **404** determines whether the web resource that is associated with the user-initiated activity is identified as being associated with a safe site. If it is, then step **406** allows the user to continue with the user-initiated activity.

[0045] If, on the other hand, the web resource is not identified as being associated with a safe site, then step **408** checks remotely from the computing device, whether the web resource is identified as at least possibly being associated with a phishing activity. The remote check that is performed can be performed in the same or similar manner as described above.

[0046] Step **410** determines whether the web resource is identified as at least possibly being associated with a phishing activity. This can be accomplished by utilizing the web resource's derived reputation score, as noted above.

[0047] Step **412** provides a notification whether the web resource is identified as at least being associated with a phishing activity and step **414** (FIG. **5**) notifies the user of this information. This can be performed in any suitable way. For example, the user might only be presented with an alert and/or dialog box when the web resource is ranked in one or more of the categories discussed above. Alternately, the user might always be presented with an alert and/or dialog box.

[0048] Step **416** gives or provides the user with an option to continue the user-initiated activity. Typically this step is performed in the event that the web resource is identified as being associated with a phishing activity, although it is illustrated slightly differently here.

[0049] One example of how steps **412-414** can be implemented, including the user interfaces that can be employed, is illustrated and discussed below in regards to FIGS. **9-10**.

[0050] Providing a User with an Option to Check a Web Resource

[0051] As described above, in order to determine whether a web resource is associated with an undesirable activity, checking occurs remotely from the user's computing device. Doing so, however, can cause privacy concerns for some users. For example, if a user wants to navigate to a certain webpage, the URL of the web page can be sent to a remote server to verify the absence of any undesirable activities, such as phishing. Certain users may be uncomfortable with the notion of allowing a remote server to see certain web pages that the user frequents. Thus, some users may find it desirable to have the option of determining whether or not the remote check takes place.

[0052] FIGS. **6** and **7** are flow diagrams that describe a method in accordance with one embodiment with the aforementioned privacy concerns in mind. The method can be implemented in connection with any suitable hardware, software, firmware or combination thereof. In one embodiment, the method is implemented in software in the form of computer-executable instructions, such as those defining an application that executes on a client computing device.

[0053] Step **600** detects a user-initiated activity on a computing device. In but one embodiment, and as noted above, one such activity takes place when the user clicks on a link associated with a web resource. Such a link might be present as part of a web page, an email document, or some other document on which a user might be working. Other examples of user-initiated activities are given above.

[0054] After detecting a user-initiated activity, the web resource can be checked locally as discussed above and as illustrated by step **602**. Step **604** then determines whether the web resource is identified as being associated with a safe site. If it is, then step **610** allows the user to continue with the user-initiated activity. Checking locally poses no security risks because all of the information is already contained on the user's computing device.

[0055] If however, the local check reveals that the web resource is not identified as being associated with a safe site (e.g., not contained in the local list of safe sites), the user can be notified as follows.

[0056] Step **606**, presents a user with a notification that enables the user to opt to have a web resource checked to ascertain whether the web resource is associated with one or more undesirable activities. This notification effectively alerts the user that the web resource is not on the local list of safe sites and asks the user whether he or she would like to check remotely from the computing device to determine whether the web resource associated with, for example an attempted navigation, is associated with any undesirable activities. Examples of undesirable activities were given above.

[0057] If, at step **608**, the user declines to check remotely, step **610** allows the user to continue with their activity. On the other hand, if the user opts to conduct the remote check, step **612** conducts the remote check by sending a request to an appropriate server or other remote device.

[0058] Step **614** determines whether the web resource is associated with any undesirable activities. This step can be performed in any suitable way, examples of which are provided above. Step **616** provides a notification to the user with regard to the remote check that was performed. Step **618** (FIG. **7**) receives this notification from the remote server and presents the notification to the user.

[0059] The notification can either tell the user whether or not the web resource is associated with any undesirable activities, or provide information that can further be used to make that decision, as described above.

[0060] If the web resource is not associated with any undesirable activities, the user can continue with his or her activity. On the other hand, if the web resource is determined to be associated with undesirable activities, step **620** can provide the user with an option to continue with the activity despite the association with undesirable activities.

[0061] In Operation

[0062] The above methodology can be implemented in any suitable way using any suitable technology. As but one example of how the above-described techniques can be implemented from the perspective of the user, consider, FIGS. **8-10**.

[0063] Specifically, if a particular user has chosen to be given the option of determining whether a remote check will occur, a notification icon, such as that shown at **800** in FIG. **8** can appear when a user-initiated activity is detected. This icon may appear in the toolbar of a web browser for the purpose of alerting the user that web resource to which he wishes to navigate is not on the local list of safe sites. When the user clicks on this icon, a list box can be presented to the user. One such list is shown at **802**. The list gives the user the ability or option to check the website, turn on automatic checking, report the website, or change phishing filter settings.

[0064] If the user selects "check this website", the website will be checked remotely from the user's computing device as described above. If the user selects "turn on automatic checking" the website will be checked remotely from the user's computing device, and the next time that a user-initiated activity is detected and the web resource is not on the local list of safe sites, the remote check will automatically occur without notifying the user.

[0065] FIG. **9** illustrates a dialog box that is presented to a user when a website that the user has attempted to navigate to has been determined to be associated with a phishing activity. There, the user is notified that the website is a reported phishing website and is given the option of either continuing to the website or of closing the web page.

[0066] FIG. **10** illustrates a dialog box that is presented to a user when a website that the user has attempted to navigate to is determined to not be associated with a phishing activity. There, the user is notified that the website is not a suspicious or reported website and the user can click "OK" to continue.

CONCLUSION

[0067] Various embodiments provide protection against web resources associated with one or more undesirable activities. In this manner, a user and/or the user's computing device can be protected from activities that could prove harmful.

[0068] Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or acts described above. Rather, the specific features and acts described above are disclosed as example forms of implementing the claims.

What is claimed is:

1. A computer-implemented method comprising:

checking locally on a computing device to determine whether a website is identified as being associated with a safe site, wherein the safe site is a site that is not associated with an undesirable activity including one or more of a phishing activity, a malware activity, or a spyware activity; and

if the website is not identified locally on the computing device as being associated with a safe site, causing a request to be transmitted for receipt by a remote resource to determine if the website is identified by the remote resource as being associated with the undesirable activity.

2. The method as recited in claim **1**, wherein the checking locally on the computing device to determine whether the website is identified as being associated with a safe site is responsive to an attempted navigation to the website via the computing device.

3. The method as recited in claim **1**, wherein the checking locally on the computing device to determine whether the website is identified as being associated with a safe site comprises checking the website against a list of sites that are considered to be safe sites.

4. The method as recited in claim **1**, wherein the checking locally on the computing device to determine whether the website is identified as being associated with a safe site occurs contemporaneously with a navigation to the website via the computing device.

5. The method as recited in claim **1**, further comprising:

receiving an indication of whether or not the website is identified by the remote resource as being associated with the undesirable activity; and

causing a visual indicia of the indication to be displayed via the computing device.

6. The method as recited in claim **1**, further comprising:

receiving an indication of whether or not the website is identified by the remote resource as being associated with the undesirable activity; and

providing an option to continue a navigation to the website.

7. The method as recited in claim **1**, further comprising receiving an indication of whether or not the website is identified by the remote resource as being associated with the undesirable activity, the indication being based on a local score from the computing device and reputation information from the remote resource.

8. The method as recited in claim **1**, further comprising, if the website is not identified locally on the computing device as being associated with a safe site, navigating to the website contemporaneously with causing the request to be transmitted for receipt by the remote resource.

9. A computer-implemented method comprising:

checking locally on a device to determine whether a network resource is identified as being associated with a safe resource, wherein the safe resource is a resource that is not associated with an undesirable activity including one or more of a phishing activity, a malware activity, or a spyware activity; and

if the network resource is not identified locally on the device as being associated with a safe resource:

causing a request to be transmitted for receipt by a remote resource to determine if the network resource is identified by the remote resource as being associated with the undesirable activity; and

receiving an indication of whether or not the network resource is associated with the undesirable activity.

10. The method as recited in claim **9**, wherein the checking locally on the device to determine whether the network resource is identified as being associated with a safe resource is responsive to an attempted navigation to the network resource via the device.

11. The method as recited in claim **9**, wherein the network resource comprises a web site, and wherein the checking locally on the device to determine whether the network resource is identified as being associated with a safe resource comprises using a web browser to check the web site.

12. The method as recited in claim **9**, wherein the checking locally on the device to determine whether the network resource is identified as being associated with a safe resource comprises checking the network resource against a list of network resources that are considered to be safe network resources.

13. The method as recited in claim **12**, wherein the list of network resources comprises uniform resource locators (URLs) for the network resources.

14. The method as recited in claim **9**, wherein the indication of whether or not the network resource is associated with the undesirable activity is based on a reputation score for the network resource, the reputation score being calculated based on a local score from the device and reputation information from the remote resource.

15. The method as recited in claim **14**, wherein the reputation score indicates that the network resource is associated with the undesirable activity, the method further comprising causing to be displayed a visual indication of the reputation score.

16. The method as recited in claim **9**, wherein the checking locally on the device to determine whether the network resource is identified as being associated with a safe resource comprises calculating a reputation score for the network resource, the reputation score being calculated based on a local score from the device and reputation information from the remote resource.

17. The method as recited in claim **9**, further comprising, if the network resource is not identified locally on the device as being associated with a safe resource, navigating to the network resource contemporaneously with causing the request to be transmitted for receipt by the remote resource.

18. The method as recited in claim **9**, further comprising presenting an option to continue a navigation to the network resource responsive to receiving the indication of whether or not the network resource is associated with the undesirable activity.

19. A computer-implemented method comprising:

calculating a local score for a network resource;

receiving reputation information associated with the network resource from a remote resource; and

calculating a reputation score for the network resource using the local score and the reputation information, the reputation score indicating that:

the network resource is known to be associated with one or more undesirable activities;

the network resource is suspected of being associated with one or more undesirable activities; or

the network resource is not known or suspected of being associated with one or more undesirable activities.

20. The method as recited in claim **19**, further comprising:

presenting via a computing device a visual indication of the reputation score; and

providing an option to navigate to the network resource via the computing device.

* * * * *