INTERNET SECURITY

Technical Field

The invention generally relates to protecting the data a user enters on the internet.

More particularly the invention relates to protecting data entered on the internet and preventing it being sent to unexpected locations, a technique known as “phishing”

Background Art

“Phishing” refers to the process of tricking or socially engineering an organisation’s customers into imparting their confidential electronic identity for nefarious use. Phishing is a serious threat to any online business and services because it leads to unauthorised information access, frauds and financial loss.

The person performing such an act is generally referred to as a “phisher”. In general, the phisher will impersonate a trusted source so that the victim will be led to intentionally perform a series of actions that will provide access to confidential information.

Common phishing techniques include tricking users into keying in fraudulent web addresses, or clicking on crafted web links on a fake email, or manipulating DNS (domain name service) information. The aforementioned techniques will eventually cause web browsers to display fraudulent web content set up by the phishers. The fraudulent web content could take the form of a look-alike web page to a genuine web page, or crafted data input fields embedded into a genuine web page, or a pop-up window appearing on top of the original website.

The ultimate objective is to lead the users into believing that the data entry fields presented are genuine and hence into submitting confidential information to the phishers. Regardless of the technique deployed, the fraudulent web content will always contain data input fields for the web users to fill in and submit. The submitted data is typically confidential information such as login names and passwords, which will allow the phishers to exploit the electronic identities of their victims.

Presently, other existing anti-phishing methods known are either ineffective against the ever innovative phishing techniques or simply too costly for large scale deployment. Anti-phishing methods based on website bookmarks are ineffective against fraudulent web links on fake emails or fraudulent login page embedded into the genuine web page using cross-site scripting method. Anti-phishing methods based on blacklist are unable to cope with the rapidly increasing fraudulent websites. Hardware token-based authentication methods are very costly for mass distribution.

The present invention provides a solution to this and other problems which offers advantages over the prior art.

Summary Of The Invention

In one exemplification the invention relates to a method of controlling the submission of user-entered information in a web browser comprising :

detecting when the user attempts to navigate to a different web address;

detecting data entry fields in the currently displayed page,

where such fields exist;

verifying that the different web address is either

in an approved list of web addresses, or

is a secure site in which the site certificate corresponds with the site address; and

allowing the transmission of the different web address if the verification is authenticated.

Preferably, if the verification is not authenticated, the user is queried for verification.

Preferably, the user may add the different web address to the approved list of web addresses.

Preferably, the approved list of web addresses may be made up of one or more of a user approved list, an embedded approved list and a web-based approved list.

Preferably, the web-based approved list is a list available from a secure server.

Preferably, the secure site is a site using the Secure Sockets Layer (SSL).

Preferably, the data entry fields are detected in the current web page by detecting web form fields of the text type.

Preferably, there are degrees of authentication and the degree is indicated to the user by colour indication.

In a second exemplification the invention relates to a web browser address authenticator including :

a web browser;

a web browser plug-in,

the plug-in adapted to intercept any request to view a web page differing from the current web page, analysing the current web page for data entry fields and, if any are detected, comparing the requested web page address with authenticated addresses, and allowing transmission of the request to view only if the web page address is an authenticated address.

Preferably, the authenticated addresses are held in lists and at least one list is embedded in the plug-in.

Preferably, the authenticator indicates its active presence in the browser by displaying a toolbar.

Preferably the toolbar indicates the status of current requests.

In a further exemplification the invention relates to a web browser plug-in including:

an interceptor which intercepts any request to view a web page differing from the current web page; and

an analyser which analyses the current web page for data entry fields and, if any are detected, compares the requested web page address with authenticated addresses,

wherein if data entry fields are present, and the requested web page address matches an authenticated address, the plug-in allows the request.

Preferably, if the address is not authenticated the plug-in queries the user for verification.

Preferably, the address authentication is carried out on at least one of an address list internal to the plug-in, an address list associated with the browser, an address list available from a web server.

Preferably, the plug-in interacts with the user via a browser toolbar.

Alternatively, the invention relates to a computer readable medium including instructions which are operable to control an internet browser to:

detect when the user attempts to navigate to a different web address;

detect data entry fields in the currently displayed page,

where such fields exist;

verify that the different web address is either

in an approved list of web addresses, or

is a secure site in which the site certificate corresponds with the site address; and

allow the transmission of the different web address if the verification is authenticated.

Preferably, the instructions are present in the form of a browser plug-in.

These and other features of as well as advantages which characterise the present invention will be apparent upon reading of the following detailed description and review of the associated drawings.

This invention is an anti-phishing process which makes use of a combination of website authentication and data submission interception. A software prototype of this process has proven to be effective against all commonly known phishing techniques.

Brief Description of the Drawings

FIG. 1 is a flow diagram of the recognition and rejection process of an embodiment of the present invention.

FIG 2 shows the use of the process.

Detailed Description

This invention is a process for the detection and interception of submission of confidential information from a web browser to a website, whereby the identity of the target website will be authenticated using multiple authentication methods prior to any further action. The said action could be to allow or deny the information submission subject to a combination of the results of authentication.

To recap, the common methods of extracting confidential information from a user, these are:

Presenting the user with a link to a website which appears to be a genuine website known to the user. Typically this might be a replica of a bank site with a domain name which is only slightly different to the actual domain name of the bank, for instance a lower case “L” may be replaced with the number “1”. At least some of the users will follow the link and be deceived enough to enter confidential information, typically for an internet banking account. The false replica will either echo the data to the real site and transfer the user at the first opportunity while retaining the entered data, or will simply provide no response, thus leading a user to assume the site is down. The link may even be set up so that the URL appears correct but has an associated script which actually connects to a different site.

Sending an email to a user which appears to originate from a trusted source, such as a bank, and which requests the user to click on a link that again leads to a website such as that referred to above.

Sending an email to a user with form fields to be filled in. Code associated with the form fields can send the information to virtually anywhere.

Overlaying legitimate entry fields in a browser with a separate window which carries equivalent entry fields. This process relies on a popup window which may have been triggered by embedded software downloaded from a supposedly innocuous site. The entry field overlaid may be the address bar of the browser and the software may only act when a known address is entered, such as PayPal, redirecting the user to a fake site

in which they enter their confidential data. Alternatively, the entry fields overlaid may be the standard fields for login, and the data may be sent to a malicious address.

The current invention proposes a web-based detection system which legitimises every call to a web URL before it is sent. The legitimacy of the site to which the data is being sent is checked in several ways. The detection system preferably is crafted as a plug-in for the email or browser in use.

When a user sends data to a web site (i.e. every time any information is sent or any web page is queried) the current page, whether an HTML email or a web page in a browser is checked to see whether there was user input.

If user input exists, typically as form fields, a URL-checking process is begun.

Firstly, the plug-in consults an embedded white list of trusted web sites. If the URL being called is not on the white list, then the request is held and the user is informed that they must authorise the request to this URL.

Secondly, the URL is compared with a user-generated list of trusted web sites. Again, if the URL being called is not on the list, the request is held and the user is informed. A decision by the user to proceed will also generate an offer to add the requested site to the user's list of trusted sites.

Thirdly, if the site being queried is a secure site (https), then the target website address is compared with the target website server security certificate. If they do not match, then again the request is held and the user is informed with a suitable message.

Fourthly, the address being queried may be queried at a web-based whitelist of legitimate addresses with authentication being supplied from a secure server in an encrypted document. If no record of the called site is held, the user is again notified that the request is suspect and a user decision awaited. Otherwise the request proceeds.

FIG. 1 shows the process, in accordance with an embodiment of the invention, followed by the web browser plug-in in which a user visits a web page at 101, at 102 either clicks a link, submits a page or attempts to move to another web site. At 103, the plug-in parses the current web page looking for text box entry fields within "<FORM>" fields. Such fields may be "<INPUT>" fields of several types. If no fields

are found, the browser request is allowed at 104 and the browser redirects to the requested site.

If any such fields are found, the site to which navigation is being directed is checked at 105 against a denied “black” list which is normally associated with the plug-in. If the site is on the black list, a message is presented to the user at 106 stating that the site requested is on the black list and it is not recommended that the site be viewed because confidential data might be transferred. The user may make a decision to drop the request at 106 or to go to the site at 109.

If the site is not on the “black” list, a check is made at 110 to see if the site is on an allowed “white” list which is held by the plug-in. If it is, the browser is allowed to navigate to the new site. If it is not, then a check is made at 111 against a second “white” list which has been approved by the user. Again, if the site is on the list the browser redirection proceeds.

If the requested site is on neither list, then if the site is running on a secure sockets layer (https), the site certificate is requested from the secure site server at 113. If the site address matches the requested address at 115, then it is assumed that the site is satisfactory and the user is redirected. If no match is made, then the user is informed again at 106 with an appropriate message.

If the site is not an HTTPS site, an attempt is made to check with a “whitelist” server on the internet whether the requested site address is satisfactory. The whitelist server is checked for availability at 115 and, if present, a check is made at 116. Failing to match the whitelist again results in a message being provided to the user at 106, though if a match is found then the browser is redirected.

FIG. 2 shows the typical examples of the colour warnings provided on detection of various sites, and a typical warning message. These may be instigated from a toolbar in the browser, the toolbar being instigated by the plug-in. The toolbar may actively show the status of any current requests.

It is to be understood that even though numerous characteristics and advantages of the various embodiments of the present invention have been set forth in the foregoing description, together with details of the structure and functioning of various

embodiments of the invention, this disclosure is illustrative only, and changes may be made in detail so long as the functioning of the invention is not adversely affected. For example, the particular order in which the checks are made may vary dependent on the particular application for which it is used without departure from the scope of the present invention.

Industrial Applicability

The method of the invention is used in the verification that user data is not being sent to an unauthorised person who may use that information to carry out an action deleterious to the user, such as funds transfer. Preventing such a fund transfer has an economic benefit to the user.

Additionally, the modification to the browser or email package by addition of a plug-in provides a tool of greater utility. The present invention is therefore industrially applicable.

Claims

1. A method of controlling the submission of user-entered information in a web browser, comprising :

   detecting when the user attempts to navigate to a different web address;

   detecting data entry fields in the currently displayed page,

   where such fields exist;

   verifying that the different web address is either

   in an approved list of web addresses, or

   is a secure site in which the site certificate corresponds with the site address; and

   allowing the transmission of the different web address if the verification is authenticated.

2. The method as claimed in claim 1 wherein, if the verification is not authenticated, the user is queried for verification.

3. The method as claimed in claim 2 wherein the user may add the different web address to the approved list of web addresses.

4. The method as claimed in claim 1 wherein the approved list of web addresses may be made up of one or more of a user-approved list, an embedded approved list and a web-based approved list.

5. The method as claimed in claim 4 wherein the web-based approved list is a list available from a secure server.

6. The method as claimed in claim 1 in which the address may also be compared with a rejection “black” list.

7. The method as claimed in claim 1 wherein the secure site is a site using the Secure Sockets Layer (SSL).

8. The method as claimed in claim 2 wherein the data entry fields are detected in the current web page by detecting web form fields of the text type.

9. The method as claimed in claim 1 wherein there are degrees of authentication and the degree is indicated to the user by colour indication.

10. A web browser address authenticator including :

a web browser;

a web browser plug-in,

the plug-in intercepting any request to view a web page differing from the current web page, analysing the current web page for data entry fields and, if any are detected, comparing the requested web page address with authenticated addresses, and allowing transmission of the request to view only if the web page address is an authenticated address.

11. A web browser address authenticator as claimed in claim 10 wherein the authenticated addresses are held in lists and at least one list is embedded in the plug-in.

12. A web browser address authenticator as claimed in claim 10 wherein the plug-in also provides rejection if a request matches a list of sites to be rejected.

13. A web browser address authenticator as claimed in claim 10 wherein the authenticator indicates its active presence in the browser by displaying a toolbar.

14. A web browser address authenticator as claimed in claim 13 wherein the toolbar indicates the status of current requests.

15. A web browser plug-in including:

an interceptor which intercepts any request to view a web page differing from the current web page; and

an analyser which analyses the current web page for data entry fields and, if any are detected, compares the requested web page address with authenticated addresses,

wherein if data entry fields are present, and the requested web page address matches an authenticated address, the plug-in allows the request.

16. A web browser plug-in as claimed in claim 15 wherein if the address is not authenticated the plug-in queries the user for verification.

17. A web browser plug-in as claimed in claim 16 wherein the address authentication is carried out on at least one of an address list internal to the plug-in, an address list associated with the browser, an address list available from a web server.

18. A web browser plug-in as claimed in claim 15 wherein the plug-in interacts with the user via a browser toolbar.

19. A computer readable medium including instructions which are operable to control an internet browser to:

detect when the user attempts to navigate to a different web address;

detect data entry fields in the currently displayed page,

where such fields exist;

verify that the different web address is either

in an approved list of web addresses, or

is a secure site in which the site certificate corresponds with the site address; and

allow the transmission of the different web address if the verification is authenticated.

20. A computer readable medium as claimed in claim 19 wherein the instructions are present in the form of a browser plug-in.