How to block phishing attacks in Firefox 3

Phishing evolved from the previous phreaking, a form of attack on long-distance telephone systems for free calls. However in Phishing, the level of influence is many times greater.

Network Administration **- The term *phishing* can evoke memories of fear or a caution in your mind. *Phishing* is the use of an error website (disguised as a friendly site) to gather sensitive information from users.** Most of these attacks appear on sites that require users to enter sensitive information such as credit card numbers or bank account information. In the case of attacks, users are unaware that their information will be sent to a malicious site.

Phishing evolved from the previous *phreaking* , a form of attack on long-distance telephone systems for free calls. However *in* Phishing, the level of influence is not a minority such as *phreaking* . Phishing now appears daily, causing millions of dollars to steal.

To protect users from these dangerous attacks, today's web browsers are much more improved and smarter than previous web browsers. Show in Firefox 3 is an anti-phishing system (anti-phishing) that is quite effective in catching phishing attempts. However, if Firefox only participates in the protection against phishing attacks, it is not enough, you still need to know some basic ways to prevent yourself. In addition to the basic knowledge of anti-phishing, in this article we will show you how to add preventive measures so that Firefox can resist the best phishing attacks, as well as test your browser. to ensure that it can catch the best efforts.

Features included

Before going into the advanced details, let's take a look at what Firefox provides by default. The built-in feature works by collating the site you are visiting with a list of known malicious sites. This method is based on Google's secure browsing protocol (Protocolv2Spec).

By default this feature is enabled; however, if you want to be sure of that, open the Preferences window and click on the Security tab (Figure A). From within this tab, you will see both the Block Reported Attack Sites and Block Reported Web Forgeries items have been integrated. If either of those checkboxes is not checked, check it and close the Preferences window.

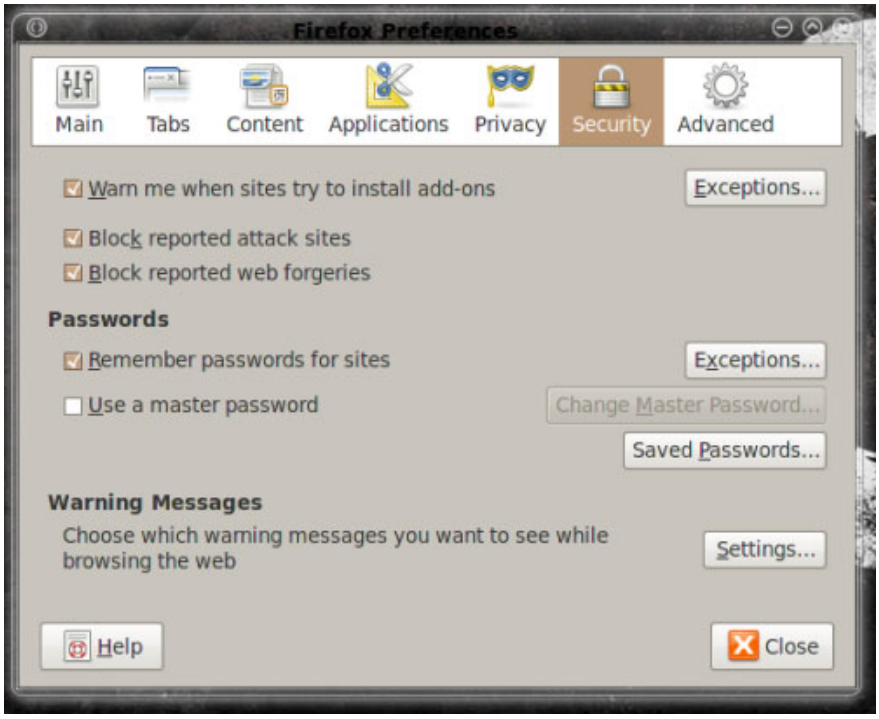

Figure A: You can check the anti-malware options that are enabled.

There are no configurations available for accompanying anti-phishing measures. However, what happens in the default mode is not enough. No matter how good this default defense is, someone can attack you. Therefore, in this case, the motto 'as little as possible' will be misapplied. So what do you need to do here?

The first thing you need to do is install the Petname Tool add-on, which is an add-on that allows you to name all the safe sites that you often visit with 'friendly names', which will added to the encoding identifier. After doing so, the next time you visit the site, you'll see the 'intimate name' you provided to the site in the **Pet Name** window on your toolbar. To install Petname Tool, follow these steps:

- Open your Add-Ons window.
- Enter the search keyword 'petname' (without quotes).
- Select the Petname Tool add-on and click the Install button.
- Restart Firefox.

Now that the add-on is installed, you will see the Petname Tool bar. Normally, this bar will be on the right side of your Search bar, as shown in Figure B below.

Figure B: By default all sites will be tagged with an 'unknown site' header until
They are named

Let's do an experiment with naming Paypal. Go to *www.paypal.com* and enter 'Paypal' (without quotes) in the Petname Tool bar and press Enter. When you enter that 'intimate name', you will see a message telling you that when you click the Petname folder (located in the Bookmarks toolbar), 'friendly name' Paypal will appear.

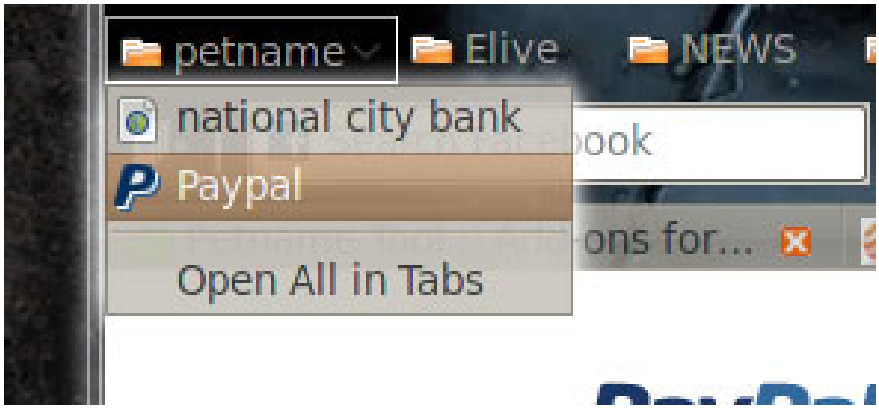

Figure C: You can name trusted sites that you often visit.

After naming the site, go back to the site and check out the Petname Tool bar. Now you will see 'intimate name' appear. If a site is a phishing site tricking your site, the 'intimate name' that you have set for that site will not appear.

Test Firefox

You can test Firefox to make sure phishing prevention is working. What you need to do now is access here. If you see a warning displayed in Figure D, Firefox is protecting you.

Figure D: If you click the Ignore This Warning link, you will see the website 'It's a trap'

Netcraft Tool

Another tool is the Netcraft Toolbar add-on, which is an add-on that uses a different method to solve the same problem. The Netcraft Toolbar (Figure E) installs a toolbar to display the site's risk, rank, and provide a report link (this report provides you with information that Netcraft gathers about the site). . Also on this tool, the bar is a drop-down menu, with this menu you can report a site.

Note : The installation of the *Netcraft Toolbar add-on is* basically the same as the Petname Tool bar installation process.

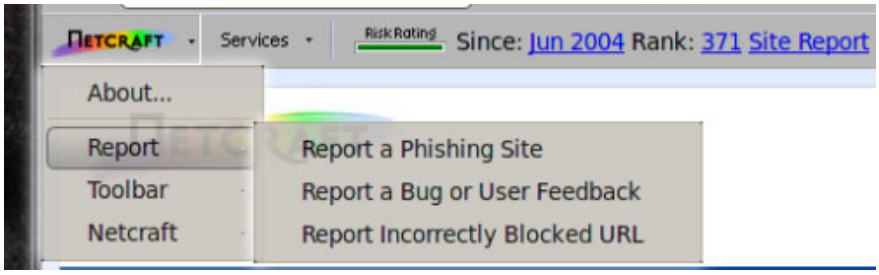

Figure E: You can report to lock a site that is misbranded

The most important feature of this tool for users is the Risk Rating. The bar will be green (if the site is low risk) or red (if the site has a high risk). There are several coefficients associated with risk calculation. The main factor is the age of the site. So you can visit a site that you know is safe (it might even be your own site) but still get a high level of warning because this tool is completely new to your site. No matter why, this is still the best way to avoid risks with sites like this.

Conclude

Phishing is an offensive action that we cannot fight against them overnight, the best way is to create appropriate protection if possible. With the two add-ons we introduced in this article and Firefox's built-in protection feature, you will get more powerful means of counteracting counterfeit attacks.