What is Pharming?

Pharming happens when a user is fooled into thinking a web site is legitimate based on how it looks. The user can be fooled into entering sensitive data such as a password or credit card number into the false web site. It is different than phishing in that the attacker does not have to rely on having the user click a link in an e-mail to deceive the user - even if the user correctly enters a URL (web address) into a browser's address bar, the attacker can still redirect the user to a malicous web site.

The threat due to **pharming** is not new, and has been known to security experts under the more technical term DNS cache poisoning. However, due to the increasing use of the Internet to conduct financial transactions, criminals are now using **pharming** for profit.

How can you protect yourself against pharming?

Look for the secure connection **https:** as part of the web protocol on the login page. For example: You will see this on the URL - web address line - of our Online Banking page. The **https** indicates the web site uses a secure connection to prevent other web sites from impersonating it and is also called a PhC web site. If an attacker attempts to impersonate a PhC web site, the user will receive a message from the browser indicating that the web site's "certificate" does not match the address being visited.