What is Pharming

Pharming is a form of online fraud where attackers (known as “pharmers”) rely upon fake websites to steal confidential information.

Victims are re-directed to fake versions of websites without being aware of it, even if they have typed the correct website address.

These fraudulent websites, which look similar to the genuine websites, collect personal user information and send them to the pharmers.

Often, the fake websites also infect the user’s computer by installing malware on it.

Pharming attacks are most often targeted to the websites of financial institutions or electronic commerce sites.

Consequences of pharming attacks

Pharming attacks can result in:

- theft of personal information such as passwords and credit card details
- financial loss
- reduced confidence in the use of the Internet for financial transactions
- malware infection
- disclosure of confidential information

Tips for preventing pharming

- Make sure you are on the authentic website by checking the website address for any spelling mistake.
- Use an updated antivirus software to reduce your exposure to pharming attacks.
- When submitting financial information, use websites whose URL starts with “https”.
- Consider using up-to-date browsers having add-ons that protect against pharming attacks by differentiating a genuine website from a fake website.
- Be suspicious of any email with urgent requests for financial information.
- Pay attention to error warnings from your browser.
- Practise safe internet surfing.

If you suspect a case of pharming when visiting a website, leave the website immediately and apply preventive measures.
Hi John, each time I am accessing my Internet Banking web page, my Internet browser gives me warning messages.

What type of warnings?

The messages say there is something wrong with the web page or the security certificate of the web site!

It could be a pharming attack.

What is a pharming attack?

It is when you are redirected to a fake website even if you type in the correct Web address in your browser.

Pharming attacks can result in:
- theft of personal information
- financial loss
- malware infection

How can I prevent pharming attacks?

Some tips for you:
- When submitting financial information, use websites whose URL starts with “https”
- Use up-to-date browsers having add-ons that protect against pharming attacks
- Pay attention to error warnings from your browser

And remember: attackers always try to find new ways to perform malicious activities. So always be on your guard when surfing the Internet.

Thanks John. I hope everyone using the Internet will follow your tips.

For sure, I will.