Ministry of Technology, Communication and Innovation

IT Security Unit

IT Security Awareness

PHARMING

"Be aware of the websites you are visiting"

November 2015 Issue 03

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.

If you suspect a case of pharming when visiting a website, leave the website immediately and apply preventive measures.

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.

Illustration