

Fluxcard.com



Original Content Articles

All content automatically monitored for theft. Any infringements, spidering or other copying is prohibited, legal action will be taken against any such behaviour.

© Fluxcard.com 2010

HOW FAKING ID AND PHISHING ARE CORRELATED

Phishing is the most popular type of fake IDs in today's world. Phishing is a technique which uses engineering and technical trick to take the person's personal confidential details, accounts, passwords and usernames. There is no need for a personal introduction; all you require is access to the internet. The internet is the medium which is used widely by many people and it helps phishers to misuse it for their benefit.

In today's world we depend mostly on internet for our daily work as it has speed and is efficient. We do all our financial transactions on net, shop online with credit cards and get in touch with our friends and business colleagues through mails. It is the duty of the bank to verify our bank details through email and one should not be surprised if the bank enquires about our details through our mail account. As it is the duty of the banks, it is also our duty to provide all the details asked.

The dependence on internet has created these new crooks called "phishers". The aim of this phisher is to gain the trust of victim by posing themselves as an established organization and fooling them to give their financial information, like card numbers, addresses, usernames, passwords etc. Whenever a person visits the website, it asks about their personal details and many people get into their trap.

But there are many sites which have a function of phishing report to make aware of the frauds going on in the websites. Technical trick of phishing is done through installing of nasty software to get the information. The most preferred tool of the phishers is the Trojan. By this new method, the phishers target social networking websites. Other methods used by these phishers are manipulation of links, where the phisher gives a link in the form of an email and when clicked, you are taken to the phisher's website. Another tactics used by phishers is phishing through phone, wherein the email message asks the recipient to call a number and if there is any problem or malpractice, then they ask you to pay the damage. It is not only monetary loss but also email access loss and false accounts in the name of the victim.

There are anti-phishing groups who try to control the phishing activity. Many companies and banks make efforts to make the transactions with their customer's phishing proof. Valid emails include part of the number/address the clients use as their own username. They include certain details in the email which is not known to the phishers. Some of the websites have included novel features which show the original domain of the website or they use softwares that are anti-phishing.

Some of the website use whitelist and blacklist and some of them provide tool to secure their password/filters to avoid phishing mails. In view of this, the US government has introduced an act on anti-phishing in the year 2005, claiming all the criminals who are into phishing will be fined \$250,000 and five years in prison.