A "black" private information stealing trojan is detected in the Indian online banking transactions space, and have alerted consumers who swipe debit or credit cards at shopping counters to make payments.

Cyber security and internet banking protection agencies have detected traces of a new kind of virus that has the ability to zero-in on point of sale (PoS) terminals. It is categorized as a 'Black' virus, this piece of code attempts to steal private and financially sensitive information in the Indian online banking transactions space. The people who regularly swipe their credit/debit card while shopping, are said to be the most vulnerable to the virus.

What is the Virus and its nature?

This trojan spreads rapidly and its class virus was recently detected at multiple POS Terminals. It has got many names such as **Dexter, Black POS, memory dump and grabber**, the virus is capable of morphing into about 7 forms of seemingly legit pieces of software, any one of which is then able to breach the security protocols of the PoS Terminal. Once the Trojan virus is able to gain entry, it manages to assimilate and send personal information of the card holder like name, account number, expiration date, CVV code and any other piece of information that can be used to later pose as the owner and carry out transactions.

A report from CERT says that the virus is especially troubling since it gathers multiple snippets of information that are routinely used by banks to authenticate the user. Hence this information can be easily used to execute phishing attacks too.

The common infection vectors for POS system malwares includes phishing emails or social engineering techniques to deliver the malware, use of default or weak credentials, unauthorized access, open wireless networks along with the methods of installing malware as a part of service.

Online banking as well as other forms of financial transactions has always been targeted by hackers. However, this is a new form of attack which takes place at the point of sale. Though the banks have taken a note of the vulnerability, it is advised to use your card with discretion.

Corrective Steps from RBI:

RBI had already made it obligatory to punch PIN of the patrons at the POS in order to save debit cards from financial frauds and loss of hard-earned capital of the holder.

Few more Counter measures:-

Keep all PoS computers thoroughly updated including PoS application software, restrict access on PoS systems to PoS related activities only, ensure the networks where the PoS systems reside are properly segmented from non-payment network and restrictive policies on usage should be deployed and enforced," the agency recommended.

The agency also pointed out that PoS counters should "maintain good security policy on the PoS computers (including physical access), disable autorun or autoplay, install and scan anti-malware engines and keep them up-to-date and exercise caution while visiting links within emails received from untrusted users or unexpectedly received from trusted users while also enabling firewall at desktop and gateway level."

Good Read: http://www.spamfighter.com/News-18801-Beware-Banking-Virus-has-been-Detected.htm