

Ramesh Mengawade, CEO, ElectraCard Services, offers guideline for a secured online transaction



For safe online transactions

For many of us, electronic transactions have become part of everyday life, from online banking to purchasing goods over the Internet.

However, not everyone is aware about small little things one needs to do for protection. It pays to know some and be aware of potential pitfalls. There is some important information one should know before dealing with money online.

Protect data

One should give the password and credit card number only in a secure connection on a web site, not in ordinary e-mail. 'Theft of identity' is a growing problem and one should carefully guard personal information so that no one is able impersonate.

Choose the password well

The best passwords are not the address, birth date, phone number or recognisable words. Choose a string combination of letters, numbers, and punctuation marks. Strong passwords are important to help have safer online transactions. The lengthier and complex the password, the stronger it is.

Know the mail

Do not respond after receiving a mail stating that it is from the bank or the

credit card issuing institution asking to update bank information or credit card information. This could be a phishing scam. Also, never respond to unsolicited e-mail offers or requests for information. Most of the banks do not use e-mail to communicate any personal information or ask to share personal data over email. Be cautious about such mails and do not provide personal or financial information online.

Signs that protect data

On the Web page where one enters the credit card or other personal information, look for an 's' after http (https) in the Web address of that page. Encryption is a security measure that scrambles data as it traverses the Internet. Also make sure there is a tiny closed padlock in the address bar, or on the lower right corner of the window.

Beware of suspicious Websites

Use a filter that warns of suspicious Websites. browser filters that warn about reported phishing sites and block the addresses to avoid visiting them.

Use mobile alert services

Register for the bank's mobile alert service to keep receiving alerts whenever there is a significant transaction

made in the account. This will also help identify and report any transactions that are not legitimate.

Always completely log off

It is important to completely log off from the Internet banking session; simply closing the window after performing the transaction may not close the banking session. This could mean that the session may become hijacked and can be used for illegitimate financial transactions.

Change the password regularly

One should always change the online banking passwords periodically at least every month.

Don't use public computers

Because public computers may have programs that log keystrokes (keyloggers), as well as other spywares that snatch sensitive information, wait to make the Internet transactions after getting home. Also avoid using public wifi connections to do any kind of financial transactions.

Use updated anti-virus programmes

Be sure that the computer is secured with updated anti-virus, anti-spyware, and firewall software.