# E-frauds threat

Dr. AbdelGadir Warsama Ghalib

Legal Counsel - Bahrain

Electronic banking is almost taking a very significant portion in the banking industry. This vast remarkable progress took its shape based on the e-banking laws and regulations issued in all countries, to give recognition and legal authority to such important banking service.

Almost, all clients are dealing with banks through internet, mobile or other IT mechanism. This new situation, has given a golden opportunity for banking services to expand and cover all corners. However, the new development was not without a price. The other side of new situation, was the appearance of fraudsters who took this opportunity to exercise their dirty criminal games. The IT revolution has opened the room for new criminals and new crimes to come to surface and destroy the new technology. New e-crimes came-up and grew rapidly to harm every person utilizing such technology.

The new e-frauds include, among others, phishing, identity theft, viruses and trojans, spyware and hadware, card skimming, mobile scams… etc. Phishing is a form of internet fraud that aims to steal information as card numbers, user IDs and passwords. A fake web site is created to look similar to that of a legitimate organization. An email or SMS is sent leading recipient to a fake web site and enter personal details, including, security access codes. The page looks genuine but users are inadvertently sending the info to fraudster.

Identity theft is increasing and takes many forms, from fraudulent credit card use, to your entire identity used to open accounts, obtain loans and illegal activities. In this respect, be suspicious if anyone asks for personal information. Scammers use convincing stories explaining why to give them money or personal details. Viruses and trojans are very harmful programs that are secretly loaded in computers without being noticed. The goal of these programs is to obtain or damage information, hinder performance of the computer or flooding with advertising.

Viruses spread by infecting computers and then replicating. Trojans appear as genuine applications and then embed into computers to monitor activity and collect information. Using firewalls and maintaining strong virus protection software can help to minimize chances of getting viruses and inadvertently downloading trojans.

Spyware and adware are there when clicking on pop-up advertisements that “pop-up” in a separate browser window. These programs often come bundled with free programs, applications or services that may be downloaded from the internet. Spyware or adware software covertly gathers user information and monitors internet activity, usually for advertising purposes. All are to be cautious about clicking on internet banners and pop-ups or downloading free programs and use security software to detect and remove spyware.

Fraudsters can use card skimming by illegal copying and capture magnetic stripe and PIN data on credit and debit cards. Skimming can occur at any bank ATM or via other compromised machines. Captured card and PIN details are encoded in a counterfeit card and used for fraudulent account withdrawals and transactions. They can attach false casings and PIN pad overlay devices in genuine existing ATMs, or attach a camouflaged skimming device in a card reader entry used with a concealed camera to capture and record PIN entry details. A foreign device is implanted in certain machines capable of copying and capturing card and PIN details processed through the machine.

Above are some of malpractices performed by fraudsters using all advanced IT programs. We need to be more careful as we may be haunted at any time and great damage and loses will be the result of such frauds.