MY SPACE

Watch out for 'skimmer' while swiping your card

By Vikas Srivastav Jun 14 2012 , Mumbai

Tech-crazed Indians, transacting online and through ATMs, may be exposing themselves to a new risk of financial fraud from a card reader with a pinhole camera that connects to ATM machines through bluetooth.

Skimmer, as the device is known, transfers data from the card to operators and money mules, helping them siphon off funds from bank accounts through subsequent online transactions.

Skimmer sells for $5,000, but is also rented in the marketplace to cheats.

Sachin Raste, senior analyst with eScan Antivirus, says the global online and ATM scam market is worth about $3 billion, with India accounting for almost five per cent of the pie. What Raste does not say upfront is that his company may be selling solutions to avert such fraud, which is not the reason we are reporting this here. We believe you should know that your bank account may be under threat, and its best to check safety precautions with your banker.

"In India, it is mostly the money mules who operate; they withdraw the money once the card is stolen and transfer the amount to anonymous accounts," Raste says.

"The money is then withdrawn by these mules who charge a commission on the total withdrawal." he adds.

He claims that the brains behind the fraud mostly operate from the CIS countries, such as Estonia, Serbia and Lithuania.

The ATM card and bank account details are sold in the black market for 50 cents to $5 depending on the country of origin, Raste said.

Skimming is not limited to ATM machines alone; bank details can also be skimmed at merchant shops that swipe credit cards twice, the second swipe could transfer details through skimmers. "The first swipe is for actual transaction and second for collecting your card details which are then stored and are further used by card cloning devices," Raste said.

Chances are that terminals at retail stores connected on LAN could be used to authenticate cards via internet. "In case their systems are compromised, then every person who has transacted would be at risk. The best example for this type of crime is the intrusion of HeartLand Payment System in the US through which 130 million credit card and debit card data was stolen," Raste said.

To prevent fraudulent use of credit and debit cards, customers should avail the option of SMS/email alerts sent to their mobile phones and other devices. An SMS/email alert, sent to the mobile phone on any activity or transaction carried out will help customers react immediately to suspicious transactions from their account.

Even mobile phone transactions can be traced and data stolen through Bluesnarfing that authorises access to information from a wireless device through bluetooth connection. The theft happens mostly from phones, desktops and laptops. This allows access to a calendar, contact lists, emails and text messages. Some phones users can also copy pictures and private videos.

One of the best ways to prevent bluesnarfing is to keep bluetooth switched off if not in use and to disable the "make device visible" option. By making the device visible only when needed, users can prevent unauthorised access to their phones.