Targets for Debit Card Fraud

Organized skimming attacks on ATMs and self-service point of sale terminals lead the pack in debit card fraud but don't rule out the possibility of having your debit card skimmed after a leisurely meal at your favorite restaurant or your PC hacked while gathering with your friends at the local coffee shop. Wait staff and Wi-Fi also figure into fraud statistics.

Restaurants

In a typical dining scenario, restaurant goers finish dining, are presented with the check and leave their payment card for the waiter to pick up and settle at the register. A corrupt waiter will pass the card through a small, handheld electronic device that scans and stores the card data from the magnetic strip. It takes only a few seconds for the card to be swiped on the way to the register. Waiters are sometimes recruited to perform skimming and are paid when they turn over the stored data. Others sell the information over the internet or to a contact.

Stand-alone ATMs

Global skimming rings still try to exploit magnetic-stripe technology with improved schemes at automated teller machines. Stand-alone ATMs, in particular, are not under the same scrutiny as ATMs located in banks and their drive-thru locations. Many times security cameras are not mounted near the stand-alone ATMs and that makes them prime targets for fraudsters to surreptitiously plant and remove skimming devices. The deceptive card reader or skimmer affixed expertly over the card acceptance slot, hidden cameras to visually record a cardholder entering their PIN onto the keypad or the keypad overlay placed directly over the factory-installed keypad to record and store keystrokes all can be installed on an unattended ATM in less than 60 seconds.

Self-service Gas Pumps

Like stand-alone ATMs, pay-at-the-pump gasoline terminals or any unmanned terminal are targets for card skimmers and are far easier to tamper with than ATMs. Fraudsters can easily set up and remove a skimming device on a terminal that is unattended. When equipment is reported or found on terminals, the skimming operators simply migrate their scams to another area, many times small communities that are less informed about the possibility of having their debit cards skimmed and counterfeited.

Public Wi-Fi

Most public Wi-Fi hotspots such as airports, coffee shops, hotels, etc., sit wide open to hackers mostly because they are unencrypted. Rogue access points that mimic legitimate networks (Wiphishing) lure users into connecting to the hacker's network. The imposter or 'evil twin' as it is called is designed to look like a real Wi-Fi hotspot. Users focused on surfing and shopping and not safety may unwittingly expose their passwords or other sensitive data like card and account information to hackers after connecting to the imposter.