

Protect Yourself From ATM Skimming

February 10, 2011 - How would you feel if a stranger stood a little too close to you the next time you are at an ATM? You might be unsettled to say the least, and may try to move around to shield that person from seeing your pin, or how much money you had decided to withdraw at that time. Thieves, known as skimmers, would try to get your receipt which had your full bank account number, and your pin code. Now there is a new trend for skimmers, and one far worse. Known as ATM skimming, it is now a global problem where a magnetic card reader is glued to the front of an ATM machine and a tiny video camera is placed with a view of the keypad. With this combination, a thief can then download hundreds of ATM-card numbers from the device, along with the personal pin number from the video recording. Then, making a new, cloned ATM card is easy and so is emptying your bank account.

Tweet

```
(function() {  
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];  
s.type = 'text/javascript';  
s.src = 'http://widgets.digg.com/buttons.js';  
s1.parentNode.insertBefore(s, s1);  
})();
```

In Europe many countries have started using cards with embedded microchips that are harder to skim. This is making the United States more of a target for ATM skimming than in past years. How successful is this business of cloning ATM cards? The estimates for bank losses are close to \$1 billion every year. Some banks have begun to invest in jammers that are installed to limit the ability to read a consumer's card information. However, these are expensive, and with over 40,000 ATMs in the United States would also be very a time consuming process.

Discrepancies in your bank account are more difficult to resolve, because ATM cards are not offered the same theft protection as regular credit cards. Most credit cards have become more aggressive at offering theft protection, and they will limit your liability if your card is stolen. In some cases, you may even have up to 90 days to resolve a dispute if you notice something is incorrect on your statement. Banks generally allow less time to notify them of any fraudulent charges. Now imagine you have no idea that your card was cloned and do not notice that anything is suspicious until you are charged overdraft fees. This is the scenario that more and more Americans are experiencing.

So what can consumers do to protect their bank accounts and ATM cards? One way is by examining the ATM machine prior to use. Look for any visible glue marks, or loose parts, especially on the card reader slot. Second, be sure to use one hand to shield the camera from viewing the pin pad when you are entering your number. If there is no camera visible, there may be one in a light or brochure holder nearby. Third, be careful when using your card in high traffic areas. According to reports, typically thieves want the most bang for their buck, so they will manipulate ATM machines in high traffic areas such as malls, airports and gas stations. Getting cash or using your ATM card in these areas will make you more vulnerable to skimming. In an emergency where using your card and pin number is unavoidable, remember to closely monitor your bank account for any unusual transactions and notify your bank immediately if something is wrong.

By: Amanda Barron and Lisa Merryman

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#).

Registration is easy and free.