TheMiddletownPress
http://www.middletownpress.com/news/article/Etips-and-traps-No-one-immune-to-ATM-skimming-11841433.php

Etips and traps: No one immune to ATM skimming

BILL MURRAY **Published 12:00 am, Tuesday, March 20, 2012**

Back in the old days - mid-1990s - Russian mobsters trained with sledgehammers to take out ATMs in seven strategic whacks. They had a solid run in Fairfield County, Connecticut.

Now, they are a lot quicker and more difficult to detect.

In the digital age, the FBI reports that Eurasian and other crime groups have refined the practice dramatically. They install hidden card readers that blend in to the façade of ATMs. These devices read your information as you insert the card into the ATM. Every keystroke is recorded. Sometimes a phony keypad is placed on top of the existing keypad to catch the pin number. ATM thieves also place hidden cameras on the machines to catch pin numbers.

Once the thieves retrieve your information, it is stored on a small laptop or cell phone and sent wirelessly. Similar tactics have worked for crooks at gas pumps.

Typically, these skilled criminal technicians make new ATM cards, use them for a couple hours and then get out of town.

The skimming devices are difficult to notice. They are usually made of plastic or plaster and painted to match a particular machine.

This practice made its way into Connecticut last year during the holiday shopping season. Three New York men were charged with skimming 11 banks and a credit union in Manchester, New Britain, Southington, Enfield and Groton. West Hartford police also acknowledged reports of skimming.

"Cover your pin somehow from what otherwise may be a pinhole camera," West Hartford Police Lt. Stephen Estes told NBC Connecticut.

We advise bank customers to look closely at ATMs before using them. See if there is any discoloration on the face near the card slot. The FBI warns to be wary of anything

loose, crooked or damaged. In particular, inspect the machine for any scratches or adhesive tape residue.

Also, see if there is a cover over the slot or if there is a seam anywhere near the plastic. If you notice anything out of place, do not use the machine. Notify bank employees or authorities immediately.

The U.S. Secret Service reports that skimming costs banks and customers about $8 billion annually. A sampling of digital bank heists in the Northeast includes $1 million in Manhattan from just two banks; $20,000 from 30 accounts in Bethlehem, Pa.; and $100,000 from a weekend spree at a single neighborhood ATM in Staten Island.

It's a global problem. Police in Australia reported more than $1 million was taken from about 40 ATMs in several cities last year. In the U.S. Northwest, a Seattle case featured withdrawals over several days from ATMs the customer never visited.

There are more than 400,000 ATMs in the U.S. among the 1.7 million worldwide, according to the ATM Industry Association. About every six minutes, a new ATM is installed somewhere in the world. Annually, there are 40 billion ATM cash withdrawals worldwide.

The security firm ADT began marketing a new anti-skimming device for banks in February. The company says that when the device detects a skimming attempt, it generates sound and visual warnings for the customer.

We suggest it would be prudent to ask your local banker what protective measures have been taken to prevent ATM skimming.

No one is immune.

Bill Murray is president of EdocMasters LLC **http://edocmasters.com/** of West Hartford, CT, a company that takes the mystery out of e-docs. Andy Thibault, author of books including Law & Justice In Everyday Life, is a contributing editor for Journal Register Connecticut Group and blogs at The Cool Justice Report, **http://cooljustice.blogspot.com/**