Beyond Blocks and Bricks

Number Nine

Ronald J. Hunsicker
Professional Engineer
Masonry Investigations
P. O. Box 6615
Wyomissing, PA 19610-6615
484-332-1164
rjhpe@ptd.net

On the road (or at home)

Over the years, I have had half-a-dozen credit cards compromised and I've become very wary. The recent article from The New York Times reproduced below offers advice about avoiding being hacked at an ATM when using a debit card or your bank card. I have learned a few other strategies:

Carry two credit cards. If one card is compromised while you are away from home, the second card will get you home.

Plan ahead; get cash for smaller purchases before you leave. Keep some cash in your pocket, Use cash instead of your debit card or ATM card.

Plan ahead; use the ATM machine that you always use, not the one at the airport.

For larger purchases, use a credit card, not a debit card or cash. Hotels and car rental agencies rely upon your credit card as a security deposit if you trash the room, bolt without paying, or steal the car. Hotels don't like cash and discourage its use. When a debit card is used to buy a night at a hotel, they often make strong demands for transferring funds now rather than later.

Call the cops. Always. If you are defrauded and you have an idea where the theft occurred, call the cops there. I had not used my business card for a few weeks and used it for dinner near home one night. Next day, a charge for $3,000 at a big-box home store 40 miles away appeared. The local cops had a chat with the restaurant after I reported the theft.

How to Spot A.T.M. Skimmers

By JENNIFER SARANOW SCHULTZ
The New York Times
6 February 2011

To help readers better protect themselves from thieves who want to swipe their sensitive debit card information, we've shared pictures in the past of how to spot skimming devices on A.T.M.'s. Skimmers applied to card readers (think fake card readers on top of the real ones) are designed to capture debit card magnetic stripe data, while tiny wireless cameras or overlays to existing personal identification number pads are designed to capture PIN information. Once thieves capture such data, they can use it to make fake cards or sell the information on the Internet to others.

Besides learning what skimming devices look like, consumers can also employ other strategies to spot the devices, according to John Pearce, director of commercial marketing for banking-financial and government systems at the security company ADT, which sells anti-skimming technology. He recently shared the following strategies with us.

Perform an A.T.M. Inspection Before swiping your card

Mr. Pearce recommended that consumers examine A.T.M.'s for tell-tale signs of skimmers like visible glue marks or residue around the reader or PIN pad. Also, look for loose parts (tug on the card reader, say, to see if it comes off or if there is a loose appendage recently added to the machine). "You want to inspect the card reader slots first and foremost," Mr. Pearce said. "If there's any residual of glue around the PIN pad area or around the card slot, there's a pretty good chance there was skimming activity in the recent past."

Perform an A.T.M. Area Inspection

Mr. Pearce also recommended that consumers look around the A.T.M. area to see if anything looks out of the ordinary. For instance, is there a cola can or pack of cigarettes on the top of the A.T.M. or promotional literature nearby? If so, look closely to make sure there's no miniature camera hidden in such spots. Check the ceiling above the A.T.M. for such cameras as well. While legitimate security cameras for the banks will be clearly overt and visible, these cameras will be hidden and about three-fourths of an inch square in size, Mr. Pearce said.

Cover Your PIN When you type in your PIN

Mr. Pearce recommended using your other hand to shield the keypad to block it from video cameras hidden in the light above the keypad or elsewhere. This can also help protect your information from "shoulder surfers," people who Mr. Pearce said stand off to the side to try to record your PIN.

Know Which A.T.M.'s to Pay Special Attention To

Mr. Pearce recommended being extra vigilant and cautious when using A.T.M.'s at heavily trafficked areas like malls, airports and gas stations. In many cases, he said, skimming can go unnoticed in such locations because there aren't any personnel monitoring the machines. In addition, if you're having problems using a machine, avoid any offers from help from strangers. "They know you are having a problem because they caused the problem to take place in the first place," Mr. Pearce said, noting that they would ask for your personal identification number as they try to enter your card.

Know When to Use Your Credit Card

In situations where your card goes out of your line of sight (like at a restaurant or hotel), Mr. Pearce recommended using a credit card rather than a debit card.