

Four Risky Places To Use Debit Cards

http://finance.yahoo.com/news/financially_fit_article_113817.html

They not only steal your identity – They steal all of your money.

Would you give a thief direct access to your checking account?

No? Unfortunately, you may be doing just that by regularly using your debit card. Debit cards may look identical to credit cards, but there's one key difference. With credit cards, users who spot fraudulent charges on their bill can simply decline the charges and not pay the bill.

On the other hand, debit cards draw money directly from your checking account, rather than from an intermediary such as a credit card company.

NEWS VIDEO

Because of that, even clear-cut cases of fraud where victims are protected from liability by consumer protection laws can cause significant hardship, says Frank Abagnale, a secure-document consultant in Washington, D.C.

He cites the example of the The TJX Companies Inc.'s T.J. Maxx data breach that exposed the payment information of thousands of customers in 2007. The incident resulted in \$150 million in fraud losses, and much of it was pulled directly from customers' bank accounts.

While credit card users got their accounts straightened out and new cards in the mail within a few days, the case created major problems for debit card holders who waited an average of two to three months to get reimbursed, Abagnale says.

While debit card fraud is always a possibility, being careful where you use it can help keep your checking account balance out of the hands of criminals.

Skimming ATMs

The idea that outdoor ATMs are among the most dangerous places to use a debit card seems a little bit absurd. But some ATMs present a perfect opportunity for thieves to skim users' debit cards, says Chris McGoey, a security consultant based in Los Angeles.

Skimming is the practice of capturing a bank customer's card information by running it through a machine that reads the card's magnetic strip. Those machines are often placed over the real card slots at ATMs and other card terminals.

"Any transaction you do outdoors at an open ATM is going to be higher risk exposure," McGoey says. "If the public has access to it, then someone has the ability to add skimming devices to it, position cameras on it and position themselves in a way where they could surveil it."

He says you're **better off using an ATM inside a retail outlet** or other high-trafficked, well-lit place.

Julie McNelley, senior analyst for Aite Group LLC, a Boston-based financial services research firm, says even the card terminals that card users must swipe to get into ATM vestibules are being used as a skimming site by criminals. You can spot ATM skimmers by checking for ATM components that look beat-up or askew, she says.

Stealing PINs at Gas Stations

Gas stations are another danger zone for debit card use.

“You go to a gas station and you stick your debit card in there, and you swipe it through a machine,” Abagnale says. “I’m sitting across the street with a laptop and an antenna. I put a skimmer in there, and I’m picking up all the information. Before you even get home, I’ve debited your account.”

Gas station payment terminals have many of the characteristics card fraudsters love, McNelley says.

“In a gas station where you do have a whole bunch of pay-at-the-pump kinds of things and minimal supervision, it’s pretty easy for a bad guy to put a skimming device on and put a little pinpoint camera there and compromise debit cards that way,” McNelley says. Thieves often use small cameras to capture footage of debit card users entering their PINs so they can have free access to their money.

She says even if the thief doesn’t manage to get your debit card personal identification number, or PIN, from such a device, he still may be able to duplicate the card’s magnetic strip and use it for “sign and swipe” Visa or MasterCard transactions.

With the high potential for fraud in pay-at-the-pump debit transactions, it might make sense to use an alternative such as cash or credit cards the next time you fill up.

The Web Is a Risky Place

Debit cards are a convenient way to buy products online, especially for those who don’t like to use credit cards. Unfortunately, the Web is one of the most dangerous places to make purchases, McNelley says.

“Online is the No. 1 place where consumers should not use their debit cards,” she says. “It’s susceptible at so many points. The consumer could have malware on their computer, so it could be at their endpoint that the data get compromised.

It could be a man-in-the-middle attack where somebody is eavesdropping on their communications via the wireless network. And then at the other end, that data goes into a database at the merchant. As we’ve seen with some of the higher-profile breach events over the last year or so, that data is going to be vulnerable if (they’re) not properly cared for.”

Aside from the potential for hacking at many different points in a transaction, Abagnale says a fundamental problem with using debit cards online is it’s impossible to know who is handling your information.

“Buying stuff online, you have to be careful because you have to know who you’re doing business with. When you buy things online, what always kills me about that is people say, ‘This is a safe site,’” Abagnale says. “Who works there?”

Restaurants Keep Customer Data on File

“Would you care for a side of debit card fraud with that?”

Restaurant servers don’t ask that question, but they might as well with the standard practice of taking customers’ debit cards to run them behind closed doors.

“Any place where the card is out of hand” can increase the chances of fraud, says McGoey. “The guy comes to your table, takes your card and disappears for a while, so he or she has privacy,” giving the person the opportunity to copy your card information.

Even restaurants without sit-down service can present a threat. McNelley says using debit cards to order delivery can be risky because cashiers tend to keep customer payment information on file. That may make future orders more convenient, but small businesses rarely take the steps necessary to safeguard payment information, she says.

Overall, she says, regardless of whether you use your debit card at a small restaurant or a big-box store, the possibility of fraud is always there. She cites the example of Michaels Stores Inc., which saw its customers’ debit card information stolen in May by debit card terminals doctored by thieves.

“Even if you do exercise caution ... there are still the Michaels-type incidents that will happen,” McNelley says.