New Credit/Debit Card Scam

Adapted from a release issued by the Institute of Consumer Financial Education

There's a new scam out there, one that may take in even the savviest consumer, because the con artists have obtained information that makes them look legitimate. By phishing and pharming on the phone and over the Internet, scammers are getting credit card numbers, personal identification numbers (PINs), and the three- to seven-digit security numbers off of the backs of credit and debit cards.

You could easily receive a call from a crook representing him- or herself as an employee of the institution that issued your personal or business credit or debit card. The caller says that he/she is processing a credit of almost $500, because one of your cards may have been used improperly. Wow, you think, a $500 credit. If you're like most cardholders, you sit up and take notice. The caller already has your credit card number(s), name, address, and telephone number, so you don't hesitate to answer his/her questions.

Stop. Hesitate. Don't answer. The reason the scammer is calling is that he/she needs the numbers from the back of your card. With this information, the caller can start running up charges on your account.

The scenario goes like this: an unsuspecting consumer answers his/her home or work phone and hears, "This is [gives a name], and I'm calling from the security and fraud department at VISA. My employee ID badge number is 3736214."

Next comes an ominous warning. "Your VISA card has been flagged for an unusual purchase pattern, and I'm calling to verify some things. This would be on your VISA card which was issued by [name of your bank or credit card company]. Did you purchase an anti-virus software program with a personal firewall for $497 from a sales and marketing company based in Georgia?"

When the consumer responds that he/she did not purchase the software, the caller continues, "Then we will be issuing a credit to your account. This Georgia-based telephone boiler room outfit is a company we have been watching. The bogus charges range from $297 to $497, which are just under the $500 purchase pattern that most cards flag. Before your next statement, the credit will be sent to [cardholder's address]. Is that correct?"

After the victim confirms that yes, that is the correct address, the con artist says, "I will be starting an internal fraud investigation. If you have any questions, you should call the 1-800 number listed on the back of your card and ask for the Security Department. You will need to refer to this control number." The caller then gives the consumer a six-digit number. "Do you need me to read it to you again?" he or she inquires politely.

Now the thief goes in for the kill—getting the target's security code or PIN. The caller states, "I need to verify that you are in possession of your card. Please turn your card over and look for the numbers on the back. There are seven numbers; the first four are part of the card number, the next three are the security numbers that verify you are the possessor of the card. These are the numbers you may sometimes use to make Internet purchases to prove you have the card in your possession." Then the scammer asks you to read the last three numbers back to them.

After the consumer tells the caller the three numbers, the con artist responds, "That is correct, I just needed to verify that the card has not been lost or stolen, and that you still have your card in your possession. Do you have any questions?" When the victim says that he/she doesn't, the caller urges, "Don't hesitate to call back if you do," and disconnects.

The victim actually says very little during this conversation and is never asked to tell the caller his/her debit or credit card number. The cardholder usually feels secure that this was a legitimate call and rarely calls back. Those intuitive cardholders who do call the bona fide VISA Security Department are informed that the call was bogus and just another scam. More upsetting, however, is that during that call, the cardholder often learns that new purchase of $497 was recently charged to his/her card.

Should you receive such a call, the Institute of Consumer Financial Education (http://www.icfe.info) advises, do not give out *any* security numbers. Make a verifiable fraud report to the issuer involved and immediately close the account(s) in question. VISA or MasterCard will reissue a new number. What the crooks really want is the three-digit Security PIN number on the back of your card. Don't give it to anyone who calls you.

Instead, tell the caller(s) that you will call VISA or MasterCard directly for verification of your conversation. According to the Institute of Consumer Financial Education, VISA and MasterCard Security Departments would never ask for anything on the card; they already know the information because they issued the card.

Don't let the promise of a refund con you out of your PIN number. If you do, by the time you receive a statement listing charges for purchases you didn't make; it may be too late to undo the damage. It could also be more much more difficult to file a fraud report.

An ounce of prevention is worth a pound of cure: should you receive a call like this, hang up immediately.