

## New Scam and Phishing Alerts

### New Credit Card Scam

Snopes.com says this is true. See this site - <http://www.snopes.com/crime/warnings/creditcard.asp>

This one is pretty slick since they provide YOU with all the information, except the one piece they want.

Note, the callers do not ask for your card number; they already have it. This information is worth reading. By understanding how the VISA & MasterCard Telephone Credit Card Scam works, you'll be better prepared to protect yourself.

One of our employees was called on Wednesday from 'VISA', and I was called on Thursday from 'Master Card'. The scam works like this: Caller: 'This is (name), and I'm calling from the Security and Fraud Department at VISA. My Badge number is 12460. Your card has been flagged for an unusual purchase pattern, and I'm calling to verify. This would be on your VISA card which was issued by (name of bank). Did you purchase an Anti-Telemarketing Device for \$497.99 from a Marketing company based in Arizona?'

When you say 'No', the caller continues with, 'Then we will be issuing a credit to your account. This is a company we have been watching and the charges range from \$297 to \$497, just under the \$500 purchase pattern that flags most cards. Before your next statement, the credit will be sent to (gives you your address), is that correct?'

You say 'yes'. The caller continues - 'I will be starting a Fraud investigation. If you have any questions, you should call the 1- 800 number listed on the back of your card (1-800-VISA) and ask for Security.'

You will need to refer to this Control Number. The caller then gives you a 6 digit number. 'Do you need me to read it again?'

**Here's the IMPORTANT part on how the scam works.** The caller then says, 'I need to verify you are in possession of your card'. He'll ask you to 'turn your card over and look for some numbers'. There are 7 numbers; the first 4 are part of your card number, the next 3 are the security Numbers that verify you are the possessor of the card. These are the numbers you sometimes use to make Internet purchases to prove you have the card. The caller will ask you to read the 3 numbers to him. After you tell the caller the 3 numbers, he'll say, 'That is correct, I just needed to verify that the card has not been lost or stolen, and that you still have your card. Do you have any other questions?' After you say No, the caller then thanks you and states, 'Don't hesitate to call back if you do, and hangs up.

You actually say very little, and they never ask for or tell you the Card number. But after we were called on Wednesday, we called back within 20 minutes to ask a question. Are we glad we did! The REAL VISA Security Department told us it was a scam and in the last 15 minutes a new purchase of \$497.99 was charged to our card.

## **Phishing, Smishing, and Vishing: What's the Difference?**

Vishing, Smishing, and U.S. Mail Phishing are new ways to bait you into divulging personal and financial information. Scammers are turning to these different methods with the hope of confusing you into thinking they can only be "phished" through the use of e-mail. These methods are defined as follows:

### **E-MAIL "PHISHING"**

Phishing (pronounced "fishing") is a scam to steal valuable information such as credit card and Social Security numbers, user IDs, and passwords. In phishing, also known as "brand spoofing," an official-looking e-mail is sent to potential victims pretending to be from their ISP, credit union, bank, or retail establishment. E-mails can be sent to people on selected lists or on any list, and the scammers expect some percentage of recipients will actually have an account with the real organization.

### **LAND LINE TELEPHONE "VISHING" & VoIP (INTERNET PHONES "VISHING")**

Vishing, (Voice phISHING) also called "VoIP phishing for the Internet phones," is the voice counterpart to phishing. Instead of being directed by e-mail to a Web site, an e-mail message asks the user to make a telephone call. The call triggers a voice response system that asks for the user's card number or other personal or financial information. The initial bait can also be a telephone call with a recording that instructs the user to phone an 800 number or another area code within or outside of the United States.

In either case, because people are used to entering card numbers over the phone, this technique can be effective. Voice over IP (VoIP) is used for vishing because caller IDs can be spoofed and the entire operation can be brought up and taken down in a short time, compared to a land line telephone.

### **TEXT MESSAGE "SMISHING"**

Smishing (SMS phISHING) is the mobile phone counterpart to phishing. Instead of being directed by e-mail to a Web site, a text message is sent to the user's cell phone or other mobile device with some ploy to click on a link. The link causes a Trojan to be installed in the cell phone or other mobile device.

### **New! Mail LETTER "PHISHING"**

This new scam occurs where the phisher is creating a letter and sending it through the mail to individuals to respond to the letter by calling a phone number. The phisher outlines in the letter that the individual must respond for their own protection. This scam is used in conjunction with other channels to steal valuable personal and financial information of the individual receiving the letter.

### **Loss Prevention Recommendations:**

- Educate yourself on "Phishing, Smishing, and Vishing."
  - If a message is received by someone claiming to be your financial institution asking for confidential information. NEVER respond unless you initiated the request.
  - If you have doubts about who's on the phone, call back the number of record at your financial institution or Card Company.

- Be wary of any message received from an unknown sender.
- Do not open unsolicited e-mails or text messages.
- Do not click on any links provided in unsolicited e-mails.
- Monitor financial accounts on a regular basis.
- If you have a land line or Voice over the Internet (VoIP), it's recommended to create a password protected account.
- Do deploy "blockers" on emails, text messaging, phone numbers, both land line and VoIP. In addition, consider "extra" caution when using "text messaging". Don't display your wireless phone number or e-mail address in public. This includes newsgroups, chat rooms, Web sites, or membership directories.
- If you open an unwanted message, send a stop or opt out message in response.
- Do check the privacy policy when submitting your wireless phone number or e-mail address to any Web site. Find out if the policy allows the company to display or sell your information.
- Do contact your wireless or Internet service provider about unwanted messages.
- If you have been victimized by a spoofed e-mail or web site, you should contact your local law enforcement, US Postal Inspector, or FBI.