Bits and Bytes

Arkansas' Premier Computer Club

September 2007
Don Hood, President

Bella Vista Computer Club - John Ruehle Center
Highlands Crossing Center, 1801 Forest Hills Blvd, Suite 120 Bella Vista, AR 72715-3016
Web site: www.bvcompclub.org
E-mail: jrc@bvcc.arcoxmail.com

==========

The following is from Cloudeight InfoAve Premium - Issue #203 - September 7, 2007

Sandi's Sister Has Online Ordering Scare - Was The Advice The Credit Card Company Gave Her Valid?

My sister had someone access her credit card and charge $5,000 on it. The credit card company called her before she even knew it and asked her if she had been in California and charged the $5000 worth of charges. Of course she said absolutely not, how had that happened, and how could it be avoided in the future. The lady at the credit card company told her during their discussion to always delete the cookies after she ordered online. Does that sound like it would work to you? I sort of thought that may be a good way to not have that happen if they are using the robots and junk to access people's computers? I would just like your input on this. I had someone use my debit card (which I had used to pay online) and send $500 by Western Union to Peter Jennings in New York City. I had to do some serious talking and filling out of paper, but I did get my $500 back. My sister wasn't charged for the $5000 because the credit card company was on top of it very quickly. I look forward to hearing from you. Sandi

Our Answer

One of the biggest bits of misinformation we see on the Web, everyday, is the belief that cookies contain all sorts of information that would be valuable to cyber thieves. This is just not true. There are no secure order pages of which we're aware that use cookies to store any personal information at all - certainly not social security numbers or credit card numbers. It is a shame that someone working at a bank or credit card company would misinform customers like the lady your reference in your question. It is not possible and it is not correct. While keeping your computer free of debris, junk files, temporary Internet files, cookies and the like is good maintenance, removing cookies isn't going to save you from identity theft.

Let's clear one thing up right now. Cookies are text files. They are not some arcane, dark threat, that can transmit data to some miscreant lurking in a dark dungeon somewhere. They are, for the most part, unreadable to anyone except the site that placed them on the computer. They are used, for the most part, to provide statistical information to a Web site (number of visitors, pages on the site that were visited, etc.). There are not used to store credit card numbers, passwords, user IDs or anything from which a cyber thief could glean information useful for stealing a person's identity. The purpose of cookies, in the vast majority of cases, is benign. And, yes, we know some anti-spyware sites make a big deal about "tracking cookies". As ominous as that misnomer sounds, all tracking cookies are used for is to track your clicks on advertisements on one site - or perhaps over a number of sites using the same advertising network. It might sound sneaky but it does prevent the surfer from viewing the same ad over and over - and even in the worst case scenario, even tracking cookies do not store any credit card numbers, personal names, addresses, or anything that could even be remotely considered useful to a cyber thief.

We don't have enough information here to determine exactly what happened to your sister, but we can offer an educated guess. Our guess is based on the very large number of people who have had their credit card information, social security numbers, financial account logins and other critical information stolen by deception. Actually the information isn't stolen at all, the victim is tricked, usually by a phishing email, into giving the cyber thief the information they need to make fraudulent charges on credit cards, or even steal a person's identity.

Your sister's scare had nothing to do with cookies, robots, or cyber thieves accessing her computer. She, like so many thousands of others, probably clicked on a link in an email that appeared to have come from her credit card company or her bank. And believe us, many intelligent people have been scammed and robbed via this method. The phishing email looks exactly like an email from a credit card company or a bank. It includes the bank or credit card logo - slogans - and anything else the bank or credit card company would include in an email. But no bank or credit card company we know of is ever going to send you an email asking you to click a link in that email and "verify" your information. Many of these phishing emails even tell users that the bank or credit card company is "upgrading their security policies" and need you to login as soon as possible and verify your details. And, if you don't, you won't be able to access your account until you do. We think your sister was fooled by a phishing email, clicked a link, gave her account number to a cyber thief, who then used the information to charge $5000.00 worth of goods to her credit card number.

As far as your $500.00 problem with your debit card, we would guess the same thing happened to you. Either someone tricked you into giving your online banking login information to them - or someone tricked you (most likely again through a phishing email) into giving them your debit card account number. The only other way we can see someone getting access to your debit card account is if someone was standing behind you at an ATM machine with a hidden camera and took a photo of your card and watched you punch in your PIN number. This might seem far fetched but it happens all the time. We've seen people stand in line at an ATM holding their credit card in their hand with the account number in plain site. You need to protect your credit card (or debit card) number at all times, on the Web, and in the real world.

Request that your name be removed from pre-approved credit card and junk mail lists and keep making the requests as they expire. Statistics show that this is one of the most common ways that thieves hijack identities. Not only will you be rid of the hassle of all that unwanted junk mail in your mail box, it will prevent thieves from getting the information they need to open an account in your good name and ruin your good name in just a few weeks. For more information on how to do this, visit www.govspot.com/ask/nameofflist.htm.

Common sense, using caution, getting your name off of junk mail, pre-approved credit card, and telemarketing lists, and MOST OF ALL: NOT clicking links in emails from financial institutions or credit card companies (or any site that has critical personal information about you like your social security number, driver's license numbers, store account numbers, passport information, etc) are the most important things you can do to prevent this sort of thing from happening to you again. And, please pass this along to your sister too.

When discarding personal papers, bills, credit card statements, or anything with anything from which personal information can be gleaned, make sure it's shredded, or torn into tiny pieces before throwing it in your trash. It's not that you can't trust your garbage man - it's just a prudent course of action. You just never know where those bills and statements might end up.

Summing up? A lot of mistakes people make that lead to identity theft are the result of a lapse in common sense or just not thinking before acting. Think, use caution, be skeptical, make sure you've got adequate security software installed, and above all, let good common sense be your guide. Chances are, if you do, you'll be safe.

==========

Mark your calendars now for the next meeting of the Bella Vista Computer Club which will be held on **Monday, October 15th at 7 p.m.** The presentation will be "Selling on eBay".

Having a problem with your computer? Having a problem doing something on the computer? Stop by one of the Open House Help Clinics we have at the John Ruehle Center and see if we can solve your problem. These clinics are from 10 a.m. to 1 p.m. on the first Saturday and the third Wednesday of the month. The clinics are open to the public so you can invite a friend or neighbor.

The Computer Club's membership year runs from September 1st to August 31st. See Mary Lou Zolli, Membership Chairperson, about renewing your membership.