

Identity THEFT

Keeping You Informed

Idahy
Federal Credit Union
1010 Rose Street • Boise, ID 83703
(208) 344-7948 • 800-877-5174
www.idahy.org



Identity Theft NEWSLETTER

Vol. 3, No. 1 Don't become the next victim...

Fast Fact...

Remove the hard drive before you trash your old computer. Anyone with a criminal mind and a bit of tech savvy can easily retrieve deleted files.



WARNING

VISHING: E-MAIL SCAMMERS TRY A NEW APPROACH

Criminals have taken identity theft scams to a new level. The newest scam is being referred to as vishing or voicemail fishing. **Vishing** mimics the more common *phishing* e-mail scam which traps unsuspecting victims into revealing their account numbers and other personal financial information to unauthorized persons.

As in phishing, vishing scams begin with an e-mail. Customers of a South California bank recently received e-mails telling them that their accounts with the company's online banking system had been disabled after the bank detected unauthorized access. They were told to dial a telephone number (with a local Southern California area code) where an automated voice prompted them to enter their account numbers, personal-access codes and other details. It's not clear who was on the other end of the phone line, but it wasn't the bank.

A tip to help you avoid the pitfalls of vishing.

- Ignore e-mail or phone calls asking for account details. If you receive a request like this, look up the business phone number or website yourself. Do not rely on the information provided in the e-mail or phone call.

A Victim's True Story

A Pennsylvania identity theft victim, Carol J., lives in the suburbs of Philadelphia. She outlined the following chronology of events that happened to her and her husband:

- 1) They received a letter from Sears thanking them for opening a Sears Credit Card Account.
- 2) When Carol called Sears to tell them she did not open a credit card account, they informed her that the account was opened with a driver's license and purchases included two 40" televisions and an iPod at the Scranton, PA (70 miles north of Philadelphia) location.
- 3) The Sears Fraud Protection Line advised Carol to call all three credit bureaus and ask them if there were any inquiries to open credit cards and if there were, then close the accounts.
- 4) Credits cards were opened at Best Buy, Circuit City and Walmart with all having purchases of high-end electronics for a total of \$13,000.
- 5) Police visited the house and took all the information and provided a police report.
- 6) Carol and her husband spent weeks cancelling and reopening all of their accounts and writing letters to the credit card companies.
- 7) The police followed up indicating that this was a day and a half buying spree and the thieves stopped all activity fearing detection. A security camera at one of the stores did capture a picture of a woman opening an account.

Since the fake driver's license used a maiden name as a middle name and Carol only signs her name that way on medical records, police suspect the information was taken from a doctor's office or hospital.

- 8) The police indicated that the chances of apprehending this identity thief were very slim.
- 9) Although all banking and credit card accounts were closed and changed, Carol and her husband still are afraid to go to their mailbox.

Be on the alert! Read your mail carefully!

The Federal Trade Commission, which is the national consumer protection agency, estimates as many as 10 million Americans have their identities stolen each year.

Why Does A Supermarket Need Your Social Security Number On Their Application For A Discount Club Card?

Don't Be Afraid To Ask The Following:

- Why do you need my Social Security number?
- How will my Social Security number be used?
- How do you protect my Social Security number from being stolen?
- What will happen if I do not give you my Social Security number?



Guard Against Identity Theft

• Never provide personal financial information, including your Social Security number, account numbers or passwords, over the phone or the Internet if you did not initiate the contact.

- Remove mail promptly from your mailbox. Never use your mailbox for outgoing mail. Identity thieves raid mailboxes for credit card offers and financial statements.
- Do not be intimidated by an e-mail or caller who suggests dire consequences if you do not immediately provide or verify financial information.
- Limit the number of I.D. and credit cards that you carry. If they are stolen, you'll have fewer to replace.
- Never click on the link provided in an e-mail you believe is fraudulent. It may contain a virus that can contaminate your computer.
- If you believe the contact is legitimate, go to the companies website by typing in the site address directly or using a page you have previously book marked, instead of a link provided in the e-mail.
- If your Social Security number is used as your driver's license number or appears on another I.D. card, ask the issuer for a new card with a different account number. If your Social Security number is printed on your checks, reorder checks without it. Also, if your driver's license number is printed on your checks, consider removing it.
- Shred all important documents before putting them in the trash.

Steps To Take If You Are An Identity Theft Victim...

STEP 1: Contact the fraud departments of each of the three major credit bureaus.

- Equifax 1-800-525-6285
- Experian 1-888-397-3742
- TransUnion 1-800-680-7289

Tell them that you're an identity theft victim. Request that a "fraud alert" be placed in your file, as well as a "victim's statement" asking that the creditors call you before opening any new accounts or changing your existing accounts. This can help prevent an identity thief from opening additional accounts in your name.

STEP 2: File a police report with your local police...

or the police in the area where the identity theft took place. Having a copy of the police report can help you when dealing with creditors.

STEP 3: Close any accounts that have been tampered with or opened fraudulently.

Credit accounts include all accounts with banks, credit unions, credit card companies and other lenders, and phone companies, utilities, Internet Service Providers (ISPs), and other service providers. Ask to speak with someone in the security or fraud department of each creditor and follow up with a letter. It's particularly important to notify credit card companies in writing because that's the consumer protection procedure the law spells out for resolving errors on credit card billing statements.

SCAM ALERT!

A Call To Jury Duty...

We all take summons for jury duty seriously, but enough people skip out on their civic duty that a new kind of scam has surfaced. Someone calls pretending to be a court official who strongly indicates a warrant has been issued for your arrest because you didn't show up for jury duty. The caller claims to be a jury official. If you state that you never received a summons for jury duty, the scammer asks you for your Social Security number and date of birth so they can verify the information and cancel the arrest warrant.

The FBI website states that the judicial system does not contact people by telephone to ask for personal information. The FBI warns people to be aware of this jury duty scam.

GUARD AGAINST IDENTITY THEFT BY CHECKING YOUR CREDIT ONCE A YEAR!

HOW TO GET YOUR FREE CREDIT REPORT

You can obtain a free credit report once a year from each of the credit reporting agencies – Experian, Equifax and Trans Union.

ONLINE AT
AnnualCreditReport.com

TOLL FREE AT
877.322.8228



Warning Signs of Identity Theft

- You receive credit cards for which you never applied.
- Bills arrive for goods or services you didn't request.
- Suspicious inquiries on your credit report.
- You stop getting bills and other mail. If this happens, a thief may have filed a change of address with the post office.
- You receive letters denying you credit, despite never having applied for any.



Fast Fact...

When choosing Personal Identification Numbers (PIN's) and passwords, avoid using easy-to-figure out codes, such as parts of your birth date, address, or phone numbers, and children's or pet's names, these are too obvious.

A better approach for an easy-to-remember password is to take the first letter from each word in an unfamiliar, but memorable phrase. You can use something like:

Initiative Without Success Is Insubordination or IWSII.