Spotlight

A Publication of Cedar Point Federal Credit Union

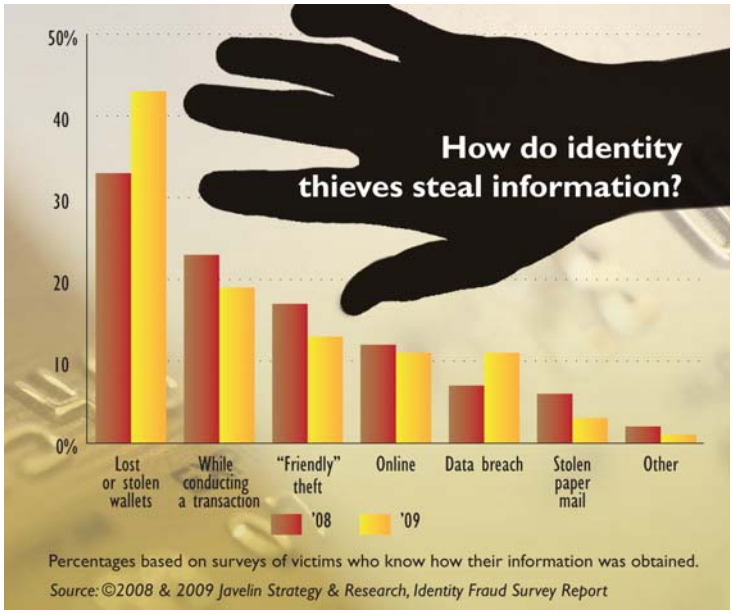
November 2009

November is Security Awareness Month

Identity Theft is a serious problem that can happen to anyone at anytime. Once you become a victim, everything you do can be affected, from a job interview to a new car or home. This newsletter is dedicated to help you protect yourself from the nightmare that Identity Theft can become.

Credit Report

Request a copy of your credit report every year or so. It tells you whether anyone has applied for credit in your name, and may reveal accounts being used without your knowledge, with the bill being sent to a different address.



Credit Cards

- Sign new cards immediately.
- Store them safely - They are money!
- Only carry the cards you will use.
- Don't write your PIN on your card.
- Shred documents that show your account number.
- Don't give your card number over the phone, unless you initiated the call.
- Remember to get your card and receipt after a purchase, and double check they are yours.
- Notify the credit card company immediately if your bill is incorrect, or your card is lost or stolen.
- Check your bill carefully, and notify the credit card company if you don't receive it on time.

Mail

- Don't write your credit card number or social security number on a postcard or the outside of an envelope.
- Collect your mail promptly.
- Have your mail held if you'll be out of town or on vacation.
- Use collection boxes or the post office for outgoing mail if your home mailbox is unattended.
- Opt-out of receiving pre-approved credit offers.

Internet

- Never e-mail your account number, credit card number, or social security number.
- Check carefully that you are on the page you intend, and not an impostor's page.
- Use only secure web pages for online ordering. To be sure the page is secure, check that the address of the page begins with http**s** or look for a padlock icon on the status bar of your browser or where you enter the information.
- Online credit applications which request a social security number should also be on secure web pages.
- Use anti-virus and personal firewall software, and keep it updated.

Cedar Point takes your safety and security very seriously. If you ever have any concerns, or would like more information, about the many ways we can help you to protect yourself, our Security Specialist, Aaron Chase, is available to assist you. Please contact Aaron at 301-863-7071 ext 252 or email him at achase@cpfcu.com.

Vishing: A New Way to Steal Your Money

What is Vishing?

Vishing: The word 'Vishing' is a combination of VoIP and Phishing, and marries an older form of communication (telephone) with modern technology (VoIP). Vishing uses the trusted telephone rather than a link in an email to obtain private, personal, and financial information.

How Does It Work?

While vishing attacks can originate as an email or a telephone call, the strategy of each is basically the same. The recipient is directed to call a phone number they believe is affiliated with their financial institution or a company with whom they do business.

In a vishing attack, the phone number dialed belongs to the perpetrator's VoIP phone, which is programmed to recognize key strokes or phone tones. Typically, the recipient will hear a message asking them to enter their account number via the phone keypad to verify their identity.

A perpetrator can easily glean valuable numeric information via the telephone. Numbers are easier than letters to transmit when responding to a vishing attack. As a result, victims are likely to divulge the following:

- Social Security numbers
- Account numbers
- Personal identification numbers (PINs)
- Credit card numbers, expiration dates, and CVN codes
- Birthdays

Due to wide use of these types of data entry methods by financial institutions, most people are comfortable doing this, and feel secure entering in the numbers.

Once the perpetrator has gained this information, it is easy for them to perform the following acts:

- Take control of victim's financial accounts
- Steal victim's identities
- Make applications for loans and credit cards
- Purchase expensive goods and services
- Transfer stocks, securities or other funds
- Receive government benefits
- Obtain personal travel documents
- Hide criminal activities, such as money laundering

Why Does It Work?

Vishing is successful and attractive to perpetrators because:

- The telephone is a trusted communication tool
- The public generally accepts and has adopted automated phone validation systems
- Specific population groups, such as the elderly, are more easily targeted due to their comfort level with the traditional telephone system
- Caller ID information is easily masked or misrepresented
- Automated calling is simple to accomplish
- The increased use of call centers, often located in foreign countries, promotes victims' acceptance of strangers requesting confidential information
- VoIP makes it very inexpensive to make and receive calls
- VoIP provides the ability to route phone traffic internationally using proxies to hide the source of the attacks

Vishing Concerns

You should also be skeptical of anyone contacting you and attempting to gain your private banking or personal information. If you receive an email directing you to call a specified telephone number, disregard it and contact the financial institution directly with a number you know is valid, such as the one from your account statement or telephone book.

What To Do If You Are A Victim Of Vishing

If you think you are a victim of vishing, contact the financial institution immediately and notify them of the issue. You can also contact the Internet Crime Complaint Center (IC3) immediately at www.ic3.gov/complaint.* The IC3 serves as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime.

The bottom line is that you should always verify the source before divulging any personal information. Once you give something to a con artist, it is gone, and there is no way to get it back completely.

*Cedar Point is not responsible for the content or update of this alternate site. The privacy and security policies may differ from those practiced by Cedar Point.

These helpful tips are provided by Digital Defense, Inc., a computer security company working with Cedar Point to help insure the privacy and security of your financial information.

For more educational materials from Digital Defense, Inc. go to www.cpfcu.com and click on the Digital Defense link.

DIGITAL DEFENSE INCORPORATED

For Your Information

As of August 31, 2009

Loans	$157,181,899
Assets	$298,478,245
Shares	$261,859,877
Members	29,282