Security Alerts

Identity Theft

Identity theft is one of the fastest growing crimes in the world. It is surprising what someone can do with a social security number or birth date. These criminals can open credit cards, make large purchases and even apply for jobs using the information of an unsuspecting consumer. The majority of the time, these crimes go undetected for a period of time and the individual doesn't realize their identity has been stolen until hundreds (and sometimes thousands) of dollars have been spent in their name.

At Nascoga FCU, we want to help you protect your personal information and that's why we're providing you with valuable information, tips and instructions on how to prevent or recover from identity theft.

Preventing Identity Theft

1. Do not give personal information, such as account numbers or social security numbers, over the telephone, through the mail, or over the Internet, unless you initiated the contact and you know who you are dealing with. Beware of phone scams. Never give your PIN or any other personal financial information to an unknown caller.

2. Do not disclose credit card or other financial account numbers on a website unless the site offers secure transactions. Look for the "padlock" icon on your browser's status bar before submitting financial information through a Web site. A simple test to make sure you are on a secure Web server is to check the beginning of the Web address in your browser's address bar. It should read https://, rather than just http://.

3. Protect your PIN and other passwords. Avoid using your mother's maiden name, your birth date, or the last four digits of your social security number as a password. These are too easily obtained.

4. Closely guard your ATM/debit card, checks and credit cards. Report all lost or stolen cards or checks immediately.

5. Shred all unwanted materials containing sensitive personal information such as credit union statements and credit card bills.

6. Sign up for E-Statements instead of receiving paper statements by mail. Check all statements carefully to ensure you have authorized all charges. With Nascoga FCU’s Home Banking, you can check your activity anytime, day or night, instead of waiting until reconciling your account at month-end.

7. Take all credit card receipts with you. Never leave them in restaurants or other public places. Also, don't dispose of them in a public trash container. Take them home and shred them.

8. Carry only essential credit cards and identification. Never carry your Social Security card or birth certificate. Store these items in a secure place, only removing them when needed and returning them promptly.

9. Place your outgoing mail into a secure official postal service collection box. Raising your mailbox flag to notify the carrier that you have outgoing mail, notifies everyone else as well.

10. Collect your mail every day. Don't leave mail in your box overnight. Credit card applications mailed to you with your personal information already filled in can easily be used by thieves to open accounts in your name.

11. The best way to monitor your account for Identity Theft is to obtain a copy of your credit report at least once a year. The Federal Fair Credit Reporting Act, enacted June 1, 2005, requires each of the nationwide consumer reporting companies to provide consumers with a free copy of their credit reports *once every 12 months*.

The three nationwide consumer-reporting companies have set up one central website and toll-free number through which you can order a free annual credit report. To order, call 877-322-8228 or visit the www.annualcreditreport.com website.

How to Detect Online Fraud

Here are some common characteristics of fraudulent e-mails and websites:

1. They often have a sense of urgency, telling clients that if they fail to update, verify or confirm their personal or account information, access to their accounts will be suspended.
2. They typically ask for personal or account information such as:
    - Account numbers
    - Credit and check card numbers
    - Social Security Numbers
    - Internet Banking sign on IDs and passwords
    - Mother's maiden name
    - Date of birth
    - Other sensitive information
3. They often include links that contain the names or web addresses of legitimate companies.
4. The fraudulent e-mails will disguise or forge the sender's email address so they appear to be from a legitimate company.
5. The e-mails and pop-up websites may include misspelled words and incorrect grammar.

How To Protect Yourself From Online Fraud

1. Never provide personal or financial information to someone who sends unsolicited e-mail or calls you on the phone, or on pop-up website requests.
2. Type web addresses into browsers instead of clicking on links in e-mails.
3. Change passwords and personal identification numbers (PINs) every 30 to 60 days.
4. Keep anti-virus and anti-spam filtering software on your computers, and keep it up to date.
5. Monitor accounts and credit reports. The three major credit bureaus are:
    - Equifax 1-800-525-6285
    - Experian 1-888-397-3742
    - TransUnion 1-800-680-7289

To learn more about email scams and what you can do to protect yourself online, go to the Federal Trade Commission website.

Protect Yourself from Phishing Attacks

Phishing is a method where account numbers, personal identification numbers, usernames, and passwords are collected from users and then used to compromise their online accounts and commit identity fraud.

Phishing attacks typically move from location to location and are online for fewer than three days at a time. Recently, US credit unions, banks, and other financial institutions have had their identities hijacked by sophisticated phishers.

Phishing emails come in different forms, and all are sent in attempt to give scammers access to your confidential information. Some phishing emails request you to send personal information back to the sender in an email. Many even include a link requesting you to enter personal information on an authentic-looking website posing as a financial institution.

Phishing emails appear authentic. Attackers copy official logos, send emails with well-crafted subject lines such as "Urgent security notification", and can provide disguised links appearing identical to a legitimate website's address.

We will NEVER contact you via e-mail to request or verify security information. If you receive a phishing email that has illegally used our name, logo, or website, please forward it to us immediately.