NIH Federal Credit Union

Understanding and Preventing ID Theft

Table of Contents

Common Practices

How Your Information Is Obtained

Thieves use a variety of illegal techniques to obtain identity information. They may:

- Take mail from a mailbox
- Divert mail to another location by filling out a change of address form with the post office
- Go through trash to find identification and financial documents
- Access credit reports by posing as landlords or employers
- Hack into personal computers
- Pose as legitimate companies or government agencies to request personal information via email (called phishing) or text message (called smishing)
- Steal hard copy or electronic files from your workplace
- Stand close to you at the ATM to learn your Personal Identification Number
- Work at restaurants, gas stations, or other businesses to steal money or information from credit/ATM/debit cards (called skimming)

How Your Information May Be Used

Once identity thieves have your personal information, they may use it to:

- Charge on existing credit cards
- Open new credit accounts in your name
- Takeover your existing accounts
- Open new checking accounts in your name and write bad checks
- Establish phone or wireless service in your name
- Use your debit cards or counterfeit checks to drain your checking account
- Take out loans to buy cars and other big ticket items

Preventing ID Theft and Fraud

NIHFCU Accounts

Setup Account Alerts to stay updated on your NIHFCU account activity.

- Receive account alerts by email or text message when specific activity occurs
- Customize your alerts to notify you of specific transactions, cleared checks and account balances
- Online Banking users can get started by logging into their account and then selecting "Email and Text Alerts" under the 'Other Services' tab
- Add a password or phrase to your account to be used when you call in about your account (DIFFERENT TOPIC)

Get our free Mobile App

- Download our free Mobile App today to check your balances and transactions on the go. Our Mobile App is available for iPhone, Android Phone, iPad, Android tablet and Kindle devices.
- To download our Mobile App or learn more about mobile and text banking, click here.

Credit Cards and Debit/ ATM

Here are some quick tips for plastic card safety:

- Carry only those cards you really need
- Keep your card secure at all times
- Shred all statements and pre-approved credit card offers with a crosscut shredder
- Opt-out of receiving pre-approved credit offers from lenders you do not trust
- Cancel unused credit card accounts
- Be aware of people behind you at the ATM or anywhere else you use your card
- When you give your credit or debit card to someone for a transaction, watch them swipe it and inspect the receipt for accuracy
- Know your billing cycles and contact creditor if bills don’t arrive on time
- Examine the charges on your credit card statements every month

Computer

Here are some quick tips for computer safety:

- Update virus protection software periodically, and after every new virus alert is announced
- Do not download files or open hyperlinks sent from people you don’t know
- Use a firewall program to prevent your computer from being accessible to hackers
- Use a secure browser to guard the security of your online transactions

- Enter personal and financial information only when there is a “lock” icon on the browser’s status bar and look for the URL to read “https” versus “http”
- If you must store personal and financial information on your laptop:
    a. Use a strong password
    b. Don’t use an automatic log-in feature
    c. Always log off when you’re finished
- Before disposing of a computer, delete personal information using a “wipe” utility program to overwrite the entire hard drive.

Checking Accounts

Here are some quick tips for checking account safety:

- Know where your checkbook is at all times
- Print firmly and use indelible ink when writing paper checks
- Review your account often via online banking for any possible fraudulent activity
- Check your account statement for fraudulent activity
- Do not give out your checking account number unless you know the company requesting the information and understand why the information is necessary

Personally Identifiable Information

Here are some quick tips for personal identifying information account safety:

- Keep all identification and financial documents in a safe and private place
- Provide personal information only when:
    a. You know how it will be used
    b. You are certain it won’t be shared
    c. You initiated contact and know who you’re dealing with
- Request a vacation hold if you can’t pick up your mail
- Deposit outgoing mail in post office collection boxes or at your local post office
- Remove mail from your mailbox promptly
- Keep your purse or wallet in a safe place at work
- Memorize your Social Security number rather than carrying your Social Security card
- Do not have your Social Security number or driver’s license number printed on your checks
- Review your Social Security annual statement for accuracy
- Provide your Social Security number only when necessary and to those you absolutely trust
- Before revealing your Social Security number, ask:
    a. Why your number is needed
    b. How your number will be used
    c. What happens if you refuse

ID Theft Recovery Guide

If you are a victim of identity theft, minimizing damage will take patience and a systematic approach. However, the sooner and more aggressively you deal with the problem, the faster you will see results.

To start, commit yourself to becoming and remaining organized. Since you will be communicating with a lot of people and have many tasks to complete, keep copies of all forms, file paperwork promptly, and store everything in a safe and accessible place**.**

NIHFCU Account or Card Fraud

- To report suspected fraud on your NIHFCU accounts, call 800.877.6440 or stop by any branch.
- To report fraudulent activity on an NIHFCU credit card, call 800.558.3424.
- To report fraudulent activity on an NIHFCU debit or ATM card, call 800.877.6440 or stop by any branch and complete the Affidavit of Fraudulent Use of a Debit or ATM Card (PDF).
- To change your PIN at any time, call our automated hotline at 866.985.2273.

Creditors and Financial Institutions

- If accounts have been used or opened illegally, contact your creditors immediately. Ask for fraudulent transaction documentation. You may use a uniform affidavit form, available on the Federal Trade Commission's website as you may need it to file a police report. Add "non-guessable" passwords to replacement cards and all existing accounts.
- If a collection agency attempts to collect on a fraudulent account, explain (in writing) that you are a victim of identity theft and not responsible for the debt. Ask that they confirm in writing that you do not owe the balance and that the account has been closed.
- For checking account fraud, contact your financial institution to place stop payments on any outstanding checks that you did not write.
- Report the crime to check reporting agencies. Close current checking and savings accounts and obtain new account numbers and passwords. Monitor all future account statements carefully for evidence of new fraud.

Local and Government Agencies

- Report the crime and file a police report. Request a copy of the report and keep the phone number of your investigator handy. For additional documentation, you may also report the crime to the Federal Trade Commission.
- Notify the U.S. Postal Inspection Service if someone has used your address or in other ways committed fraud through the mail.

Credit Reporting Bureaus

- It is very important that your credit report lists only factual information. To know what is being reported, you will need to obtain a credit report from each of the three major credit bureaus. If you are married, your spouse should also check his or her report.
- You can request a free copy of your credit report from each of the major credit bureaus (Equifax, Experian, TransUnion) once a year. Visit annualcreditreport.com.
- Even if the fraudulent information hasn't yet appeared on your reports, be proactive and report the crime now. Call any one of the three credit bureaus to place a fraud alert on your credit report. The company you contact will notify the other two, who will then place alerts on their reports as well.
    - If you have proof that identity theft has occurred and you have filed a police report, you may request that the fraud alert be placed for seven years instead of the initial time frame of 90 – 180 days. While fraud alerts are in effect, no new credit should be granted without your explicit approval.
- You may also write a victim's report – a brief statement describing the details of the crime – and send it to all three bureaus to be added to your reports.
- The first reports with the fraud alert are free and will be sent to you automatically. Check your credit report for accuracy every three months for a year, then at least annually after that.

Credit Monitoring and Protections

If you are especially concerned about the possibility of identity theft, you may consider paying for added protection of monitoring service – but do so only after carefully reading the fine print and weighing the risks against the benefits. Some of these businesses are scams themselves. Research the company's history and check the Better Business Bureau's complaint log before signing an agreement.

Credit Monitoring

- Each of the three major credit bureaus offers a fee-based credit monitoring service. They typically provide regular credit report updates about fraudulent activity, new inquiries, new accounts, late payments, and sudden changes in your credit card balances. These plans often include a specific number of credit reports being mailed to you automatically or at your request, and access to individualized customer services.

Credit Protection

- Credit protection is offered by private companies and some financial institutions, and the price and service varies considerably. Most will reimburse victims of identity theft for out-of-pocket expenses (up to a certain dollar amount) and help you through the process of contacting creditors, writing affidavits, and filing reports.

Credit/Security Freeze

Placing a credit freeze on your credit report helps block fraudsters from opening new accounts in your name by restricting access to your credit files. You will need to contact each credit bureau and fees may apply.

- Equifax - https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
- Experian - https://www.experian.com/freeze/center.html
- Transunion - http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page

Password Safety Tips

Create Strong Passwords

The first rule of thumb is to use a different password for each of your accounts. It may be easier to keep track of just one password, but if a crook discovers that one password, he or she can access all of your accounts. This tip has been well publicized, but the Accenture consultancy's survey of 800 U.S. and U.K. consumers revealed that 88% use just one, universal password.

The second key to a robust password is to make it lengthy. According to a Microsoft spokesperson, each character you add to your password increases the protection it affords many times over. At a minimum, your passwords should be eight digits long, and 14 digits or more is ideal.

A compromised password could lead to identity theft or other dire consequences.

Using the greatest variety of characters possible in your passwords—letters, numbers, symbols—makes them harder to guess or uncover with malicious software. Microsoft's spokesperson says the fewer types of characters you use, the longer your password needs to be—if you use only letters and numbers make it 15 characters long.

Consider using words and phrases you can remember, but that others wouldn't guess. You can use the first letter of each word in a sentence, plus some numbers, mix upper- and lowercase, and include some misspellings and symbols. Here's one example: "I went to Hawaii in August 2009 with Bob," becomes "iWThI082009wB." Include a few symbols and it's "!WT*h;I082009w%B:." (The exclamation point substitutes for "I" and the randomly selected symbols bracket "Hawaii" and "Bob.") Who would ever guess that one? You can also substitute numbers for letters: "hate" becomes "h8."

After creating your password, you can test its strength with one of the "password checkers" available online such as Microsoft's Password checker and The Password Meter. If your password tests as weak, make it more complex.

Some password don'ts include:

- Using personal information such as family names, birthdays, or your address
- Using sequences or repeated numbers, like abcd, 1234, or 9999
- Using any words listed in a dictionary—they're easy for scammers to guess.

Keep passwords secret

Of course, the strongest password is useless if you share it with others, so guard yours closely. Don't reveal your passwords to family or friends. Children, particularly, may unwittingly pass them on to others, Microsoft's spokesperson reminds.

You shouldn't type passwords into public computers, such as those at libraries or in hotel lobbies. Even if you instruct the computer not to save the password, there could be malicious software on the computer that records your keystrokes for a criminal's use.

Also, you shouldn't send passwords via e-mail—it isn't a secure delivery channel—and you shouldn't enter a password if requested to do so via an e-mail.

If you see suspicious activity, notify the authorities and contact your credit union for help.

Don't store a list of your passwords on your computer—that would be a goldmine to a crook. Microsoft's spokesperson says it's safer to record your passwords on paper, and then hide the paper where others won't find it. Make sure it's a location you'll remember, though. What about between the pages of a book on your shelf? Another idea is to store the word file on a thumb drive and hide the thumb drive, says Ian Forkash, an information technology manager for the Credit Union National Association in Madison, Wis.

If you add encryption software to your computer, which codes information for privacy, you can store passwords there. Some versions of the software are available at no charge, such as a limited version of RoboForm for Windows. There's a fee for more comprehensive programs, such as Symantec's Endpoint Security.

Change your passwords frequently. While a very strong password can be good for several years, a weak one is only good for about seven days, Microsoft's spokesperson says.

Keep track of passwords

So, how do you remember your many passwords? Your secret list is one way, of course. And using a familiar phrase when creating the passwords, as described above, is another.

Consumer Reports suggests developing a couple of basic passwords you can memorize, and then adding different prefixes or suffixes to them for different accounts or Web sites, or scattering different symbols throughout.

Then, on your password list, you can write down just the add-ons and where they appear in the password. For example, if you add an asterisk as the second character in the password for one account, on your list you can just write: 2*.

Don't store a list of your passwords on your computer—that would be a goldmine to a crook.

Vince, who lives in Louisiana, uses a consistent approach to make his passwords memorable. "I use a combination of the Web site's name, along with recognizable information," he says. "For Yahoo, my password could be the first three letters of Yahoo, the first three letters of my pet's name, and the number of my birth month. So, my password for Yahoo might be: yahspo04. This way my password is always different, but still is easy enough to remember." Vince was one of several Home & Family Finance Resource Center's What's Your Story respondents.

Stephanie, from West Virginia, has another approach. "I have a good memory for numbers and things such as passwords, so I can typically remember many of them. But when I first change my password, I enter it in my rolodex as a code," she recounts. "Say my user name is 'username,' I would put down 'un.' If my password is 'password1,' I would put down 'pw1.' If I enter a year behind a password like 'password2009,' I would write down 'pw yr full.' Full means I've used a four-digit number instead of two." (Of course, Stephanie would want to use a combination of various characters rather than words that appear in dictionaries.)

When it comes to password storage, Catherine, from California, has a creative method. She uses a set of small index cards, hole-punched at the corner and attached to a metal ring made for organizing papers. "Every time I sign up on a new Web site I write its name on a card, along with the user name and password and other relevant information," she says.

She stores the cards in a safe place that she can remember. "The cards are small enough to drop in my bag, and easy enough to hide from prying eyes," she says. "It works very well for me."

Paul, from New Mexico, stores his online. "I use the Secure Login add-on available for the Firefox Web browser," he explains. "It uses one master password to give you automatic access to an encrypted database containing all your individual passwords."

Take action if someone gets your password

If, despite your best efforts, your password is compromised—possibly through a security breach at a business—don't panic. Monitor all the information you protect with that password, such as online shopping accounts or investment accounts, and request free copies of your credit reports from the national credit bureaus.

Using a variety of characters in passwords—letters, numbers, symbols—makes them harder to guess or uncover with software.

If you see suspicious activity in any of these places, notify the authorities and contact your credit union for help. If you're a victim of identity theft, the Federal Trade Commission's Web site includes information about what steps to take. But remember, the stronger your passwords, the less likely this is to happen.

Additional Resources

Credit Reporting Bureaus/Accessing Credit Reports

Equifax
To order a credit report call: 800.685.1111
To report fraud call: 888.766.0008
Equifax Credit Information Services, Inc.
P.O. Box 740241, Atlanta, GA 30074
www.equifax.com

Experian
To order a credit report and report fraud, call: 888.397.3742
Experian, P.O. Box 2104, Allen, TX 75013-2104

TransUnion
To order credit report call: 800.888.4213
To report fraud call: 800.680.7289
TransUnion, 2 Baldwin Pl, P.O. Box 2000, Chester, PA 19022
www.transunion.com

Annual Credit Report Request Service
To order a credit report call: 877.322.8228
Annual Credit Report Request Service,
P.O. Box 105281, Atlanta, GA 30348-5281
www.annualcreditreport.com

In addition to reporting checking account fraud to your financial institution, you can report it to these agencies that monitor checking account transactions:

ChexSystems
800.428.9623
Chex Systems, Inc., Attn: Consumer Relations,
7805 Hudson Rd Ste 100, Woodbury, MN 55125
www.consumerdebit.com

TeleCheck
800.710.9898
TeleCheck Services, Inc., Attn: Forgery Department,

P.O. Box 4451, Houston, TX 77210
www.telecheck.com

Government Agencies

U.S. Federal Trade Commission (FTC)

The FTC oversees the operation of credit bureaus and maintains a database of identity theft cases used by law enforcement agencies for investigations.
Consumer Response Center: (877) ID-THEFT, or online at www.ftc.gov
ID Theft hotline: 877.438.4338, or online at www.ftc.gov/idtheft
FTC Identity Theft Affidavit Instructions and Form:
https://www.identitytheft.gov/

U.S. Postal Inspection Service

Call the U.S. Post Office to obtain the phone number of the nearest postal inspector:
877.876.2455
Criminal Investigations Service Center, Attn: Mail Fraud, 222 S Riverside Plaza Ste 1250, Chicago, IL 60606
usps.com/postalinspectors

More

Balance Financial Fitness

Click here for a wide range of identity theft educational material for NIHFCU members downloadable booklets, articles, podcasts, and more.

To opt out of receiving pre-approved credit offers:
888.567.8688
www.optoutprescreen.com

To get information from the FTC on recent scams and to sign up for scam alerts from the FTC:
www.consumer.ftc.gov/scam-alerts?utm_source=takeaction