



Protecting Your Identity and Accounts

For more information:

Federal Trade
Commission
consumer.gov/idtheft

Privacy Rights
Clearinghouse
privacyrights.org/identity.htm

Navy Federal contact
information:

Member &
Account Services

Toll-free in the U.S.
1-888-842-NFCU
(6328)

Toll-free Internationally
800-0-842-NFCU (6328)

Collect Internationally
1-703-255-8837

At Navy Federal, we are committed to ensuring that your account information via the Internet is safe. We take all possible steps to establish a secure, encrypted connection after you enter your Account Access sign-on information. It is important that you help protect your PC and account information, too.

In addition to having the opportunity to select your own password for Account Access, you can self-select the PIN you use with your Navy Federal Visa® Check Card. To self-select your check card PIN, visit www.navyfcu.org and sign on to Account Access, click on the "Other Services" tab, then click on "Change Your Debit Card PIN" under "Checking, Share Savings & NAVchek® Services." You can also select it at a branch or by calling 1-888-842-NFCU (6328).

NOTE: When you change your PIN online or by phone, your current check card and PIN will be deactivated for 14 business days from the date of request. A new card will be sent via U.S. mail to your address of record in 7 to 10 business days. When you change your PIN at a branch, you'll receive a new card and PIN immediately.

Be assured that Navy Federal accesses your personal information only when necessary to service and maintain your accounts. We do not share any of it with third parties except as allowed or required by law and as necessary to provide you with services—such as processing check reorders.

Precautions You Can Take

When someone pretends to be you, it's called Identity Theft. By getting possession of your name, Social Security Number (SSN) or some other key piece of personal information about you, in a matter of hours they can:

- take over your existing accounts
- open a new account and take out loans
- get credit cards, driver's licenses and passports in your name

They can even change your mailing address, diverting your bank and credit card statements to another address.

Here are steps to take to help prevent this from happening:

- Review your financial statements for correctness as soon as you receive them—**or better yet**, elect to receive them online and turn off the paper mailed to you.
- Enroll your credit cards in a password protection program, such as Navy Federal's free CardGuard® Program. Should your card become lost or stolen, no one can use it to shop online without your personally selected password.
- Don't give out your SSN or credit card numbers to anyone over the phone unless you know the caller or are sure the organization is legitimate.
- Limit the number of ID and credit cards you carry.
- Use only your initials and last name on your printed checks, but sign your checks with your full name. Don't have your SSN printed on your checks or use it for your driver's license number.
- Destroy copies of financial statements, ATM receipts, etc. before discarding them.
- If you suddenly stop receiving mail or certain statements and bills without your request, contact your local post office.
- If you haven't received the new credit card you applied for or your renewed card by the "Good Thru" date on your existing card that has expired, notify the issuer.
- Don't leave incoming mail in an unlocked mailbox overnight or on weekends.
- Deposit outgoing mail in U.S. Postal Service collection boxes only.
- Review a copy of your credit bureau report at least once a year. You're entitled to one free report from each of the three major bureaus every 12 months. To receive a free credit report, visit www.annualcreditreport.com, call 1-877-322-8228 or write: Annual Credit Report Request Service, PO Box 105281, Atlanta, GA 30348-5281.

Protecting Your Accounts and Identity

- Sign up for Equifax's credit monitoring service to be automatically alerted to a change in your credit report—a potential sign that someone is tampering with your identity and accounts. This service is offered to Navy Federal members at discounted rates. Visit www.navyfcu.org or call Equifax at 1-800-437-5015.
- If you are active duty personnel away from your usual duty station, place an "active duty alert" on your credit file to minimize the risk of identity theft while deployed. You can place and remove the alert by contacting Equifax at www.equifax.com or calling 1-800-525-6285. Equifax will contact the other two credit bureaus for you.
- Don't give your PINs or passwords to anyone.

Protecting Yourself in Cyber Space

The following tips can help protect your personal information when you go online:

- Use "strong" passwords. The more numbers or characters the better. Each one increases your protection. Random characters—including upper and lower case letters—can help. Mix letters, numbers and symbols. Do not choose a password that can be easily guessed by others, such as your street number or address, phone number or date of birth.
- Protect your personal information. It's valuable. Be choosy and limit the amount of personal information you give to a site. Be sure to treat your SSN with care and read the site's privacy statement.
- Know who you are dealing with online. When shopping online, if you're not familiar with the company, check to see if they have a physical address, not just a PO Box.
- Protect your credit card when shopping online. When you get to the screen where you enter your credit card number, make sure there is an "s" (stands for "secure") in the beginning of the Web address. For example, <https>. Also check to see if there is a tiny locked padlock in the bottom right of the screen.

- Use online account access and payment services. Sign up for Navy Federal's Account Access and Web Bill Pay.
- Use anti-virus software, a firewall and spyware detection software to help keep your computer safe and secure. Update your software often. Back up important files to a disk to protect them from viruses.
- Take steps to keep your kids safe online. Set family rules. Decide where your children can and can't go on the Internet.

Remind them not to talk to strangers.

Scams to Avoid

"Phishing" is the online scam that hopes you'll bite and give out personal information that can be used to steal your identity.

Here's how you protect yourself from "phishing":

- If an e-mail looks at all suspicious to you, don't click on links or provide any information.
- Don't trust a link from an e-mail just because it takes you to a site that looks legitimate. Scammers can copy those easily.
- Verify with the company that the e-mail is really from them before submitting any personal information online or by phone.
- Try not to fill out forms in e-mail messages. You can never be sure where the information is going or who sees it along the way.
- E-mail headers can be forged. Be suspicious until you know for sure.
- If you click on a link from an unsolicited e-mail, make sure there's an "s" after the <http> in the address and a lock at the bottom of the page, signifying a secure site that is encrypted. This is no guarantee, however, that the site is legitimate.

When Navy Federal Contacts You by E-mail

Navy Federal will never send you an e-mail asking you to verify personal information, either by calling or clicking on an e-mail link.



Protecting Your Accounts and Identity

We may contact you by e-mail if you have made an application with us and we need information from you or want to provide you with the status of your application.

We may send you an e-mail you have signed up to receive about a Navy Federal product or service. In these instances, this may simply be to provide you with more information about the product or service.

If you believe that you have received a “phishing” e-mail, rather than a legitimate e-mail from Navy Federal, send it to:

phishalert@navyfederal.org
along with the name of your Internet Service Provider (ISP)

Note: This phish alert e-mail address is only to be used to provide copies of suspected phishing e-mails for credit union review—these e-mails are not intended for issues that need a response. Navy Federal will not respond to e-mails sent to the phish alert address.

If You Become a Victim

If you believe your identity has been stolen, contact one of the credit bureaus—they will contact the other two—and report the incident. Have them place a fraud alert on your credit file.

Credit Bureaus

Equifax

PO Box 740241
Atlanta, GA 30371-0241
1-800-525-6285

Experian

PO Box 919
Allen, TX 75013-0919
1-888-397-3742

TransUnion

PO Box 390
Springfield, PA 19064-0390
1-877-322-8228

After you’ve reported to the credit bureaus:

1. Contact Navy Federal and your other financial institutions to get new account numbers and PINs, and have a code word placed on your accounts.
2. File a report with your local law enforcement agency and get a report number for your future reference.
3. Contact the Federal Trade Commission to report the situation at **1-877-ID-THEFT** (1-877-438-4338) or **www.consumer.gov/idtheft**.
4. Report the fraudulent use of your SSN to the Social Security Administration at **1-800-269-0271**.