

National Credit Union Administration

Tips to
Safely
Conduct
Financial
Transactions
Over the
Internet



Introduction

As use of the Internet continues to expand, more credit unions are using it to offer products and services or otherwise enhance communications with members.

The Internet offers the potential for safe, convenient new ways to shop for financial services and conduct credit union business, any day, any time. However, members need to make good on-line choices—decisions that may help avoid costly surprises or scams.

This brochure offers information and tips to help you if you are thinking about, or are already, using the Internet to conduct on-line financial transactions. It will tell you how to:

- Confirm that an on-line credit union is legitimate and that your share deposit is insured;
- Keep your personal information private and secure;
- Learn where to go for more assistance; and
- Locate helpful on-line resources.

So, before you click there, read here.



Credit Union Web Site Legitimacy & Share Deposit Insurance

When performing transactions on the credit union's Web site, it's wise to make sure that it is legitimate and that your deposits are federally insured. Here are some tips specifically designed for members to consider when performing credit union transactions over the Internet.

Read key information about the credit union posted on its Web site.

Most credit union Web sites have an "About Us" section or something similar. You may find a brief credit union history, its name and address, and information about its insurance coverage from NCUA.

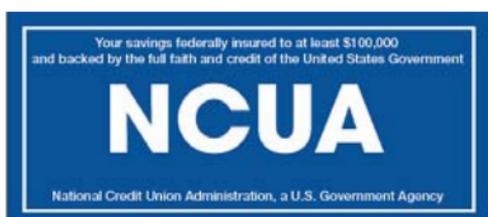
Protect yourself from fraudulent Web sites.

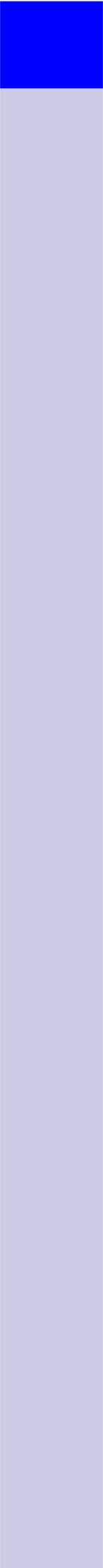
For example, watch out for copycat Web sites that deliberately use a name or Web address very similar to, but not the same as, that of a real credit union. The intent is to lure you into clicking onto their Web site and give your personal information, such as your account number and password. Always check to see if you have typed the correct Web site address before conducting any business.

Check the credit union's insurance status and Web site address.

To check a credit union's insurance status, look for the familiar NCUA logo or the words "Insured by NCUA" on the Web site.

To independently verify a credit union's





insurance status or Web site address, you can check NCUA's on-line database of credit unions. Go to NCUA's home page at <http://www.ncua.gov> and select "Credit Union Data" then "Find a Credit Union". From there enter the first letters of the credit union's name or the city and state and click the "Find" button. A positive match will display the credit union's information, including Web site address ("URL"), on the screen. The credit union type code also appears. This code indicates whether NCUA insures the accounts at the credit union. There are three different credit union types:

- 1 - Federal credit union (NCUA insured)
- 2 - Federally-insured State credit union (NCUA insured)
- 3 - Non-federally insured State credit union (not NCUA insured)

Please remember that not all credit unions operating on the Internet are insured by NCUA. Only federal credit unions and federally-insured state-chartered credit unions are insured by NCUA. Check with your credit union or NCUA if you are not sure of your credit union's insurance status.

Know where to get more information about NCUA insurance.

If you or your family have less than \$100,000 in all your accounts at the same NCUA-insured credit union, the entire amount is insured. If your accounts total \$100,000 or more, find out if your total shares are within the insurance limit. The NCUA brochure "Your Insured Funds" can help you determine the insurable amount. You can obtain the brochure from your credit union, the appropriate NCUA Regional Office, or view it via a link in NCUA's Web site at http://www.ncua.gov/Publications/brochures/insured_funds/funds.pdf.

You may also determine your share insurance coverage by using NCUA's Share Insurance Estimator available via NCUA's web site at <http://webapps.ncua.gov/ins/>.

Realize that not all financial services offered via a credit union's Web site are necessarily insured.

It is important to note that only **shares** offered by NCUA-insured credit unions are protected by NCUA. Non-insured investment and insurance products, such as mutual funds, stocks, annuities, and life insurance policies that may be sold through Web sites or at the credit union itself, are **not** NCUA insured, are not guaranteed by the credit union, and may lose value.

Remember that non-financial Web sites that are linked to your credit union's site are not NCUA-insured.

As an added convenience to their members, some credit unions offer on-line links to other sites. An outside company's products and services are not insured by NCUA, and your credit union may not guarantee the products and services.

As in everyday business, before you order a product or service on-line, make sure you are comfortable with the reputation of the company making the offer. Only then should you give out your credit card or debit card number. Never give the number unless you initiated the transaction.





Protect Your Privacy

Some consumers may want to know how their personal information is used by their credit union and whether it is shared with credit union affiliates or other parties.

Since July 2001, credit unions are required to give members a copy of their privacy notice, regardless of whether you are conducting business on-line or off-line. This notice outlines the credit union's information sharing practices. Credit unions may want to share information about you to help market products to your specific needs and interests. If you do not wish to participate in information sharing, you have the right to prevent your credit union from sharing your private personal information with non-affiliated parties, except in certain limited circumstances. As of July 2001, your credit union should provide a clear method for you to "opt out" of this type of information sharing. Some credit unions post a copy of their privacy notice on their Web site.

Some organizations track your Web browsing habits while at their site, to understand your interests and then to market particular services or promotions. You may want to ask whether your credit union tracks your browsing habits if these practices concern you. Some credit union Web sites post an Internet privacy statement on their Web site describing such practices. By reviewing these practices, you can learn what information the credit union collects, and what information, if any, it shares with other organizations.

Your Web browser may enable you to block the ability of outside companies to track your browsing habits. Your credit union and your Internet service provider may have more information about how

to protect your privacy on-line.

Keep Your Transactions Secure

The Internet is a public network. Therefore, it is important to learn how to safeguard your credit union account information, credit card numbers, Social Security Number, and other personal data.

Look at your credit union's Web site for information about its security practices, or contact your credit union directly.

Also learn about and take advantage of security features. Some examples are:

- ***Encryption*** is the process of scrambling private information to prevent unauthorized access. To show that your transmission is encrypted, some browsers display a small icon, usually in the lower right hand corner of your screen, that looks like a "lock" or a "key" whenever you conduct secure transactions on-line. In addition, if you are in a secured session your browser's URL should start with https\\ (the "s" indicates a secured or encrypted status). Frequently e-mail is unsecured, even if you access it from a secured web page. Therefore, avoid sending sensitive information, such as account numbers, through e-mail unless added security measures are in place.
- ***Passwords and/or personal identification numbers (PINs)***, as a minimum, should be used when accessing an account on-line. Your password should be unique to you and you should change it regularly. Do not use





birth dates, Social Security Number, or other numbers or words that may be easy for others to guess. Be careful who you give your password to. For example, if you use a financial service that requires you to provide your password in order to gather and display your financial data in a consolidated format from various on-line sources, make sure you learn about the company's privacy and security practices.

- General security over your personal computer such as virus protection and logical access controls (i.e., passwords) should be used and updated regularly. Contact your hardware and software suppliers or Internet service provider to ensure you have the latest browser version. Also, consider the use of a personal firewall to minimize unauthorized access from the Internet.

If you have a security concern about your on-line accounts, contact your credit union to discuss your concerns and determine what options or alternatives your credit union may have available for you.

For More Help

Answers to your questions.

Many regulations provide consumer protection for both traditional and on-line transactions. If you have any questions or concerns, first try to get guidance from your credit union. If you are still not satisfied and your credit union is a "Federal Credit Union" (FCU), contact the appropriate NCUA Regional Office (see the following pages for NCUA Regional Office locations and contact information). Otherwise contact the State Supervisory Authority where the credit union's main office is located.

How to file an FCU complaint.

You should file your complaint in writing. This may be on-line via e-mail or sent by fax or regular mail. Your complaint should include:

- *Your full name, address, and telephone number*
- *Your e-mail address (if applicable)*
- *The credit union's official name and main office address*
- *Specific information regarding the nature of your complaint (if filing via unsecured e-mail, do not include sensitive information such as account numbers or Social Security Numbers)*
- *Any supporting documentation*

Retain a copy of your letter and supporting documents for your records.

Where to file a complaint

NCUA Regional Offices

Region I—Albany

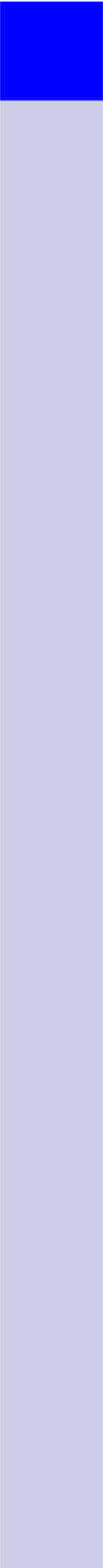
(Connecticut, Maine, Massachusetts, New Hampshire, New York, Rhode Island, Vermont)

NCUA Region I
9 Washington Square
Washington Avenue Extension
Albany, New York 12205
Telephone: (518) 862-7400
Fax: (518) 862-7420
E-Mail: region1@ncua.gov

Region II—Capital

(Delaware, District of Columbia, Maryland, New Jersey, Pennsylvania, Virginia, West Virginia)

NCUA Region II
1775 Duke St., Suite 4206
Alexandria, Virginia 22314-3437
Telephone: (703) 519-4600
Fax: (703) 519-4620
E-Mail: region2@ncua.gov



Region III—Atlanta

(Alabama, Florida, Georgia, Indiana, Kentucky, Louisiana, Mississippi, North Carolina, Ohio, Puerto Rico, South Carolina, Tennessee, U.S. Virgin Islands)

NCUA Region III

7000 Central Parkway, Suite 1600
Atlanta, Georgia 30328
Telephone: (678) 443-3000
Fax: (678) 443-3020
E-Mail: region3@ncua.gov

Region IV—Austin

(Arkansas, Illinois, Iowa, Kansas, Louisiana, Minnesota, Missouri, Nebraska, North Dakota, Oklahoma, South Dakota, Texas, Wisconsin)

NCUA Region IV

4807 Spicewood Springs Road
Suite 5200
Austin, TX 78759-8490
Telephone: (512) 342-5600
Fax: (512) 342-5620
E-Mail: region4@ncua.gov

Region V—Tempe

(Alaska, Arizona, California, Colorado, Guam, Hawaii, Idaho, Montana, Nevada, New Mexico, Oregon, Utah, Washington, Wyoming)

NCUA Region V

1230 W. Washington Street, Suite 301
Tempe, AZ 85281
Telephone: (602) 302-6000
Fax: (602) 302-6024
E-Mail: region5@ncua.gov

Where to report a suspected fraud.

If you have been a victim of credit union fraud or if you have visited a credit union Web site that appears to be fraudulent, please contact either the appropriate NCUA Regional Office (please see contact information above) or NCUA's Fraud Hotline.

The Fraud Hotline toll-free number from anywhere in the United States is (800) 827-9650 or in the Washington, D.C. area (703) 518-6550.

Who to contact if you've been a victim of identity theft.

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

You should contact the Federal Trade Commission (FTC) by telephone, toll-free at 1-877-ID-THEFT (438-4338); by postal mail: Federal Trade Commission, Identity Theft Clearinghouse, 600 Pennsylvania Avenue, NW, Washington, DC 20580; or electronically via an on-line complaint form, located at [https://rn.ftc.gov/pls/dod/widtpubl\\$.startup?Z_ORG_CODE=PU03](https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03).

The FTC puts your information into a secure consumer fraud database and may, in appropriate instances, share it with other law enforcement agencies and private entities, including any companies about which you may complain.





For more information to help you guard against and recover from identity theft, you can request the booklet **Take Charge: Fighting Back Against Identity Theft** from the FTC or view it on their Web site at <http://www.ftc.gov/bcp/online/pubs/credit/idtheft.htm>. This Web site also has an ID Theft Affidavit to alert companies where a new account is opened in your name. The Affidavit, as well as other useful consumer information, can be found on the FTC's Web site at <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/consumer-publications-old.html>.

Helpful On-line Resources

Below is a listing of some additional useful Web sites.

First Gov for Consumers

Consumer information from the federal government.

- <http://www.consumer.gov/>

OnGuard Online

Computer security tips from an alliance of government and business organizations.

- <http://onguardonline.gov/index.html/>

Internet Crime Complaint Center

FBI and National White Collar Crime Center partnership addressing fraud via the Internet.

- <http://www.ic3.gov/>

Dot Cons

Internet scam awareness information from the Federal Trade Commission.

- <http://www.ftc.gov/bcp/online/pubs/online/dotcons.htm>

This brochure is intended to provide the credit union member with information about transactions on the Internet. It is not intended to be a legal interpretation of the regulations and policies of the National Credit Union Administration.

May be reprinted without restriction.