

permission – to telephone callers, on the Internet, to door-to-door salespeople, etc.

Learn What To Do If Something Goes Wrong

If you suspect that your finances have been compromised, there are several places to go for assistance. The most important thing is to act quickly. Your prompt action may prevent further damage to your financial situation and assist in catching whoever is responsible. Depending on the situation, you can call the financial institution or company where you have an account that you suspect has been compromised. Call your local police department to report theft. Visit the Federal Trade Commission's Web site, www.ftc.gov/idtheft, for other steps you should immediately take if someone has hijacked your personal information.

Your credit union is always available to assist if you have any questions about the security of your accounts, and can help advise you should you suspect an account has been compromised. We are here to help.



United States
SENATE
Federal Credit Union

National Capitol Station
P.O. Box 77920
Washington, DC 20013-8920

(202) 224-2967
(800) 374-2758

www.ussfcu.org



Presented by the National Association of Federal Credit Unions, an independent trade association representing federally chartered credit unions nationwide.

© 2008 National Association of Federal Credit Unions.

SF89-608

PROTECTING YOUR FINANCES AT HOME



**A checklist of safety measures
you can take in your own home**

In an era of sophisticated technology – and increasingly sophisticated criminals – it’s especially important to be educated about how to keep your finances safe and secure. Here’s a checklist of basic “how-to’s” for keeping your finances safe in your home.

Financial Records

- ✓ **Buy a shredder.** Shred all unwanted financial applications, old financial records and any other unneeded records that contain personal information.
- ✓ **Keep important financial records in a secure environment,** such as a lockable filing cabinet, safe or safety deposit box.
- ✓ **Make a copy of important records.** Make paper copies, or scan documents and save them on your computer (make sure to back up your computer regularly). Copy credit cards, Social Security cards, passports and more, and store copies in a secure location.

Mail

- ✓ **Purchase a lockable mailbox.**
- ✓ **Place outgoing mail in a U.S. Postal Service mailbox.** Don’t leave it in your mailbox for pickup.

- ✓ **Don’t leave mail in your mailbox overnight.**
- ✓ **Pay attention to when you normally receive bills.** If you do not receive a bill when expected, call the company immediately. It’s a possible sign of identity theft.

Credit/Debit Cards

- ✓ **Report lost or stolen cards immediately.**
- ✓ **If you are expecting a new credit or debit card and don’t receive it in a reasonable time,** call the financial institution.
- ✓ **Sign new credit cards immediately.**
- ✓ **Destroy old or expired cards.** Be sure to cut through the account number and magnetic strip before disposing of a card.
- ✓ **Carefully monitor credit card statements for accuracy.**

Home Computer

- ✓ **Purchase and regularly update security software.**
- ✓ **Put passwords on the computer,** on all programs that deal with your finances and on all of your online financial accounts.

- ✓ **Be smart about passwords.** Don’t use your birth date, last name, street address or any other easily accessible personal information as a password. Use a combination of letters and numbers, and if possible use both uppercase and lowercase letters. Memorize passwords if possible, and also write them down and store them in a secure place.

- ✓ **Don’t disclose credit card or other financial account numbers** on a Web site unless you are absolutely sure of site security.
- ✓ **Keep your computer in a location where you can monitor its usage.**

Telephone Calls

- ✓ **Never reveal personal information** unless you are absolutely sure who you are speaking to.
- ✓ **Beware of solicitations** (by phone, email, or even in-person salespeople) that offer prizes. Don’t supply any personal information unless you are sure the offer is legitimate. Usually, it isn’t.

Teach Your Children

- ✓ **It’s wise to start teaching safe practices early.** Children should learn to *never* provide personal information without parental