Safeguarding Your Information

Four basic ways to protect your personal information and reduce your risk of identity theft are:

- Know who you share your information with.
- Store and dispose of your personal information securely.
- Ask questions before deciding to share your personal information.
- Maintain appropriate security on your computers and other electronic devices.

In addition, following the steps below can further protect your identity:

Guard your Social Security number

Do not carry your Social Security card with you and do not use your Social Security number as a PIN or password unless the financial institution, merchant or other business with which you are dealing absolutely requires it.

Never give out personal information unless you are the one who initiated the contact.

Shred, shred, shred

Invest in a micro-cut shredder, an inexpensive countertop model will work and use it to shred bills, receipts, bank statements, or any other confidential information. Destroy labels on prescription bottles before you throw them out. Also shred any other items that contain personal or financial information such as credit card or insurance offers – that you do not keep.

Protect your mail

If you are going to be out of town, even for a few days, either have the post office hold your mail or ask a neighbor, family member or friend to pick it up. When mailing something, particularly if it contains a check or other personal information, mail it from a secure location rather than leaving it for the postman or even worse, an identity thief. If you are ordering checks from your financial institution, pick them up instead of having them mailed to you. Sign up for informed delivery from www.USPS.com to ensure you are receiving all your mail.

Do not share your information

Identity thieves get lots of information simply by asking us what they want. They contact us by phone, email or regular mail posing as our bank, credit card company, or even the IRS. They ask us to "verify" information like account numbers, Social Security numbers or passwords. Legitimate companies or agencies do not do this, so if you are ever asked for this information it is likely to be a criminal trying to steal your identity. Never give out personal information unless you are the one who initiated the contact.

Do not overshare on social networking sites

If you post too much information about yourself, an identity thief can find information about your life, use it to answer 'challenge' questions on your accounts, and get access to your money and personal information. Consider limiting access to your networking page to a small group of people. Never post your full name, Social Security number, date of birth, address, phone number, or account numbers in publicly accessible sites.

Turn on two-factor authentication if offered

Two-factor authentication is an added layer of security that combines something you have, a physical token such as a card or a code, with something you know, something memorized, such as personal identification number (PIN) or password.

Stop pre-approved credit card offers

Unless you are really shopping for a credit card, stop pre-approved credit card offers. They are easy to spot in your mail box and can easily be used by identity thieves to get a credit card in your name. You can have your name removed from credit reporting agencies lists by calling toll-free to 888-5OPTOUT (888-567-8688) or visiting the Opt Out website at www.optoutprescreen.com.

Check your bills and bank statements

If an identity thief strikes, you might first notice it on your bills or bank statements. If you can, it is best to review your bank statements and bills online, where most transactions are visible within a few days. Monitor your bills and bank statements for unauthorized charges as soon as they arrive. Report any issues as soon as possible. If your bill or statement does not come at the normal time, call and ask about it; since late arrival could be another indication of identity theft.

Pay attention to internet security

Make certain you have adequate security on your computer. Install a firewall and virus and spyware protection. Choose your passwords with care and make them unique. Experts recommend using a password that has at least 8 characters, with a mix of numbers, symbols, and upper and lower case letters. Do not click on pop-up ads or open emails and attachments from persons you do not know and trust. Be especially wary of phishing emails from imposters posing as legitimate companies. Check your browser security settings to make certain that they are not too low. Also check the security of the website. Generally, “https” and/or a small padlock in the address bar means that the site is secure.

Read privacy statements

In this information age, there is a large market for personal information. Some of the companies with which we do business share or even sell our personal information to others. Before purchasing online, check the privacy policy of the business. Also, read the privacy statement that your credit card company sends you. In certain cases, you might be able to opt out of that company sharing all or a part of your information by contacting the company.

Check your credit report regularly

Obtain your credit report free from each of the three major credit reporting companies each year. Credit reports contain a wealth of information about a consumer’s financial history and checking them regularly is one of the best ways to protect against identity theft. If you notice a credit card or bank account that you do not think you have, or a listed address or name that is not correct, it might mean that an identity thief is at work. You can obtain your free credit report from Equifax, Experian, and TransUnion by calling toll-free to (877) 322-8228 or online at www.annualcreditreport.com.

Safely dispose of personal information

Before you dispose of a computer, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive. Before you dispose of a mobile device, check your owner’s manual, the service provider’s website, or the device manufacturer’s website for information on how to delete information permanently, and how to save or transfer information to a new device. Remove the memory or subscriber identity module (SIM) card from a mobile device. Remove the phone book, lists of calls made and received, voicemails, messages sent or received, organizer folders, web search history, and photos.

For more information or to file a complaint,
visit our website or contact:

Wisconsin Department of Agriculture,
Trade and Consumer Protection
Bureau of Consumer Protection
2811 Agriculture Drive, PO Box 8911
Madison, WI 53708-8911

Email: DATCPHotline@wi.gov
Website: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058