

NOTES TO AGENTS: This release is part of the Money Matters series offered by the Family Financial Education Team. This release will not be sent to statewide media.

-- Please add local contact information.

-- Please remember to alter the quotes if you substitute your own name in the release.

-- An optional sidebar focuses on home computer protection.

For Release: June 2006

Contact: Brenda Janke, 715-536-0304, brenda.janke@ces.uwex.edu

Money Matters: Minimizing your identity theft risks

[YOUR TOWN] MERRILL, Wis.— When it comes to identity theft, you can't control all the circumstances, but there are steps you can take to minimize your risk.

Begin by ordering a copy of your credit report. An amendment to the federal Fair Credit Reporting Act requires each of the three major nationwide consumer reporting companies to provide you with a free copy of your credit reports, at your request, once every 12 months.

To order your free annual report from one or all the national consumer reporting companies, visit www.annualcreditreport.com, call toll-free 877-322-8228, or print the Annual Credit Report Request Form from ftc.gov/credit. Do not contact the three companies individually. If using the web, be sure you are on the official web site; avoid fraudulent sites with similar web addresses. You can request that only the last four digits of your Social Security number will appear on your credit reports.

U.S. Federal Trade Commission recommends to protect yourself from identity theft.

Place passwords on credit card, bank, and phone accounts. Avoid using easily available information, such as your mother's maiden name, your birth date, the last four digits of your Social Security number or your phone number. If account applications call for your mother's maiden name, request to use a password instead.

Ask about information security procedures in your workplace or at businesses, doctor's offices or other institutions that collect your personal information. Find out who has access to the information and verify that it is handled securely. If your information is to be shared, ask how it can be kept confidential. As of June 1, a new federal rule requires businesses and individuals to take appropriate measures to dispose of sensitive information derived from consumer reports.

Don't give out personal information on the phone, through the mail, or on the Internet unless you initiate the contact or know the person you're dealing with. Identity thieves have posed as representatives of banks, Internet providers, and even government agencies to get people to reveal identifying information. Before you share personal information, confirm that you are dealing with a legitimate organization. Check an organization's web site by typing its web address, rather than cutting and pasting it. Call customer service at the number on your

account statement to verify that they need your personal information. Do not use a cell phone to give out personal information such as your Social Security number.

Treat your mail and trash carefully. Don't just throw out all junk mail; many solicitations include private information. Tear or shred charge receipts, credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards and credit offers. To opt out of receiving credit offers in the mail, call 1-888-5-OPTOUT (1-888-567-8688). (You will be asked to provide your Social Security number, which the consumer reporting companies need to match you with your file.) Be cautious when responding to promotions. Identity thieves may create phony offers to get your personal information.

Deposit outgoing mail in postal boxes or the post office, rather than in an unsecured mailbox. Remove mail from your mailbox promptly. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to request a vacation hold. Your local post office will hold the mail until you can pick it up or have returned home. Pick up new checks at the bank instead of having them mailed to your home.

Don't carry your Social Security card; leave it in a secure place. Carry only the identification, credit and debit cards that you'll actually need when you go out. Photocopy the cards in your wallet so you'll have a record in case of theft or loss. When signing a credit card slip, always check that the name imprinted on the slip is actually yours. Be watchful of someone taking a photo of your check or credit card with a camera phone.

Give your Social Security number only when absolutely necessary, and ask to use other types of identifiers. Do not use your Social Security number as your driver's license number, or health insurance policy number. Your employer and financial institutions will need your Social Security number for wage and tax reporting purposes. Other businesses may ask for it to do a credit check if you are applying for a loan, renting an apartment, or signing up for utilities, however, they may simply want the number for general record keeping.

Last but not least, don't let the fear of identity theft rule your life. Although the above precautions may seem like a lot, these tips are meant to simply keep us watchful and help us use common sense safety tactics to secure our personal information.

A free brochure called "Identity Theft: Your Good Name Gone Bad!" and other publications are available in Spanish and English from Call for Action at 1-800-647-1756 or online at www.callforaction.org. To learn more about family financial management, contact your county UW-Extension office [ADD LOCAL CONTACT INFORMATION].

###

<http://www.uwex.edu/ces/news>

File: Consumer Issues, Family financial management, Finance

SIDEBAR:

Your home computer and identify theft concerns

Depending on what you use your personal computer for, an identity thief may not need to set foot in your house to steal your personal information. Janke [YOUR NAME] offers the following recommendations from the Federal Trade Commission for protecting your identity online.

- Update your virus protection software regularly, and install patches for your operating system and other software programs to protect against intrusions and infections that can lead to the compromise of your computer files or passwords. Ideally, virus protection software should be set to automatically update each week. The Windows XP operating system also can be set to automatically check for patches and download them.
- Do not open files sent via email by strangers, or click on hyperlinks or download programs from people you don't know. Be careful about using file-sharing programs. Opening a file could expose your system to a computer virus or a program known as "spyware," which could capture your passwords or any other information as you type it into your keyboard.
- Use a firewall program, especially if you use a high-speed Internet connection like cable or DSL that connects your computer to the Internet 24 hours a day. The firewall program allows you to stop uninvited access to your computer. Without it, hackers can take over your computer, access personal information stored on it, or use it to commit other crimes.
- Use a secure browser—software that encrypts or scrambles information you send over the Internet—to guard your online transactions. When submitting information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission.
- Don't store financial information on your laptop unless absolutely necessary. If you do, use a strong password with a combination of letters (upper and lower case), numbers and symbols. A good way to create a password is to think of a memorable phrase and use the first letter of each word as your password, converting some letters into numbers that resemble letters. For example, "I love Felix; he's a good cat," would become 1LFHA6c. Don't use an automatic log-in feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it's harder for a thief to access your personal information.
- Before you dispose of a computer, delete all the personal information it stored. Deleting files using the keyboard or mouse commands or reformatting your hard drive may not be enough because the files may stay on the computer's hard drive, where they may be retrieved easily. Use a "wipe" utility program to overwrite the entire hard drive.
- Be careful of using a wireless connection for transmitting personal or banking information. Wireless connections may be able to be intercepted if not set up correctly.