DIVISION OF AGRICULTURE
RESEARCH & EXTENSION
University of Arkansas System

Handout

United States Department of Agriculture, University of Arkansas, and County Governments Cooperating

The Cooperative Extension Service is your source for reliable, research-based information to improve quality of life. Discover the latest recommendations for money management, nutrition, health, parenting, relationships, and personal development. Learn more at www.uaex.edu.

Six Important Steps for Consumer Protection

1. **Guard personal information and PINs.** Carefully guard social security number, bank account numbers, personal identification numbers, etc. Any financial documents (including checks) that you keep at home should be in a secure location – preferably locked. "Phishing" refers to calls or emails that are used by thieves to obtain information from consumers. Beware of calls or emails that ask for personal or financial information. Never give out information over the phone unless you initiated the call or are certain you are talking to a reputable person. If someone claims to be a relative or from your bank – verify their identity. It's okay to hang up and place a direct call to verify the identity of the caller. The National Do Not Call Registry is a free, easy way to reduce telemarketing calls. To register or to get information, visit www.donotcall.gov or call 1-888-382-1222 from the phone number you want to register. Don't open files or click on links in emails from someone you don't know. Thieves use phishing scams to try to access your information. Cut back on the amount of legitimate marketing emails you receive by contacting the Direct Marketing Association (DMA). Opt out of receiving unsolicited commercial email from DMA members at www.dmachoice.org. Registration is free and lasts six years.

2. **Shred mail and documents.** Dumpster diving can give thieves access to bank statements, credit card statements, health insurance numbers, pre-approved credit card offers and other personal information. Shred anything that might have your personal financial information. Opt out of pre-screened credit card and insurance offers. Call 1-888-5-OPT-OUT (1-888-567-8688) or visit www.optoutprescreen.com. Opt out of receiving unsolicited commercial mail from many companies for five years by registering with the Direct Marketing Association (DMA). Your name will be put on a "delete" file and made available to direct-mail marketers and organizations. This registry applies only to organizations that use DMA's Mail Preference Service. To register, go to www.dmachoice.org.

3. **Shop at reputable businesses.** Whether in person or online, one of the best ways to be sure you won't be swindled is to shop at businesses you know are legitimate. If shopping online, look for a physical address and phone number, check refund and return policies and read privacy and protection information. Pay by credit card. Under the Fair Credit Billing Act, you're financial responsibility is limited to $50 in the event that unauthorized charges are made on your credit card account. Keep records/receipts of your transactions. For more information, see the Shopping Online handout (optional).

4. **Keep devices secure.** Do you shop or bank online? Have you used a mobile app to check your account balance? Do you receive email messages from your credit card company? Make sure you keep virus software up to date. Log-out of accounts, exit websites and close apps as soon as you are finished. Password protect your phone, tablet or computer. Use strong passwords. Avoid obvious passwords such as your birthdate, address, maiden name, etc.

5. **Limit the cards you carry**. You'll have less to lose if your purse or wallet is stolen. It's easier to contact companies and stop transactions on only one or two cards than on six or eight cards. Carry only the cards you need and leave the others at home. Leave your Social Security card at home. "Skimming" refers the theft of card information from an account-access device. If the card-reading device at a gas-pump or ATM looks as if it's been tampered with, don't swipe your card.

6. **Monitor accounts and statements.** Keep a close eye on your bank accounts. Always check statements. View account information online and/or sign up for text alerts to monitor more frequently. Check your credit report regularly. You are entitled to one free annual credit report from each of the three major credit reporting bureaus. Spread these out over the year and check one every four months. Be sure to go to the right website: www.annual-creditreport.com. Other websites may charge a fee. Your credit report is free, but there is a small fee ($10 to $20) to obtain your credit score. Monitor your report for errors or signs of fraud. You can place an Initial Fraud Alert on your report, and creditors or business must verify your identity when anyone applies for credit in your name. The initial alert expires in 90 days but can be renewed. Victims of proven fraud are allowed a seven-year fraud alert. Visit www.annualcreditreport.com and click on a link for any of the credit bureaus. Placing a Fraud Alert with one bureau automatically places the alert with the other bureaus. Contact the bank, creditor and/or credit bureau if you notice anything suspicious.

References:

- Office of the Arkansas Attorney General
- Federal Trade Commission

Prepared by Laura Connerly, Ph.D., Assistant Professor - Family and Consumer Economics, University of Arkansas Division of Agriculture (lconnerly@uaex.edu).

The Arkansas Cooperative Extension Service offers its programs to all eligible persons regardless of race, color, national origin, religion, gender, age, disability, marital or veteran status, or any other legally protected status, and is an Affirmative Action/Equal Opportunity Employer.