USEFUL TIPS & SUGGESTIONS

Protecting Your Family Against Identity Theft

Review your annual credit report for fraud	Each year you are entitled to one free credit report from each of the three credit reporting agencies. These reports are an excellent source for uncovering suspicious activity and should be closely examined. Order online via www.annualcreditreport.com, by telephone at (877) 322-8228, or by mail after downloading https://www.annualcreditreport.com/cra/requestformfinal.pdf.
Guard your wallet and limit its contents	Your wallet or pocket book and the sensitive personal information it contains are prime targets for identity thieves. Do not carry your Social Security card on your person unless absolutely needed, and restrict the number of credit and debit cards to those needed for everyday use.
Keep your computer secure	The unfortunate reality is that we live in a world of malicious viruses and hackers. Never open unusual or suspicious email from unknown sources. Install virus protection software and a firewall to thwart hackers from stealing personal data. All stored data should be encrypted and password protected. When disposing of an old computer, use software that securely wipes your hard drive; do not rely on the "permanently delete" function in your trash folder to remove sensitive information.
Limit transactions to secure websites	Online purchases should be restricted to secure websites. Be sure the merchant uses secure data transmission in conjunction with rigorous security and privacy policies.
Keep your mail safe	Many people now use commercial mail-boxes or P.O. mailboxes to safeguard their mail, particularly when travelling for extended periods.
Store sensitive information securely	Secure information storage is essential. Predators take countless forms: roommates, domestic employees, loitering outside contractors – anyone with malicious intent and access to your documents. Prepare copies of all accounts, including expiration dates and customer service phone numbers. Securely store this information so that you can institute immediate action if cards are lost or stolen.
Systematically review all statements for improper use	Make a point of reviewing your Social Security, phone, bank and credit card statements. Your Social Security statement is mailed about three months prior to your birthdate.
Check and payment security	Stolen checks can easily be altered and cashed. Never allow new checks to be mailed; pick them up at the bank. Mail your monthly payments from inside a post office, and avoid workplace drop boxes and your own mailbox for pick up. Store cancelled checks in a safe place.

USEFUL TIPS & SUGGESTIONS

Protecting Your Family Against Identity Theft

Minimize the number of credit cards	Cancelling credit cards can negatively affect your credit scores. But maintaining inactive accounts provides targets for identity thieves. Track new or reissued cards sent to you, and contact the issuer if the card does not arrive within two weeks.
Secure passwords and PINs	Passwords should be alphanumeric (combination of letters and numbers). Thieves will attempt easily guessed passwords such as children's or pet's names. Likewise, easily guessed pass codes should be avoided, such as the last four digits of your Social Security number or birth date. Create unusual passwords and keep a record of them in a safe place, and avoid carrying them on your person.
Stay vigilant at the ATM	It's easy to drop your guard during rote activities like punching in your code at the ATM. Always be mindful of your surroundings, as you never know who's peering over your shoulder.
Stop unrequested marketing	To stop annoying, untrusted marketing, call **1-888-5-optout** to have the three credit bureaus remove your name from marketing lists. This will limit pre-approved credit offers and reduce exposure to fraudulent accounts opened in your name. You can also visit www.donotcall.gov or call 888-382-1222. They will place your name on the *National Do-Not-Call Registry*. You can call your State office and add your name to the Do-Not-Call list, if they have one. Never allow any financial information to be shared with other financial institutions, credit card companies, insurance or investment firms.