YOUR IDENTITY - PROTECTED IT!

KRESS NATIONAL BANK P O BOX 660, KRESS, TEXAS 79052 806.684.2231

Your Name - Your Social Security Number - Your Drivers License their yours protect them.

How Can I Protect Myself from Identity Theft Online?

Identity theft is any kind of deception, scam, or crime that results in the loss of personal data, including the loss of user names, passwords, banking information, credit card numbers, Social Security Numbers and health ID's, that is then used without your permission to commit fraud and other crimes.

Up to 9 million Americans have their identities stolen each year according to the FTC1 , and at least 534 million personal records have been compromised since 2005 through attacks on the data bases of businesses, government bodies, institutions, and organizations2. If those breaches were spread evenly across the U.S. population of 310 million, everyone would have had their identities stolen one and two-thirds times.

For some consumers, identity theft is an annoying inconvenience and they can quickly resolve their problems and restore their identity. For others recovering their identity can cost hundreds, even thousands of dollars, take months to resolve, cause tremendous damage to their reputation, cause them to lose job opportunities, even influence the rejection of loan applications for school, homes or cars because would-be employers or loan companies see the damage on your credit scores. Some consumers have even been arrested for crimes committed by someone using their identities and have had to prove that they were not guilty.

How are identities stolen?

Consumers become victims of identity theft through many types of exploits. These can happen the old fashioned ways when crooks (including family members!) steal mail from your mailbox, rummage through your trash for bills and bank statements, steal wallets and purses, or make an extra copy of your credit card - perhaps when your waiter or clerk walks off to process your payment.

Online identity theft occurs when users fall for tactics like phishing and confidence scams; or download malware onto their computers or smartphones that steals their information; use wireless networks that are insecure; take out money from an ATM that has been rigged with a skimming device that collections your information; share their passwords with untrustworthy people, or by having their information stolen when data records are breached on companies, government, and educational sites.

7 key steps to preventing identity theft online:

1. Protect your computer and smartphone with strong, up-to-date security software. If your computer or phone is infected with malicious software, other safeguards are of little help because you've given the criminals the key to all your online actions. Also be sure that any operating system updates are installed.
2. Learn to spot spam and scams. Though some phishing scams are easy to identify, other phishing attempts in email, IM, on social networking sites, or websites can look very legitimate. The only way to never fall for phishing scam is to never click on a link that has been sent to you. For example, if the email says it's from your bank and has all the right logos and knows your name, it may be from your bank - or it may not be. Instead of using the link provided, find the website yourself using a search engine. This way you will know you landed on the legitimate site and not some mocked up fake site.
3. Use strong passwords. Weak passwords are an identity thief's dream - especially if you use the same password everywhere. Once the thief knows your password, they can log you're your financial accounts and wreak havoc. You need passwords that are long (over 10 characters), strong (use upper and lower case letters, numbers and symbols), and that have nothing to do with your personal information (like name, age, birth date, pet)
4. Monitor your credit scores. By law you have the right to three free credit reports per year; from Experian 800.397.3745, Trans Union 800.525.6285, and Equifax 800.525.6285. These three credit bureaus work together through a website called AnnualCreditReport.com so you can quest all three reports at once in one of the following ways:
   - Go to the Web site. Through this highly secure site, you can instantly see and print your credit report.
   - Call toll-free: (877) 322-8228. You'll go through a simple verification process over the phone after which they'll mail the reports to you.
   - Request by mail. If you live in certain states, fill out the request form and mail it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. (Get more details.)

   Note: Remember that after you request a report, you will have to wait a year to get it free of charge again from the same credit reporting company. (Of course you can pay for a copy of your credit report at any time.)
   - If you suspect Fraud or Identity Theft contect:
     - ➤ Federal Trade Commission 877.438.4338
     - ➤ Social Security Administration 800.269.0271
     - ➤ Contact your local Post Office
     - ➤ Contact the IRS 800.829.0433
     - ➤ Contact Kress National Bank 806.684.2231
5. Review your credit score. Look too see if there are new credit cards, loans or other transactions on your account that you are not aware of. If there are, take immediate steps to have these terminated and investigated.

6. Freeze your credit. Criminals use stolen ID's to open new lines of credit. You can thwart their efforts to use your identity by simply locking (called freezing) your credit so that no new credit can be given without additional information and controls. Many states have laws giving you the right to a free credit freeze, but even where states don't provide legal mandates, the large credit bureaus provide a voluntary security freeze program at a very low cost. To determine whether there are any costs associated with placing a security freeze on your credit, and for temporarily lifting that credit freeze when you do seek credit, see State Freeze Requirements and Fees.

7. Only use reputable websites when making purchases. If you don't know the reputation of a company that you want to purchase from, do your homework. How are they reviewed by other users? Do they have a strong rating with the Better Business Bureau? Do they use a secure, encrypted connection for personal and financial information? (You should see an Https in a website's URL whenever they ask for personal or financial information).

8. Stay alert. Watch for common signs of identity theft like: ?False information on your credit reports, including your Social Security number, address(es), name or employer's name. ?Missing bills or other mail. If your bills don't arrive, or come late, contact your creditors. A missing bill may indicate that an ID thief has hijacked your account and changed your billing address to help hide the crime. ?Getting new credit cards sent to you that you didn't apply for. ?Having a credit approval denied or being subjected to high interest rates for no apparent reason. ?Receiving calls or notices about past due bills for products or services you didn't buy.

Consistently applying these steps to both defend and monitor your credit score will reduce the risks of having your identity stolen, and alert you instantly if such a problem arises.