Protect Yourself from Identity Theft

Scammers can steal your identity by obtaining your personal financial information online, at the door or over the phone. What they want are account numbers, passwords, Social Security numbers, and other confidential information that they can use to loot your checking account or run up bills on your credit cards.

Identity thieves can take out loans or obtain credit cards and even driver's licenses in your name. They can do damage to your financial history and personal reputation that can take years to unravel. But if you understand how to protect yourself, you can help stop this crime.

How to Protect Yourself

- **Never provide personal financial information**, including your Social Security number, account numbers or passwords, over the phone or the Internet if you did not initiate the contact. E-mails created by scammers may look exactly like the real thing and may contain viruses that can contaminate your computer.
- **Never click on the link provided in an e-mail** you believe is fraudulent.
- **Do not be intimidated by an e-mail** or caller who suggests dire consequences if you do not immediately provide or verify financial information.
- **If you believe the contact may be legitimate, contact the financial institution yourself.** You can find phone numbers and Web sites on the monthly statements you receive from your financial institution, or you can look the company up in a phone book or on the Internet and contact them directly.
- **Never provide your password over the phone or in response to an unsolicited Internet request.** A financial institution would never ask you to verify your account information online. Thieves armed with this information and your account number can help themselves to your savings.
- **Review account statements regularly to ensure all charges are correct.** If your account statement is late in arriving, call your financial institution to find out why. If your financial institution offers electronic account access, periodically review activity online to catch suspicious activity.
- **If you fall victim to an attack, act immediately**. Alert your financial institution. Place fraud alerts on your credit files. Monitor your credit files and account statements closely.
- **Report suspicious e-mails or calls** to the Federal Trade Commission through the Internet at www.ftc.gov/idtheft, or by calling 1-877-IDTHEFT.

What to do if you fall victim to identity theft:

- Contact your financial institution immediately and alert it to the situation.
- Call the three major credit bureaus to place a fraud alert on your file, preventing thieves from opening a new account in your name.
    - **Equifax**, 800-685-1111
      P.O. Box 740250
      Atlanta, GA 30374
    - **Experian**, 888-397-3742
      P.O. Box 1017
      Allen, TX 75013
    - **TransUnion**, 800-493-2392
      P.O. Box 6790
      Fullerton, CA 92634
- Call the security numbers located on the back of your stolen credit cards. These numbers can also be found on your credit card billing statements
- Report the theft and your response to Attorney General Derek Schmidt's Office.
  Call **785-296-3751** or **1-800-432-2310** to request a complaint form.

Provided by:

Kansas Attorney General
Derek Schmidt

Consumer Protection Division
120 SW 10th Avenue, 2nd Floor
Topeka, KS 66612-1597
PHONE: (785) 296-3751 or (800) 432-2310
FAX: (785) 291-3699 ● *www.ag.ks.gov*