YOU CAN PROTECT YOURSELF BY TAKING THESE BASIC PRECAUTIONS:

Shred or tear up credit card & ATM charge receipts, credit card solicitations & bills, cancelled checks, account statements, expired cards & similar documents.

Outgoing mail should be deposited at the post office rather than the mailbox, and incoming mail should be promptly removed to avoid thieves from gaining access to your personal information, especially in rural areas.

Review your monthly bank & credit card statements promptly and carefully for any unauthorized activity. Report anything suspicious immediately. With the age of electronic transactions, fraudulent activity can easily slip by.

Do not put the complete credit card account number on the memo of your checks when paying your bill. Instead, write only the last 4 numbers. This is all the information necessary for your payment to be applied correctly, and limits the information to those who might abuse it.

Never give your personal information over the telephone! Be especially cautious of anyone posing as a law enforcement individual, bank representative, or someone from "prize headquarters". A good rule of thumb is to never give information to anyone if you did not instigate the telephone call. Once a crook has access to your account number, they can create and issue drafts with your account number to steal funds directly from your account. Never "verify" your account number or social security number over the telephone or Internet.

Guard your social security number. Never carry it in your wallet, and avoid having it printed on your checks.

Protect your password & PIN. Never lend them to anyone even if it's someone you trust, they may be careless and leave it in plain view for a scam artist. Be mindful around the ATMs for "shoulder surfers", persons watching to steal your PIN to gain access to your account(s).

Question credit card denials that you receive for no apparent reason.

Periodically check your credit report to see if there are any credit cards and or loans in your name that you didn't generate. A free credit report is available at www.annualcreditreport.com.

Limit what you carry. When you go out, take only the identification, credit, and debit cards you need. Leave your Social Security card at home.

When you order new checks, don't have them mailed to your home, unless you have a secure mailbox with a lock.

Consider opting out of prescreened offers of credit and insurance by mail. You can opt out for 5 years or permanently. To opt out, call 1-888-567-8688 or go to optoutprescreen.com. The 3 nationwide credit reporting companies operate the phone number and website. Prescreened offers can provide many benefits. If you opt out, you may miss out on some offers of credit.

Keeping Your Personal Information Secure Online

Be Alert to Impersonators

Make sure you know who is getting your personal or financial information. Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or know who you're dealing with. If a company that claims to have an account with you sends email asking for personal information, don't click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service. Or, call the customer service number listed on your account statement. Ask whether the company really sent a request.

Safely Dispose of Personal Information

Before you dispose of a computer, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive.

Before you dispose of a mobile device, check your owner's manual, the service provider's website, or the device manufacturer's website for information on how to delete information permanently, and how to save or transfer information to a new device. Remove the memory or subscriber identity module (SIM) card from a mobile device. Remove the phone book, lists of calls made and received, voicemails, messages sent and received, organizer folders, web search history, and photos.

Encrypt Your Data

Keep your browser secure. To guard your online transactions, use encryption software that scrambles information you send over the internet. A "lock" icon on the status bar of your internet browser means your information will be safe when it's transmitted. Look for the lock before you send personal or financial information online.

Keep Passwords Private

Use strong passwords with your laptop, credit, bank, and other accounts. Be creative: think of a special phrase and use the first letter of each word as your password. Substitute numbers for some words or letters. For example, "I want to see the Pacific Ocean" could become 1W2CtPo.

Don't Overshare on Social Networking Sites

If you post too much information about yourself, an identity thief can find information about your life, use it to answer 'challenge' questions on your accounts, and get access to your money and personal information. Consider limiting access to your networking page to a small group of people. Never post your full name, Social Security number, address, phone number, or account numbers in publicly accessible sites.

Use Security Software

Install anti-virus software, anti-spyware software, and a firewall. Set your preference to update these protections often. Protect against intrusions and infections that can compromise your computer files or passwords by installing security patches for your operating system and other software programs.

Avoid Phishing Emails

Don’t open files, click on links, or download programs sent by strangers. Opening a file from someone you don’t know could expose your system to a computer virus or spyware that captures your passwords or other information you type.

Be Wise About Wi-Fi

Before you send personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected.

Lock Up Your Laptop

Keep financial information on your laptop only when necessary. Don’t use an automatic login feature that saves your user name and password, and always log off when you’re finished. That way, if your laptop is stolen, it will be harder for a thief to get at your personal information.

Read Privacy Policies

Yes, they can be long and complex, but they tell you how the site maintains accuracy, access, security, and control of the personal information it collects; how it uses the information, and whether it provides information to third parties. If you don’t see or understand a site’s privacy policy, consider doing business elsewhere.