

How to Avoid Identity Theft

The best protection against identity theft is to carefully protect your personal information, for example:

- Do not share personal information over the phone, through the mail, or over the internet unless you initiated the contact or know the person you are dealing with;
- Be suspicious if someone contacts you unexpectedly online and asks for your personal information. It doesn't matter how legitimate the e-mail or website may look. Only open e-mails that look like they are from people or organizations you know, and even then, be cautious if they look questionable. Be especially wary of fraudulent e-mails or websites that have typos or other obvious mistakes;
- Don't give out valuable personal information in response to unsolicited requests. Social Security numbers, financial account information and your driver's license number are some of the details that should be kept confidential;
- Shred old receipts, account statements, and unused credit card offers;
- Choose PINs and passwords that would be difficult to guess and avoid using easily identifiable information such as your mother's maiden name, birth dates, the last four digits of your social security number, or phone numbers;
- Pay attention to billing cycles and account statements and contact your bank if you don't receive a monthly bill or statement since identity thieves often divert account documentation;
- Review account statements thoroughly to ensure all transactions are authorized;
- Guard your mail from theft, promptly remove incoming mail, and do not leave bill payment envelopes in your mailbox with the flag up for pick up by mail carrier;
- Obtain your free credit report annually and review your credit history to ensure it is accurate;
- Use an updated security program to protect your computer; and
- Be careful about where and how you conduct financial transactions, for example don't use an unsecured Wi-Fi network because someone might be able to access the information you are transmitting or viewing.

How to Avoid Frauds & Scams

There are numerous scams presented daily to consumers so you must always exercise caution when it comes to your personal and financial information. The following tips may help prevent you from becoming a fraud victim.

- Be aware of incoming e-mail or text messages that ask you to click on a link because the link may install malware that allows thieves to spy on your computer and gain access to your information;
- Be suspicious of any e-mail or phone requests to update or verify your personal information because a legitimate organization would not solicit updates in an unsecured manner for information it already has;
- Confirm a message is legitimate by contacting the sender (it is best to look up the sender's contact information yourself instead of using contact information in the message);
- Assume any offer that seems too good to be true, is probably a fraud;
- Be on guard against fraudulent checks, cashier's checks, money orders, or electronic fund transfers sent to you with requests for you to wire back part of the money;
- Be wary of unsolicited offers that require you to act fast;
- Check your security settings on social network sites. Make sure they block out people who you don't want seeing your page;
- Research any "apps" before downloading and don't assume an "app" is legitimate just because it resembles the name of your bank or other company you are familiar with;
- Be leery of any offers that pressure you to send funds quickly by wire transfer or involve another party who insists on secrecy; and
- Beware of Disaster-Related Financial Scams. Con artists take advantage of people after catastrophic events by claiming to be from legitimate charitable organizations when, in fact, they are attempting to steal money or valuable personal information.