



avoiding identity theft

Every year, millions of people become victims of identity theft. At Vantage Point Bank, we have employed some of the latest technologies to help detect and deter both fraud and identity theft. You must also play an active role in protecting your personal and financial information. If you use common sense and follow the suggestions outlined below, you can avoid becoming a victim.



Do not give out personal information such as your social security number, bank account numbers, credit card or debit card numbers online unless you are certain the website you are visiting or the email you are responding to is legitimate. You can avoid becoming a victim of identity theft by calling the company who is requesting the information and verifying that the website is secure and legitimate.



Verify the privacy policies of all of the companies you work with, including banks and online investment companies. One of the easiest ways to avoid becoming a victim of identity theft is to avoid companies that do not have secure websites or who sell your personal information.



Immediately upon receipt, review your bank and credit card statements and report any suspicious charges. If you do become a victim of identity theft, detecting the problem early and alerting your creditors can save you money and prevent issues with your credit report.



Shred all bank statements, credit card receipts, credit card offers, or financial information before throwing them away. Investing in a paper shredder can save you from becoming a victim of identity theft. "Dumpster diving," or going through recycling bins and trash containers, is a common way that thieves steal your identity.



Do not leave credit cards, bank statements, or other financial information in your car, on your desk at work, or in any other public place. You run the risk of becoming a victim of identity theft if you leave your

In addition to identity theft, there are many different types of scams that an unsuspecting person could fall victim to. Below are some examples of common scams.



Phishing is the act of sending an email to a user while falsely claiming to be an established legitimate company or enterprise, in an attempt to scam the recipient into surrendering private information that will be used for identity theft. The email directs the user to visit a web site where they are asked to update personal information, such as passwords, as well as credit card, social security, and bank account numbers that the legitimate organization already has. The web site, however, is bogus and set up only to steal the user's information.



Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), landline, or cellular phone. The potential victim receives a message indicating that suspicious activity has taken place in a credit card account, bank account, mortgage account, or other financial service in their name. The victim is told to call a specific telephone number and provide information to "verify identity" or to "ensure that fraud does not occur." If the attack is carried out by telephone, "caller ID spoofing" can cause the victim's set to indicate a legitimate source, such as a bank or a government agency.



Share the wealth fraud schemes combine the threat of impersonation fraud with a variation of an advance fee scheme in which a letter, email, or fax is received by the potential victim. The communication, which is from individuals representing themselves as foreign government officials or persons in need of assistance, offers the recipient the "opportunity" to share in a percentage of millions of dollars, soliciting for help in placing large sums of money in overseas bank accounts. Payment of taxes, bribes to government officials, and legal fees are often described in great detail with the promise that all expenses will be reimbursed as soon as the funds are out of the country. The recipient is encouraged to send information to the author, such as blank letterhead stationery, bank name and account numbers, and other identifying information using a facsimile number provided in the letter. The scheme relies on convincing a willing victim to send money to the author of the letter in several installments of increasing amounts, for a variety of reasons.