UNITED COMMUNITY BANK
Your Community Bank.
Perham • Dent • Frazee

Member FDIC

What is Identity Protection

Identity theft affects over 11 million people every year – typically taking 165 hours to restore (ITRC), with $54 billion in losses (Javelin Strategy & Research). Identity theft is when someone, without your permission, uses any of your personal information (Credit Card, SSN, Address, etc..) to commit fraud or other crimes. Identity Theft is against the law and costs millions of Americans like you time and money every year. Javelin Statistics

How does it happen? Could it happen to you?

Vishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward. Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

SMSishing occurs when you receive an SMS message that is purportedly sent from a reputable source, such as your bank, asking for personal details. The SMS message directs you to a dangerous website with the goal of stealing your identity.

Keystroke Logging is the action of tracking the computer keys struck on a keyboard, typically in a covert manner, so that the person using the keyboard is unaware that their actions are being monitored. User names, passwords, and Pin #s are all examples of what criminals aim to steal via this method of identity theft.

Man-in-the-Browser is a proxy Trojan horse that infects a web browser by taking the advantage of vulnerabilities in Web browser security to modify web pages, modify transaction content or insert additional transactions, all in a completely covert fashion invisible to both the user and host web application.

Dumpster diving occurs when someone goes through your trash looking for bills, or other mail including your personal information. SHRED YOUR MAIL, CREDIT CARDS, ETC. BEFORE YOU THROW THEM AWAY.

Phishing occurs when someone sends you a pop-up or spam message claiming to be an institution asking for your personal information. DO NOT RESPOND TO THE EMAIL OR MESSAGE, CONTACT YOUR FINANCIAL INSTITUTION DIRECTLY, AND AVOID CLICKING ON POP-UPS.

Skimming occurs when someone steals your credit card or debit card number through a special device when processing your payment. WHEN PAYING WITH A CREDIT OR DEBIT CARD, PAY ATTENTION TO THE PERSON PROCESSING YOUR TRANSACTION.

Change of address occurs when an identity thief fills out a change of address form and diverts your billing statements, and other mail, to another address. CHECK YOUR ACCOUNT STATEMENTS ON A REGULAR BASIS FOR FRAUDULENT CHARGES.

Pretexting occurs when false pretenses are used by the thief to obtain personal information through telephone companies, financial institutions, surveys, or other sources. The pretexter will ask for your name, date of birth, social security number, and other identifying information. Often this information is then sold for personal gain. CONFIRM WITH YOUR FINANCIAL INSTITUTION OR CREDITOR BEFORE GIVING ANY INFORMATION.

Stealing your personal belongings, such as a purse, wallet, or backpack, which may contain credit cards, debit cards, checks, driver's license, and mail containing personal information can also lead to identity theft. REPORT THE THEFT IMMEDIATELY AND ALWAYS KEEP SAFE A COPY OF YOUR CRITICAL PERSONAL AND FINANCIAL INFORMATION.

Start your protection today!

With our customizable services, you can choose the right protection to balance your budget and risk tolerance from month-to-month. With our Identity Restoration we will strive to restore your identity to pre-theft status giving you and your family peace of mind. Don't wait another minute. Start your protection with our simplest Identity Protection package and start enjoying the peace of mind you and your family deserve.

Stay Alert!

• Monitor your accounts and monthly statements to ensure their accuracy. •
• Never put outgoing mail that may contain checks or tax documents in your mailbox at home. •
• Every year, order copies of your credit report from each of the three major credit bureaus to verify their accuracy. •
• Keep a checklist of the critical items stored in your wallet, purse, laptop and/or PDA. •
• Thoroughly shred documents containing any personal information before disposing of them. •
• Only order from Internet sites that use secure methods of obtaining personal account or credit card information.•
• Never write your Personal Identification Number (PIN) on your ATM/Debit card. •
• Never write your Social Security Number or credit card number on a check. •
• Always log off after an online banking session. •
• Remove passwords, PIN numbers and identification cards containing your social security number from your purse or wallet. •