O ARMA

Anna Police Department

101 South Powell Parkway Anna, Texas 75409 T 972.924.2848 | F 972.924.3162 policecomments@annaTXpolice.com www.annaTXpolice.gov

Crime Prevention Tips

Creating a Safer Anna Community





Prevent Identity Theft During Summer Travel

Travel plans this summer? Avoid identity theft by being a savvy traveler.

Summer travel can be great, but it can also make you an easy target to identity thieves. Here are some suggestions to help lower your risk of being a victim.

REDUCE WHAT YOU CARRY.

Before you leave, clean out your purse and/or wallet. Remove all unnecessary cards or items. Carry nothing with your Social Security number on it. Make note of which cards and documents you decide to carry in case of loss or theft.

TAKE CARE IN TOURIST AREAS.

These are favorite payment card skimming spots as well as popular with purse snatchers and pick-pockets.

AVOID USING PUBLIC OR SHARED COMPUTERS.

They could have information-stealing software in place. If you must use one, avoid entering any personal information or logging onto on-line banking or credit card accounts.

AVOID TAKING YOUR CHECKBOOK.

Who writes checks these days? If you are one who does, keep in mind your checks provide a wealth of personal information that identity thieves love. Your checks show your name, address, bank name, checking account number, and checking account routing number – a whole "kit" thieves can use to take over your account. They can also forge checks to withdraw money. If you don't like using cash or payment cards, use traveler's checks.

VERIFY CALLERS TO YOUR HOTEL ROOM.

A common scam involves a call to your hotel room from a "desk clerk." This person tells you about a problem that requires you to provide your credit card number over the phone. If this happens, hang up and call or visit the front desk personally to check.

DOWNSIZE DELIVERY DANGERS.

Identity thieves will slide fabricated fliers for fake food delivery services under hotel room doors, hoping you will call and order using your credit card. Check the validity of all fliers with the desk clerk.

WATCH OUT WHEN USING PUBLIC Wi-Fi.

Airports, hotels, and other public places offer Wi-Fi, or wireless networks, for Internet access. A secure wireless network encrypts all the information you send using that network (it scrambles it into secret code so unauthorized persons cannot read it). However, Wi-Fi hotspots are often not secure. This means information you send through some websites or mobile apps can be accessed by other network users. If you choose to use public Wi-Fi, be very cautious. Keep the following in mind when using public Wi-Fi:

- Make sure it's an authenticated Wi-Fi network. Always manually select network connections and know the exact name of the establishment's network. Scammers may set up "free" computer-to-computer networks with look-alike names to fool you.
- Never log in or send personal information to unencrypted websites and be aware that for security, the site should be fully encrypted (use encryption on every page).
- Always log off an account as soon as you have finished using it.
- Don't use apps that require personal information.

If you become a victim of identity theft, or want more information on how to prevent becoming a victim, here are a few helpful resources:

- The Better Business Bureau
 - o www.bbb.org
- The Federal Trade Commission (FTC)
 - o www.consumer.ftc.gov
 - o www.identitytheft.gov
- The Financial Fraud Enforcement Task Force
 - o www.stopfraud.gov
- Internal Revenue Service (IRS)
 - o www.irs.gov/individuals/identity-protection
- The Internet Crime Complaint Center
 - o www.ic3.gov
- National Cyber Security Alliance
 - o www.StaySafeOnline.org
- U.S. Department of Homeland Security
 - o www.dhs.gov
 - o www.US-CERT.gov
 - o www.dhs.gov/stopthinkconnect (Stop. Think. Connect. [™] Campaign)
- U.S. Government's Online Safety Site
 - o <u>www.OnGuardOnline.gov</u>

STAY SAFE AND HAPPY TRAVELS - ANNA POLICE DEPARTMENT

