Newsletter Vol.13 Winter 2018

State National Bank
Big Spring Lamesa O'Donnell
901 Main Street, Big Spring, TX 79720
(432) 264-2100
www.statenb.com
Member FDIC

Learn how to protect yourself

Guard Against Identity Theft

Selling Your Car?

Clear your personal data first.

Think of how you protect your privacy when using your smartphone or home computer. Similarly, you should also think of the sorts of information that may be stored by the services you enable in your vehicle, whether it is a car you have owned for years or a weekend rental.

What types of data would you want to remove before transferring the device to another person, and what subscription services would you want to cancel, such as mobile Wi-Fi hotspot or data services?

Phone Contact/Address Book – remember that your personal contact information can be downloaded when you "sync" your phone with a vehicle. Remember to delete this information when selling a car or returning a rental vehicle. Also, be cautious when valeting or lending your car. Some vehicles are equipped with a valet function, which temporarily locks out access to this information, preventing unwanted access.

Mobile Applications in the Car – numerous personal mobile applications gather and store personal data, and when your phone is used with your vehicle, some or all of that data may be stored in the car as well. Reset/delete the car applications that contain personal information. Also, delete applications that you may have purchased and should not be accessed by others.

Vehicle Hard Drive Storage – many of today's vehicles include built-in hard-drive storage (often for music or other "infotainment" features). Remember to delete the data on this hard drive when you're selling or returning your vehicle.

Home, Work, and Favorite Places on Navigation – delete this information when selling a car or returning a rental vehicle. Also, be cautious when valeting or lending your car. Some vehicles are equipped with a valet function, which temporarily locks out access to this information.

Garage Door Programming – reset all garage door programming when selling a vehicle.

As vehicles become more connected, it will be important to keep up with new technologies and understand how your information is collected and shared.

For more information about the technology in your car, contact your local dealer and review your vehicle's owner's manual.

Don't Give to a Charity Scammer

When a natural disaster hits or a tragic event happens, you might be looking for ways to help the people and communities affected. Unfortunately, scammers are also busy trying to take advantage. There is a particular urgency in responding to disasters because the victims often lack the supplies or help they need to survive. As a result, donors often choose to contribute as soon as possible to a charitable organization that pledges to help the disaster victims.

It's suspicious for a charity to:

- Request donations in the form of a **wire transfer or cash**.
- **Convey incorrect details in the solicitation**, such as thanking the recipient for a donation that he never made.
- **Use high-pressure tactics**, such as pressing for immediate donations over the phone or requesting an overnight delivery service for payment.
- Have a name that **closely resembles a recognized charity**.
- **Fail or hesitate to provide information** about organizational leadership, contact information or other identification.
- Operate a social media account (e.g., Twitter) **with little or no activity prior to a disaster**.
- Operate a social media account **with multiple handles on the same site**.
- **Fail to provide receipts** for tax-deduction purposes.
- **Request payments to the solicitor** as opposed to the beneficiary.

Here's a list of vetted charities:

Give.org
Charitynavigator.org
Charitywatch.org
Guidestar.org

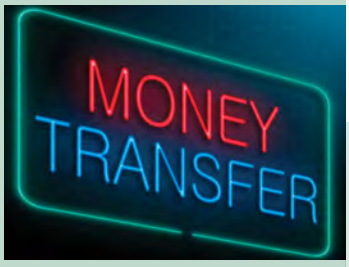
Nationwide Utility Scams Are on the Rise

Scammers use a variety of tricks to prey on utility customers. A "representative" may appear at your door in a work uniform claiming that your electric meter is not working properly and must be immediately replaced— at your expense. In a particularly alarming form of this con, the scammer may gain access to your home to perform "repairs" or an "energy audit" with the intent of stealing your valuables. These cons may also involve promises of energy discounts with the aim of taking your money, personal information, or possibly the account details needed to switch you to another utility provider without your consent (an illegal practice known as "slamming").

In another common scam, a person claiming to be a water, electric, or gas company representative threatens residents and business owners with deactivation of service if they don't pay a past due balance immediately. These imposters will typically reach you by phone or knock on your door.

Here are some red flags:

- If a caller specifically asks you to pay by prepaid debit card or wire transfer, this is a huge warning sign. Your utility company will accept a check or credit card.
- Pressure to pay immediately.



Protect Yourself Against This Scam

Call customer service. If you feel pressured for immediate action by a caller, hang up the phone and call the customer service number on your utility bill. This will ensure you are speaking to a real representative.

Never give your personal or banking information to an unverified or unsolicited caller.

Never allow anyone into your home unless you have scheduled an appointment or reported a problem. Also, ask utility employees for proper identification before letting them enter.

If You Are An Identity Theft Victim –

- **Contact your credit card company and your financial institution and close your accounts.**
- **Contact the fraud departments of each of the three major credit bureaus to place a fraud alert on your credit file.**

  Equifax: **1-800-525-6285**
  Experian: **1-888-397-3742**
  TransUnion: **1-800-680-7289**

  Tell them that you're an identity theft victim. Request that a ***"fraud alert"*** be placed in your file, as well as a ***"victim's statement"*** asking that the creditors call you before opening any new accounts or changing your existing accounts. This can help prevent an identity thief from opening additional accounts in your name.
- **Contact the Federal Trade Commission (FTC) theft hotline: 877-438-4338 or www.ftc.gov/idtheft**
- **You should not only file a report with the police, but also get a copy of the report** in case you need proof of the crime later for credit card companies, etc.
- **Call the Social Security Fraud Hotline 800-269-0271.**

Your SSN Will *Never* Be Suspended

Reports about scammers trying to trick people out of their personal information by telling them that they need to "reactivate" their supposedly suspended SSN. The scammers say the SSN was suspended due to some connection to fraud or other criminal activity. They instruct you to call a number to clear it up then that person asks you for personal information.

This is a government imposter scam that's after your SSN, bank account information or other personal information.

Never give out or confirm personal information over the phone, through an email or on a website until you've checked out its legitimacy.

Never trust a name, phone number, or email address just because it seems to be connected with the government. Con artists use official-sounding names and may fake caller ID or email address information to make you trust them. The government normally contacts people by mail.

Always contact government agencies directly by using telephone numbers and website addresses you know to be legitimate.

How to Spot Government Imposter Scams

Some scams are easy to spot. Free vacations, a lottery, a grant or suspicious inheritances.

Other scams are much more difficult, thanks to scare tactics and intimidation. They may claim to be a U.S. Marshal and say you must pay a fine for missing jury duty or claim to be from the IRS saying that you owe thousands in back taxes. Some may threaten legal action, deportation or arrest if you don't pay or give them your financial information. In the moment, scammers rely on you to panic and make a rash decision.

The more you can accustom yourself to their tactics, the better chance you have at spotting the scam. The Federal Trade Commission advises that if someone calls, texts or emails saying they're with the government and that you must pay, **stop**.

Never wire money. You won't get that money back.

Never send money especially by gift card or cash reload card.

Never give your financial or personal information.

Don't trust a name or caller ID. Con artists use official sounding names to make you trust them, and many go as far as spoofing real government numbers.

Put your number on the National Do Not Call Registry. Most legitimate sales people generally honor the Do Not Call list, but scammers will always ignore it. So if you do get a call, it's likely to be a scam.