TRTA Convention: March 27-29, 2017
Day at the Capitol, March 30, 2017
Reservations at the Hilton Austin
500 E. 4th Street, Austin 78701

Call 1.844.291.8931 or 512.482.8000
Use "TRT" as your reservation code
$199 plus tax: Start saving now!

Quick Blips

October 2016

TRTA'S INFORMATION AND PROTECTIVE SERVICES COMMITTEE

Mystery Phone Charges

by Federal Trade Commission

Cramming a phone bill is illegal; cramming happens when a company adds a charge for a service you did not order or use.

The company may use your phone bill like a credit card and add charges for services like trivia, ringtones, daily horoscopes or love tips to your bill that you did not agree to or use.

Make it a habit to read your monthly bill. Keep an eye out for generic-sounding fees like *Min. Use Fee, Activation, Member Fee, or Subscription.* You may not have ordered these services. Pay special attention to "miscellaneous" and "third-party" charges. Mobile phone carriers allow third-parties to place charges on your phone bill, so there may be some from anyone other than your phone company.

Your statement should tell you how to dispute charges. If you suspect you have been a victim of phone cramming, file a complaint online with the FTC or call 1-877-382-4357, that is 1-877-FTC-HELP.

Follow the Latest Scams in Your Area

No matter where you live, fraud is never far away. But, you can protect yourself by knowing what to watch out for—and by telling others about scams. Check out the AARP Fraud Watch Network scam-tracking map at <aarp.org/fraudmap>.

[Obtained from the *AARP Magazine*, September 2016, submitted by Dr. Thalia F. Matherson]

TX TRS and Office of Attorney General Pay Out $430K since 2014

The State Auditor's Office at the behest of the House Committee on General Investigating and Ethics detailed that TRS and the Office of the Attorney General paid out more than $432,000 in emergency leave to ex-employees. Presumably the agencies paid the money because they are not permitted to give severance pay, but are unrestricted in giving emergency leave for any reason and however long they want.

The Associated Press: Austin. Rpt. in *Amarillo Globe-News*, 9.17.2016. A6.

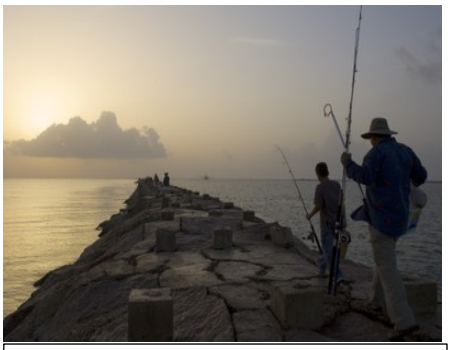
Algae Bloom

Red Tide found in Texas Waters

The Texas Parks & Wildlife Department confirmed red tide in areas of the Rio Grande Valley and near Corpus Christi. Other affected waterways include waters from Padre Island at Malaquite Beach, in the Laguna Madre, from Beach Access 6 to the Brazos Santiago jetties, and at the Isla Blanca Park boat ramp.

Red tide aerosols can cause breathing troubles in humans. The reddish bloom can kill fish and lead to shellfish poisoning in humans who consume them.

[AP: Corpus Christi, rpt. *Borger News-Herald,* 9.14.16. 4]



South Padre Island, Jetty 37, from TX Parks and Wildlife

App Developers and the Dilemma of Ad Agents Wanting Your Information

Seventy percent of American adults own smartphones. Eighty-nine percent of the time is spent on apps. App developers generate revenue by selling apps directly to users, in-app purchases, and selling ads within the apps. Consumer privacy comes in when ad developers want specific information about users. They seek permissions such as Internet access, network, state, etc. They now know your mobile devices network connections. They ask for access to your location, permission to write on your calendar, and connect to your Bluetooth devices. They want to access the vibrate function, record audio, and get a list of all registered Google and other contacts. App developers who do not ask for unnecessary consumer information make their apps less attractive to attackers.

Reduce the app's unnecessary access to your personal information.
[FTC Commission: Andrea Arias. Sept. 16, 2016]

10 Things You Can Do to Avoid Fraud

1. Spot Imposters: Scammers pretend to be someone you can trust, like a government official, a family member, a charity, or a company you do business with. Don't send any money or give out any personal information in response to an unexpected request—whether it comes from a text, phone all, or an email.
2. Do Online Searches: type a company or a product name into your search engine with words like "review," "complaint," or "scam." You can even search the phone numbers to see if other people have reported them as scams.

3. Don't Believe Your Caller ID: Technology makes it easy to fake caller ID information, so the name and number you see aren't always real. If they ask for money or personal information, hang up. If you think it may be a legitimate caller, you call a number that you know is genuine.

4. Don't Pay Upfront for a Promise: Some scammers ask you to pay in advance for debt relief, credit and loan offers, mortgage assistance, or a job.

5. Consider How You Pay: Credit cards have significant fraud protection built in. Wiring money and reloadable cards are risky. Government offices and honest companies will not require you to use these options.

6. Talk to someone you trust before you give up any personal information. Con artists want quick decisions.

7. Hang Up On Robocalls. These recorded sales pitches are illegal. Report them to the FTC.

8. Be skeptical about free trial offers.

9. Don't deposit a check and wire money back. You're responsible for depositing bad checks.

10. Sign up for free scam alerts at <ftc.gov/scams>.