

# Fraud and Scam Resources Guide

## Presented by Texas Public Employees Association

### Informative Websites (news and information on current fraud and scams)

- Texas Office of Consumer Credit Commissioner - <https://occc.texas.gov/>
- Consumer Financial Protection Bureau - <https://www.consumerfinance.gov/>
- Federal Trade Commission - <https://www.ftc.gov/>
- AARP - <https://www.aarp.org/money/scams-fraud/>

These sites offer up-to-date information on what's happening in the world of scams and fraud. They all offer resources for detecting fraud as well as contact options to report suspected fraud.

---

### If your online identity is compromised (name, email, passwords)

- Change your passwords
- Look into two-factor authentication using an authenticator app (Google Authenticator, 2FA Authenticator, Microsoft Authenticator)
- Consider switching to a random password generator for extra safety (LastPass, 1Password, Random.org)

### If your identity/financials have been compromised (name, SSN, bank account, credit/debit cards)

- Notify your identity protection provider if you have one
- Notify your bank/ freeze cards and accounts as needed
- Monitor your credit report for suspicious activity
- Notify your mortgage company/ landlord
- Notify your insurance companies (auto, health, life, etc)

**When you've been the victim of a scam, contact your local law enforcement. They can take a report and/or direct you to the best place to report.**

**Verify Everything! Scammers feed on emotional responses and often want to rush you to make a snap decision.**

- Disconnect calls demanding information/money and offer to call back
- Set up a code word with family members so you can verify their identity
- Be on guard and be skeptical