

Fraud Safety Tips



Empower yourself to stay safe, online and offline.

Top Red Flags

- Unsolicited calls, texts, or emails asking for money, gift cards, or personal info.
- Pressure to act now or keep it secret ("urgent," "don't tell anyone").
- Requests for payment by gift card, wire transfer, or crypto.
- Caller ID, email addresses, and websites can be spoofed—don't trust them at face value.

Public Wi-Fi Safety

- Avoid banking or shopping on public Wi-Fi—use your mobile hotspot or wait.
- If you must use it, ensure websites show HTTPS and use a VPN.
- Turn off Auto-Join/Auto-Connect for networks you don't control.
- Enable two-factor authentication (2FA) on important accounts.

Protect Your Home & Property

- Sign up for county property alert services to get notified of deed changes.
- Freeze your credit with Equifax, Experian, and TransUnion.
- Use strong, unique passwords and a password manager.
- Keep your devices updated and secure.

If You Think You Were Scammed

- Contact your bank or card company immediately.
- Report to the FTC at [ReportFraud.gov](https://www.ftc.gov) and [IdentityTheft.gov](https://www.identitytheft.gov).
- If it's local, contact police and your state Attorney General's office.
- Share what happened with friends to help others stay safe.

Remember: Pause before you pay, click, or share.

Stay Alert • Stay Connected • Stay Protected

