Tips to Stay Safe from Fraud & Scams

The Basics:

- Don't use public wi-fi
- Use strong, unique passwords or **phrases**
- Use Two Factor Authentication
- Keep applications, browsers, anti-malware, and anti-virus programs up to date

Gift Card Scams:

- If buying in-store, inspect the card for tampering
- Buy online directly from the merchant
- Keep receipt

Package Delivery Scams --- Recognize the red flags:

- You receive a notification (text or email) but aren't expecting a package
- Fake notifications about shipment or delivery problems
- You receive demands for payment (gift card, Bitcoin, wire) or "urgent" requests for personal information
- Guard against "Porch Pirates"

Be Safe Shopping Online:

- "Malvertising" – scams, viruses, malware, trackers hidden behind ads that sit at the top of search pages
- Google, Bing, Edge, DuckDuckGo, Safari, and Firefox are paid to put ads there so you see them first
- Don't click on search ads, scroll further down the page to real results

- Install an ad-blocker app in your browser – won't see any ads, good or bad
- Fake Websites: Unrealistic offers, shoddy page design, sloppy English, urgency to act fast
- Type in full address: "citibanklogin" – NO!! **"citi.com" –YES!!**
- Save browser bookmarks for often-used sites
- Protect yourself – proceed with caution

Be Alert for Charity Scams:

- Urgent request for action
- A phone call, text, email – spoofing an organization or a person
- Demand payment via gift cards, wire transfers, or Bitcoin
- Research: Give.org or Charitywatch.org