Common Holiday Scams & Tactics

Tax/Toll Collection Texts

These are smishing attacks.
Smishing = a fake text trying to get you to take action

AI and Deepfake

Voice tactics used to impersonate loved ones are still utilized and often effective around the holidays

Social Media Ads

Fraudsters will trick users into:
- sending funds
- sharing private data
- downloading malware



Holiday Fraud by the Numbers

Americans reported nearly **$893 million in losses** across 22,364 complaints **involving AI** in 2025** Averaged, that's a loss of **$40,000 per person**.

Nearly **30% of people** who reported losing money to a scam in 2025 said it **started on social media**.*

$2.1 billion lost to scams that started on social media in 2025.*

Americans reported **$470 million in losses** from scams that started with text messages in 2024, more than 5X the amount reported in 2020*

Seasonal Job Scams

Tips for your customers.

P **Pay**
Are they asking me to pay money to get the job?

A **Applied**
Did I apply for this position?

U **Urgency**
Am I being pressured to act immediately?

S **Sensitive Information**
Are they asking for banking, Social Security, or identity information unusually early?

E **Employer Verified**
Have I independently contacted the organization using information I found myself?

If one of those raises concern, pause before proceeding.

Gift Card Scams

Tips for your customers.

Never pay with gift cards
No legitimate business, tech company, or government agency will ever ask for gift card codes as payment.

Inspect the packaging
Check for tears, loose stickers, or scratched-off PIN areas before buying. Buy from behind the counter if possible and check the balance after purchase. Keep your store receipts as well.

Hang up immediately
If someone stays on the phone with you and pressures you to buy multiple gift cards, it is a scam.

If you sell gift cards at your branch locations this is a great time to let your cardholders know you are a trusted location for their gift card needs!