

Scam **Red Flags** You Should Know



Email

Scammers send millions of holiday-targeted emails. Watch for:

Generic greetings: "Dear Customer," "Valued Member," "Friend."

Urgency or threats: "Act now," "Final notice," "Your account will close."

Holiday bait: Fake Black Friday orders, missed deliveries, Christmas deals.

Too-good-to-be-true promises: 80–90% off, "guaranteed income systems."

Requests for personal data: SSN, passwords, one-time codes.

Link mismatch: Hover over links, if the URL doesn't match, don't click.

Unexpected attachments: "Shipping labels," invoices, statements.

Bad grammar or odd formatting: The classic scammer fingerprint.

If an email feels even slightly wrong... it probably is.



Online Ads

Fake storefronts explode during the holidays. Here's how to spot them:

Suspicious URLs: "[AmazonDeals-24.com](#)," "[Walmart-HolidaySale.net](#)."

Sloppy design: Weird logos, mismatched branding, poor English.

No physical address: Or a fake one when you check with Google Maps.

Only risky payment methods: Crypto, wire transfers, gift cards, Zelle.

Ridiculous discounts: "90% off TODAY ONLY."

AI-generated fake testimonials: Too polished, too generic.

Celebrity endorsements that feel... off: Because they are.

When in doubt:

If it doesn't accept a credit card, it's not a real store.



Pop-up & Fake Alerts

These are designed to scare you into acting fast.

Flashing warnings, sirens, countdowns.

Fake "Microsoft/Apple Security" alerts telling you to call a number.

Messages urging you to install remote-access software. BIG red flag.

Screen lock pop-ups claiming your computer is infected.

Threats of hacking or data loss to pressure immediate action.

Real companies do not communicate through browser pop-ups. Ever.



Holiday Scams

These surge between Thanksgiving and New Year's:

Fake delivery notifications ("Your package is delayed, click to reschedule")

Charity scams using emotional pressure and stolen logos

Gift card scams ("Buy discounted cards!" or "Pay using gift cards")

Grandparent/emergency scams using AI voice cloning to mimic loved ones

If someone asks you to pay fast, pay emotionally, or pay differently, pause.

Your future self will thank you.

When something online feels wrong, use this: Rushed - Secret - Strange - Surprise Money

See one of these, stop immediately. Does it make you feel rushed? Are you asked to keep it secret? Does something feel strange or "off"? Are you promised money or massive savings?

If yes → Walk away before you pay.

Brought to you by
Retire & RISE

