



## Top Scams Targeting You in 2025

As we head into 2025, scams are becoming increasingly sophisticated, preying on people's trust, emotions, and financial concerns. Staying informed about these schemes can help you avoid becoming a victim. Scammers are becoming more innovative, but staying informed is your best defense. Trust your instincts, research thoroughly, and remember that legitimate businesses or individuals will never pressure you into quick decisions or payments.

- **Employment Scams** – With the rise of remote work, scammers pose as employers offering too-good-to-be-true job opportunities. Victims are often asked to pay upfront fees for training or equipment, only to discover the job doesn't exist. *How to Protect Yourself:*
  - Verify the company and job listing through official channels, like the company's official website.
  - Never pay for job-related expenses. Legitimate employers cover these costs.
- **Cryptocurrency Scams** – Crypto remains a popular target for fraudsters. Scams include fake investment platforms, fraudulent tokens, and phishing schemes to steal digital wallets. These often promise high returns with little risk. *How to Protect Yourself:*
  - Research any crypto platform thoroughly.
  - Never share wallet keys or credentials.
  - Be skeptical of "guaranteed" returns.
- **Celebrity Imposter Scams** – Scammers impersonate celebrities online, asking for donations to fake charities or offering exclusive "fan experiences" for a fee. With deepfake technology improving, these schemes are harder to spot. *How to Protect Yourself:*
  - Verify social media accounts for the blue checkmark.
  - Never send money to someone claiming to be a celebrity.
- **Tech Support Scams** – Fraudsters pretend to be from trusted tech companies, claiming your device is compromised. They might ask for remote access or payment to "fix" nonexistent issues. *How to Protect Yourself:*
  - Never respond to unsolicited tech support calls, emails, or pop-ups.
  - Contact companies directly, using only official information, if you're concerned about your device.
- **Card Declined Scams** – This new scam targets businesses and customers. Fraudsters claim a card transaction has been declined and trick victims into paying via alternative methods, like a peer-to-peer payment app. In these instances, both the "declined transaction" and peer-to-peer transactions actually go through. *How to Protect Yourself:*
  - Always double-check declined transactions directly with your bank.
  - Use secure payment methods and avoid giving out financial information to strangers.