



# DON'T BE A TARGET

# Top Scams to LOOK For in 2025

A scam is any illegal mechanism used by an individual or entity to get money or some other benefit from another individual or entity. In 2025, scams have become increasingly sophisticated, preying on people's trust, emotions and financial concerns. Staying informed about these schemes can help individuals to avoid becoming victims. Scammers have become much more innovative, however being informed is always the best defense against them. This year, the Financial Services Regulatory Commission (FSRC) is urging everyone to become more *scam savvy* on whatever platforms they use, from emails and Facebook to suspect calls and text messages.

## EMPLOYMENT SCAM

With the rise of remote working opportunities, scammers pose as employers offering too-good-to-be-true job opportunities. Victims are often asked to pay upfront fees for training and equipment, only to discover that the job or even the company does not exist.



## STAYING SAFE FROM EMPLOYMENT SCAMS

- Always verify the company and job listing through official channels, for example, the company's official website.
- Never pay for job-related expenses such as training. Legitimate employers cover these costs.
- Do not send personal and banking information or any funds in response to these advertisements.

## CRYPTOCURRENCY SCAM

Cryptocurrency 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. Signs of cryptocurrency scams include poorly written advertisements, excessive marketing pushes and get-rich-quick claims.

## STAYING SAFE FROM CRYPTOCURRENCY SCAMS

- Research any crypto platform thoroughly before using or investing.
- Never share wallet information or credentials.
- Be suspicious of "guaranteed returns".

## CELEBRITY IMPOSTER SCAM

In this scam, scammers impersonate celebrities online, asking for donations to fake charities or offering exclusive fan experiences for a fee. With deepfake technology (images, videos or audio which are edited and depict real or non-existent people) improving, these imposter schemes are now harder to detect.



## STAYING SAFE FROM CELEBRITY IMPOSTER SCAMS

- Never send money to someone claiming to be a celebrity.
- Always verify social media accounts for the blue checkmark. This signifies that the account belongs to a legitimate person or entity, like a celebrity, brand or public figure, and is considered authentic by the platform. It is a visual cue that helps users to identify real accounts and avoid imposters.

### TECH SUPPORT SCAM

Tech support scams are when scammers pretend to offer technical support services to trick you into paying for unnecessary services or giving them access to your computer.

#### **How they operate:**

Scammers may create fake pop-ups that look like error messages or help lines. They may also call and pretend to be from a reputable company.

### STAYING SAFE FROM TECH SUPPORT SCAMS

- Never respond to unsolicited tech support calls, emails or pop-ups.
- Contact companies directly, using only official information, if you are concerned about a legitimate fault.



### CARD DECLINED SCAM

This new scam targets businesses and customers. Fraudsters claim that a credit or debit card transaction has been declined and trick victims into paying via alternative methods like a peer-to-peer payment application. In these instances, both the 'declined transaction' and peer-to-peer transactions were actually processed.



### STAYING SAFE FROM CARD DECLINED SCAMS

- Always double-check declined transactions directly with the bank.
- Use secure payments and avoid giving out financial information to strangers.

### IMMIGRATION SCAM

Scammers love nothing more than a desperate and vulnerable person looking for help online. They reach out to individuals via social media with offers to help with immigration-related paperwork and then request money using a money transfer service. The scammers then seal the deal by posing as immigration officers in video calls on WhatsApp or Zoom.

### STAYING SAFE FROM IMMIGRATION SCAMS

- Be suspicious of anyone promising quick or guaranteed results.
- Always verify the legitimacy of any immigration service provider.

### SIGNS OF A POTENTIAL SCAM ATTEMPT

- 1) You have been asked to wire money or send cheques and money orders by courier or overnight delivery. Scammers request these routes so they can get the money before you realize you have been cheated.
- 2) You have been asked to pay before collecting winnings. Legitimate sweepstakes do not require payments for insurance, taxes or shipping to claim a prize.
- 3) They claim to be employed by a government agency. Scammers may try to tell you they work with the Federal Bureau of Investigations (FBI) or Customs Department. Government agencies do not run or operate sweepstakes.
- 4) They want you to act promptly. The more time you have, the more likely that you may figure out that someone is trying to scam you.
- 5) They claim to be someone you care about.
- 6) If it seems too good to be true, it probably is..



### TIPS FOR RECOGNISING AND AVOIDING SCAMS

- 1) An offer seems too good to be true.
- 2) Communication does not appear to be genuine.
- 3) Do not send money to someone you do not know.
- 4) You have been asked for personal information.
- 5) Do not reply to email messages or phone calls that ask for financial information or Social Security numbers.
- 6) Resist the pressure to act immediately. Always tell the caller that you need time to think things through.
- 7) Do not open attachments or links that come from strange emails.
- 8) Do not agree to deposit checks from individuals that you do not know.
- 9) Research charities and other organizations before making donations.

