

FRAUD ALERT- SOCIAL MEDIA SCAM

FINANCIAL INTELLIGENCE AGENCY TURKS AND CAICOS ISLANDS



Issue No. 1/2024

The Financial intelligence Agency of the Turks and Caicos Islands has noticed an increase in the occurrence of "Social Media Scams" within the Turks and Caicos Islands. This notice is published to advise the public of this developing trend.

SOCIAL MEDIA SCAMS

Social media scams are a type of fraud that is committed via social media sites such as Facebook, Instagram, TikTok, Threads, and X (formerly known as Twitter).

Social media platforms offer unique settings for related and unrelated individuals to interact and connect. This can pose a threat to unsuspecting online individuals. Criminals can use social media channels to lure victims and scam them of their money, personal information, or identity.



HOW CAN YOU BE SCAMMED ON SOCIAL MEDIA?

Scammers can use social media to target unsuspecting individuals. These are some common methods:

- Malicious links can be sent via email or direct message to infect devices with malware.
- Fraudulent online dating scams may convince users to send funds or make fake investments.
- Ads and fake stores may be created to capture personal information, steal identities or money.
- Individuals can be tricked into sharing personal information via social media accounts.



PROTECT YOURSELF

- Use strong and unique passwords for each social media account.
- Adjust your social media privacy settings.
- Check profiles carefully before you accept friends and followers.
- Be careful of what you share online.
- Enhance your knowledge of various social media scams such as phishing scams, romance scams, job offer scams and purchase scams.
- Avoid clicking on suspicious links in direct messages, emails, posts, or text messages.
- Hover over links received from people you know to examine the URL before clicking the link. Refrain from clicking on misspelled web addresses.

Report suspicious online fraud activity to the Royal Turks and Caicos Police Force.