Protect yourself from online scams

1. Verify the caller’s identity. If someone claims to be from a Law Enforcement Agency, do not engage over video calls or transfer money.
2. Government agencies do not use platforms like WhatsApp or Skype for official communication. Verify their identity by directly contacting the relevant agency.
3. Do not panic, as scammers use fear and urgency to manipulate victims. Take a moment to assess the situation calmly before responding.
4. Never disclose sensitive personal or financial details over the phone or video calls, especially to unknown numbers. Avoid sharing personal information.
5. Never install remote access software on your device for anyone: This software gives individuals complete control over your device, creating a significant security risk.
6. Do not transfer money under pressure: Legitimate Law Enforcement Agencies will never pressure you into sending money immediately. If someone demands money over the phone or online, it’s most likely a scam.
7. Staying vigilant and informed is crucial to protect yourself from this emerging cyber threat. By being aware of the tactics used by scammers and taking necessary precautions, you can minimize your risk of falling victim to online scams.
8. Avoid clicking on links or attachments from unknown senders. Instead, enter the organization's URL directly in your browser or use bookmarks. Always verify the legitimacy of the links and emails. For example, check for spelling and grammatical errors in the URL, or whether the sender is trustworthy.
9. Carefully consider before providing personal information to any person or organisation. If the website does not use HTTPS for encryption, please be careful and do not provide sensitive information.
10. Do not install apps shared by unknown individuals. Download apps only from official app stores to avoid malware.
11. Do not share your device with strangers.
12. Verify call forwarding and mobile settings in case you accidentally share your device with strangers.
13. If you experience a sudden loss of service, report it immediately to your provider, as it may indicate a SIM swap attempt.
14. Regularly monitor your bank and credit card statements for unauthorized transactions.
15. Never pay for job offers. Verify job postings and companies before applying or providing personal data.
16. Verify requests for urgent money transfers by calling directly your relatives/friends.

17. Always remember, you don't need a UPI PIN or OTP to receive money.
18. Verify the sender’s banking name before making payments using QR codes.
19. Carefully review the loan terms, including interest rates and fees. Be wary of apps that use vague or confusing language.
20. Always use genuine and up-to-date software.
21. Stay informed about common scams and tactics used by fraudsters to better protect yourself.
22. Report suspicious activity: If you suspect you’ve been targeted by any online scam and you gave sensitive information, don’t panic — reset your credentials on sites you've used them and then report it to the police **dialling 1930** and cybercrime authorities immediately.