

- Beware of offers for cheap travel that are 'too good to be true'
- Only buy from trusted sources. For Internet purchases, make sure you use the Internet security protocol called 3D Secure - Verified by Visa/SecureCode/SafeKey. Ask your bank or your card issuer about it
- Your bank/your credit card issuer will never ask you to disclose your complete card number or account details in an email or over the phone
- Keep your debit/credit cards safe, don't write or store your PIN code. Protect your cards as you protect your cash.
- Check your credit card statements upon receipt – saving your card receipts will help you verify your statement
- Consider as suspicious all emails requesting personal information
- Beware and never respond to 'phishing' emails which ask for personal details and to unsolicited propositions offering easy money
- Download files or software only from trusted sources
- Protect your PC, tablet, smartphone with strong passwords and with security programs such as anti-virus/anti-spyware
- Never write or store your passwords
- Protect your computer when using WIFI in public places – unprotected use can reveal personal information you send