DIGITAL FOR LIFE

Staying Safe Online

4 common scams

Banking-related Phishing Scam

- Scammers pretend to be from the bank;
- Ask for your internet banking usernames, Personal Identification Numbers (PIN) and OTP.

Example of scam SMS:

> Your 'bank' account transaction has been suspended, please update it on December 28 otherwise the account will be locked. Please access bit.ly/abc123

Loan Scam

- Scammers pretend to be a staff from a licensed moneylender;
- Usually send a SMS text or WhatsApp message offering loan services.

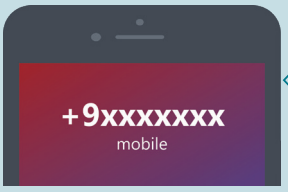
Example of scam SMS:

> PROMO Mthly Instalment Plan:
> 8.88-10.88% (Business)
> 6.88-8.88% (Personal)
> $5-300K Loan up to 60 mths
> no hidden rate
> SMS/WSAPP to xxx1231

Tech-support Scam

- Scammers pose as tech support from government or businesses.
- They will:
  - Ask for your personal information, or
  - Ask you to download a software which will give them control to your device and information, or
  - Ask you to not check your SMS, emails or Bank account for the next 24hours

Example of scam call with a "+" Sign Prefix:



> Hello, I am the tech-support of xx company. your computer alerted us that it has been infected with virus and spyware. Please download this software now to prevent your computer being locked in the next 5mins.

E-Commerce Scam

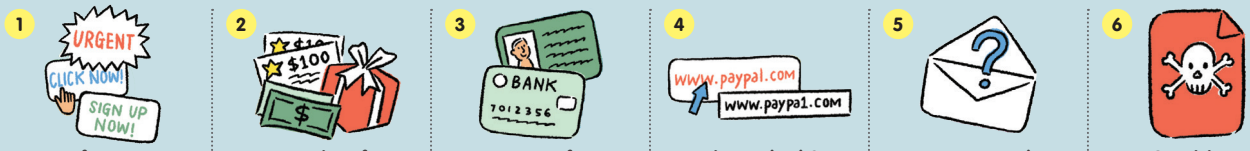
- Scammers attract you with low prices;
- Ask you to make payment in advance or tell you payment made.

Example of scam SMS:

> I have paid for your item but the money is locked on your account. You will need to go to the email I've sent to your email account to accept the money.

Phishing is a method used by cybercriminals to trick victims into giving out your personal and financial information such as passwords, One Time Passwords (OTPs) or bank account numbers.

Learn the 6 signs of phishing



https://go.gov.sg/csa-spotssignsofphishing

Dos & Don'ts to protect yourself against online scams

1. Enable 2-factor authentication (2FA) where available. Besides internet banking, 2FA is available for social media, email, shopping, and government accounts.
2. Always verify suspicious calls or messages by calling government/business official hotline or official app/website directly.
3. If the message from your family and friends is suspicious, call them directly to check if they have sent the message.
4. Set strong passwords using uppercase and lowercase letters, numbers and symbols. Use words that relate to a memory unique to you to form a phrase e.g. **IhadKAYAtoastAT8AM**!
5. Download and Set-up Scamshield app from Apple App Store. *(Android coming soon)*. https://go.gov.sg/scamshield-setupguide

A list of trusted government-related websites can be found at **www.gov.sg/trusted-sites**.

Visit **www.scamalert.sg** for more info or call the Anti-Scam helpline at **1800-722-6688** for scam-related advice.

1. **DO NOT** immediately click on links in message or emails that claim to be from the government or from a legitimate business when you receive them.
2. **DO NOT** share your personal or financial information, passwords and OTPs.
3. **DO NOT** call the sender directly through the contact details given in an unsolicited email or text message. First check the contact number on the official website.
4. **DO NOT** panic when you receive an unsolicited urgent advertisement or message to follow some instructions. Delete and block user, and report the messages on the platform.

Credit: Singapore Police Force and Cyber Security Agency of Singapore

An initiative by:

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

Supported by:

SG :DIGITAL OFFICE