Better Cyber Safe Than Sorry

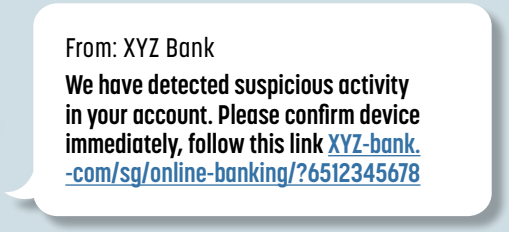
Types of online scams

1 Impersonation scams

Pretending to be employees from reputable organisations such as government agencies, banks or telcos, cybercriminals will try to steal your money via a phone call, WhatsApp or SMS.

They will ask you to:

- follow urgent instructions claiming that your devices have been hacked or have technical issues
- provide your personal particulars, banking details and OTPs (One-Time Passwords) due to an issue with your bank account, or to sign up for fake offers or lucky draws



They may also pretend to be your friends, colleagues or family members and contact you on social media accounts or WhatsApp. They will claim that you have won a prize, or sign you up for lucky draws, and ask you to:

- provide your personal details; or
- forward them the OTP sent to you by mistake

2 E-commerce scams

Cybercriminals also lure you with cheap deals. They would insist on immediate payment, bank transfers before delivery or request to transact off-platform. After obtaining your money, they will be uncontactable.

Do not be a victim of online scams. Here's how.

- **DO NOT** share your personal or financial information, passwords and OTPs
- **DO NOT** call the sender directly through the contact details given in the email or text message. Only do so through the contact details listed on the official website
- **DO NOT** trust links or email addresses that claim to be from the government but do not have "**gov.sg**" in them, unless you are already familiar with them. A list of trusted government-related websites can be found at **www.gov.sg/trusted-sites**
- **DO NOT** panic when you receive an unsolicited urgent advertisement or message to follow some instructions. Call your family members or friends for advice. Visit **www.scamalert.sg** for more info or call the Anti-Scam helpline at **1800-722-6688** for scam-related advice

What is phishing?

Cybercriminals commonly use a method called "phishing" to trick victims into giving their personal and financial information such as bank account numbers, login details including passwords and OTPs.

Learn the 6 signs of phishing

1

Mismatched & Misleading Information

2

Unexpected Emails

3

Use of Urgent or Threatening Language

4

Suspicious Attachments

5

Promise of Attractive Rewards

6

Request for Confidential Information

Activity:
Spot the signs of phishing

Did you spot the 6 signs?

- Use of urgent language
- Promise of attractive rewards
- Grammatical errors
- Non-existent ministry in Singapore
- Mismatched information
- Suspicious attachments

Better cyber safe than sorry

For more information, visit Cyber Security Agency of Singapore (CSA) and the Scam Alert website.

www.csa.gov.sg **www.scamalert.sg**

Get more cyber tips at:

For the latest scam info, visit: