Recognising Scams

Your guide on how to avoid being tricked by scammers.

The different types of scams

and how to recognise them

Scams have unfortunately become more widespread in today's world. Even the most cautious person has fallen victim to unscrupulous criminals who appear to be everywhere.

We hope that this information will assist you in spotting such scams, by demonstrating how they work and how to safeguard from becoming a victim.

Table of Content

RHB

FRAUD AWARENESS
The Money Mule

The Money Mule

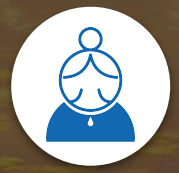
A scam where your bank account is used to facilitate movement of fraudulent funds by third parties.

Target victim segment

Students

Unemployed

Housewives



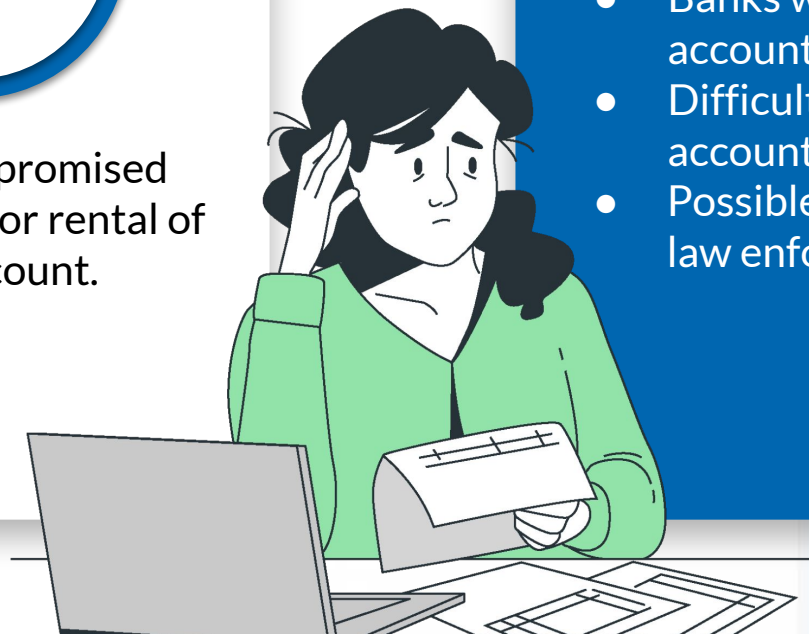
Retirees

FRAUD AWARENESS
The Money Mule

How it Works

Scammers post advertisements on **social media** looking for **accounts to "rent"**

Payment is promised every month for rental of your account.



The Consequences

- Banks will blacklist your account.
- Difficulties in opening new accounts in the future.
- Possible prosecution by law enforcement agencies.

The Investment Scam

Scammers entice you to invest your money in fake financial products or services. They will promise unrealistic profit with an emphasis on time-limited offers to pressure you into sending your money over immediately.

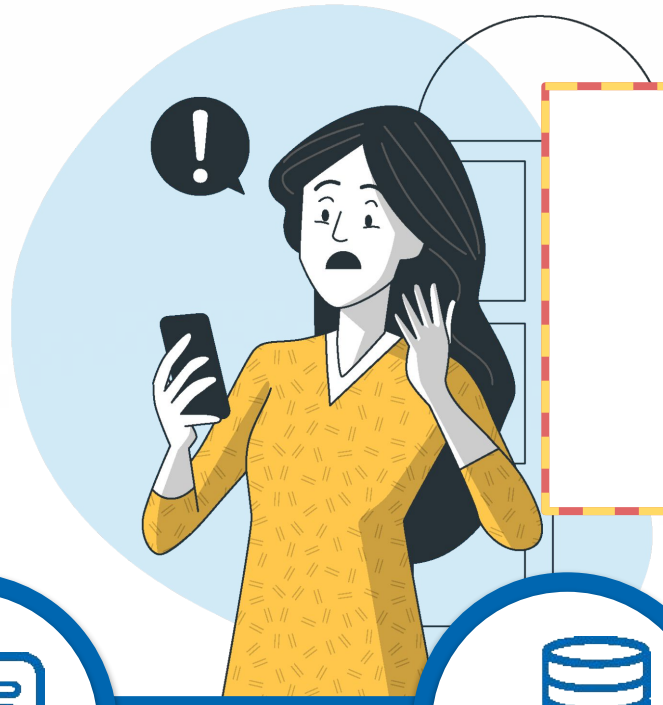
Target victim segment

Students

Retirees

FRAUD AWARENESS
The Investment Scam

How it Works



Promises of high investment returns, with little or no risk, are classic warning signs of a scam.

Investment ads are **posted on social media**, complete with reputable brand logos and **prominent ambassadors**.

The victim is required to transfer an initial amount that will generate some return to gain trust.

Subsequently, the investment amount would get higher with a promise of higher returns.

Once the higher amount is transferred, the investment agent / group will be uncontactable.

FRAUD AWARENESS
The Job Scam

The Job Scam

A scam involving fake recruiters offering attractive employment opportunities.

Target victim segment

Students

Unemployed

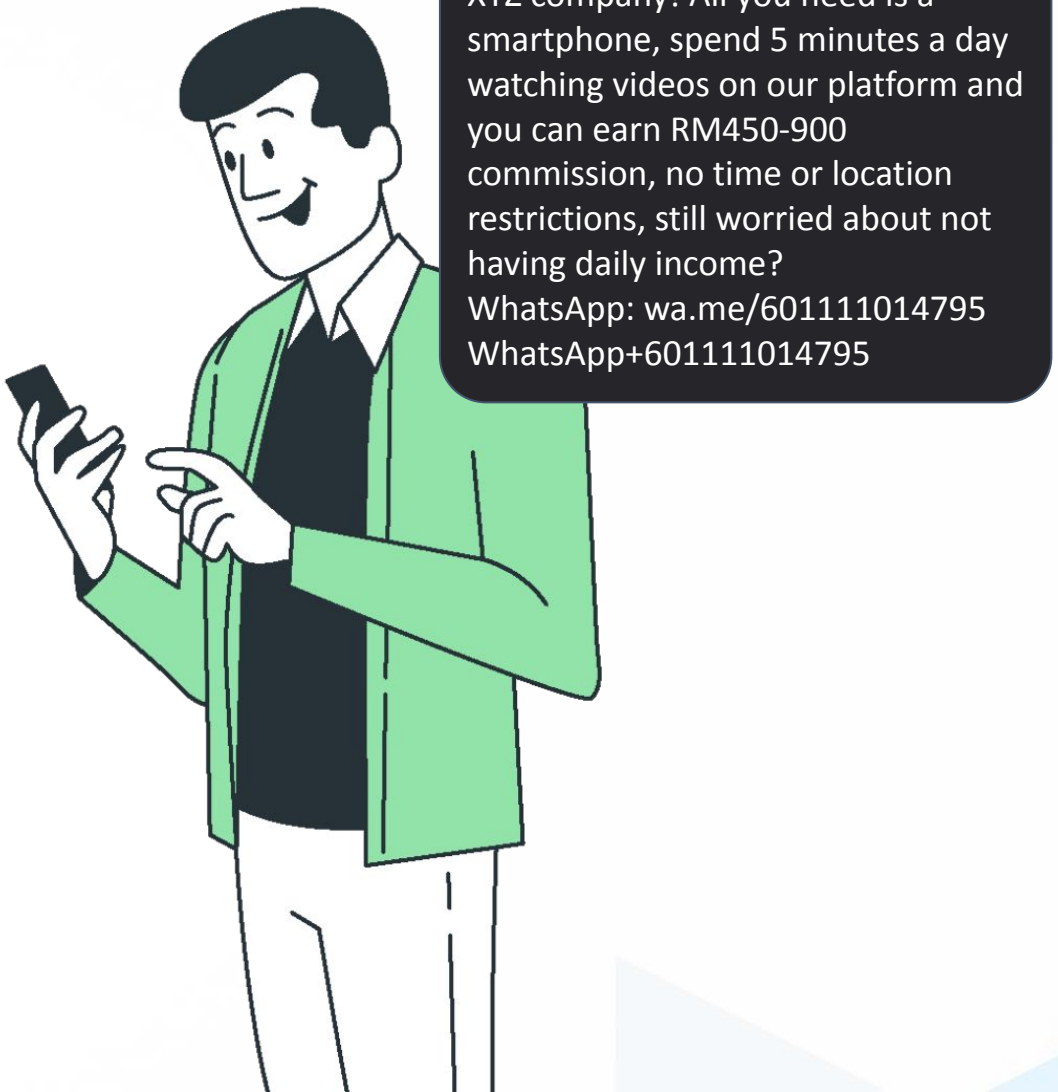
Housewives

FRAUD AWARENESS
The Job Scam

How it Works

Victim receives a text message offering a job with a **high salary** and **no experience required**.

Victim needs to pay a deposit to secure the job.



FRAUD AWARENESS
The e-Commerce Scam

The e-Commerce Scam

A scam offering unbelievably low prices on products, which are either fake or doesn't exist.

Target victim segment

Anyone/Everyone

FRAUD AWARENESS
The e-Commerce Scam

How it Works

Products are **advertised on social media** at **unbelievably low prices**.

Victim is **rushed into making payment** as "stocks" are limited.

When the parcel is received, if at all, it is not the item that was ordered.

FRAUD AWARENESS
The Kidnapping Scam

The Kidnapping Scam

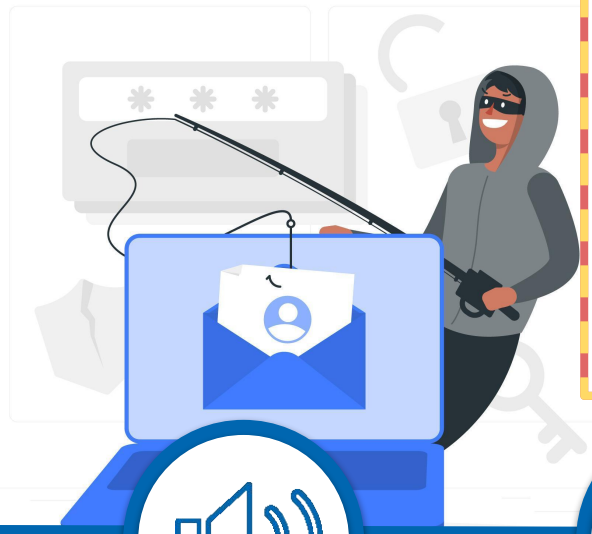
A scam where the victim is tricked into believing their loved ones have been kidnapped.

Target victim segment

Anyone/Everyone

FRAUD AWARENESS
The Kidnapping Scam

How it Works



Don't easily trust any phone call from unknown individuals. Check with the school or get confirmation from the school teacher.

1. Victim receives a call informing them their loved ones have been kidnapped.
2. Specific details, taken from social media about the loved ones are provided to ensure believability.
3. Sometimes background noise, ie recorded screams or cries, is used to create the sense of urgency and panic.
4. Victim is asked to stay on the line and not hang up or contact anyone else to ensure they cannot verify the kidnapping.
5. Ransom is demanded to release their loved ones.

FRAUD AWARENESS
The Scam App

The Scam App

A scam where victims are tricked into downloading and installing apps **(also known as Android Packed File "APK")** that give access to your online banking credentials.

Target victim segment

Anyone/Everyone

FRAUD AWARENESS
The Scam App

How it Works

You are prompted (via phone call, SMS or social media) to **download an e-form or an app** (from unofficial stores) to complete an order or claim your winnings.

Once the link is clicked, a **pop-up will appear asking for permissions**. This actually allows malware to take control of your phone.

Upon obtaining your banking details, the scammer will gain access to your online banking account to transfer your funds out.

Types of Dubious Advertisements

- Job/Part time Vacancy
- Fake Investment Opportunity
- Fake seller
- Cleaning Services Scam
- Wedding Invitation

FRAUD AWARENESS
The Macau Scam

The Macau Scam

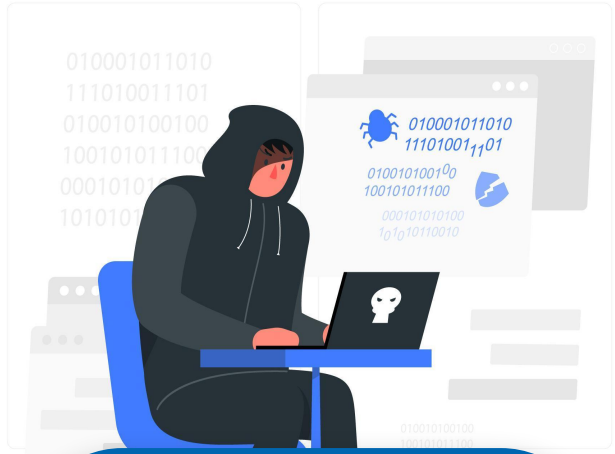
A scam where the victim is tricked into disclosing their personal banking details or transfering money into another third-party account by someone impersonating police, government or bank official.

Target victim segment

Anyone/Everyone

FRAUD AWARENESS
The Macau Scam

How it Works



Victim **receives a call** claiming to be their bank (or Government Agencies) asking them to confirm an unauthorized credit card transaction.

The call is **transferred to the "Police"** asking for **personal banking information**.

The "Police" suggest transferring their funds into a **"Safe Account"** to **'facilitate investigations'.**

Scammers often imitate:

- Police officer
- Bank officer
- Financial regulatory officer
- Postal officer
- LHDN/Tax officer

FRAUD AWARENESS
The Love Scam

The Love Scam

A scam where vulnerable victims looking for love on online dating app are manipulated into parting with their money.

Target victim segment

Anyone/Everyone

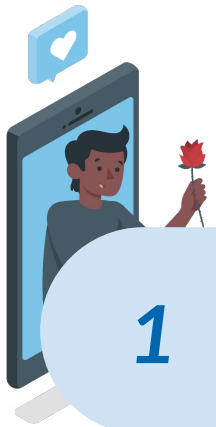
FRAUD AWARENESS
The Love Scam

How it Works

The scammer takes on a **fake online identity** on online dating apps.

Once matched the scammer **sweet talks the victim** into trusting them.

After trust is gained, the scammer **manipulates the victim** into believing they are in financial difficulty and **persuades the victim** into sending them money.



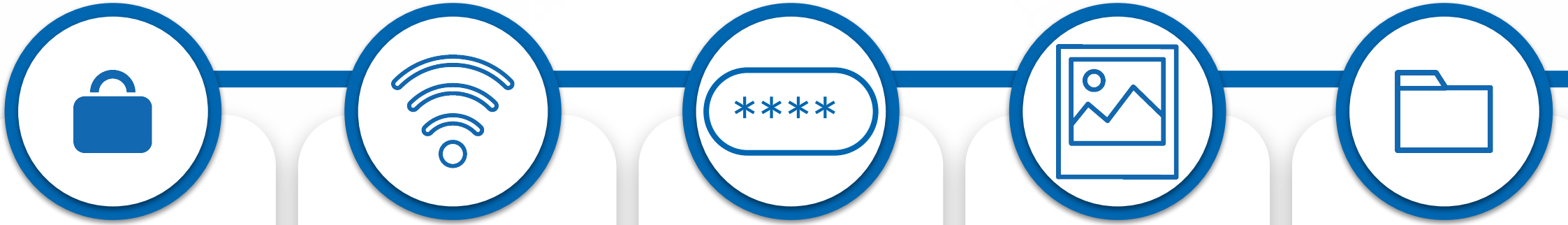
Red flags of a Love Scam

1. They are **not in the same geographical location** and most of the time claim to be **overseas**.
2. Their profile always appears **too good to be true**.
3. They'll **never** want to see you in person.
4. They constantly **present themselves as very successful individuals** with a **variety of businesses ventures**.
5. They **will** claim to be in a tight spot and **will** need financial assistance.

FRAUD AWARENESS
Online Security Tips

Online Security Tips

FRAUD AWARENESS
Online Security Tips



Always ensure the bank's website is secure with a **padlock icon** "🔒" or " **https://** "

Avoid using **public access Wi-Fi** when accessing your online banking account.

Never create a **password that contains details** from your name, initials, or date of birth.

Always ensure your **security image/security word** are correct before entering your password.

Do not share your online banking credentials **(User ID & Password)** with anyone.

FRAUD AWARENESS
Online Security Tips

Do not respond to any **unknown messages or suspicious links**.

Do not store or save your **passwords** on the device or browser.

Ensure mobile apps are **downloaded from official** or **trusted platforms**.

Check your banking **transaction activities regularly**.

Do not download any **personal documents** when you login from shared devices.

What to do?

If you suspect you have been scammed, immediately call :

RHB Contact Centre at **03-9206 8118** and **"Press 1"** for Lost, Stolen & Fraud.

Or the **National Scam Response Centre (NSRC)** at **997** (between 8am - 8pm daily including weekends and public holidays).