The HSBC Guide to Scam Awareness

Digital safety starts with knowing the signs and how you can protect yourself.

Spot the traps.
Stay protected.

HSBC

Contents

HSBC

Phishing Scam
Protect Yourself from Fake Messages and Links

Phishing is a scam where criminals send fake messages that look like they come from trusted sources to trick you into revealing sensitive information.

They often impersonate:

- Banks or e-wallet providers
- Online platforms or government agencies
- Delivery or courier companies

The ultimate goal is to steal your:

- Login credentials
- OTPs or transaction codes
- Debit or credit card information, including CCV

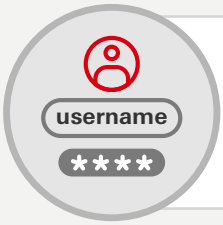
HSBC/HSBC Amanah will never contact you by email/phone/sms to ask you to confirm your username, password or account numbers.

How it works

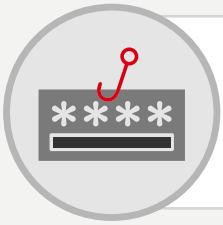
Phishing usually starts with a message containing a link. When you click it:

1. 

You are directed to a **fake website that looks legitimate.**

2. 

You may be asked to **enter passwords, OTPs, or card details.**

3. 

Scammers immediately **capture the information and use it for fraud.**

THESE MESSAGES CAN ARRIVE VIA:

Online ads on social platforms

Messaging apps like WhatsApp or Telegram

Email

SMS (sometimes called "smishing")

They often use urgency, fear, or excitement to pressure you into acting quickly.

HSBC

How to protect yourself

- Pause and validate the sender before you click, reply, or pay.
- Never click links or open attachments from unknown sources.
- Type the official website address directly into your browser.
- Call the official company hotline to verify messages.
- Enable transaction notifications for your accounts.
- Keep your devices and apps updated.

Your OTPs and passwords are for you only.
No legitimate company will ask for them.

HSBC

Red flags to watch for

Requests for **OTPs, passwords**, or **full card details**

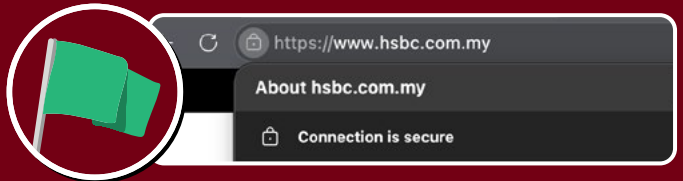
Messages with **urgent or threatening language** ("Your account will be suspended!")

Messages about **transaction/request you did not initiate**

Slightly **misspelled website addresses** or **fake URLs**

Hyperlinks that look genuine but lead to a different (fraudulent) website

Looks like an HSBC link, but the **real URL is different** when you hover / press-and-hold.



HSBC secure link: **the URL matches HSBC** and shows a secure connection (padlock).

TIP: Transaction alerts add an extra layer of awareness by notifying you when credit card transactions happen, helping you detect suspicious activity early. Read more about SMS transaction alerts to see how it works.

REMEMBER: Scammers rely on urgency. If a "deal" is pushing you to pay immediately, take a moment to verify before you proceed.

HSBC

Impersonation Scam
When Scammers Pretend to Be Someone You Trust

Impersonation scams occur when criminals pretend to be someone trustworthy to trick you into revealing personal information or transferring money.

Scammers may claim to be:

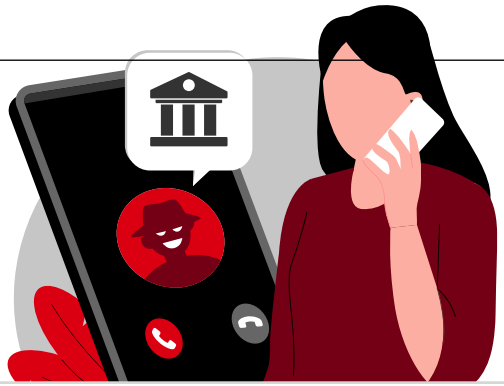
- Bank officers
- Police or government officials
- Court representatives
- Delivery staff
- Even family members or friends

Their goal is to create urgency or fear so that you act without thinking.

HSBC

How it works

Impersonation scams often follow this pattern:



1. You receive a call, SMS, or message **from someone claiming authority**.
2. The scammer says there is a **serious problem or emergency**.
3. They pressure you to **act immediately**, often by transferring money or sharing sensitive information.
4. You comply because of **fear, urgency, or trust**, and the scammer takes your money or data.

COMMON TACTICS INCLUDE:

- **Threatening** arrest or legal action
- Claiming **unusual transactions** on your account
- Requesting **"confidential"** transfers
- **Pretending** a loved one is in **urgent trouble**

HSBC

How to protect yourself

- Hang up and call official numbers from verified sources.
- Never share OTPs, passwords, or full card details.
- Do not transfer money under pressure.
- Verify any emergency directly with family members or authorities.
- Stay calm, scammers rely on panic to trick you.

Legitimate authorities **never ask for money over the phone** or demand secrecy.

Red flags to watch for

- The caller **pressures you to act** immediately.
- You're **told to keep** the situation **secret**.
- You're asked to **transfer money to unfamiliar accounts.**
- The caller is **aggressive** or **threatening**.
- The contact method is **unusual or inconsistent** (for example, WhatsApp instead of the official hotline).

TIP: If you're unsure whether a call or message is genuine, use HSBC Malaysia's Security Centre (Safeguard) to learn how to verify communications and protect yourself from common scam tactics. Read more about Safeguard to see how it works.

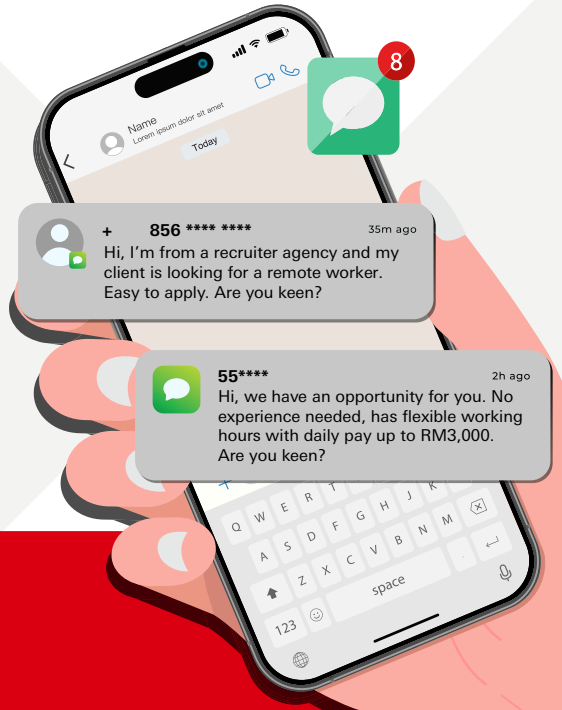
REMEMBER: HSBC will never ask you to share your passwords, OTPs, or security codes, even if the caller sounds convincing.

HSBC

Job Scam

When a Job Offer Becomes a Financial Trap

Job scams are fake employment opportunities designed to trick job seekers into giving money or sensitive information.

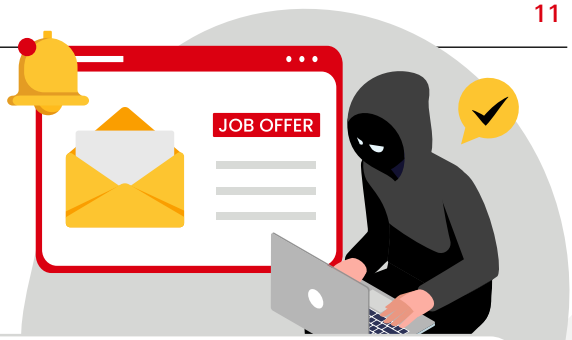


Scammers often target people who are:

- Between jobs or not earning
- New graduates
- Seeking flexible or extra income (especially remote)
- Looking for work

They promise **high pay, flexible hours, or "easy work,"** but the job either does not exist, or requires upfront payments.

HSBC



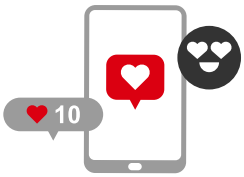
How it works

Job scams often follow this pattern:

1. You spot a **"too good to miss"** job posting or are contacted directly through email, messaging apps, or social media ads.
2. The role is pitched as **easy**, **flexible work-from-home** tasks.
3. The scammer requests personal details or payment for **"training," "equipment,"** or **"processing fees."**
4. You may initially receive small payments or **false confirmations** to build trust.
5. Eventually, you are asked to **pay more or transfer money**, and the job disappears.

COMMONLY USED ROLE TITLES INCLUDE:

Data Entry Clerk



Social Media Assistant

Personal Assistant

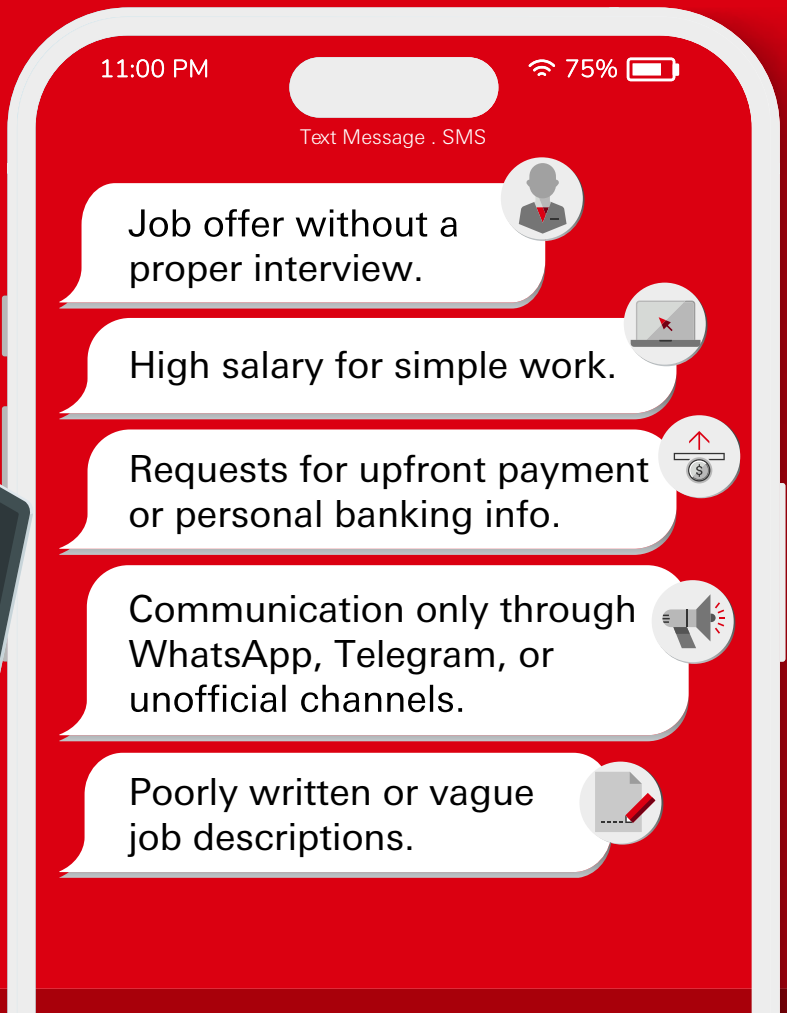
HSBC

How to protect yourself

- Research the company independently and verify their HR contacts.
- Never pay upfront fees for a job.
- Protect your personal information (ID numbers, bank details).
- Be cautious of unrealistic salaries or immediate start promises.

REMEMBER: A legitimate job will never require you to pay to start working.

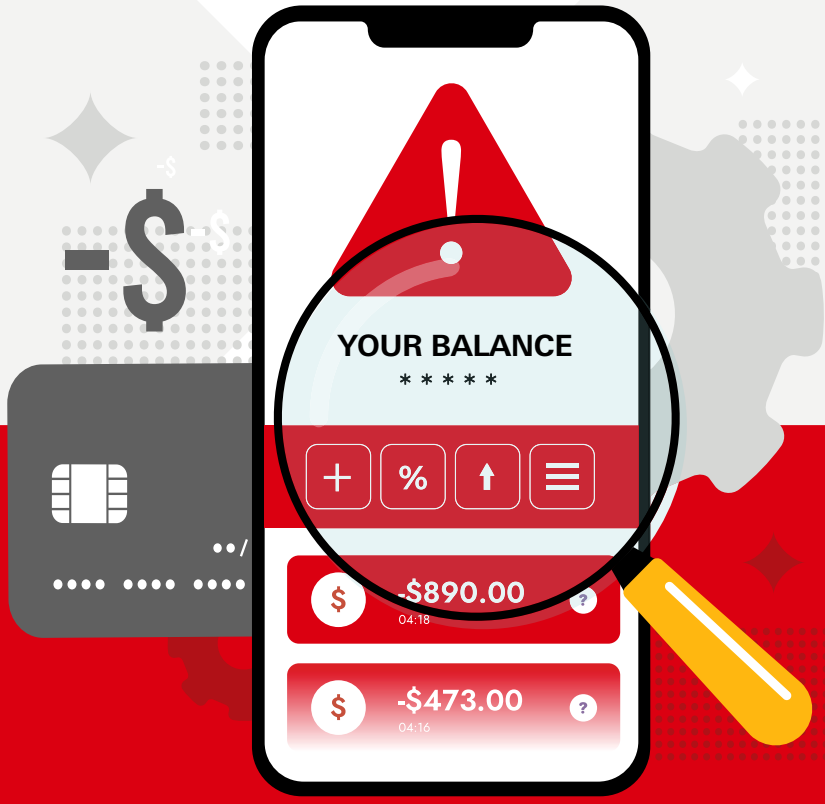
Red flags to watch for



HSBC

Money Mule Scam
When You Rent Your Bank Account for a Fee

A money mule is someone whose bank account is used to transfer or receive money on behalf of criminals.



Being a money mule can make you legally responsible for illegal activity.

Scammers often target:

- Students
- Job seekers
- People looking for side income

They make **the opportunity** seem safe and legitimate.

HSBC

How it works

Money mule scams usually happen like this:

1. You are recruited through a **"job" or payment** processing offer.
2. You are asked to **receive** money in your account and **transfer** it elsewhere.
3. You may be told it is **"safe"** or that you will **earn** a commission.
4. The money you handle is **linked to fraud, scams, or illegal activity**.

COMMON TACTICS INCLUDE:

- "Payment processing" roles
- Renting out your account for "commission"
- Job scams that later involve moving funds

Even if you don't steal the money yourself, your account is being used for crime.

HSBC

How to protect yourself

- Never share your bank account for unknown purposes.
- Avoid offers that require transferring money for someone else.
- Reject jobs or opportunities that involve handling others' funds.
- Keep full control over your banking access.

Legitimate companies will not ask you to use a personal account for business transactions.

Red flags to watch for

- Requests to use your personal bank account for "company transactions."
- Promises of easy commission for transferring money.
- Lack of clear company information.
- Pressure to act quickly.
- Payments coming from unknown or suspicious sources.

If money is moving through your account and you don't fully understand why, stop immediately.

HSBC

Investment Scam
High Returns That Can Cost You Everything

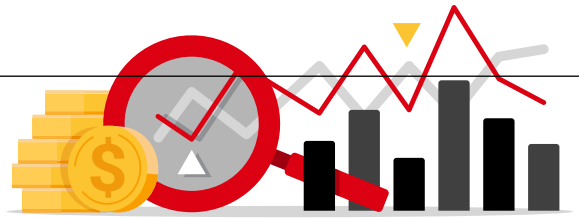
Investment scams are fraudulent schemes that promise quick, guaranteed profits with little or no risk.

They often appear professional, with:

- Polished websites
- Fake testimonials
- "Expert" guidance

The goal is to get you to invest money that you will never get back.

HSBC



How it works

Investment scams typically follow this pattern:

1. You are approached with a **lucrative opportunity**, via **social media, messaging apps**, or **emails**.
2. You are told to make a payment or transfer to a **nominated account or platform controlled by fraudsters**, supposedly to invest.
3. **Fake profits** may be shown to build trust.
4. Fraudsters may **pay you small, early profits** to win your confidence and encourage you to invest even more.
5. When you try to withdraw, your **access is blocked** and the fraudsters disappears.

COMMON TYPES INCLUDE:

- Guaranteed high-return schemes
- Fake investment platforms or trading apps
- Social media investment groups
- Celebrity or influencer impersonation

How to protect yourself

- Verify companies through official regulators.
- Avoid unsolicited investment offers online.
- Never rush into investments. Take your time to research.
- Be wary of pressure tactics and “limited-time” opportunities.

Legitimate investments carry risk and allow transparent withdrawals.

Red flags to watch for

- Promises of guaranteed returns or “no-risk” investment.
- Pressure to invest quickly.
- Unlicensed or unverified platforms.
- Requests to transfer money to multiple personal accounts.
- Communication done only through messaging apps.

If it sounds too good to be true, it probably is.

HSBC

E-Commerce Scam

When Online Stores Trick You

E-commerce scams happen when fake sellers or online stores trick you into paying for items that never arrive or are not as described.

These scams often appear on:

- Social media marketplaces
- Fake websites
- Messaging apps
- Online ads

The goal is to get your money or steal your payment information.

HSBC

How it works

E-commerce scams typically follow this pattern:

1. You see a product or promotion that **looks real and appealing**.
2. You are **asked to pay** via bank transfer, e-wallet, or outside a secure platform.
3. The product **never arrives**, or you **receive counterfeit items**.
4. The **scammer disappears**, often with no way to recover your money.

COMMON TACTICS INCLUDE:

Fake online stores copying real brands

Social media sellers asking for direct payment

Off-platform payment requests

HSBC

How to protect yourself

- Buy only from verified and trusted sellers.
- Use secure payment platforms that offer buyer protection.
- Avoid sending money directly to unknown accounts.
- Check reviews and seller history carefully.
- Compare prices to avoid deals that seem too good to be true.

Using official channels greatly reduces the risk of losing money.

Red flags to watch for

If something feels rushed or suspicious, step back before paying.

Seller insists on **payment outside the platform.**

No clear contact information for the seller.

Website looks polished but **doesn't stand up to verification.**

Prices far **below market value.**

Newly created accounts or suspicious websites.

TIP: Turning on transaction alerts can help you spot unrecognised credit card activity quickly, so you can act faster if something doesn't look right. Read more about SMS transaction alerts to see how it works.

REMEMBER: If a seller pressures you to pay outside a trusted platform, pause, once money is sent, it can be difficult to recover.

HSBC

Shopping Scam
When "Amazing Deals" Are Too Good to Be True

Shopping scams trick shoppers with flash sales, limited-time promotions, or huge discounts to get them to pay for products that aren't real or steal their payment information.

These scams often appear on:

- **Social media ads**
- **Fake websites**
- **Messaging apps**
- **Email promotions**

Unlike general e-commerce scams, shopping scams focus on **urgency and excitement** to make you act fast.

How it works

Shopping scams typically work like this:

1. You see an **attractive deal**, “90% off” or “limited stock!”
2. You are redirected to a **fake checkout page** or asked to pay via unsafe methods.
3. Once payment is made, the product **never arrives or the site disappears**.
4. Scammers may even request **multiple “additional payments”** for shipping or handling.

COMMON TACTICS INCLUDE:

- **Fake brand** promotions
- Sponsored social media **ads directing to fake sites**
- Flash sale scams with **countdown timers**

HSBC

How to protect yourself

- Always shop from verified sellers or official brand websites.
- Avoid deals that push you to act immediately.
- Never pay outside secure payment platforms.
- Check reviews, website URLs, and seller history carefully.
- Compare prices to see if the deal is realistic.

A legitimate sale **will not pressure you to pay instantly** or bypass secure payment channels.

Red flags to watch for

- **Unrealistically low prices** for high-demand items.
- Seller asks for **direct bank transfer** or **e-wallet payment.**
- **Newly created accounts** or suspicious websites.
- **Poorly designed sites** with broken links or missing contact info.
- Urgency cues like countdown timers or **“only a few left”** messages.

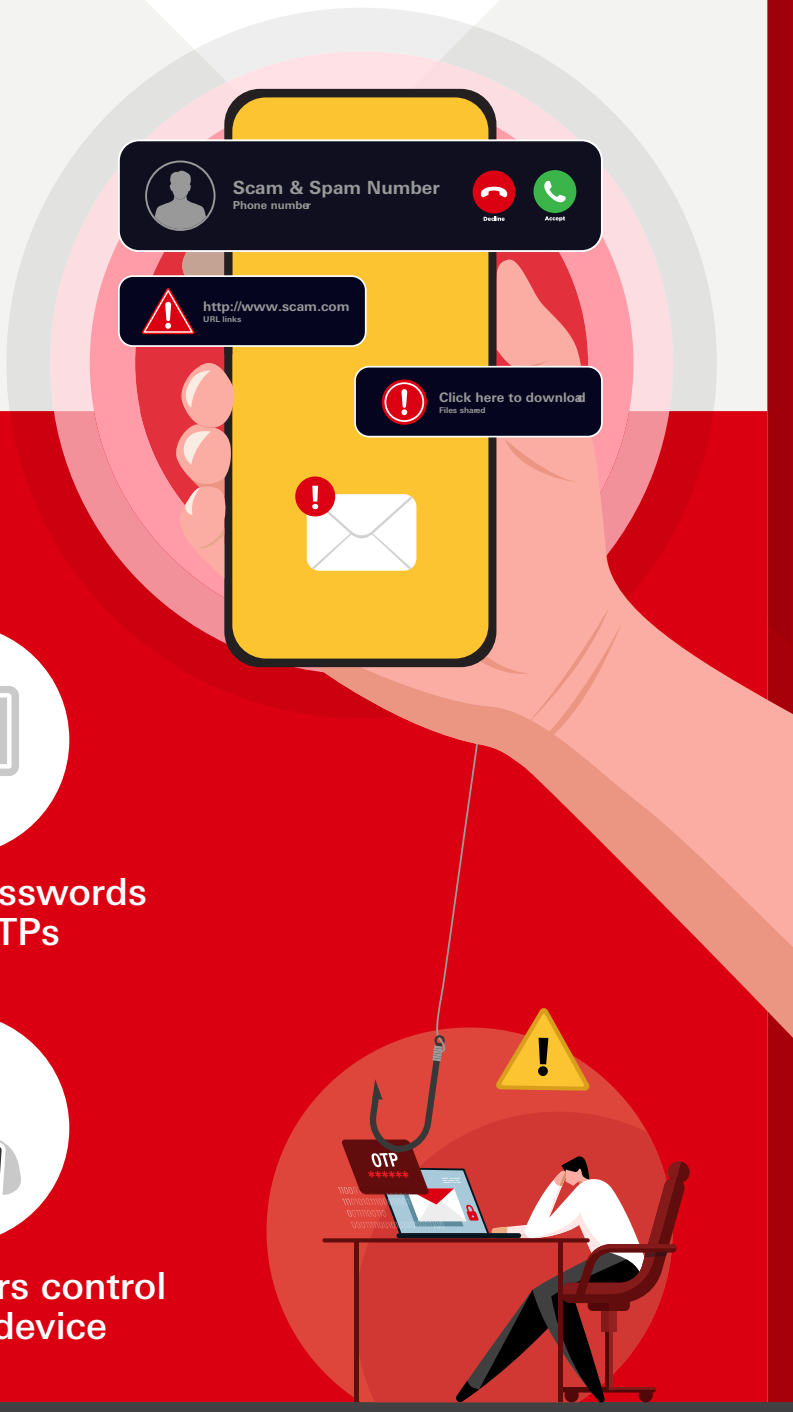
TIP: Transaction alerts add an extra layer of awareness by notifying you when credit card transactions happen, helping you detect suspicious activity early. Read more about SMS transaction alerts to see how it works.

REMEMBER: Scammers rely on urgency. If a “deal” is pushing you to pay immediately, take a moment to verify before you proceed.

HSBC

Malware Scam
When a Simple Download Can Compromise Your Device

These scams often appear as apps, files, or links that seem legitimate but are designed to harm your device.



Malware scams trick you into installing harmful software that can:

- Steal your banking information
- Capture passwords and OTPs
- Monitor your activity
- Give scammers control over your device

HSBC

How it works

Malware scams typically follow this pattern:

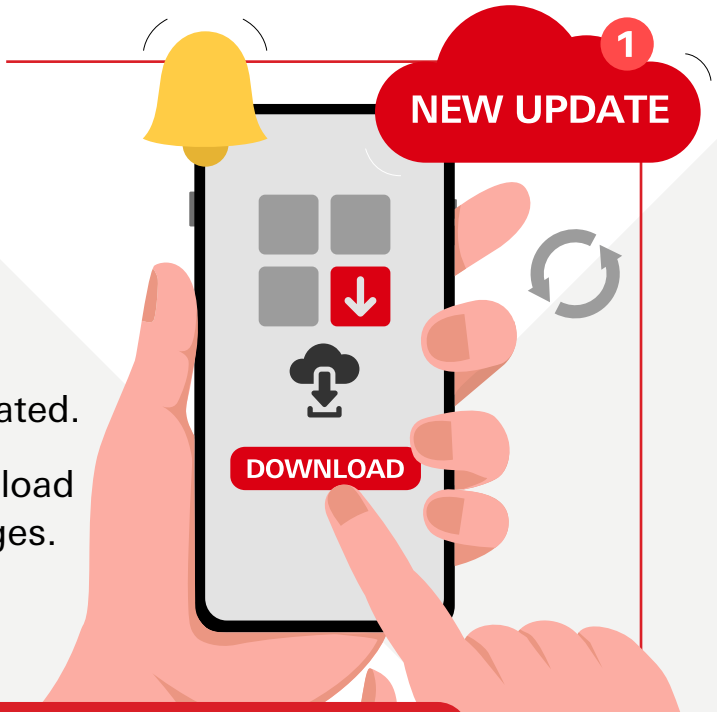
1. You are asked to **download an app**, file, or software for a "service" (e.g., parcel tracking, job tasks, or security verification).
2. The file **installs secretly and runs** in the background.
3. **Scammers collect sensitive information** like login credentials, card details, or personal data.
4. The malware may **spread further** or give scammers **remote access** to your device.

COMMON TACTICS INCLUDE:

- Fake apps on unofficial app stores
- Fake updates or security alerts prompting you to install software
- APK or file downloads from unknown links

How to protect yourself

- Only download apps from official app stores.
- Do not install apps or files from unknown links.
- Keep your device software updated.
- Avoid clicking suspicious download links in emails, SMS, or messages.
- Check app permissions before installing.



Think twice before installing anything, your device is the first line of defence.

Red flags to watch for

- Requests to download apps from unknown sources.
- Apps asking for excessive permissions.
- Instructions to disable security settings.
- Files with unfamiliar extensions (e.g., .apk from unknown websites).
- Messages urging immediate installation.

TIP: Keeping your phone protected starts with safe download habits. HSBC Malaysia's Android malware safety measures share practical steps to reduce the risk of malicious apps and links. Read more about Android Malware Safety Measures to see how it works.

If a download seems suspicious or comes from an unverified source, do not install it.

REMEMBER: Don't install apps or files from unknown links, and never disable your device's security settings at someone else's request.

HSBC

Device Takeover Scam
When Scammers Take Control of Your Phone or Computer

Device takeover scams happen when scammers gain remote access to your phone, tablet, or computer.

Once they have control, they can:

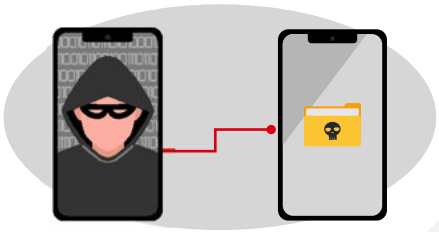
- View your screen in real time
- Access your banking apps
- Capture passwords and OTPs
- Perform transactions without your knowledge

This can lead to immediate financial loss and compromised personal data.

HSBC

How it works

Device takeover scams usually follow this pattern:



1. You receive a call, message, or email claiming to be from “technical support” or a trusted organisation.
2. The scammer asks you to install a remote access app or share your screen.
3. They guide you step-by-step to log in to banking apps or approve transactions.
4. While you are distracted, the scammers take control and steal money or data.

COMMON TACTICS INCLUDE:

- Remote access apps for “account verification”
- Step-by-step instructions to perform banking actions
- Screen sharing for “technical support”

HSBC

How to protect yourself

- Never install remote access apps at someone's request.
- Do not share your screen with unknown parties.
- Perform banking activities privately and securely.
- End the call if any instruction feels suspicious.
- Always contact official support channels directly.

You should always remain in control of your device.

Red flags to watch for

- Requests to install remote access or screen-sharing apps.
- The caller insists on guiding you through banking actions.
- Pressure to ignore security prompts.
- Unfamiliar or unofficial support contact channels.
- Threats of account suspension or legal action if you refuse.

TIP: Device takeover often starts with a malicious install or remote-access app. HSBC Malaysia's Android malware safety measures explain how to protect your device and reduce the risk of compromise. Read more about Android Malware Safety Measures to see how it works.

Legitimate organizations do not need full control of your device. Always say no.

REMEMBER: You should always stay in control of your device, never share your screen or install remote-access tools because someone tells you to.

HSBC

Love Scam
When Romance Is Used to Steal Money

Love scams are when scammers build fake romantic relationships online to manipulate victims into sending money or sharing personal information.

Scammers often target people on:

- Dating apps and websites
- Social platforms
- Messaging apps

Scammers often target people on platforms like:

Dating:
Tinder, Bumble, Match

Social:
Instagram, Facebook, LinkedIn, TikTok, X

Messaging:
WhatsApp, Telegram, WeChat, Signal, SMS

They exploit emotions, trust, and loneliness to commit fraud.

HSBC

How it works

Love scams usually follow this pattern:

1. The scammer may already have information about you from what you've **shared online or leaked data** and use it to gain your trust.
2. They then contact you **to build a relationship**, often over weeks or months.
3. They share a **convincing personal story**, often involving hardship or urgent need.
4. They **ask for money** for:
   - Medical emergencies
   - Legal fees
   - Travel expenses
5. Once you send money, the requests continue, or they **disappear completely**.

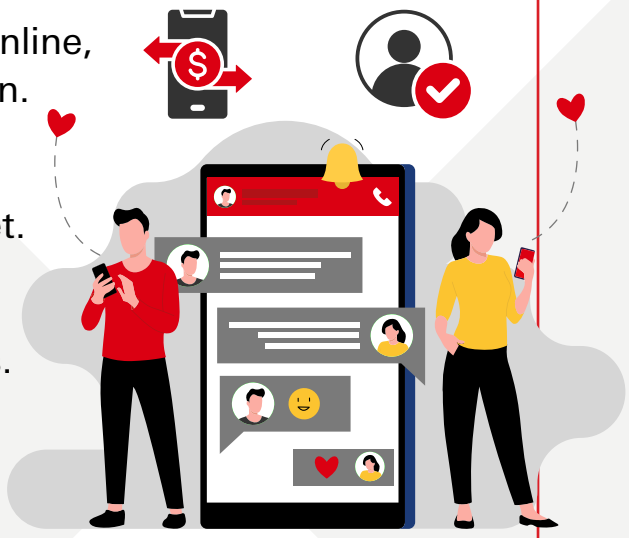
COMMON TACTICS INCLUDE:

- Moving conversations to private channels quickly
- Using attractive photos and fake identities
- Pretending to be from overseas or in crisis situations

HSBC

How to Protect Yourself

- Be cautious about people you meet online, especially if you haven't met in person.
- Never send money or share financial details with someone you haven't met.
- Verify photos and information using reverse image search or other checks.
- Talk to trusted friends or family if someone asks for money.



True romance does not require financial help from strangers.

Red flags to watch for

- Requests for money, especially for emergencies or travel.
- Love interests who refuse to meet in person or video chat.
- Stories that are overly dramatic or urgent.
- Moving conversations quickly to private messaging apps.
- Inconsistencies in their stories or background information.

If someone pressures you for money or personal information, step back. Love should never feel like a financial trap.

HSBC

Loan/Financing Scam
When Your Identity Is Used to Borrow Money

A loan/financing scam often happens when a fraudster steals your personal details and uses them to apply for a real loan/financing or credit product in your name (sometimes with a legitimate bank).

They often target:

- **People who share personal details online**
- **Anyone whose data may have been exposed in a breach**
- **Customers tricked into revealing OTPs/ passwords**

The goal is to take out **borrowing using your identity** and leave you with the debt and stress.

How it works

1. The scammer gets your information via **phishing, fake websites, calls/SMS, malware, or leaked data**.
2. They may contact you to **"confirm" details**, then ask for:
   - ID documents/selfies
   - Bank details
   - One-time passcodes (OTPs)
   - Passwords or security answers
3. They use your details to **apply for a loan/financing/credit** and try to intercept verification (e.g., OTPs or calls).
4. The funds are **paid out** to an account they control or **moved quickly** to other accounts.
5. **You only find out later** through missed payment alerts, credit report changes, or collection contact.

COMMON TACTICS INCLUDE:

Pretending to be from a bank, regulator, or "loan/financing agent"

Creating urgency ("Your loan/financing is approved act now")

Asking for OTPs "to verify" or "to cancel an application"

HSBC

How to protect yourself

- Never share OTPs, passwords, or PINs, not even with someone claiming to be your bank.
- Apply only through official websites/apps/ branches (avoid links from ads or messages).
- Lock down your personal data (privacy settings on social media; don't post ID/addresses).
- Check your credit report regularly for new loans/financing/queries you don't recognise.
- If you suspect your identity is compromised, contact your bank immediately and report it.

If it feels too easy or too good to be true, it probably is a scam.

Red flags to watch for

Calls/messages asking you to "confirm" ID details, passwords, or OTPs.

Sudden changes to your contact details (email/phone/ address) with a provider.

You receive OTPs or verification **messages you didn't request.**

Pressure to act fast or keep the conversation secret.

Alerts about a loan/ financing application approval you didn't make.

HSBC

Your Support Hotline
Spot. Prevent. Protect.

All HSBC hotlines remain available 24/7 for scam reporting, lost or stolen card(s) or mobile device(s), and unauthorised transaction(s).

Services	Contact numbers	Operating hours
HSBC (Banking & Cards)	Local: 1300 88 1388 International: +603 8321 5400	8am – 8pm daily (Emergency services available 24/7) To activate kill switch
HSBC Amanah (Banking & Cards)	Local: 1300 80 2626 International: +603 8321 5200	8am – 8pm daily (Emergency services available 24/7) To activate kill switch
HSBC Premier & Amanah Premier	Local: 1300 88 9393 International: +603 8321 5208	24 hours To activate kill switch
HSBC Card Activation & PIN Hotline	Local: 03 8321 8999 International: +603 8321 8999	24 hours To activate your credit card
HSBC Safeguard	Local: 1800 88 1098 International: +603 8319 9119	Mondays to Fridays 9am – 6pm (excluding public holidays)
Visa Emergency Assistance	Malaysia: 1800 80 2997 Singapore: 800 4481 250 Australia: 1800 450 346 UK: 0800 169 5189 USA: 1866 765 9644	24 hours
MasterCard Global Services	From Malaysia: 1800 80 4594 From Overseas: 1636 722 7111	24 hours
HSBC Fraud Operations	+603 8800 7420	Mondays to Sundays, 24 hours

Alternatively, customers may also contact the National Scam Response Centre (NSRC) at 997, available daily from 8am to 8pm.

Notice:
Government, banks, or law enforcement agencies will never ask for your login details, OTP, security code, or account numbers. If you receive such a request via call, SMS or email, contact our Customer Centre to verify.

HSBC