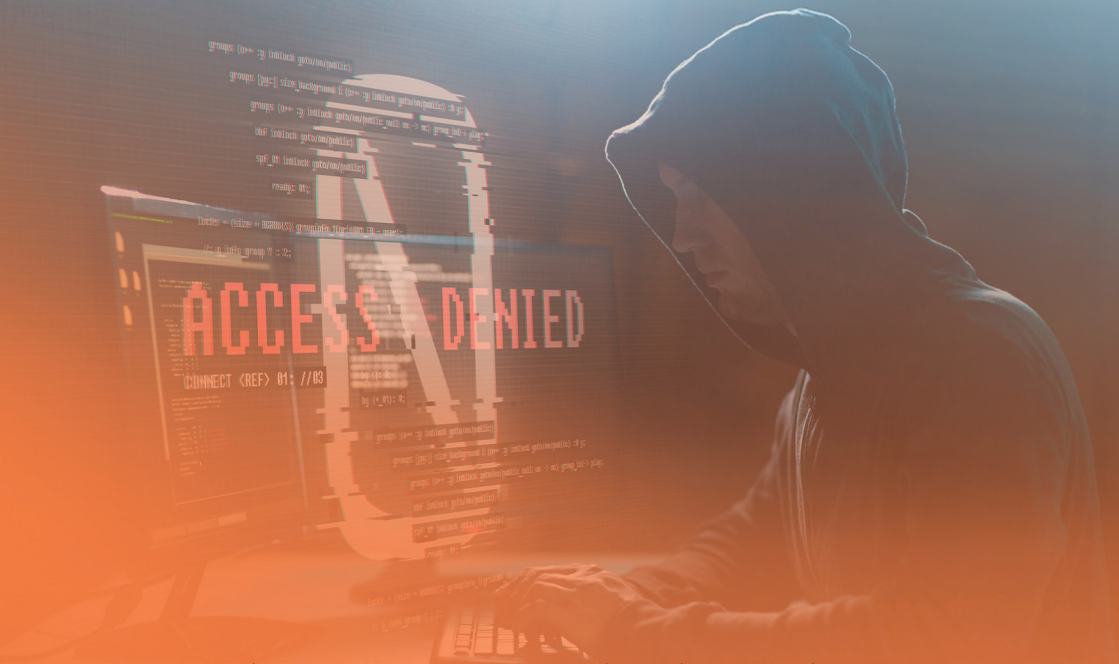
بنك معاملات
Bank Muamalat
Better lives, together

COMMERCIAL CRIMES GUIDEBOOK

A guide to common Modus Operandi scams and smart banking tips to keep your money safe



By Fraud & Intergrity Management Section, Regulatory Advisory & Compliance Division

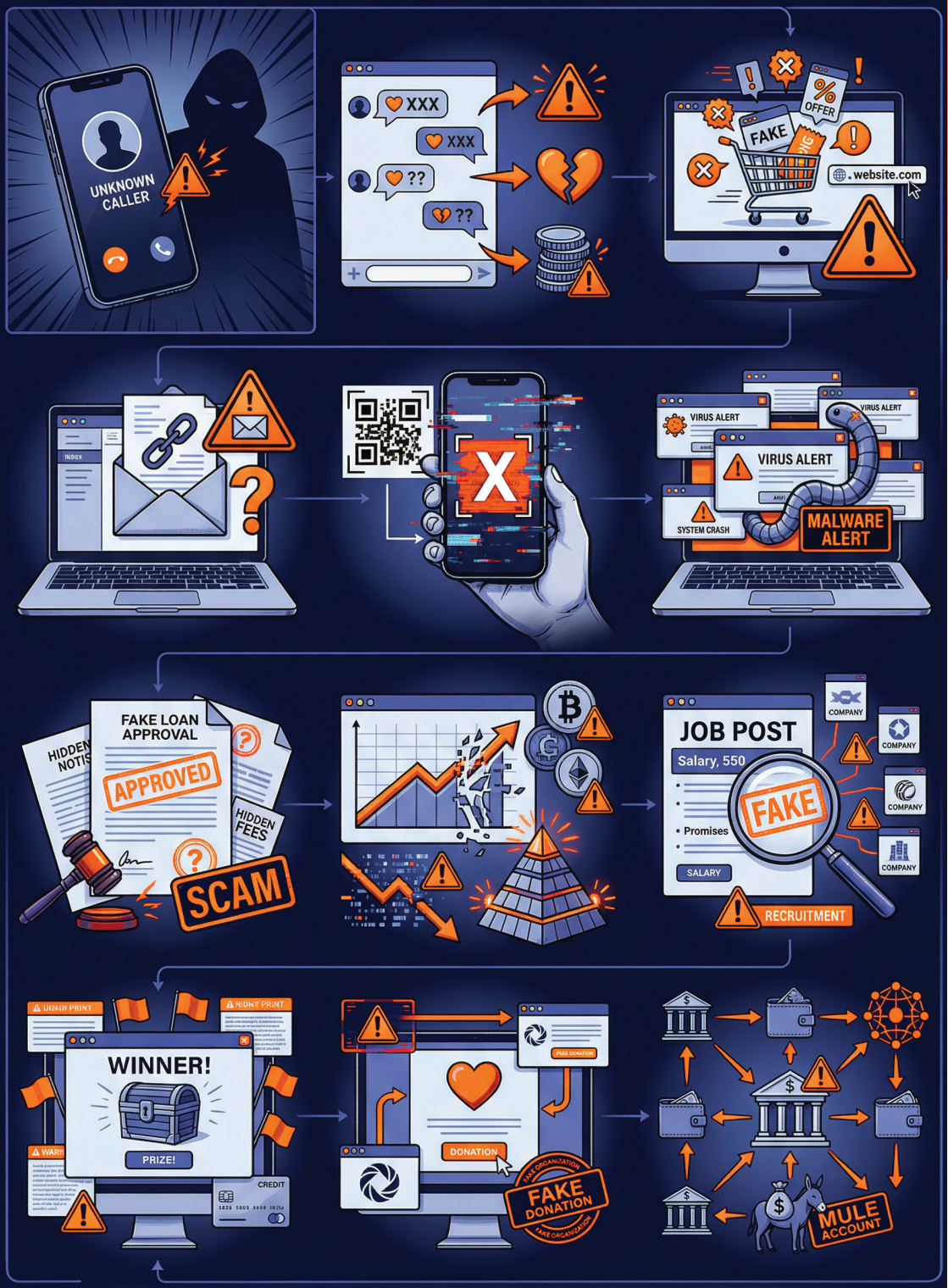

UNKNOWN CALLER
XXX
XXX
??
??
FAKE
OFFER
.website.com
INBOX
X
VIRUS ALERT
VIRUS ALERT
VIRUS ALERT
SYSTEM CRASH
MALWARE ALERT
FAKE LOAN APPROVAL
APPROVED
HIDDEN FEES
SCAM
JOB POST
Salary, 550
Promises
SALARY
FAKE
COMPANY
COMPANY
COMPANY
COMPANY
RECRUITMENT
WINNER!
PRIZE!
CREDIT
DONATION
FAKE DONATION
FAKE ORGANIZATION
MULE ACCOUNT

Table of Content

Introduction

Bank Muamalat Malaysia Berhad created this Commercial Crimes Guidebook to help you stay alert, informed and protected. Inside, you'll find clear explanations of common scam modus operandi along with safe banking tips and practical steps to recognise, avoid and respond to commercial crime threats.

The Core of Numerous Scams

Online scammers also known as cybercriminals, rely on social engineering to trick victims into revealing confidential information. They use suspicious emails, calls or messages and often pretend to be authorities, regulators or familiar individuals. Once they obtain your details, they can commit financial fraud and drain your funds.

Scams typically rely on three (3) elements:

1. **Emotion:**
   fear, love, sympathy, greed.
2. **Urgency:**
   "act now", "last chance", "immediate action".
3. **Trust:**
   pretending to be authorities, banks, companies, friends or family.

If you feel **emotional + rushed + pressured to trust**, pause and verify.

Types of Scam

Phone/ Macau Scam

Scammers impersonate authorities (police, Bank Negara Malaysia (BNM), Lembaga Hasil Dalam Negeri (LHDN), customs, etc.) over the phone, accuse you of serious crimes and force you to transfer money or take financing.

How This Scam Hooks You:

- You receive a suspicious call from someone claiming to be an officer.
- **They accuse you of crimes:** money laundering, drugs, unpaid tax, hacked accounts.
- **They create fear and urgency:** threats of arrest, freezing accounts, and blacklisting.
- They instruct you to transfer money to a 'safe account' or to take financing and hand over the proceeds or your ATM card.

Red Flags:

- Calls from unknown mobile numbers claiming to be 'official'.
- 'Do not tell anyone, this is confidential.'
- Instructions to transfer money to third-party accounts 'for investigation'.

Protect Yourself:

- Hang up. Call the agency back using official numbers from their website.
- Never share your PIN, OTP, password, or full account details over the phone.
- No authority will ever ask you to move money to a personal or third-party account.
- Before transferring to unknown accounts, use Semak Mule at **https://semakmule.rmp.gov.my/** to check.

If This Happens to You:

- Stop all communication immediately.
- Do not transfer any funds.
- Contact your bank and the National Scam Response Centre (NSRC) at 997.

Types of Scam

Love Scam

Scammers build online romantic relationships and use love, sympathy and trust to get victims to send money or move funds.

How This Scam Hooks You:

- Scammer creates a fake profile on dating apps or social media.
- They shower you with attention, affection and promises.
- They quickly call you 'wife/husband', 'soulmate' without meeting you.
- Then come the 'emergencies': medical bills, business problems, travel issues.
- They ask you to send money or use your account to receive funds.

Red Flags:

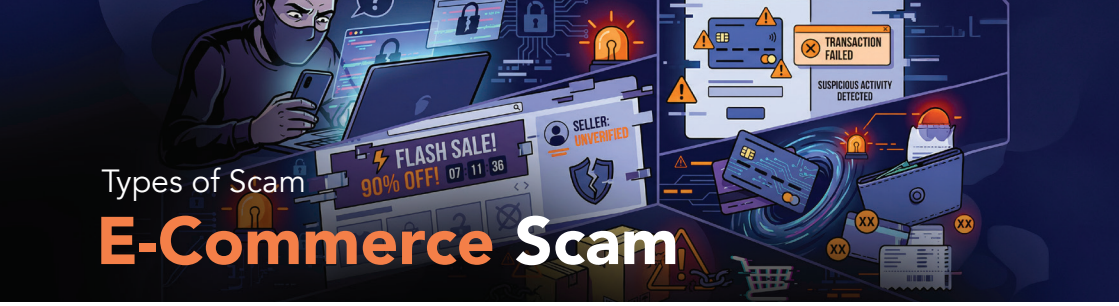
- 'I love you' very fast, without meeting in person.
- Constant excuses not to meet.
- Requests for money, gifts or help with transfers.
- They push you to chat off-platform (WhatsApp, email, etc.).

Protect Yourself:

- Never send money to someone you have never met in person.
- Check their photos using reverse image search.
- Search their job description with the word 'scammer' (e.g. 'oil rig scammer').
- Listen if family and friends are concerned.

If This Happens to You:

- Cut off contact immediately.
- Do not send further money or details.
- Keep all chats and proof; lodge a police report and inform your bank if any transfers were made.



Types of Scam

E-Commerce Scam

Scammers use fake online shops or social media accounts to advertise cheap goods. Once payment is made, goods are not delivered.

How This Scam Hooks You:

- Fake or suspicious seller advertises on social media, websites or messaging apps.
- Prices are far below market rate to attract quick buyers.
- Seller demands bank transfer instead of platform payment.
- After payment, seller vanishes, changes username or blocks you.

Red Flags:

- Prices that look 'too good to be true'.
- New or unknown sellers, no proper reviews.
- Refusal to use secure payment methods.
- Extra 'administrative' or 'shipping' fees suddenly added.

Protect Yourself:

- Use reputable platforms and secure payment methods.
- Check reviews, ratings and transaction history.
- Avoid direct transfers to personal accounts.
- For large purchases, be extra cautious and verify seller details.

If This Happens to You:

- Collect evidence: screenshots, accounts, chats.
- Lodge a report with the platform (if any), your bank and the police.
- Check the account number on Semak Mule at **https://semakmule.rmp.gov.my/** and report if flagged.

Types of Scam

Phishing Scam

Phishing uses fake emails, SMS or messages to trick you into entering login details or downloading harmful files.

How This Scam Hooks You:

- You receive a message from what appears to be a bank or company.
- Message contains a link to a fake website that looks genuine.
- You key in your username, password and sometimes OTP.
- Scammers use this information to access your real account.

Red Flags:

- 'Your account will be blocked in 24 hours' type messages.
- Links that look slightly different from the official URL.
- Requests for full credentials or multiple OTPs.

Protect Yourself:

- Do not click links in suspicious messages.
- Type the bank's URL manually or use your saved bookmark.
- Check for the correct URL and security indicators before logging in.
- If unsure, call the bank using the official contact number.

If This Happens to You:

- Immediately contact your bank to block access and cards.
- Change your passwords and PINs.
- Report to NSRC 997 and lodge a police report.

Types of Scam

QR Phishing (Quishing)

Quishing hides harmful links behind QR codes to steal data or install malware.

How This Scam Hooks You:

- Scammers place QR codes in emails, posters or messages.
- When scanned, the code opens a fake website or file.
- You are asked to enter login or payment details, or your device gets infected.

Red Flags:

- Random QR codes from unknown sources.
- No clear explanation of who is behind the QR or what it does.
- Messages urging you to 'scan now' for prizes or urgent actions.

Protect Yourself:

- Only scan QR codes from trusted organisations or venues.
- Where possible, preview the URL before opening.
- Avoid entering sensitive banking details after scanning a random code.
- Enable two-factor authentication on your accounts.

If This Happens to You:

- Close the page immediately and do not enter any data.
- If you did key in banking details, contact your bank at once.
- Run a security scan on your device.

Types of Scam

Malware Scam

Malware is harmful software that can read SMS (including OTP), steal credentials and take control of your device.

How This Scam Hooks You:

- You receive links or APK files via SMS, social media or messaging apps.
- You are told to install an app to proceed with payment, booking, jobs or invitations.
- The app secretly gains permission to read SMS, access banking apps and capture data.

Red Flags:

- Requests to install apps sent via WhatsApp or SMS.
- Apps asking for permission to read SMS or become default messaging app.
- Ignored browser or phone security warnings.

Protect Yourself:

- Only install apps from official stores (Play Store, App Store, AppGallery).
- Never install APK files received from strangers.
- Keep your device and security software updated.
- Do not click unknown ads or pop-ups.

If This Happens to You:

- Disconnect your device from the internet.
- Uninstall suspicious apps and run a full security scan.
- Change your passwords and contact your bank immediately.

Types of Scam

Financing Scam

Financing scams offer easy and fast financing but their real aim is to collect upfront fees and misuse your personal information.

How This Scam Hooks You:

- Scammers contact you via SMS, calls or social media.
- They promise quick approval and no credit checks.
- They ask for personal details and upfront payments (processing, tax, admin).
- No actual financing is disbursed.

Red Flags:

- Unsolicited financing offers via WhatsApp, SMS or social media.
- 'Guaranteed approval' and 'no documents' claims.
- Requests for payment before financing disbursement.

Protect Yourself:

- Apply for financing only through official bank channels or licensed providers.
- Do not share online banking credentials or OTPs.
- Do not pay any fee to unknown parties to 'secure' a financing.

If This Happens to You:

- Stop all communication and do not pay further.
- Record details of the offer and report to the authorities and your bank.

Types of Scam

Investment Scam

Investment scams promise high returns with little or no risk, often using fake platforms and testimonials.

How This Scam Hooks You:

- Scammers promote schemes via social media, messaging groups or websites.
- They use fake testimonials, 'proof' of profit and sometimes false celebrity endorsements.
- Early investors may receive small returns to build trust.
- After you put in more money, you cannot take your money out and the investment stops completely.

Red Flags:

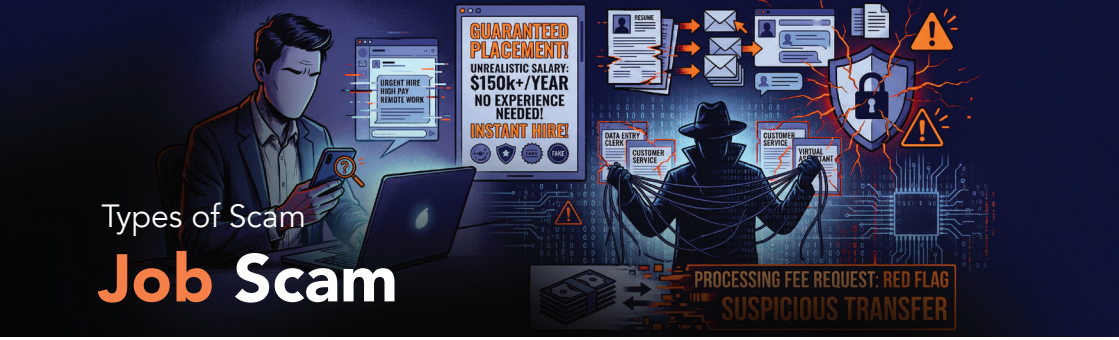
- Guaranteed or very high returns in a short time.
- Strong pressure to 'join now or miss out'.
- Company not listed with regulators or hard to verify.

Protect Yourself:

- Check with the Securities Commission (SC) and Bank Negara Malaysia (BNM) whether the entity is authorised.
- Research the company name together with 'scam' or 'complaint'.
- Walk away from any investment that sounds too good to be true.

If This Happens to You:

- Stop putting in more money.
- Record all evidence: receipts, chats, platform details.
- Report to SC, BNM, your bank and the police.



Types of Scam

Job Scam

Job scams pretend to offer employment but aim to take your money or use your bank account for illegal activities.

How This Scam Hooks You:

- Job ads appear on social media, messaging apps or websites.
- Roles are vaguely described but promise high income.
- Applicants are asked to pay fees or use personal accounts for 'company transactions'.
- In some cases, tasks involve topping up or transferring money to other accounts.

Red Flags:

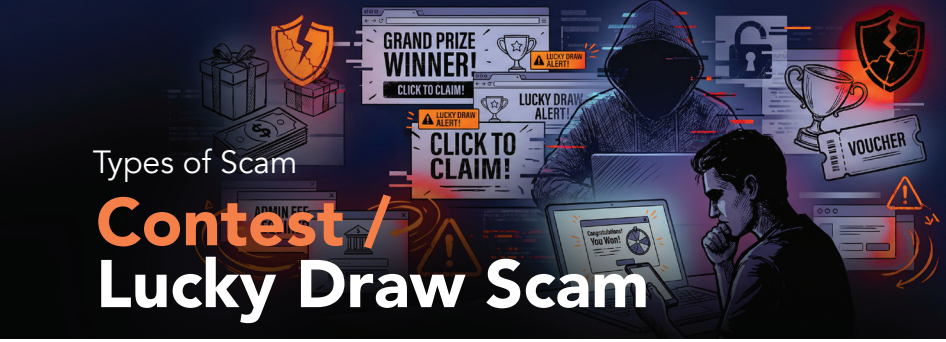
- No proper interview or formal process.
- Job involves using your personal bank account.
- Requests for training, registration or placement fees.

Protect Yourself:

- Verify the company via its official website and contact channels.
- Do not pay any fee to secure a job.
- Never allow your personal account to be used for employer-related transfers.

If This Happens to You:

- Stop engaging and do not make further payments.
- If your account has been used for unknown funds, inform your bank and lodge a police report.



Types of Scam

Contest / Lucky Draw Scam

Scammers claim you have won a prize and then demand money or confidential information to release it.

How This Scam Hooks You:

- You receive calls, emails or messages claiming you are a lucky winner.
- They request your personal and banking details.
- They ask you to pay charges before the prize is released.
- Once paid, the scammers disappear.

Red Flags:

- You do not remember joining any contest.
- Requests for PIN, OTP, CVV or full card number.
- Pressure to pay quickly to avoid losing the prize.

Protect Yourself:

- Be wary of prizes from contests you did not enter.
- Never share sensitive banking details.
- Do not pay money to claim any prize.

If This Happens to You:

- Decline the offer and end the call or chat.
- If you already shared details, contact your bank immediately.

Types of Scam

Charity Scam

Charity scams exploit generosity, especially during crises or festive seasons, to collect money that never reaches those in need.

How This Scam Hooks You:

- Scammers pose as volunteers or representatives of charities, NGOs or religious bodies.
- They approach people in public areas or online with emotional stories.
- Donations are requested to personal bank accounts or via suspicious links.

Red Flags:

- No clear registration with authorities.
- Vague information about how funds will be used.
- No official receipts or documentation.
- Pressure to donate immediately.

Protect Yourself:

- Check if the charity is registered with authorities such as Companies Commision of Malaysia (SSM) or Registrar of Societies(ROS).
- For religious funds, ensure there is written approval from the religious council.
- Donate through the charity's official website or authorised channels.
- Request official receipts with proper details.

If This Happens to You:

- Avoid donating through suspicious channels.
- Report the incident to authorities if you suspect fraudulent collection.

Types of Scam

Mule Account

A mule account is a legitimate bank account used to move illegal funds. Account holders can be investigated and charged.

How This Scam Hooks You:

- Scammers recruit individuals to 'lend', rent or sell their bank accounts.
- They ask for ATM cards, PIN or online banking access.
- The account is then used to receive money from scam victims and transfer it onwards.

Red Flags:

- Offers of 'easy side income' by renting out your account.
- Unlicensed moneylenders asking for your ATM card as collateral.
- Job offers that require you to receive and forward money.

Protect Yourself:

- Never share your ATM card, PIN or login details.
- Do not allow anyone to use your bank account for their own transfers.
- Regularly monitor your account for unknown transactions.

If This Happens to You:

- Immediately stop sharing access.
- Inform your bank and lodge a police report.
- Cooperate fully with investigations if your account is misused.

If You Have Been Scammed: What to Do Now

Contact Your Bank Immediately

BMMB Scam Hotline: **+603-2615 8000** (24 Hours daily)

Email: **feedback@muamalat.com.my**

Ask Them to:

- Block your cards and/or online banking access
- Freeze suspicious transactions where possible

Call the National Scam Response Centre (NSRC)

Hotline: **997** (24 Hours daily)

Provide:

- Your full name and IC number
- Bank name and account details
- Time, amount and description of the incident

Lodge a Police Report

Visit the nearest police station

Provide:

- Screenshots, phone numbers, account numbers
- Chat logs, emails and any documents

** Keep a copy of your report and reference numbers.


بنك معاملات
Bank Muamalat
Better lives, together