# SCAM: THE ART OF NOT GETTING FOOLED (WITH LEGAL KNOW-HOW)

**Scams are fraudulent schemes designed to deceive someone. Usually, the scammer's main goal is monetary gain or personal information. According to Gogolook, a leading trust tech company, Malaysia is losing a total of RM 54 billion (3% of Malaysia's GDP) to scams in a year. Research indicates some 70% of scam victims do not report their cases to authorities. According to an article by Scoop, this matter is of such grave concern that His Royal Highness Sultan Ibrahim Sultan Iskandar at the Dewan Rakyat has emphasized the need for the public to remain vigilant against online crimes, including scams.**

## EMAILS

You might think the emails you receive are just regular emails, but in today's digital world, you could fall for a scam just by replying. Scam emails often look like normal emails you get every day, but they are actually trying to steal your personal information—such as your banking details, passwords, or other private data. One common type of scam email is a phishing email. These emails pretend to be from a legitimate organization, urging you to respond quickly.

### EXAMPLES

**Phishing Emails from "Banks"**

An email claiming to be from your bank, urging you to click a link to secure your account or risk it being restricted.

**EPF or Tax Refund Scams**

Fake emails or calls claiming you are eligible for an EPF withdrawal or an LHDN tax refund, asking you to provide personal details.

**Love or Romance Scams**

Scammers on dating apps or social media pretending to form a relationship before asking for money due to a "family emergency" or other excuses.

## PHONE CALLS

Scam phone calls are made to trick people into revealing their sensitive information. By now, almost everyone has received a scam call at least once in their life. These calls can come through your personal phone or even your office phone. Scammers usually get your phone number from data leaks, your company's website, or social media platforms like Facebook or LinkedIn.

### EXAMPLES

**Phone Calls from "Bank Officers"**

A caller pretending to be from your bank, warning you about unauthorized transactions and asking for your banking details to "fix the issue."

**Fake Police or MACC Calls –**

A caller pretending to be from the police, MACC, or Bank Negara, claiming you are involved in a crime and must transfer money for "investigation purposes."

**Fake Charity Scams –**

Messages or calls asking for donations for a supposed charity, often using emotional stories to pressure people into transferring money.

## WHATSAPP

You don't have to give someone your phone number for them to have it. Almost all Malaysians use WhatsApp for personal chats, work, or even university communication because it's free, efficient, and easy to use. That's exactly why scammers target it. Scammers often get phone numbers from data leaks or social media platforms.

### EXAMPLES

**Parcel Delivery Scams –**

A message or call claiming your parcel is stuck at customs or needs additional payment before it can be released.

**Job Offer Scams –**

Messages offering high-paying jobs with minimal work, requiring you to pay a "processing fee" upfront.

**WhatsApp Hijacking –**

A scammer pretending to be a friend or family member, asking for a verification code sent to your phone to gain access to your WhatsApp account.

# HOW CAN WE SPOT SCAMS?

## EMAILS

### Check the Email Address (Spoofing)

Scammers often use fake or suspicious email addresses that look similar to real ones. Always check the sender's email carefully. If it's from a bank or company, verify the official email on their website. If it's from someone you know, call them to confirm.

✅ Legitimate email: moneybank@gmail.com

❌ Scammer email: m0neybank@gmail.com

### Sense of Urgency

Scam emails often try to make you panic. They might say your account will be locked or that you must act immediately. This is a trick to make you act without thinking. Stay calm and verify before doing anything.

### Fake Invoices and Payment Requests

Many scammers are after one thing—money. Be extra cautious with emails asking for payments or invoices. Always double-check before making any transfers.

### Poor Language and Grammar

Legitimate organizations use proper grammar and professional language in their emails. Scam emails often have typos, weird phrasing, or awkward sentences—something people tend to overlook.

## PHONE CALLS

### Unknown Numbers

Scammers usually call from numbers you don't recognize. They do this to avoid detection and blocking. If you receive a call from an unfamiliar number, be cautious.

### Impersonating Real Organizations

Scammers often pretend to be from trusted organizations like LHDN or banks because people are more likely to believe them. If you get a call claiming to be from a company or government body, verify it before sharing any details.

### Creating a Sense of Urgency

They will try to make you panic by saying there's a problem—like suspicious transactions, unpaid bills, or legal trouble. Their goal is to pressure you into reacting quickly without thinking.

### Asking for Personal Information

Legitimate companies will never ask for your banking details, passwords, or OTP over the phone. If a caller requests this, it's a scam. Hang up immediately.

### Use Caller ID Apps

A useful tool to help identify unknown numbers is the Whoscall app, which you can download on your phone. It helps detect and block potential scam calls.
https://whoscall.com/en

## WHATSAPP

### Messages from Unknown Numbers

Scammers often contact you from numbers you don't recognize. If you receive a message from an unknown number, be cautious—especially if they ask for personal details or money.

### Creating a Sense of Urgency

Scammers try to make you panic by saying something urgent—like a problem with your bank account, a prize you must claim immediately, or a friend in trouble. They want you to act fast without thinking.

### Impersonating Someone You Know

A common trick is pretending to be a friend or family member who has "changed their number." They might ask for money or sensitive information. Always verify by calling the person directly before responding.

### WhatsApp Scam Awareness Guides

WhatsApp provides official resources on how to recognize and avoid scams. You can learn about suspicious messages, fake files, and tips for staying safe here:
https://faq.whatsapp.com/2286952358121083

## HOW CAN YOU OR YOUR EMPLOYEES AVOID GETTING SCAMMED?

### Employee Training

**The best way to prevent scams is through proper training. Companies should educate employees on recognizing and responding to scams.**

### Conduct Anti-Scam Workshops

**Organize workshops where professionals, such as lawyers or representatives from NSRC, can teach employees how to identify and handle scams. Practical examples and real-life case studies can make learning more effective.**

### Regular Reminders

**People tend to forget over time, so it's important to send regular reminders. Use emails, internal newsletters, or the company's social media to keep employees aware of the latest scam tactics.**

### Encourage a Culture of Caution

**Make it a habit for employees to verify unusual requests, especially those involving payments or personal information. A simple double-check with the relevant department can prevent major losses.**

## WHAT NOT TO DO?

### Don't Panic

**The worst thing you can do is panic. When we're stressed, we don't think clearly, and that's exactly what scammers want. Take a deep breath and respond carefully.**

### Don't Engage with Scammers

**Some people, especially younger individuals, may think it's fun to play along when they recognize a scam. But experienced scammers are skilled at extracting information without you even realising it — including recording your voice to replicate it. The safest approach is to ignore and block them.**

### Don't Stay Silent

**Many people feel embarrassed, afraid of consequences, or assume there's no chance of recovering their losses after being scammed. But reporting is crucial—not only for potential recovery but also to warn others and prevent the scam from happening again.**

**By taking the right steps and spreading awareness, you can help protect yourself and others.**

# ARE THERE LAWS TO PROTECT YOU?

## Communications and Multimedia Act 1998

- Section 233: Addresses the improper use of network facilities or services. It criminalizes actions such as using network services to transmit false, indecent, obscene, or offensive content with the intent to annoy, abuse, threaten, or harass others.
- Penalties: Offenders may face fines up to RM50,000, imprisonment for up to one year, or both.

## Personal Data Protection Act 2010

- Purpose: Regulates the processing of personal data in commercial transactions, ensuring data privacy and protection.
- Penalties: Non-compliance can result in fines ranging from RM100,000 to RM500,000, imprisonment for one to three years, or both.

## Computer Crimes Act 1997

- Section 3: Criminalizes unauthorized access to computer material, commonly referred to as "hacking."
- Penalties: Convicted individuals may face fines up to RM150,000, imprisonment for up to ten years, or both.
- Section 5: Addresses unauthorized modification of computer contents, such as introducing malware or viruses.
- Penalties: Convicted individuals may face fines up to RM100,000, imprisonment for up to 7 years, or both.

## Penal Code

- Section 416: Covers "cheating by impersonation," applicable to phishing scams where individuals deceive others by pretending to be someone else.
- Penalties: Punishable by imprisonment of up to five years, a fine, or both.

**These laws collectively aim to protect Malaysians from various forms of cybercrime. If you believe you've been targeted or affected by a cyber scam, it's crucial to report the incident to the relevant authorities promptly.**

# WHAT TO DO IF YOUR ORGANISATION'S EMAIL OR IDENTITY IS MISUSED IN A SCAM?

## Stay Calm and Act Quickly

**Being targeted by a scam can be distressing, but panicking won't help. The key is to respond swiftly and effectively.**

## Report It Immediately

**If your organization's email or identity has been misused in a scam, take immediate action:**

- **Contact your bank's hotline (available 24/7) if financial details were involved.**
- **Call the National Scam Response Centre (NSRC) at 997 for guidance.**
- **Follow their instructions, which may include filing a police report.**

## Alert Employees and Clients

**Scammers may continue targeting your organization, so it's crucial to inform others:**

- **Notify HR to issue an internal alert to employees.**
- **Publish a public notice on your website and social media to warn clients.**
- **Advise employees to be extra cautious about suspicious emails or calls.**

## Seek Legal Advice

**If you're unsure how to handle the situation, consult a lawyer. Legal counsel can guide you on necessary steps, such as taking legal action against fraudsters or implementing stronger cybersecurity measures.**

# WHAT TO DO IF YOU FALL VICTIM TO A SCAM

### Stay Calm and Assess the Situation

- Do not panic. Scammers rely on fear and confusion to manipulate victims. Take a moment to evaluate what has happened.

### Report the Incident Immediately

- If money was involved, contact your bank's hotline immediately to block transactions and secure your account.
- Call the National Scam Response Centre (NSRC) at 997, available daily from 8 AM to 8 PM, for assistance in reporting and handling scam cases.
- File a police report at your nearest police station to document the scam and support any potential investigation.

### Secure Your Personal Information

- If you shared sensitive details like passwords or banking information, change your passwords immediately and enable two-factor authentication (2FA) for added security.
- Notify your employer if your work email or company details were compromised.

### Warn Others

- Inform colleagues and clients if your name, email, or organization has been misused in a scam to prevent further victims.
- Issue an internal alert within your company and a public notice on your website and social media if necessary.

### Seek Legal Advice

- Some scams may involve identity theft, fraud, or misuse of company information. If you're unsure about your next steps or need guidance on legal action, consulting a lawyer is highly recommended.
- Suppiah & Partners is here to assist you. Contact us for expert legal advice and the best course of action to protect your rights and recover from the incident.

Taking immediate action can make a difference in preventing further losses and protecting yourself or your organization. Stay alert and always verify before responding to suspicious messages or calls.

## REFERENCE


- **Communications and Multimedia Act 1998:** An act to provide for and to regulate the converging communications and multimedia industries, and for incidental matters.
- **Personal Data Protection Act 2010:** An Act to regulate the processing of personal data in commercial transactions and to provide for matters connected therewith and incidental thereto.
- **Computer Crimes Act 1997:** An Act to provide for offences relating to the misuse of computers.
- **Penal Code:** An Act relating to criminal offences.
- **Scam statistics:** https://www.malaymail.com/news/malaysia/2024/10/03/scam-epidemic-malaysians-lose-us128b-annually-equivalent-to-3pc-of-gdp-amid-rising-ai-threats/152485
- **Scoop:** https://www.scoop.my/news/246047/agong-wants-to-combat-red-tape-culture/


SUPPIAH & PARTNERS
since 2007

THIS COMMUNITY SERVICE ALERT IS BROUGHT TO YOU BY:


SUPPIAH & PARTNERS

03-4142 3766

https://suppiahlaw.com/

thulasy@suppiahlaw.com

UG-13, LEXA Galleria,
No. 45, Jln 34/26, Wangsa Maju, 53300 Kuala Lumpur, Malaysia

Prepared By: Adilah Rafi