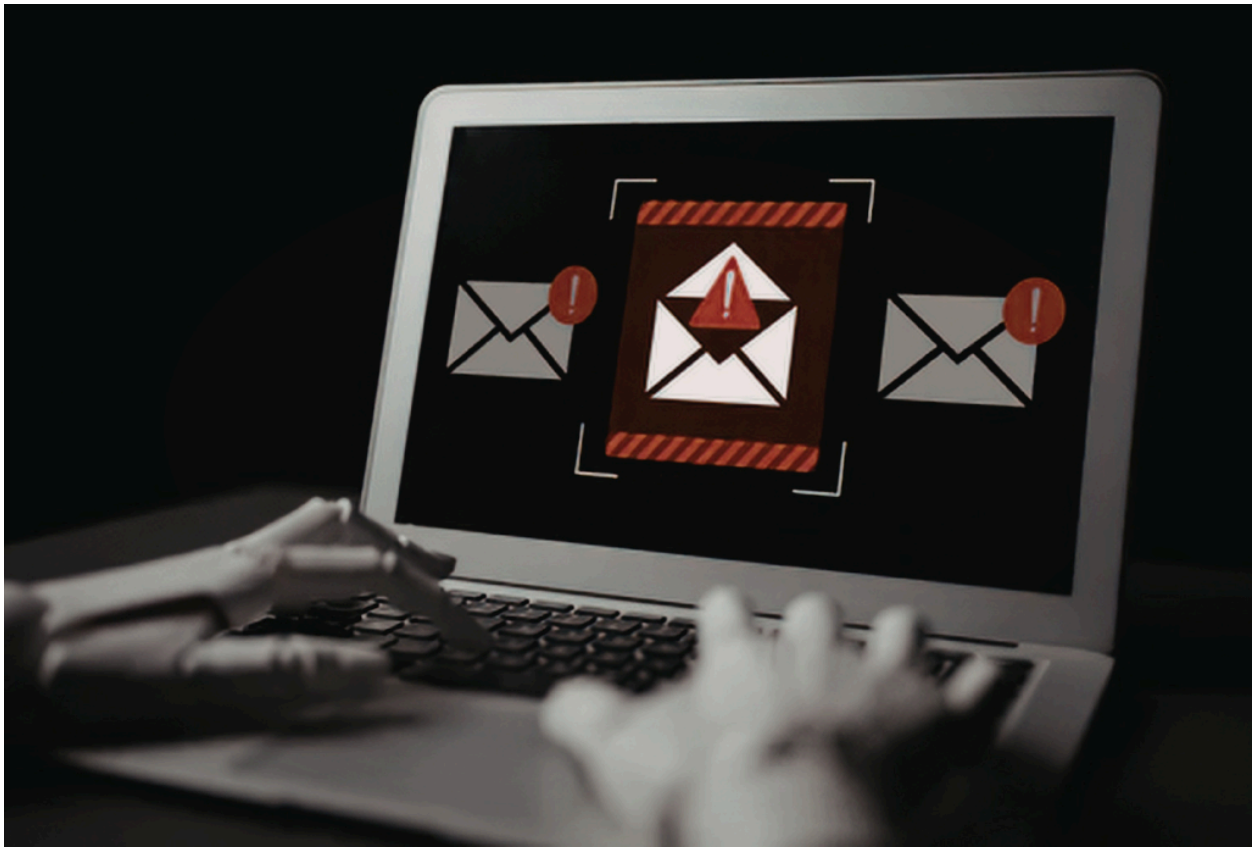
# Online Scams Are Getting Smarter: How to Protect Yourself in 2026



With the rapid advancements of technology, Malaysians increasingly rely on digital platforms for work, payments, and daily communication. While this brings greater convenience, it also makes it more challenging to stay safe from online threats and scams. These scams have evolved beyond basic "*Congratulations, you've won a prize!*" text messages. Today, simply having an email address, a bank account, or a social media profile makes you a potential target.

Online scams aren't slowing down anytime soon. While older adults are often seen as the most vulnerable, youths are increasingly being targeted as well especially through daily-use platforms.Here's a breakdown of the most common ones and how to protect yourself before it's too late:

## 1. Telecommunication Fraud: Deepfakes & Voice Phishing

Scammers are now using AI to impersonate real people, ranging from government officials to even your own family members.

Deepfake technology can mimic voices and faces with alarming accuracy. You might receive a call that sounds like a relative asking for urgent financial help, or a "government officer" claiming you're involved in a legal case and giving you instructions to transfer money immediately to resolve the issue.

These scams rely on panic and urgency to stop you from thinking critically.

| How to protect yourself |
| --- |
| • **Pause before reacting**: Scammers rely on panic (using words like "*urgent*", *"legal action*", *"emergency"*). Remember, official authorities will **not** pressure you for immediate payment.<br>• **Verify through a second channel:** If a "family member" calls asking for money, verify that it is actually them by contacting their actual number. If it's someone claiming to be from law enforcement or the government, contact the organisation directly using their official contact (e-mail, phone number, website).<br>• **Create a personal verification habit:** Agree on a simple 'code word' or question with close family members for emergencies. This makes impersonation much harder. |

## 2. Fake Deals & Too-Good-To-Be-True Offers

Scammers are quick to capitalise on trends and public interest. Whether it's concert tickets, exclusive reservations, or limited-time promotions, fake deals are designed to create urgency and excitement.

For example, during the first few months after the opening of the popular Rembayung restaurant, members of the public became targets of fraudulent reservation slots, where they paid for what they believed were legitimate bookings, only to later discover that they had been scammed.

These scams work because they feel timely and relevant. If everyone is talking about it, it becomes easier to trust.

| How to protect yourself |
| --- |
| • **Slow down your decision-making:** Limited-time offers and “last slots available” reminders are designed to rush you. Take a few minutes to verify before paying.<br><br>• **Check digital footprints:** Look closely at the seller’s account.<br>  ○ When was it created?<br>  ○ Are the comments genuine or spam-like?<br>  ○ Is there consistent posting history?<br>  ○ New or suspicious accounts are a red flag.<br><br>• **Search before you commit:** Look up the deal, seller, or event name with keywords like “scam” or “review”. If others have been targeted, you’ll likely find warnings.<br><br>• **Use secure payment methods:** Avoid direct bank transfers to unknown individuals. Use platforms that offer buyer protection where possible. |

## 3. Hidden Malware Scams

Not all scams rely on tricking you into transferring money directly. Some are designed to quietly infiltrate your device and steal information without you realising.

These are known as malware scams: malicious software hidden in links, attachments, apps, or downloads. Once installed on your phone or computer, malware can track your activity, access your personal files, capture passwords, or even monitor your banking sessions.

Hidden malwares may appear as delivery tracking messages, fake banking alerts and download links for documents.

| How to protect yourself from malwares |
| --- |
| • **Think before you click**: Do not open links or attachments unless you are expecting them or can verify the source.<br><br>• **Check the message carefully:** Look out for spelling errors in URLs or email addresses and unusual sending times or strange formatting<br><br>• **Avoid unofficial downloads**: Only install apps from trusted sources such as official app stores. Avoid APK files or third-party download links.<br><br>• **Keep your devices updated:** Software updates often include security patches that protect against new types of malware. |

- **Act quickly if something feels wrong:** If you suspect your device is infected, you should disconnect from the internet, change important passwords using a safe device and contact your bank immediately if financial accounts may be affected

## 4. Fake Alerts & Personal Data Scams

Scammers are constantly coming up with new ways to trick you into giving away your personal and financial information, such as your bank login details, or your credit or debit card number. To do that, they disguise their attempts through everyday messages that feel urgent or important.

For example, you might receive a text saying your credit card points are expiring or that your card has been used for a large purchase *(e.g. "RM3,000 spent on jewellery")*, prompting you to click a link or call a number. In many cases, the details aren't even accurate, such as an incorrect points balance or a partially masked card number that isn't yours.

However, the urgency can cause people to overlook these inconsistencies and react immediately. Once engaged, scammers may trick you into revealing personal and financial information. As a general rule, legitimate banks in Malaysia will not send clickable links via SMS, so treat any message that does with caution.

**How to protect yourself**

- **Verify directly with your bank:** Do not click on links or call numbers provided in suspicious messages. Instead, use your bank's official app or contact details to check if the alert is real.
- **Check your statements regularly:** Monitor your bank and card transactions closely to spot any unauthorised charges early, including unfamiliar subscriptions or ad payments**.**
- **Look out for inconsistencies:** Pay attention to small details like incorrect card numbers, unusual amounts, or generic messaging—these are often signs of a scam.

## Protecting Your Privacy in a Digital-First World

One of the most overlooked aspects of scam prevention is personal data. The more information scammers have about you, the easier it is for them to create convincing, targeted scams. Something as simple as your phone number, workplace, or daily routine can be used against you.

Protecting your privacy isn't just about security—it's about reducing your visibility to potential scammers. Some may also overlook this when using AI for work or studies, where sensitive information is sometimes shared without much thought. Learn how to protect yourself while using AI with our guide here.

The best defence against online scams is not just awareness, but consistent vigilance in your daily digital habits. When something feels off, take a moment to pause and verify. Acting too quickly is exactly what scammers rely on.

If you encounter a suspicious situation or believe you've been targeted, report it to the relevant authorities. Speaking up not only protects you, but also helps prevent others from becoming victims.

Want to learn more about other types of scams? Check out our previous blog on Job Scams: How to Spot the Warning Signs!

**Resources**


1. https://www.freemalaysiatoday.com/category/leisure/2025/03/26/how-to-protect-yourself-from-online-scams-this-hari-raya
2. https://www.malaymail.com/news/malaysia/2026/04/15/scams-in-the-digital-age-how-hackers-and-ai-are-reshaping-online-fraud-in-malaysia/215123
3. https://dollarsandsense.my/8-common-online-scams-that-malaysians-fall-for/
4. https://www.scoop.my/news/245487/online-scams-in-malaysia-cost-victims-over-rm3-18-billion-in-less-than-three-years/
5. https://www.malaymail.com/news/malaysia/2025/08/04/it-sounded-just-like-my-brother-how-deepfake-voices-are-fuelling-money-scams/183345
6. https://www.bharian.com.my/hiburan/selebriti/2026/03/1520041/daiyan-trisha-dakwa-jadi-mangsa-scam-slot-rembayung