THE RM750 MILLION SCAM WAVE:

WHAT MALAYSIAN SME'S MUST WATCH OUT FOR IN 2026...

In the first half of 2025 alone, Malaysians lost more than **RM 750 million to investment scams,** with **4,368 cases as reported by RinggitPlus**.

This is a very worrying number indeed. Scariest thing is that most of us do not have these amounts readily at our disposal. Thus, this only means that either life savings or loan sharks are involved.

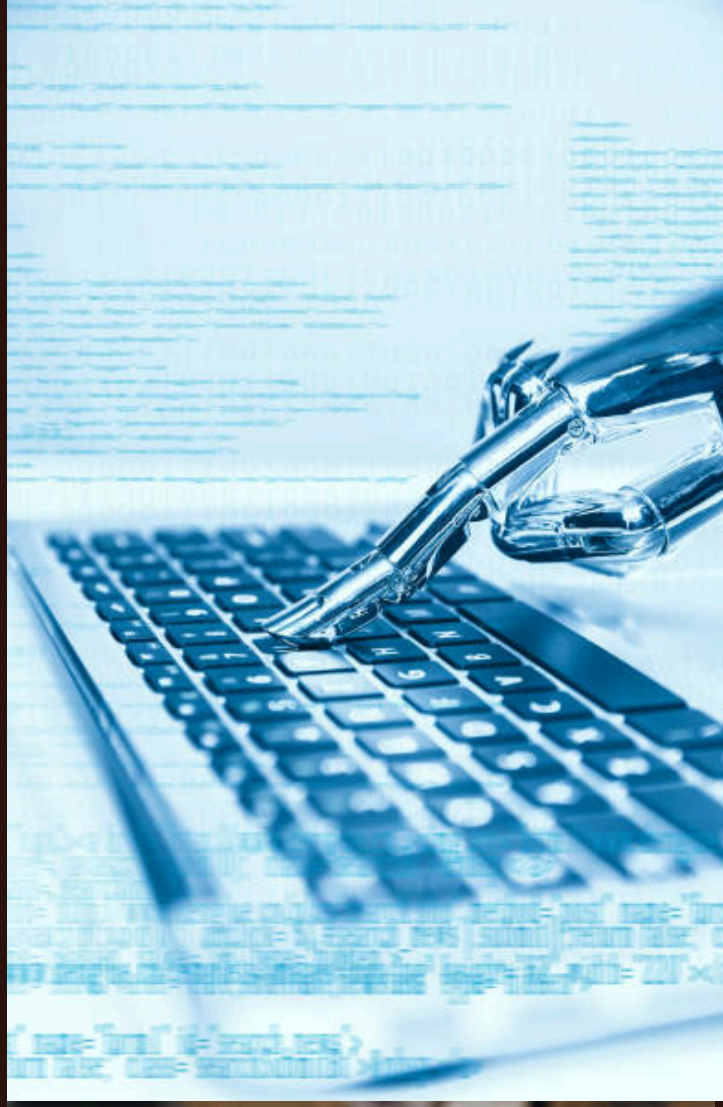
Moreover, behind those numbers are real businesses, mostly SMEs that believe in promises of “guaranteed returns,” only to find themselves empty-handed in the end. Here’s the hard truth: when trust is weaponized, you don’t lose just money, you lose your business.

If you’re running an SME in Malaysia, 2025 is NOT the year to gamble on glossy ads or whispering promises. You need a strategy to see through the lies before your money vanishes. Let’s take a closer look at what to look out for:

1. FAKE INVESTMENT PLATFORMS & BOGUS DASHBOARD RETURNS

Most Scammers build a glossy website, showing fake profits to reel you in. They first show you that you are making money, but when you try to withdraw, you hit on-line glitches, **"maintenance," or blocked accounts**.

Example: Victims are asked to pay **"withdrawal fees" or "tax surcharges"** before taking out their own money. RinggitPlus reports this method is rampant in the current **RM 750M wave.**

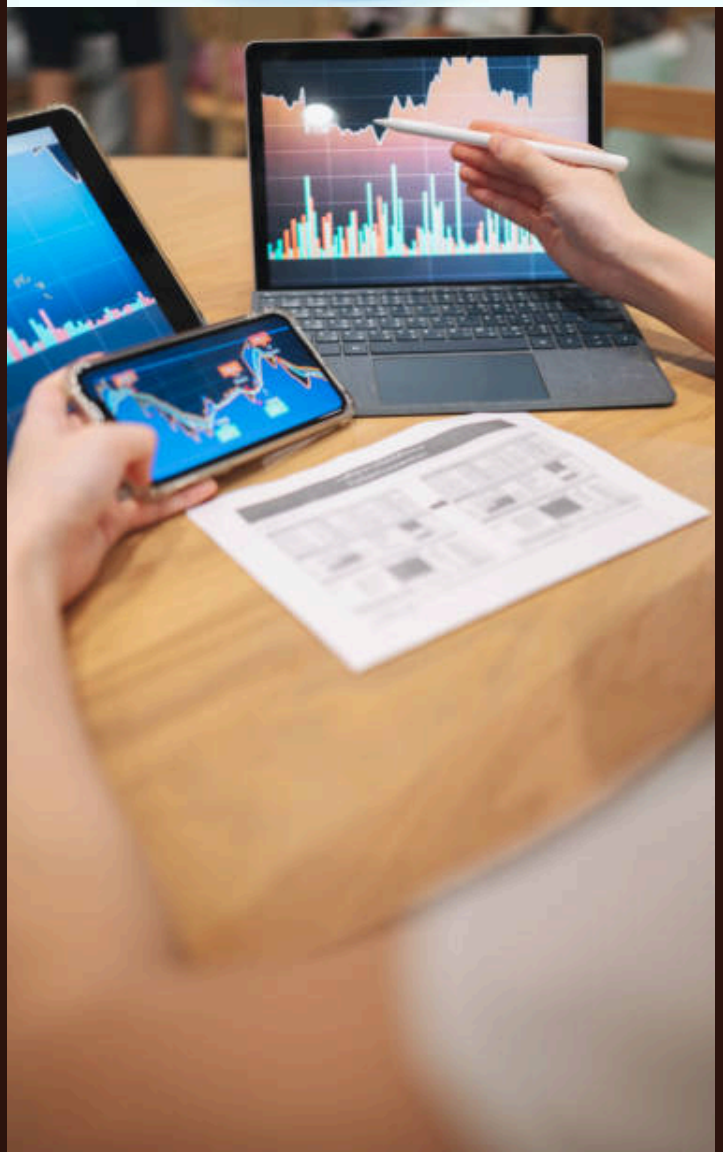


WHAT IS YOUR DEFENSIVE STRATEGY?

Always Validate the Platform's Registration Check with **Securities Commission Malaysia (SC) or Bank Negara's list of approved investment entities**. Never rely on just a website. **Ask for license numbers, registration proofs, and cross-check them** with the promoter and method of Investment.

2. SOCIAL MEDIA ADS LURING WITH TOO-GOOD-TO-BE-TRUE PROMISES...

When you see ads that promise **2–3% daily returns**, or **"turn RM1,000 into RM10,000 in days."** SMEs, especially non-finance savvy ones, click, thinking **"this could be my fast breakthrough"**. But behind the scenes, they're entering subgroup funnels, manipulated to deposit more and more.



Think about it, as a SME Business Owner, does these returns make sense to you?

If it does not compute to make that type of profit at least **legally**, then you know it's a **scam**.

DEFENSIVE STRATEGY : ALWAYS DEMAND WITHDRAWAL PROOF & TEST WITH SMALL AMOUNTS.

If you do decide to Invest, after considering the pros and cons, before sending large capital, test with the investment with small sums. **See if you can withdraw within 24–48 hours.** If delays or excuses pop up, that's a red flag to watch out for.

3. THE NEW WORLD OF AI / DEEPFAKE IMPERSONATIONS

Scammers now clone voices (WhatsApp calls that sound like your CEO), or **Deep-fake videos of VIPs endorsing "Investment Opportunities." I have seen some Ex-prime ministers and current famous politicians in these type of ads on-line and was shocked myself.**

In one reported case, a travel agent in Terengganu lost **RM49,800 after a voice impersonation scam according to daily The Malay Mail**. I personally have seen clients been scammed into Gold and other supposedly sure-fire investments over the last 2 years.

DEFENSIVE STRATEGY : MAINTAIN INDEPENDENT CONTROL OVER FUNDS & CREDENTIALS.

Never allow someone else (an "employee") trusted or not to control your bank accounts, crypto wallets, or private keys. Keep your financial processes internal.

Sometimes unfortunately they may be thinking they are doing it for you with their best intentions.

4. PONZI & MLM FRONTS DISGUISED AS LEGIT FUNDS.

Now with **sophisticated AI**, **they create amazing websites and E-Brochures to entice you**. They lure you into chain-based schemes disguised as **"Investment Systems."** They pay early participants with funds from new participants until the flow collapses.
These often look **"exclusive" and "limited participation,"** making them harder to spot.

DEFENSIVE STRATEGY : DO A COMPANY SEARCH AND CHECK OUT THEIR PAID-UP CAPITAL.

Request for their Company Documents and Paid-up capital confirmation. If possible, also ask for third-party audits or evidence of actual operations (offices, staff, contracts). **Scam fronts often skip real operations (Very Important)** as they live on paperwork and virtual dashboards.

5. UNAUTHORIZED AGENTS & RECRUITMENT-LINKED SCAMS.

Some scammers pretend to be agents who guarantee funding or business development advice.
They mostly target SMEs in cross-border trade or manufacturing, especially when it comes to fund raising and bank loans.
Once they get your involvement, they ask for **"legal or processing fees," "registration charges," or "compliance deposits."** Many go into escrow accounts or fixed deposits that can never be released.

DEFENSIVE STRATEGY : EDUCATE YOUR TEAM AND IMPLEMENT "SCAM REVIEW" PROTOCOLS

Train your finance/operations team to spot irregularities:

1) Someone pushing for immediate funding.

2) Pressure to recruit others

3) Unusual payment routes (mules, multiple bank transfers)

4) Always pause and review before making decisions.

MY CLOSING MESSAGE:

The **RM 750 million loss** is not just a statistic, it's a **WARNING**. It says loud and clear: SMEs that don't equip themselves will become prey.

But knowledge is your shield. When you join **The Business Conclave, you don't just get lessons**, you get real stories, tested frameworks, and a community that has your back.

Don't let your next business decision be a gamble! Inflate your defenses, sharpen your senses and let the Vault at The Business Conclave be your war chest.

This is how smart businesses survive. This is how they thrive.