How to Spot a Scam So You Don't Become the Next Victim

Description

In December, Singaporeans lost over S$8.5 million to scammers. Of this sum, about S$2.7 million was lost to phishing scams masquerading as OCBC over the Christmas weekend alone.

Source: Business Times

Some scammers are even worse than scum, and continue to prey on the same victims by running a "recovery room" scam. This basically exploits our feelings of loss and shame, and how the scammers do it is that they pretend to be someone who can help you get back your money, such as a "bank officer", the "police", or the "CIA", or even the "FBI" *(don't laugh – that's exactly what happened to my mom).*

It is sad but this will continue to happen if we're not careful. And while this time the scammers pretended to be OCBC, it could very well be DBS or UOB tomorrow, or even SingPost, the police, the Ministry of Health, or any other institution.

When you click on suspicious links or input your login details into fraudulent websites, it is extremely difficult for the bank / PayPal / financial institution to be able to verify whether that particular transaction is authentic or not.

Scammers may create SMSes th
they are from "OCBC", BUT:

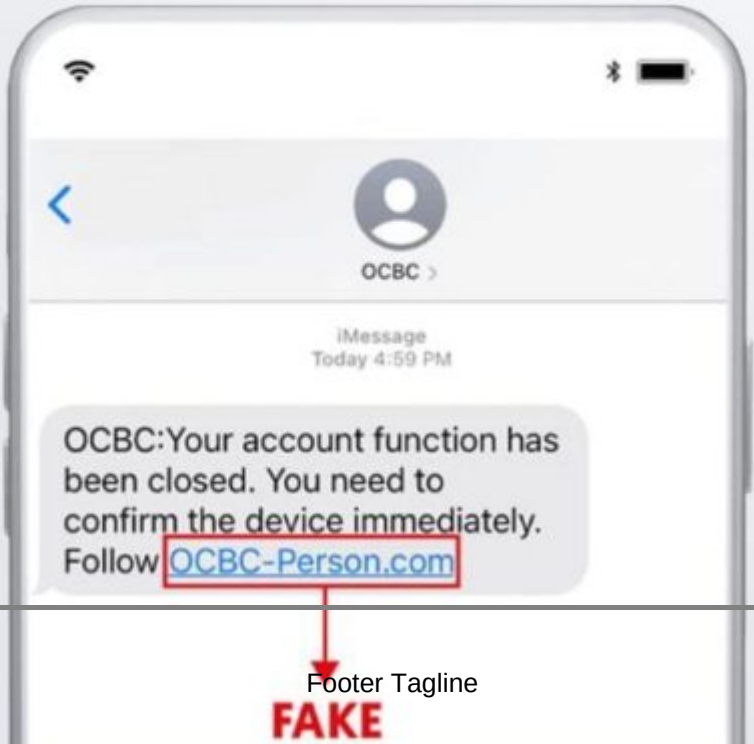
1. We will **never** send an SMS to inform you about
   or being locked out of your account.

2. We will **never** send an SMS with a link to reacti

3. **Don't** click on links in SMSes. Use OCBC's officia
   app or type www.ocbc.com directly in your br

4. **Don't** provide your log-in ID, password or OTPs
   (One-Time Passwords received via SMS) to any
   into unverified webpages.

5. If you're ever in doubt, call our hotline directly
   Do not call any numbers provided in the SMS.



And while it is easy for us to point fingers and say – SingTel should have been more careful! OCBC / DBS should have warned us! – the truth is, **the scammers are always changing their tactics.**

Once a number has been flagged as a potential scam number, they can easily just buy a new SIM card and use a new contact to continue cheating more victims.

Once a scam tactic has been exposed, they can easily change their story.

So if you don't learn how to be careful and protect yourself, you may very well become the very next victim.

And the worst thing is, **you're not likely to get any of the money back.** By the time you realised you've been scammed, the scammers would have likely already made multiple transactions and transfer to hide their digital footprints, making it extremely difficult to trace it back to them.

Based on what we've seen so far, there are more than one type of scams:

- Parcel / Delivery scam
- E-commerce scam (cash on delivery)
- Tech support scam
- Pretending to be government *e.g. "police" scams, "MOH" covid-19 scams*
- Job scams
- Love scams
- Investment scams
- Phishing scams

I can only imagine that more versions and scams will evolve and we'll be adding to that list as the years go on.

I've written extensively about scams in the past, but here's a quick summary of (updated) tips on how you can try to keep safe:

1. Do not pick up any calls that start with a +65.

Do not pick up any calls from a number that starts with a +65. That's just an overseas scammer masking their identity as a local line to cheat you.

2. Do not respond to unsolicited text messages or emails.

If you are using an iPhone, download the ScamShield app here which should help to protect you against known scam numbers that have been reported to the police.

And my mantra is, if someone needs to reach you urgently, they can always find other ways to contact you.

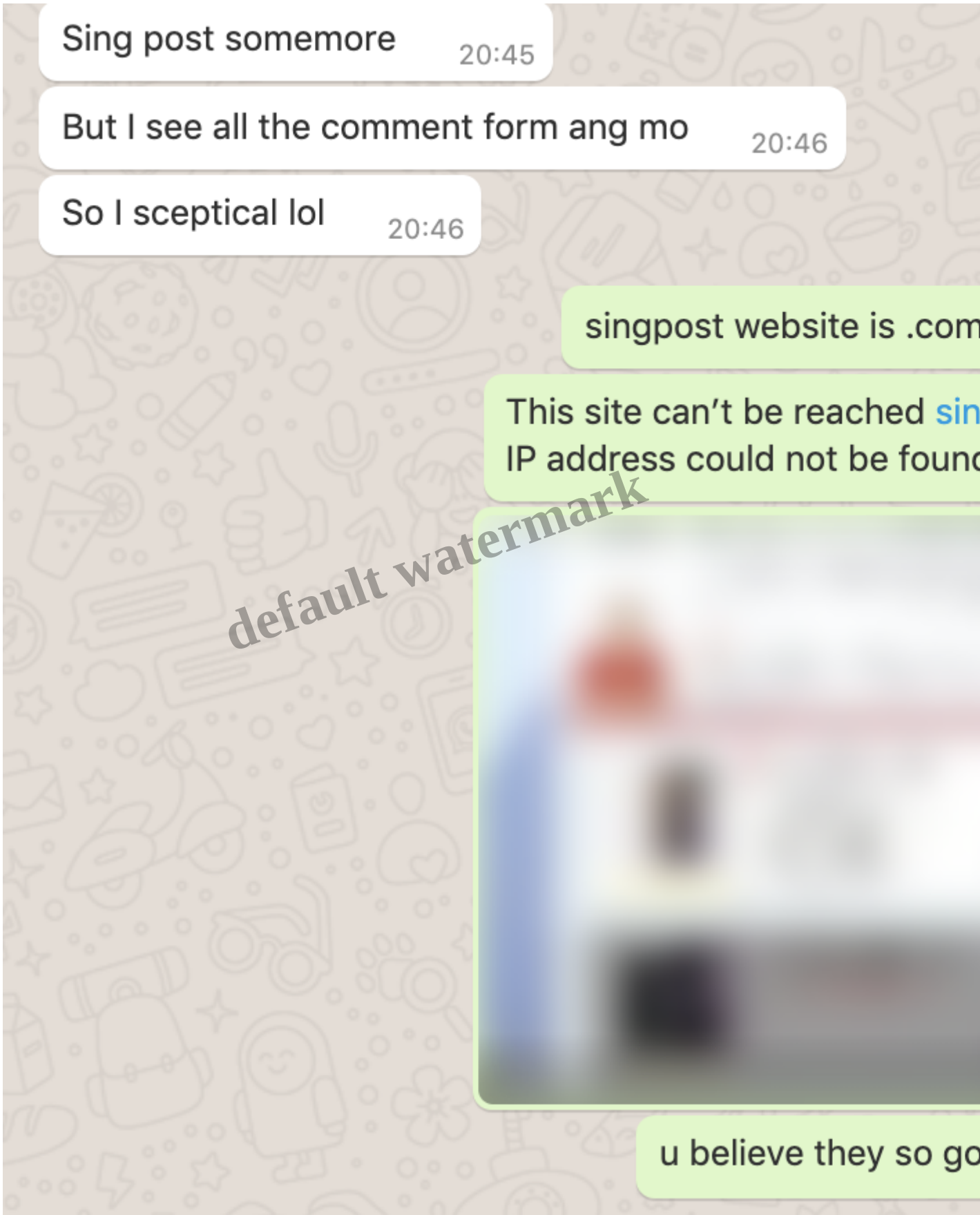
3. Never click on dubious URL links.

No decent institution or organisation will ever send you a bit.ly link! (and any that does is being very unprofessional so you can ignore them).

4. Even if a link looks legitimate, look out for potential red flags.

It will only take a few seconds for you to run a Google search to verify if a link is legitimate.

Earlier this year, even my husband nearly fell prey to a Singpost SMS scam where the URL was singpost.sg. While it looks legit, a quick search online will show you that the URL is fake.



I also almost got fooled by a Singpost scam SMS a few months ago which contained a perfectly legitimate-looking URL (of which I can no longer recall, because I've deleted the SMS). The SMS was supposedly for tracking the status of a delivery, and coincidentally, I was indeed expecting a registered parcel from Singpost at that point in time as well.

The website also looked exactly like Singpost's, but when I scrolled down and tried clicking around to confirm, I realized that the "Investor Relations" link did not work. Which makes no sense, because any listed company will definitely make sure their IR page is working.

That little error by the scammers saved me from putting in my personal details into that dodgy-but-perfectly-legitimate-looking website.

But now that I've shared this, I won't be surprised if future scammers make sure their IR links is working. They adapt fast, you see.

5. Double-check with friends or family members first.

Before you fill in and submit any personal details, make any payments or even right before you click any links, it never hurts to check with someone you trust.

A second eye might very well spot something that you've overlooked.

6. Verify the authenticity of the information with the official website or sources.

If you're lazy and don't even want to double-check, then the fault is entirely on you.

If you tried checking but the official source(s) aren't responding / are slow to respond, you can always just ignore the link / payment request / verification request.

7. NEVER ever disclose your personal details, Internet banking details or One-Time Password to anyone!

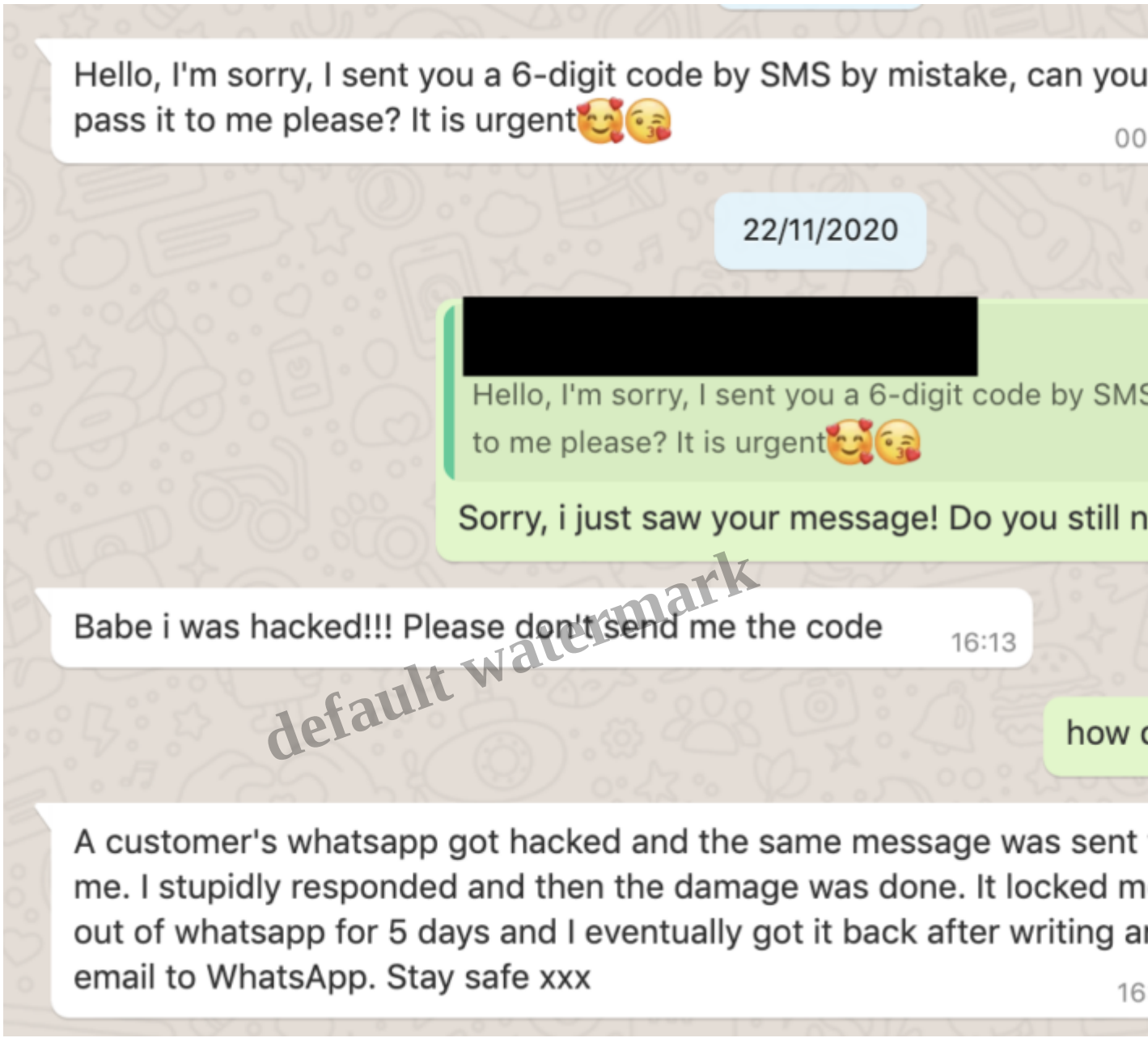
If you give scammers your login details, that's on you.

If you give scammers your OTP, then that's on you too.

So…just don't.

8. If you receive an OTP for a transaction you didn't make, check or report it.

An OTP could be a sign that someone has logged in with your online banking credentials (or credit card / account details) and is trying to make a payment, which triggered the OTP SMS. So if you're not doing any transactions then, this would be one red flag to check.



Sometimes, it could be a genuine error – this happened in my case where someone transacted on a platform and accidentally keyed in my phone number while setting up their 2FA. I immediately called DBS to check when I received the OTP SMS.

It never hurts to double check.

9. Only access payment portals via its official website or mobile banking app.

For the elderly, you can even bookmark the official websites for them so that they won't click on fake links that are being advertised on Google.

10. Have a habit of checking your online statements at least once a month.

This not only helps you to spot unauthorized transactions, but also helps you get a better sense of what you've spent on, and can even save you money when you see subscriptions that you may no longer be using but are still being billed for.

Conclusion

Scams are becoming more commonplace these days. Even educated folks can fall victim to these scammers, which is why your best defense is to always remain skeptical and extra careful. Having a good command of English helps as well (for now, at least until the scammers catch up), and when in doubt, always double-check with either your loved ones or the party itself / himself / herself.

With love,
Budget Babe

Category

1. Savings