Scam Alert! DHL Scammers Are Now Impersonating OCBC, DBS, MOM & SP Services

Description



Here are their tactics.

It could happen to any of us – the latest news is that of a 30-year-old couple falling prey to a phone scam in Singapore and losing \$70,000 in savings to the scammers.

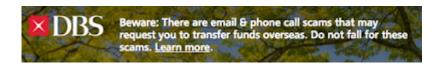
My guess is that the couple are probably a highly-educated pair, considering that they've earned enough to be able to upgrade from their five-room HDB flat to an executive condominium recently. FYI: Most ECs sell up north of \$750,000 – \$1 million, whereas a five-room HDB averages \$350,000 to \$550,000.

Don't you hate it when stuff like these happen? I mean, here on Budget Babe I've been writing about how to save more, invest better, and other tips on managing your personal finances...yet all that money can be lost in minutes if you fall prey to the scammers.

Lest you think you're too "smart" to be tricked, note that the scammers are also becoming smarter in their tactics. So do yourself a favour, keep yourself informed of their latest methods, and share this with your friends and loved ones (especially elderly parents) to prevent them from becoming the next victim.

The online scammers call us Singaporeans "easy targets" and many make a living out of scamming us — let's not let them have it easy...least of all not our hard-earned money!

Here are some of the latest ones:



OCBC / DBS scam

Type 1:

You'll get a call from a scammer claiming to be a bank officer from OCBC or DBS, saying that there were credit cards applied in your name which were swiped overseas and you're overdue for payment.

Type 2:

You get a automated call from the "bank" informing you that you have an important letter or bank statement which you have to collect.

Sample of the phishing email pretending to be sent from DBS.



Type 3:

This one is an email scam, rather than a phone call. I recently received an email from DBSAdvice@dbs.com with "Transaction Advice" as the subject, containing a zip file attachment titled "Account Statement".



MOM Employment scam

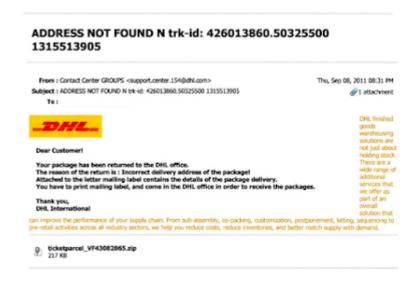
You receive a call from "MOM" informing you that there has been issues with your work pass application, and that you're requested to transfer money to resolve this.



w watermark

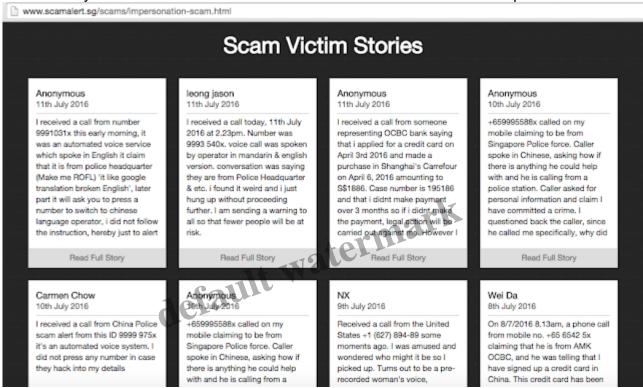
SP Services scam

You'll get a call from "Singapore Power Services", telling you that your utilities accounts are in arrears or that your electricity meters require changing. You'll then be asked to make payments to a designated bank account.



Parcel / DHL scam

You get a call from a "courier company" (often DHL) informing you that your parcel had not been picked up. When you get connected to a "courier staff member", they'll tell you that your parcel has been held as it was found to contain prohibited items (either fake passports or weapons). They'll then request for your personal and bank information, or transfer you to a "customs officer" who will instruct you to remit money to an overseas bank account to avoid action from the local police.



You can read more about them here.

Within this year alone, Singapore has lost over \$4 million to these scammers. Don't be the next victim! I've consolidated the tips provided by the police, government and banks below, together with some of my own:

1. Do not pick up calls from unknown numbers.

Scammers are now using caller ID spoofing technology to display a different number from their actual ones. Calls that appear to be from a local number may not actually be made in Singapore. If you receive a suspicious call from a local number, hang up, wait five minutes, then call the number back to check the validity of the request.

If people really need to reach you, they'll find another way of contacting you. I never pick up calls from anyone who isn't in my contact book; even if it is a friend, they'll eventually message me so I can call them back.

BB tip! Activate caller ID services through your local telco for \$5 a month, or download Contactive the app to try to figure out who's behind the number calling. The app has saved me from many unwanted marketing calls this year!

2. Do not provide any personal info or bank details over the phone.

This includes your bank account number, telephone PIN, online banking username and password, OPT token code, and more.

If you're concerned, you can always call the bank directly to verify if the call is genuine before divulging any personal data.

3. Hang up when you're asked to transfer or remit money.

No bank or government agency will ever inform you to transfer money through a phone call, especially to a third party's bank account. Demand for a physical statement as proof to confirm the authenticity of the claim, or verify with the agency directly by calling back.

4. Call a friend or a trusted relative before you act.

In the latest case, the 30-year-old woman admitted that she was too emotionally distraught to think logically when everything was happening. Seek a second opinion before you do anything, especially when it concerns money.

Keep your hard-earned money safe and to yourself. Don't lose it to these scammers.

With love, Budget Babe Category

1. Family