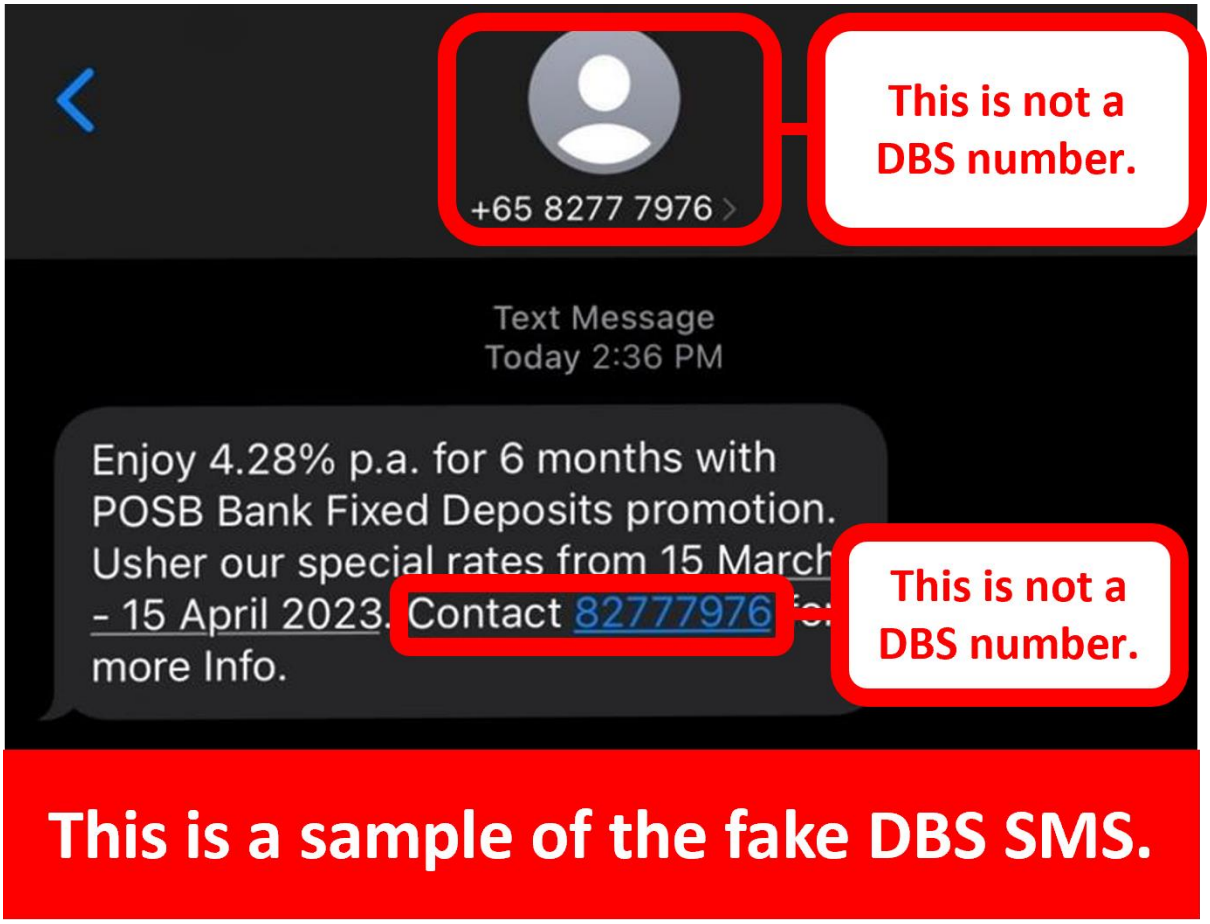
## DBS SMS Phishing Alert

**Date:** **06 April 2023**

**Description:** Beware of phishing SMSes targeting you with fake DBS promotions, such as DBS Fixed Deposits offering 4.28% p.a. for 6 months. These SMSes may ask you to contact a phone number to learn more. However, these SMSes are scams, and the person on the other end is not a DBS representative.




The scammer may attempt to trick you into transferring money to their bank account, or they may request your DBS login information and digital token approval code. If they acquire this information, they can use it to steal your bank funds or access your account without your permission.

Never reveal sensitive details to scammers, such as your login credentials or PINs, as they can use this information to conduct unauthorized transactions on your cards or bank account.

If you have shared your Username-PIN Code combination with any non-DBS websites or mobile applications, we strongly advise changing your PIN Code immediately.

You may do so by following the instructions here.

**Customers are advised to be mindful of such scams.**

Customers are reminded to ensure they are on DBS's official website or use DBS's official mobile applications to conduct any DBS bank-related requests. Go directly to https://www.dbs.com to ensure that you are on our website.

Remember: Do not give out your Internet Banking credentials, OTP, Digital Token, or any DBS-related email or SMS verification approvals to other individuals, non-DBS websites, or mobile applications. Do not give your credit or debit card details out to unknown websites.

- Emails and SMSes from DBS will not include clickable links. Always go directly to our website to verify the authenticity of any banking-related requests or offers.
- DBS will never ask you for your credit or debit card details, CVV, SMS or email OTPs, or Digital Token approvals to verify or unlock your account.
- Do not call phone numbers, click on URL links, or scan QR codes in unsolicited emails, SMS, or other Messaging Application messages.
- Never disclose your card numbers or OTPs to unverified sources. Bank staff and government officials will never request your card details, OTPs, or Digital Token Approvals through SMS, voice calls, or unofficial websites.

**Call us immediately at the hotlines below, message our chatbot, or visit our Quick Links for Self-Service page (if available in your country) if you suspect you're a victim of fraud or notice any unexpected banking or card transactions.**

**Singapore:** 1800-339-6963 or 6339-6963

**Singapore Quick Links for Self-Service:** https://www.dbs.com.sg/personal/bank-with-ease/contact-us

**China:** 400-820-8988

**Hong Kong:** 2290 8888

**Hong Kong Quick Links for Self-Service:** https://www.dbs.com.hk/personal/contact-us.page

**India:** 1-860-210-3456

**Indonesia:** 0804 1500 327

**Taiwan:** (02) 6612 9889 / 0800 808 889

**Scamshield Feature - For Singaporean customers**

ScamShield is an initiative by the Singapore Police Force and the National Crime Prevention Council. Singaporean customers may find more information on ScamShield at https://www.scamshield.org.sg/.

**Block scam calls** – ScamShield compares an incoming call against a list maintained by the Singapore Police Force to determine if the number has been used for illegal purposes and blocks it.

**Filter scam SMSes** – When you receive an SMS from an unknown contact, ScamShield will determine if the SMS is a scam using an on-device algorithm, and filter the messages to a junk SMS folder. Scam SMSes will be sent to NCPC and SPF for collation to keep app updated and help protect others from such scam calls and messages.

**Report scam messages** – You can also report scam messages from other chat apps such as WhatsApp, Wechat, IMO, Viber, etc. You can forward the messages via ScamShield's in-app reporting function.