Scams

Phone Scams (New)

24 January 2020

It has been brought to our attention that there is a party or parties involved in making phishing telephone calls purporting to be representing Maybank. The caller impersonates a Maybank staff and informs the victim that his/her account will be closed within 10 minutes, and requests for the victim to provide personal information (e.g. NRIC/Passport number, bank account number and name of account holder) if he/she does not wish for the account to be closed. We wish to alert the public to phone scams and customers should never divulge their personal information to unsolicited callers. Maybank will not request for customers' PIN, password or OTP through phone call, email or SMS. Do not proceed with the call if you suspect that the caller is asking you to conduct suspicious transactions.

How to protect yourself

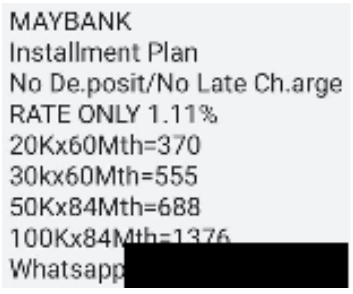
- Stay alert. Never provide personal or confidential banking account information to unsolicited callers.
- Alert Maybank if you receive an email, letter or a telephone call requesting for personal or confidential banking account information.
- Contact us at **1800-MAYBANK** (1800-629 2265) or (65) 6533 5229 (Overseas) to verify the contents of the call.

Customer Advisory (SMS Scams)

14 January 2020

We have received reports of ongoing SMS scams impersonating Maybank to offer loans. If the victim contacts the number provided in the SMS, the scammer may attempt to impersonate Maybank staff in order to steal personal information (e.g. NRIC details) from the victim.

Samples of the SMS – January 2020



Note : This SMS is NOT from Maybank.

How to protect yourself from scams

- Be alert and always verify the details in the messages from Maybank. Always check that the message reflects your intended actions and do not proceed or authorise suspicious transactions.

- Contact us at **1800-MAYBANK** (1800-629 2265) or (65) 6533 5229 (Overseas) to verify the contents of the SMS.
- Never reply to unsolicited SMSs or emails. Responses to such SMSs or emails could be used by fraudsters to socially engineer information or trick users into performing unwanted actions. Be cautious of "unsubscribe" links as these may also be used to socially engineer information as well.

Technical Support Scams

There are reports of cases whereby the call scammers contact the members of the public claiming to be investigating a cybersecurity issue. The victims were led to believe that they were talking to a staff of the Cyber Security Agency of Singapore (CSA) or a government agency that deals with cybersecurity. The scammers would then attempt to trick victims into logging into their online banking accounts and transferring money to them. We would like to share that government agencies will never request for access to your online banking accounts or ask for transfers of money over the phone.

How to protect yourself from scams

- Beware of any unsolicited calls from persons claiming to be a staff of a government agency.
- Do not install any applications suggested by the scammers.
- Do not panic and do not follow any instructions to install any applications, type the commands into your computer or log into your online banking accounts.
- Ignore the calls and the callers' instructions.
- Call us immediately at **1800-MAYBANK** (1800-629 2265) or (65) 6533 5229 (Overseas) if you notice any unknown transactions appearing on your account or if you suspect that you have been a victim of fraud.

Reference
SingCERT, last retrieved on 06/12/2019

Business Email Scams

There are email scams targeting businesses by impersonating the businesses' CEOs, business partners or suppliers. Scammers used spoofed email accounts to pose as business partners, requesting for funds. Victims were led to believe that they had received genuine requests and transferred funds to the requested bank accounts.

Spoofed email addresses often include slight misspellings or replacement of letters, which may not be obvious at first glance.

Genuine email address	Spoofed email address
123@gmail.com	I23@gmail.com
abc@deshipping.com	abc@deshpping.com
lisa@faber.com.cn	lisa@faber-cn.com

Some scams may also imitate legitimate emails sent by businesses using logos, adding links to the business websites or adopting the business messaging formats.

What to do next?

- Educate your employees.
- Update your business operating system with new security patches regularly.

- Ensure that the sender's email address is genuine.
- Verify such requests by using the sender's official contact details, instead of using the contact details provided in the emails.

Reference
Channel News Asia, last retrieved on 26/11/2019, 1747hrs GMT+8.

Debt Collection, Kidnapping and Other Scams

Debt Collection Scams

It has been brought to our attention that there is a party or parties involved in making telephone calls to members of the public, purporting to be representing Maybank, collecting debts on behalf of the Bank. The caller(s) will claim that the customer has outstanding amounts owing to the Bank due to their spending on their credit cards, and request that they pay up the money by cheque. Most of these calls are made via an Overseas Number and on some occasions, the party has identified himself as a "Steven Lim Mun Kin" or "Vincent Tan".

We wish to inform members of the public that these calls are not made by representatives of Maybank and these people are not Maybank staff. You may make a report to the Police if you should receive similar calls.

Kidnapping scams

There has been a rise in the number of cases reported on people being threatened with the lives of their loved ones in exchange for ransom money which the "kidnappers" demand to be transferred to an overseas bank account. These "kidnap conmen" would insist that the victims continue with the telephone conversation and not hang up their mobile phones for as long as the transfer has not been completed. Under duress, for fear that the lives of their loved ones may really be threatened, the victims give in to the conmen's request.

On 4 Sep 2007, one such incident occurred at Maybank@JurongEast. The staff attending to the victim then was vigilant and calm, hence, managed to understand the situation by asking the victim to scribble useful information on a piece of paper. The conmen's plans were then thwarted after the victim's son contacted her upon being alerted by our staff.

Other scams

Whatever the reasons the conmen have, the ultimate request on the victims will be to transfer their hard-earned money to another account. Some of the ploys used to entice or coerce the victims to comply include:

- Lure of fictitious lottery or lucky draw winnings
- Lure of fortune from a fictitious will
- Prey on fear of the law (posing as police officers or Supreme Court staff)

Please do not hesitate to call us on **1800-MAYBANK** (1800-629 2265) or (65) 6533 5229 (Overseas) if you need further clarification.

SMS Scams

It has been reported widely that an ongoing scam targets victims not familiar with Internet Banking (IB) and its related controls.

- A potential victim receives an SMS congratulatory text or call to inform that they have won prizes from a well-known organisation

- He/She is then tricked into applying for Internet Banking features for his/her account using the fraudster's mobile number
- Victim is also asked to reveal the User ID and Password to the fraudster
- With the Internet Banking User ID and Password, the fraudster can then log into the victim's account and receive a One-Time Password (OTP) via SMS (as a result of applying for IB features with the fraudster's mobile number) to perform illegal transactions

Please be reminded that all information used to perform banking transactions **should never be disclosed to any unknown parties**. When applying for Internet Banking, customers should use **ONLY** their personal mobile number for registration and to receive their SMS OTP.

Customers should always contact the Bank when in doubt and to report any discrepancies.

Alert Archives

Phishing - SingHealth Data Breach

24 July 2018

SingHealth reported that its database containing about 1.5 million patient particulars and outpatient dispensed medicines had been the target of a major cyberattack. The patient data stolen included information such as name, NRIC number, addresses, gender, race and date of birth. Information on the dispensed medicines of about 160,000 of these patients had also been stolen.

Customers are advised to be cautious of the potential use of these stolen credentials by hackers to conduct social engineering and phishing scams on your financial account. Such scams utilize personally identifiable information to appear legitimate.

How to protect yourself

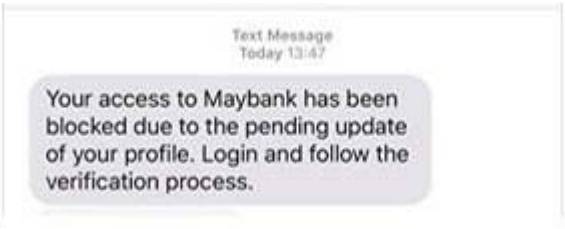
- **Stay alert.** Never provide personal or banking information to unsolicited callers.
- **Never disclose any sensitive personal information (such as login passwords or one-time passwords) over the phone or email.** Maybank will never request such information from our customers.
- **Call Maybank immediately if you are in any doubt of a call, SMS or email's authenticity.** Contact our Customer Relationship Executives immediately at 1800-MAYBANK (1800-629 2265) or (65) 6533 5229 (if you are calling from overseas), if you receive such calls.

Phishing - SMS Phishing Alert

20 June 2018

We have been alerted of a phishing SMS that leads to phishing webpages targeting Maybank customers. If a customer receives the phishing SMS and clicks on the link, he/she will be redirected to a page requesting for user ID and PIN combinations, credit card number, expiration date and CVVs. Such websites are used to conduct card not present transactions but may also be utilized in order to steal personally identifiable data or promote fraudulent applications.

Sample of the malicious SMS. This is **NOT** from Maybank.



How to protect yourself

- **Be alert.** Minimize clicking on links in SMSs as these may not be legitimate.
- **Ensure you are using the official Maybank website.** Always type the Maybank website URL (www.maybank2u.com.sg) directly into your web browser. If you are on mobile, consider using our official Maybank Mobile Banking (Maybank SG) App.
- **Do not reply to unsolicited SMSs**. Responses to such SMS could be used by fraudsters to socially engineer information or trick users into performing unwanted actions.
- **Provide your credit card details only if you are making a direct purchase**. Always check that you intend to conduct a credit card transaction and do not provide an OTP to authorize payment if you are not.
- Maybank will never request for your PIN, password or OTP through SMS, phone call, or email. Should you have further queries, please do not hesitate to contact our Customer Relationship Executives on 1800-MAYBANK (1800-629 2265) or (65) 6533 5229 (if you are calling from overseas).

---

25 May 2018
We have been alerted of a phishing email campaign impersonating the Monetary Authority of Singapore (MAS) recently with the following details:
Sender email information displayed: Monetary Authority of Singapore. info@mas.gov.sg

Summary of email information:
The email informs the recipient that Singapore banks have been attacked by hackers, and MAS has enacted a new law mandating all customers to update their details with the banks, as well as to register for insurance under the authority. A link is provided for you to update your account.

Phishing details:
Upon clicking the email, the link will re-direct you to a spoofed MAS website. In the following page, it displays the logo of various banks for you to select. After clicking on the bank's logo, you will be taken to a spoofed internet banking page, prompting you to enter your user ID and password. Upon submission, it will prompt for a one-time-password which you will receive on your mobile device. The subsequent page will prompt you for your IC/Passport number, mobile phone number, and date of birth.

Potential impact:
The attacker may use your stolen information to conduct fraudulent transfers on your internet banking account or for fraudulent online purchases.

How to protect yourself

- Alert Maybank if you receive an email, letter, notification or a telephone call requesting for information relating to your PIN/access ID or username/password
- Do not provide your banking particulars, such as ID, password, bank account numbers, credit card or account details by email
- If you receive an email asking you to reactivate or update your account for any purpose or to provide personal account information, please contact Maybank to confirm the validity of the email
- For secured online banking access, always enter the URL address (www.maybank2u.com.sg) directly on your web browser.
- Should you have further queries, please do not hesitate to contact our Customer Relationship Executives on 1800-MAYBANK (1800-629 2265) or (65) 6533 5229 (if you are calling from overseas).

18 May 2018

There is a phishing email reported to be in circulation currently. Phishing emails are fraud attempts as the senders take on the identity of well-known companies such as banks or financial institutions to obtain personal information from the recipients of the email. These emails will often ask recipients to visit a fake website of a bank through links provided in the email, or ask for personal information such as credit card numbers or online banking IDs and passwords, in order to commit identity theft. They will then use the information they have acquired for illegal purposes or to perform unauthorised access to the recipient's online banking account.

How to protect yourself

- Alert Maybank if you receive an email, letter, notification or a telephone call requesting for information relating to your PIN/access ID or username/password
- Do not provide your banking particulars, such as ID, password, bank account numbers, credit card or account details by email
- If you receive an email asking you to reactivate or update your account for any purpose or to provide personal account information, please contact Maybank to confirm the validity of the email
- For secured online banking access, always enter the URL address (www.maybank2u.com.sg) directly on your web browser.

Should you have further queries, please do not hesitate to contact our Customer Relationship Executives on 1800-MAYBANK (1800-629 2265) or (65) 6533 5229 (if you are calling from overseas).

Maybank Singapore Limited (UEN: 201804195C)