Phishing Alert

Customer Advisory

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.

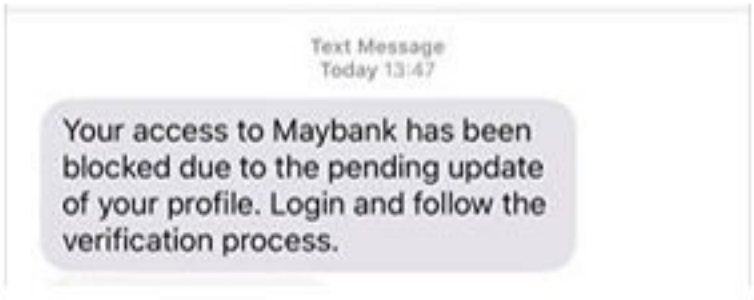
How to protect yourself

- **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.

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).

---

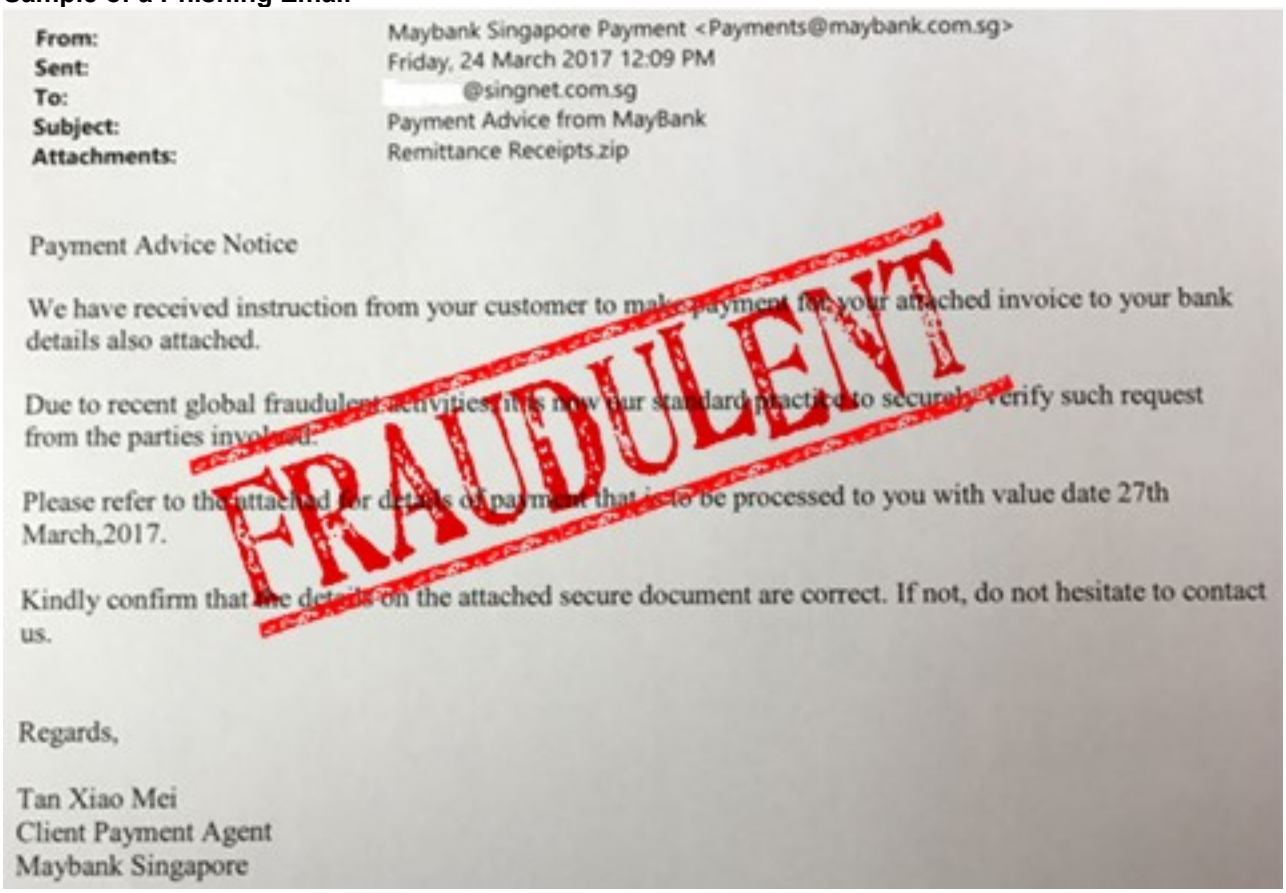
18 May 2018
There is a phishing email reported to be in circulation currently. Phishing emails are fraud attempts as the senders take on the identity of well-known companies such as banks or financial institutions to obtain personal information from the recipients of the email. These emails will often 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).

---

03 Apr 2017
It has been brought to Maybank's attention that some members of the public have received email from Maybank (e.g. payments@maybank.com.sg) requesting customers to either click on a website link or an attachment to verify accounts or transactions. This is done with the intention to illegally obtain customers' credentials or execute malicious activity on customers' personal computers or laptops.
Maybank would like to clarify that such email messages are not issued by Maybank and advise customers NOT to click on any links or attachment contained in the email. Customers who have clicked on the link in such emails are advised to change their passwords immediately, by **directly logging** into **Maybank2u.com.sg**. Maybank would like to advise all customers to **NOT** reveal or disclose your passwords to anyone at any time online or on the telephone.
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 oversea

Sample of a Phishing Email



---

11 Feb 2016
Dear Customer

Recently, there were URLs discovered, such as **http://maybankk2u[dot]com** and **http://maybank2u-my[dot]com** that lead to a fake website which is a phishing site (see below). These phishing websites had malware in them that will infect your computer.
This is **not** a Maybank webpage

Here are some precautionary measures to protect your computer:

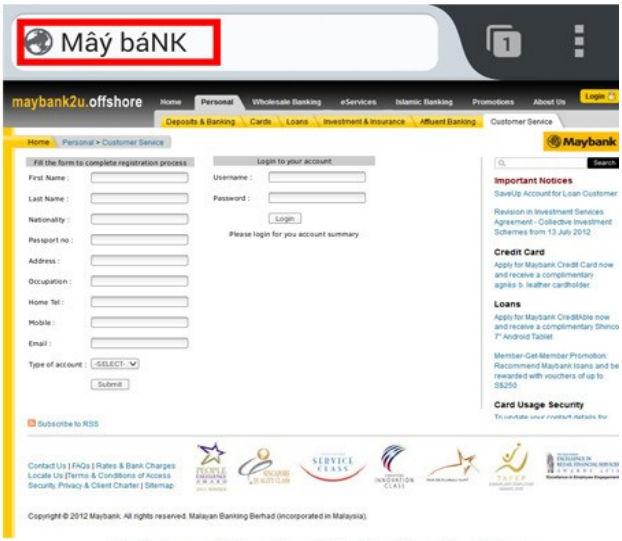
- Do not open any attachments in emails from unknown senders
- Always enter the URL address (www.maybank2u.com.sg) directly into your web browser
- Keep your computers, devices and softwares up-to-date
- Use a professional anti-virus software and keep it up-to-date
- Perform regular anti-virus scan
- Perform regular update of your browsers and operating systems whenever an update is available
- Make sure that your Internet browsers and plugin/extensions are all up-to-date
- Disable plugins/extensions that are not frequently used or are potentially dangerous

Should you notice any unauthorised transactions, please change your passwords immediately, and contact us at **1800-MAYBANK** (1800-629 2265) or **(65) 6533 5229**(Overseas).
For Business Internet Banking users, please call **1800 777 0022**.

Dear Customer

There is a phishing email reported to be in circulation currently.

If you receive such an email, please delete it immediately and do **NOT** click on the url or link **www.mbsgoffshores.com** in the email. The url will lead you to a **fake** website, which is a phishing site. This phishing website will attempt to solicit your Maybank Online Banking credentials for further fraudulent activity. (See below)
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).



This is **not** Maybank's Online Banking login page

How it works

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.

Examples of phishing emails in circulation

- Urgent Alert - 3 Jun 2011
- Maybank Alert: Account Maintenance Update - 30 May 2011
- You have a tax refund of RM5, 500 - 19 May 2011
- Unlock Your Account - 19 May 2011
- Your account have been suspended - 10 May 2011
- Important Message - 24 Apr 2011
- Maybank2u.com Electronic Payment - 8 Apr 2011
- Account Reconfirmation - 7 Apr 2011
- You Have Got A New Message - 5 Apr 2011
- Final Notification - 30 Mar 2011
- Account Alert !- 29 Mar 2011

- Payment has been made to your account - 28 Mar 2011

- Maybank2u.com Account Update - 28 Mar 2011
- M2U Important Message - 22 Mar 2011
- The next level of Maybank2u.com security features! - 19 Mar 2011
- M2U Account Notice - 16 Mar 2011
- New Message from Maybank - 15 Mar 2011
- --virus-- Electronic Fund Transfer - 11 Mar 2011
- Electronic Fund Transfer - 10 Mar 2011

- New Login Activation (Urgent-Mandatory) - 9 Mar 2011
- Payment Transaction - 9 Mar 2011
- You have one security message - 8 Mar 2011
- Important Security Alert! - 7 Mar 2011
- Account Validation Is Required - 3 Mar 2011
- Police Alert! - 22 Feb 2011
- Important Message - 23 Feb 2011
- MayBank2u - Online Security - 22 Feb 2011
- The next level of Maybank2u.com security features - 21 Feb 2011
- Important - Resolve issues on your account - 7 Feb 2011
- [Security] Maybank2u.com Transaction Limit Update Required - 7 Feb 2011
- Maybank Alert- February 2011 Security Update - 7 Feb 2011
- [Urgent Notice] Maybank2u.com Account Update - 19 Jan 2011
- Your Profile Needs to be updated - 19 Jan 2011
- 1 Secure Unread Message - 7 Jan 2011

more...

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

Maybank Singapore Limited (UEN: 201804195C)