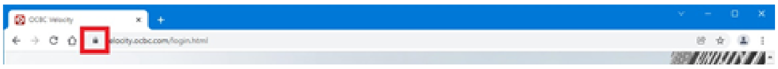
Frequently Asked Questions:
How to safeguard my OCBC Velocity Access

Q1. How do I confirm the OCBC Velocity site that I am accessing is legitimate?

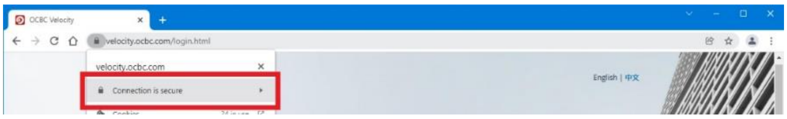
You can follow these steps:

A. If browser is **Chrome** –

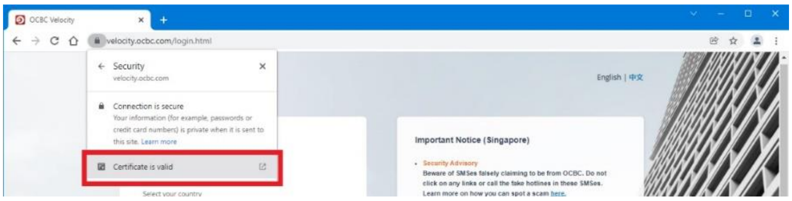
i. Check that the secure lock is enabled. Click on the lock icon next to the address bar.



ii. Click on “Connection is secure” in the drop down.



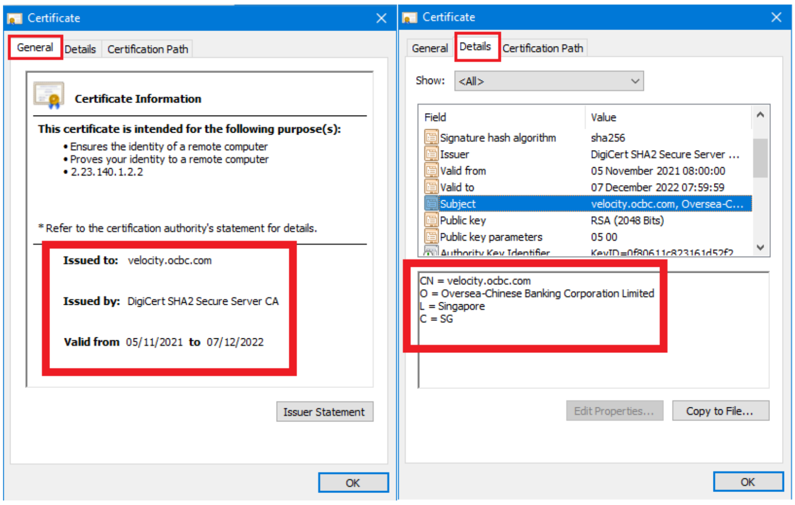
iii. Click on “Certificate is valid” and a window with certificate information will appear.



Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Beware of SMSes falsely claiming to be from OCBC. Do not click on any links or call the fake hotlines in these SMSes. Learn more on how you can spot a scam here.

iv. Verify the issuer information that the certificate is issued to Velocity.ocbc.com, subject is correct, and the validity is current.



Certificate Information

This certificate is intended for the following purpose(s):
- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.23.140.1.2.2

* Refer to the certification authority's statement for details.

Issued to: velocity.ocbc.com

Issued by: DigiCert SHA2 Secure Server CA

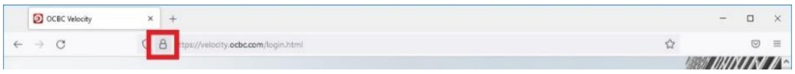
Valid from 05/11/2021 to 07/12/2022

Field	Value
Signature hash algorithm	sha256
Issuer	DigiCert SHA2 Secure Server ...
Valid from	05 November 2021 08:00:00
Valid to	07 December 2022 07:59:59
Subject	velocity.ocbc.com, Oversea-C...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Key Identifier	KeyID=0f80611c823161d52f2

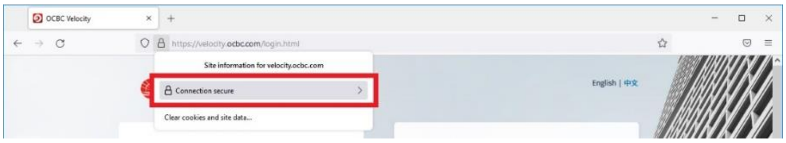
CN = velocity.ocbc.com
O = Oversea-Chinese Banking Corporation Limited
L = Singapore
C = SG

B. If browser is **Firefox** –

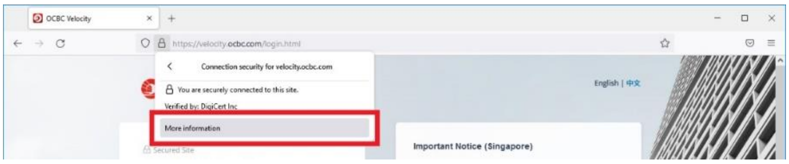
i. Check that the secure lock is enabled. Click on the lock icon next to the address bar.



ii. Click on “Connection is secure” in the drop down.


OCBC Velocity
https://velocity.ocbc.com/login.html
Site information for velocity.ocbc.com
Connection secure
Clear cookies and site data...
English | 中文

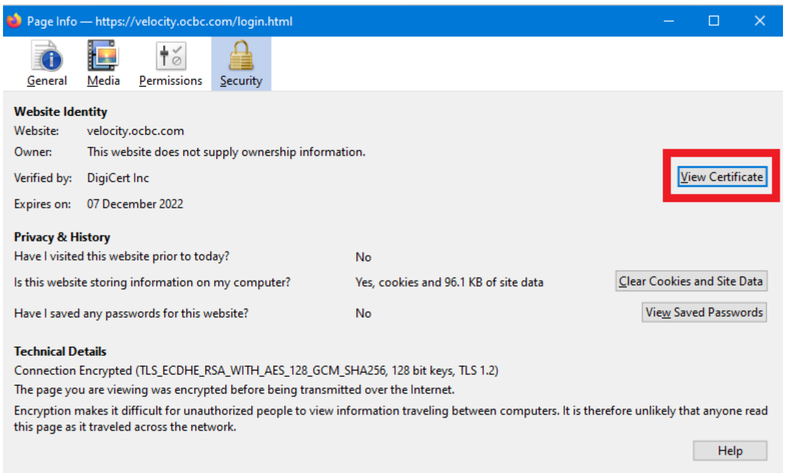
iii. Click on “More information” and a window with website information will appear.


OCBC Velocity
https://velocity.ocbc.com/login.html
Connection security for velocity.ocbc.com
More information
Secured Site
English | 中文
Important Notice (Singapore)

You are securely connected to this site.

Verified by: DigiCert Inc

iv. Click on “View Certificate” button and a new tab with certificate information will appear.


Page Info — https://velocity.ocbc.com/login.html
General
Media
Permissions
Security
View Certificate
Clear Cookies and Site Data
View Saved Passwords
Help

Website Identity

Website: velocity.ocbc.com

Owner: This website does not supply ownership information.

Verified by: DigiCert Inc

Expires on: 07 December 2022

Privacy & History

Have I visited this website prior to today? No

Is this website storing information on my computer? Yes, cookies and 96.1 KB of site data

Have I saved any passwords for this website? No

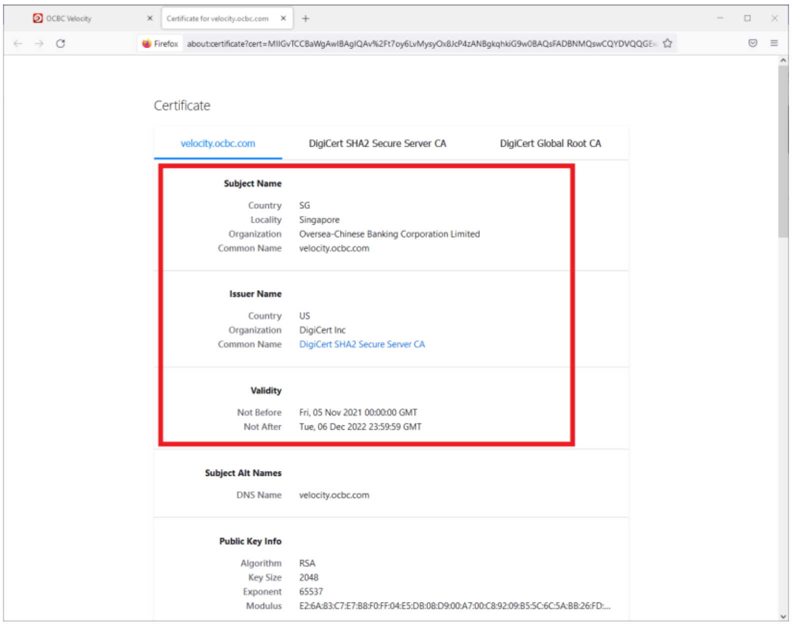
Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

v. Verify the certificate information and ensure validity is current.


OCBC Velocity
Certificate for velocity.ocbc.com
Firefox
about:certificate?cert=MIIGvTCCBaWgAwIBAgIQAv%2Ft7oy6LvMysyOx8JcP4zANBgkqhkiG9w0BAQsFADBNMQswCQYDVQQGE
velocity.ocbc.com
DigiCert SHA2 Secure Server CA
DigiCert Global Root CA

Certificate

Subject Name

Country SG
Locality Singapore
Organization Oversea-Chinese Banking Corporation Limited
Common Name velocity.ocbc.com

Issuer Name

Country US
Organization DigiCert Inc
Common Name DigiCert SHA2 Secure Server CA

Validity

Not Before Fri, 05 Nov 2021 00:00:00 GMT
Not After Tue, 06 Dec 2022 23:59:59 GMT

Subject Alt Names

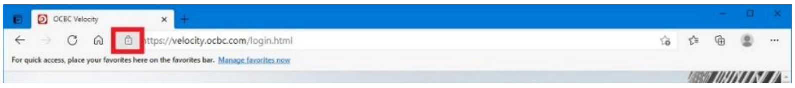
DNS Name velocity.ocbc.com

Public Key Info

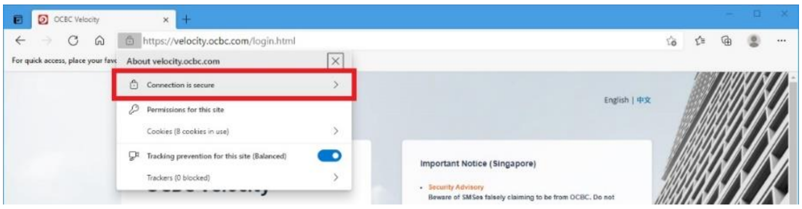
Algorithm RSA
Key Size 2048
Exponent 65537
Modulus E2:6A:83:C7:E7:B8:F0:FF:04:E5:DB:08:D9:00:A7:00:C8:92:09:B5:5C:6C:5A:BB:26:FD:...

C. If browser is **Microsoft Edge** -

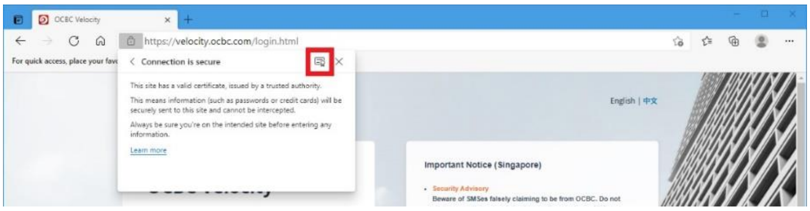
i. Check that the secure lock is enabled. Click on the lock icon next to the address bar.


OCBC Velocity
https://velocity.ocbc.com/login.html
For quick access, place your favorites here on the favorites bar. Manage favorites now

ii. Click on “Connection is secure” in the drop down.


OCBC Velocity
https://velocity.ocbc.com/login.html
For quick access, place your fav
About velocity.ocbc.com
Connection is secure
Permissions for this site
Cookies (8 cookies in use)
Tracking prevention for this site (Balanced)
Trackers (0 blocked)
English | 中文
Important Notice (Singapore)
Security Advisory
Beware of SMSes falsely claiming to be from OCBC. Do not

iii. Click on the certificate icon and a window with certificate information will appear.


OCBC Velocity
https://velocity.ocbc.com/login.html
For quick access, place your fav
Connection is secure
English | 中文
Important Notice (Singapore)
Security Advisory
Beware of SMSes falsely claiming to be from OCBC. Do not

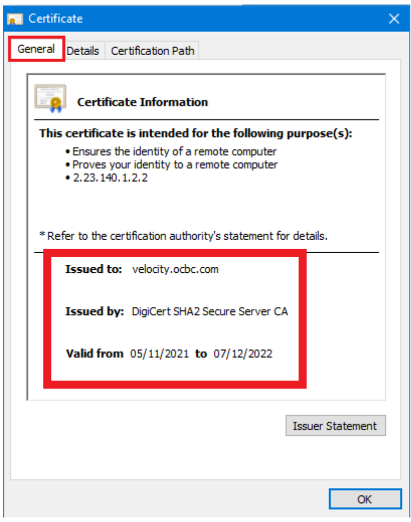
This site has a valid certificate, issued by a trusted authority.

This means information (such as passwords or credit cards) will be securely sent to this site and cannot be intercepted.

Always be sure you're on the intended site before entering any information.

Learn more

iv. Verify the issuer information that the certificate is issued to Velocity.ocbc.com, subject is correct, and the validity is current.



Certificate Information

This certificate is intended for the following purpose(s):

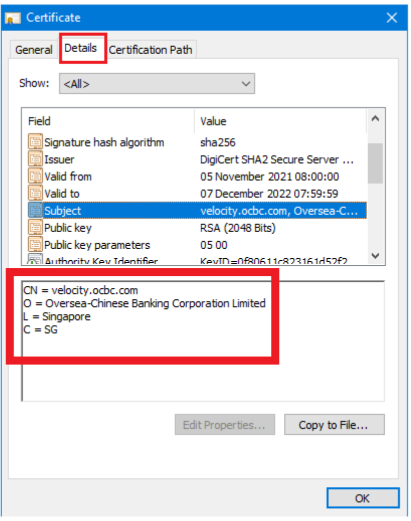
- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.23.140.1.2.2

*Refer to the certification authority's statement for details.

Issued to: velocity.ocbc.com

Issued by: DigiCert SHA2 Secure Server CA

Valid from 05/11/2021 **to** 07/12/2022



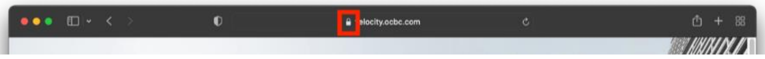
Show: <All>

Field	Value
Signature hash algorithm	sha256
Issuer	DigiCert SHA2 Secure Server ...
Valid from	05 November 2021 08:00:00
Valid to	07 December 2022 07:59:59
Subject	velocity.ocbc.com, Oversea-C...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Key Identifier	KeyID=0f80611c823161d52f2

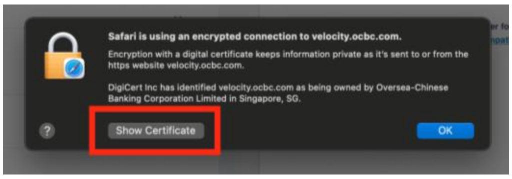
CN = velocity.ocbc.com
O = Oversea-Chinese Banking Corporation Limited
L = Singapore
C = SG

D. If browser is **Safari** -

i. Check that the secure lock is enabled. Click on the lock icon in the address bar.



ii. Click on “Show Certificate” in the pop-up window.

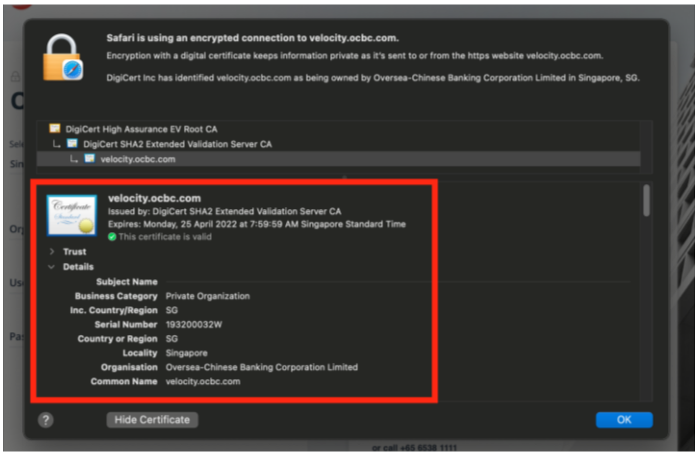


Safari is using an encrypted connection to velocity.ocbc.com.

Encryption with a digital certificate keeps information private as it's sent to or from the https website velocity.ocbc.com.

DigiCert Inc has identified velocity.ocbc.com as being owned by Oversea-Chinese Banking Corporation Limited in Singapore, SG.

iii. Expand the "Details" section and verify the issuer information that the certificate is issued to Velocity.ocbc.com, subject is correct, and the validity is current.



Safari is using an encrypted connection to velocity.ocbc.com.

Encryption with a digital certificate keeps information private as it's sent to or from the https website velocity.ocbc.com.

DigiCert Inc has identified velocity.ocbc.com as being owned by Oversea-Chinese Banking Corporation Limited in Singapore, SG.

DigiCert High Assurance EV Root CA
└ DigiCert SHA2 Extended Validation Server CA
  └ velocity.ocbc.com

velocity.ocbc.com
Issued by: DigiCert SHA2 Extended Validation Server CA
Expires: Monday, 25 April 2022 at 7:59:59 AM Singapore Standard Time
This certificate is valid

> Trust

⌄ Details

Subject Name	
Business Category	Private Organization
Inc. Country/Region	SG
Serial Number	193200032W
Country or Region	SG
Locality	Singapore
Organisation	Oversea-Chinese Banking Corporation Limited
Common Name	velocity.ocbc.com

Q2. I received a message or call from OCBC. How can I verify that the caller is from OCBC and for legitimate purpose?

Verify the person and know the purpose of the call. You may want to take down the number and request for full name and department of the person calling. The email should be "xxx@ocbc.com". When in doubt, you can call us at +65 6538 1111 for assistance required.

Be vigilant and protect yourself from scams. Beware of such messages or calls from persons impersonating as employees from OCBC.

Do adopt the following measures to prevent your bank accounts from being compromised:

- **NEVER** disclose your online banking login details such as Organisation ID, User ID, PIN, and OTPs to anyone. OCBC Bank employees will not request you to reveal your PIN and/or OTP.
- **DO NOT** respond to or authorise any authentication requests (through your OneToken or hardware token) if you did not initiate any online banking transaction.
- If you receive a suspicious message or call purporting to be from OCBC Bank, do not call the number provided in the SMS or by the caller. Please call us at +65 6538 1111 to verify the authenticity of the request.

Q3: How do I ensure that my OCBC Velocity User ID is not compromised?

i. **DO NOT** click on any links provided in suspicious emails or SMS

ii. **NEVER** divulge banking credentials or one-time passwords to anyone or any organization, or key such confidential info into unverified webpages

iii. If you have an employee leaving the organisation, make sure you submit the request to us to remove the user's to OCBC Velocity. While waiting for the request to be processed, these are the precautions that you should take.

   a. Block his/her access via the "Block my access temporarily" hyperlink on the OCBC Velocity login page. You will need to enter his/her OCBC Velocity login credentials, AND

   b. Delete OCBC Business Mobile Banking app from their device.

Look out for notifications from OCBC either via SMS or email notifying of major changes or transactions. Notify the bank immediately at +65 6538 1111 if these are not valid actions initiated by you.

Q4: Are there any actions I can take as a OCBC Velocity User, to minimize my risk from Phishing scams?

i. **DO NOT** click on any links provided in suspicious emails or SMS

ii. **NEVER** divulge banking credentials or one-time passwords to anyone or any organisation, or key such confidential info into unverified webpages

Look out for notifications from OCBC either via SMS or email notifying of major changes or transactions. Notify the bank immediately at +65 6538 1111 if these are not valid actions initiated by you.

Q5: I received an SMS which contains OCBC hotline number. What shall I do / How do I know this is legitimate?

Beware of SMS scams which direct you to call a fake hotline.

Do NOT call any numbers within SMSes or click on any links in SMSes.

When in doubt, call our official OCBC Business Banking hotline number +6538 1111.

Q6: What should I do if I receive an email/SMS notification from OCBC informing me that my OneToken has been activated when I have not applied for a new one?

This could be a situation where your OCBC Velocity ID/Password may have been compromised.

We recommend that you block your own ID access

- Via the "Block my access temporarily" hyperlink on the OCBC Velocity login page immediately, and submit your request to us to delete and re-apply for a new user ID
- Via OCBC Business Mobile app > click More > Block Access > Key in your Org ID, User ID, Password > Block Access

Alternatively, call us at +65 6538 1111 for assistance required.

Q7: If the SMS is not legitimate, why did it appear under OCBC SMS thread? Why do these SMS appear under the same folder as other OCBC SMS on my phone?

Scammers are using technology to spoof the SMS sender name as "OCBC". When the spoofed SMS is received on the user's mobile phone, the spoofed SMS with the name "OCBC" will appear in the same SMS conversation thread with OCBC.

These messages usually come with a phishing URL link to obtain your details in a look-alike OCBC login page. It is therefore important to stay vigilant against phishing scams.

Do not click on such phishing SMS links. The links will lead you to a fake website controlled by the scammers. You should always type URLs directly into the address bar of the browser or login via the official OCBC Mobile Banking app ("OCBC Business"). Never key in your login credentials through the phishing URL link in the SMS.

Q8: How does the scammer know that I have an account with OCBC? Is the bank's system compromised?

Scammers are sending mass phishing SMS/emails, not knowing if the recipients are OCBC customers or not. Should you click on the link and provide your login credentials, they would then know that you have an account with OCBC. It is therefore important to stay vigilant against phishing scams. Do not click on such phishing SMS links.

We wish to assure you that our banking systems remain secure and have not been compromised.

Q9: Has the OCBC system been hacked? Are you sure that your system has not been hacked?

Answer:

We wish to assure you that our banking systems remain secure and have not been compromised.

Q10: With so many SMSes sent by scammers, how can I differentiate if the SMS is legitimate from OCBC?

We will not send you any message asking you to click into a link to verify or validate certain transaction information. If in doubt, please call us at +65 6538 1111.

We wish to assure you that our banking systems remain secure and have not been compromised.

Q11: What should I do if I suspect my OCBC Velocity User login credentials have been compromised?

You can login to OCBC Velocity and change your password immediately.

You may also block your own ID access

- Via the "Block my access temporarily" hyperlink on the OCBC Velocity login page immediately, and submit your request to us to delete and re-apply for a new user ID

- Via OCBC Business Mobile app > click More > Block Access > Key in your Org ID, User ID, Password > Block Access

Alternatively, call us at +65 6538 1111 for assistance required.

To reactivate your account, please submit a request form. You may retrieve it via OCBC Business Banking website > Help & Support (top of webpage) > Banking forms > Apply & Manage OCBC Velocity

Q12: What should I do if I lose my mobile?

You can activate OneToken on another mobile device, and this will automatically deactivate OneToken on your previous device. Download OCBC Business Mobile Banking app on your new device. Log in with your OCBC Velocity credentials and follow the steps via the "Lost/Changed Phone" hyperlink.

i. Alternatively, you can block your own access

    i. Via the "Block my access temporarily" hyperlink on the OCBC Velocity login page and submit a request to us to delete and re-apply for a new user ID

    ii. Via OCBC Business Mobile app > click More > Block Access > Key in your Org ID, User ID, Password > Block Access

    iii. You can also call us at +65 6538 1111 for assistance required.

ii. To reactivate your account, please submit a request form. You may retrieve it via OCBC Business Banking website > Help & Support (top of webpage) > Banking forms > Apply & Manage OCBC Velocity

Q13: Customer did not login but received a push notification from our app on 2FA login. What precautions can we advise customer to take?

This could be a situation where your OCBC Velocity ID/Password might be compromised.

We recommend that you login to OCBC Velocity and change your password immediately and call us at +65 6538 1111 to report suspicious login. We will investigate the case for any abnormality.

You may also block your own ID access

- Via the "Block my access temporarily" hyperlink on the OCBC Velocity login page immediately, and submit your request to us to delete and re-apply for a new user ID
- Via OCBC Business Mobile app > click More > Block Access > Key in your Org ID, User ID, Password > Block Access

Q14: I would like to switch from OneToken to Hardware Token. How do I proceed?

The standard process for request of hardware token applies.

While customers are given a choice to choose between OneToken or Hardware Token, we encourage customers to apply for OneToken, given the following benefits:

- The processing time taken to equip you with the OneToken is shorter.
- Simpler and more convenient as the OneToken will be installed on your mobile phone.

Alternatively, you can call us at +65 6538 1111 for assistance required.

Q15: What should I do if I lose my Hardware Token?

We recommend that you block your own access

- Via the "Block my access temporarily" hyperlink on the OCBC Velocity login page immediately and submit your request to us to apply for a new token
- Via OCBC Business Mobile app > click More > Block Access > Key in your Org ID, User ID, Password > Block Access

When applying for new token, you may want to consider switching from Hardware Token to OneToken, given the following benefits:

- The processing time taken to equip you with the OneToken is shorter.
- Simpler and more convenient as the OneToken will be installed on your mobile phone.

Alternatively, you can call us at +65 6538 1111 for assistance required.

To request for a new token, please submit a request form. You may retrieve via OCBC Business Banking website > Help & Support (top of webpage) > Banking forms > Apply & Manage OCBC Velocity

Q16: What should I do if I suspect that my mobile phone has been hacked?

This could be a situation where your OCBC Velocity ID/Password might be compromised.

We recommend that you block your own access

- Via the "Block my access temporarily" hyperlink on the OCBC Velocity login page immediately using another device, and submit your request to us to delete and re-apply for a new user ID
- Via OCBC Business Mobile app > click More > Block Access > Key in your Org ID, User ID, Password > Block Access

Alternatively, you can call us at +65 6538 1111 for assistance required.

To reactivate your account, please submit a request form. You may retrieve via OCBC Business Banking website > Help & Support (top of webpage) > Banking forms > Apply & Manage OCBC Velocity

Q17: What safeguards have the Bank implemented to prevent against scams and phishing?

The Bank is diligently monitoring and taking down phishing sites 24/7.

To better safeguard customer’s interest, we have rolled out the following measures:

- Increase the soft token provision cooling period to 12 hours before the user can login
- Remove any link in SMS

Q18: What should I do if I discover a fraudulent transaction from my account?

Answer:

We recommend that you block your own ID access:

- Via the “Block my access temporarily” hyperlink on the OCBC Velocity login page immediately and submit your request to us to delete and re-apply for a new user ID
- Via OCBC Business Mobile app > click More > Block Access > Key in your Org ID, User ID, Password > Block Access

Please call us immediately at +65 6538 1111.