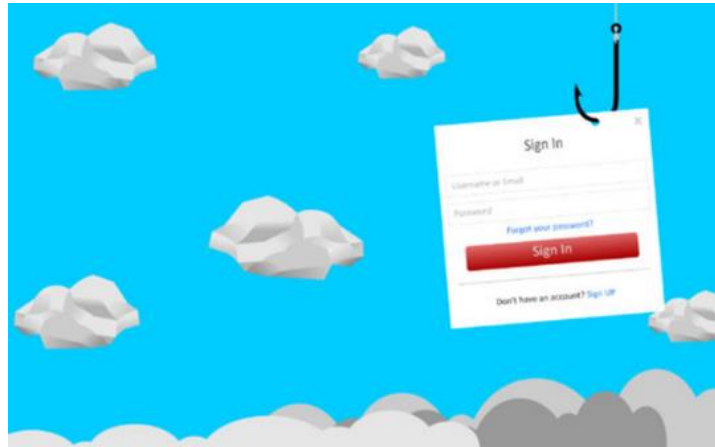


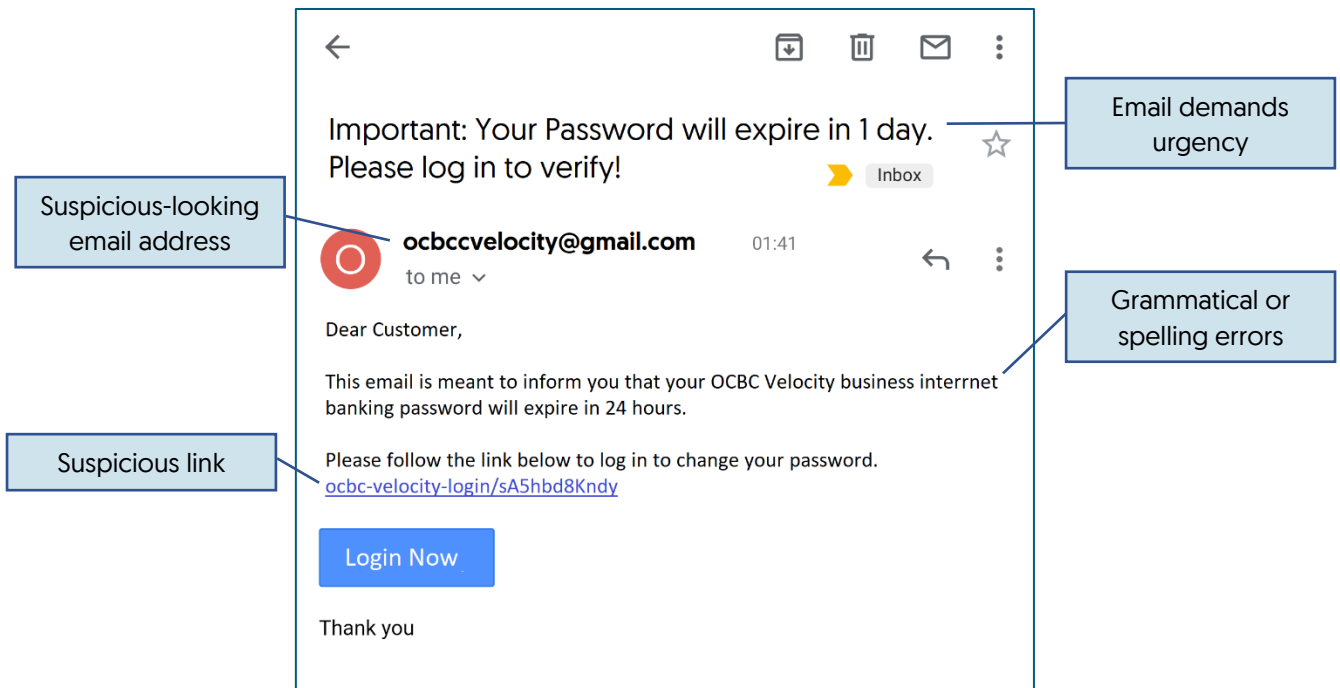
Beware of Phishing Emails



What it does?

Phishing emails are always disguised to look like they are from a trusted organisation. This is intended to trick people into clicking on the phishing website or downloading malicious files. The hyperlink in the email might redirect you to a phishing website resembling OCBC Velocity, prompting you to enter your login credentials such as your organisation ID, user ID, password or One Time Password [OTP].

Identify the tell-tale signs

A screenshot of an email interface showing a phishing message. The email is from "ocbccvelocity@gmail.com" and contains a "Login Now" button. Callout boxes point to various suspicious elements: "Suspicious-looking email address" points to the sender's email address; "Suspicious link" points to the URL "ocbc-velocity-login/sA5hbd8Kndy"; "Email demands urgency" points to the subject line "Important: Your Password will expire in 1 day. Please log in to verify!"; and "Grammatical or spelling errors" points to the text "This email is meant to inform you that your OCBC Velocity business internet banking password will expire in 24 hours.".

←

Important: Your Password will expire in 1 day. Please log in to verify! ☆

o c b c c v e l o c i t y @ g m a i l . c o m 01:41

Dear Customer,

This email is meant to inform you that your OCBC Velocity business internet banking password will expire in 24 hours.

Please follow the link below to log in to change your password.
ocbc-velocity-login/sA5hbd8Kndy

Login Now

Thank you

Suspicious-looking email address

Suspicious link

Email demands urgency

Grammatical or spelling errors

How to protect yourself?



Do's

- Pay attention to the URL as malicious websites may appear identical to a legitimate site, but with a slight variation to the URL.
- Use different passwords especially for your OCBC Velocity login and email account.
- Always keep your contact details with the bank up to date.



Don't

- Reveal or key in your banking details into suspicious websites or emails soliciting your account credentials.
- Open any attachments or links in suspicious emails.

Stop. Think. Before You Act.

Stay vigilant and do not respond to any email or SMS that asks for your confidential information. If you are unsure, please validate the request by contacting an official through a registered number.

If you notice an unusual or unauthorised transactions taking place – either via SMS alerts or email notifications – please call us immediately at **603-8317 5200**.