OCBC Bank

Stay Protected Against Malware Attacks

How malware works

Hackers send phishing emails with hyperlinks or attachments that appear to originate from trusted sources.

Malware will be downloaded onto the user's device once the link/attachment is opened.

The installed malware will search and intercept files/online banking activities, maliciously stealing your banking credentials.

Common types of malware

Virus	Ransomware	Trickbot	Spyware
Viruses can spread across devices and execute its own code to steal sensitive information. They can corrupt files through fake pop-ups that lure a person to visit unusual sites.	Computers infected with ransomware will result in restricted access until a ransom is paid.	Once your computer is infected, trickbot intercepts your communication with the internet banking site. Fake screens and pop-ups will appear to lure you into entering your login credentials.	Spyware maliciously watches and monitors user activity and harvests confidential data without their knowledge.

How to tell if your devices have been infected

- The URL or screen shown on the login page is different from the official page: https://velocity.ocbc.com/login.html.
- You are repeatedly prompted to key in your login credentials even after you have entered it correctly.
- Suspicious account activities where you receive SMSes and OTPs for transactions you did not perform.
- You receive excessive pop-up messages or redirection to third-party websites.

How to protect yourself

- Key in the domain name of the bank in your browser to log onto OCBC Velocity rather than copying and pasting or via a pre-existing link.
- Install and maintain the latest anti-virus software.
- Do not open any unsolicited email or email from suspicious sources.
- Do not use public computers or connect to unsecure or publicly available WiFi to perform online banking activities.
- Do not install software or run programmes of unknown origin.

We would like to assure you that our OCBC Velocity is secure. As malicious software is constantly evolving, we strongly recommend that payment makers and authorisers always stay vigilant and verify the authenticity of all outgoing payment instructions, on top of scanning your devices for potential attacks regularly.

If you notice any unusual or unauthorised transactions that you did not initiate, please inform us immediately by calling **603-8317 5200.**