Deutsche Bank
Private Bank

Deutsche Bank Aktiengesellschaft
(Incorporated in the Federal Republic of Germany & members' liability is limited)
Hong Kong Branch, Wealth Management
Level 60, International Commerce Centre
1 Austin Road West, Kowloon, Hong Kong
Tel +852 2203 8888 (main)

2025-02-12

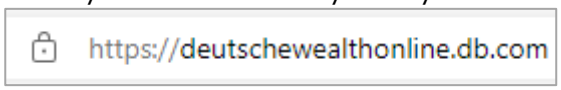
Dear Valued Client,

Scam education alerts

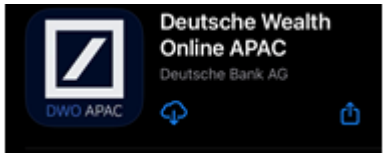
Cybersecurity is our utmost priority. As we continue to enhance our security measures, your vigilance plays a vital role in preventing scams and fraudulent activities. There has been an increase in phishing websites where you may be requested to provide your login details of your bank account(s), as well as scammers impersonating certain authorities calling to induce you to divulge internet banking credential, personal information, and transaction verification codes for fraudsters to conduct unauthorized transactions over your account(s). Please see some tips to protect yourself from scams:

1. Emails from Deutsche Bank AG, Hong Kong Branch and/or Singapore Branch (the "Bank") and messages sent by your Relationship Manager via Instant Chat may contain clickable links to either a Deutsche Bank AG website https://deutschewealth.com/en.html and/or external websites which generally do not require you to provide any of your personal details. If,
   - You are required to provide any of your personal details, these details will be limited and with the express purpose of allowing you to receive further services provided by us. You will never be asked to provide information pertaining to your account(s) with us.
   - The message is claiming to be from Deutsche Bank and looks suspicious in any way, please do not click on the link and contact your Relationship Manager immediately. If you have an online banking account with us through Deutsche Bank Online (DWO), please also note point 5 and 8 below.
2. Verify the authenticity of the information received through SMS or email notifications by reaching out to your Relationship Manager.
3. In compliance with the SMS Sender Registration Scheme in Hong Kong (the "Scheme"), since 2 May 2024, the Bank has been utilizing "Registered SMS Sender IDs" with prefix "#" when sending SMS to eligible clients with local subscribers of mobile services in Hong Kong. More information about the Scheme can be found on the website of the Office of the Communications Authority in Hong Kong.

4. Be cautious of the sender's email address as it could be spoofed to appear similar to the Bank's or the Bank staff's email address. If in doubt, please contact your Relationship Manager.
5. Ensure that your contact details registered with the Bank and/or DWO for the purpose of receiving important notifications from the Bank and/or DWO are up-to-date to allow relevant notifications to be delivered to you on a timely basis.
6. Keep apprised of online fraud and scam advisories and alerts put out by the Bank, other banks, relevant local authorities and regulatory bodies. Stay alert to any impersonation of certain authorities with suspicious requests, such as:
    - requesting you to divulge internet banking credential, personal information and transaction verification codes issued by the Bank
    - requesting you to install suspicious mobile applications from unofficial websites and
    - asking you to ignore SMS/emails/phone calls from the Bank
7. Please be aware of bank staff impersonation phone calls:
    - Generally, your relationship manager/ DB staff who has been introduced to you will be contacting you in relation to your account.
    - If you believe, you have been contacted by scammers and have divulged any personal information, kindly contact your Relationship Manager and report to the police about the incident.
8. If you have an online banking account with us through DWO, please read further.
    a. SMS and emails from DWO are sent via dbwmapac-notifications@db.com and they do not contain clickable links. If you receive an SMS or email claiming to be from DWO and containing clickable links, DO NOT click these links. If you are unsure about any communication which is or claims to be issued by DWO, please contact your Relationship Manager or DWO Support Team. The contact details of the DWO Support Team can be found on the DWO homepage.
    b. Verify that you are at the Bank's official website before making any transactions, or transaction through the Bank's official mobile app.
    c. Access the Bank's website only by typing in the URL (as shown below) in the address bar of your browser. Always end your sessions by logging out and closing the browser.



    d. To minimize the risk of navigating to fraudulent websites, we strongly encourage you to use mobile banking apps, as opposed to web browsers.
        ✓ You can install mobile apps from official app stores (Apple App store or Google Play store) as unofficial app stores may carry malware. As shown below the official name of the app is "Deutsche Wealth Online APAC" and developer name is "Deutsche Bank AG".



        ✓ Please exercise caution when installing apps on your device, also note the permissions granted when installing applications.
        ✓ Turn on the in-app notifications on your mobile device so that you can receive notifications.

e. Closely monitor all online banking or DWO related notifications so that any unauthorized transactions are reported as soon as possible. In particular, please check any information about the date and time of your last login.
f. Never reveal your internet banking credentials or passwords to anyone. In the same vein, never disclose any personal information (account numbers, passwords, or personal information that could be used in ID theft).
g. Strong password will help prevent unauthorized use, hence secure your device with strong password. It's highly recommended to change your passwords once in 90 days.
h. Biometric login is a secure and powerful tool for identification and authentication. However careful considerations must be given to security and privacy aspects of biometric data to ensure its responsible and secure usage. Use reputable biometric devices and services and keep abreast of latest news and developments regarding biometric security risks, such as identity theft. This helps you stay aware of potential threats and how to mitigate them.
i. If you suspect unauthorized access to your online banking account, use the Report Suspicion/Block DWO Access feature in the DWO application, to report the activity or immediately block your online banking access.
j. You can use the Activity Dashboard feature in the DWO application, to monitor your DWO account activity and ensure your security by tracking any unauthorized access or unusual behaviour.

Thank you for banking with us and for continuing to keep your trust in us.

Sincerely yours,

Deutsche Bank AG Singapore/ Hong Kong Branch

David Weis
Head of Strategy
Private Bank Emerging Markets

Cherris Wong
Chief Operating Officer
Private Bank - North Asia