UNION BANCAIRE PRIVÉE

WHAT WE ARE DOING TO MAKE YOUR EBANKING ACCESS SECURE

UNION BANCAIRE PRIVÉE is paying increased attention to security and making every effort to ensure data confidentiality. Even so, internet security is a joint effort. While UBP employs various security practices and measures in order to protect the confidential information of its clients, as the end user, you play an important role in safeguarding against risks such as those related to virus attacks, unauthorized access and fraudulent online activities. The hereunder information is designed to let you know about the precautions that we are taking to guarantee service security and to inform you about how to use internet services safely.

Complex Authentication

The connection system requires four separate elements. Only the “physical” holder of the digital key will be able to connect, but he or she must also have the passwords required for connection.

HID Authentication

- Enter eBanking user ID and password (unique to each user)
- Validate login request from a registered HID Approve app

Encrypted Data Transfer

Data is encrypted and sent over a secure channel. This limits the risk of data being intercepted and the loss of confidentiality of the data being sent .

Regular Security System Audits

Our eBanking application and installation are regularly audited and tested for intrusions in order to check their level of security and make sure they are not vulnerable.

Secure Your System or Devices

Protect Your Computer

- Protect your computer with antivirus software, a firewall and spyware protection.
- Regularly update your security software.
- Update your operating system and internet browser.
- Regularly back-up your data.

Protect Your Mobile Device

- Always update your device to the latest available OS version. These patches normally carry security and bug fixes that will help secure your device and the information stored on it
- Do not make modification to your mobile electronic device not authorized by the operating systems issuer and the device manufacturer (often called “jailbreaking” or “rooting”)
- Avoid auto-complete features which remember user names or passwords.

Password Management

- Never give out your password
- Create complex passwords that include special characters as well as letters and numbers.
- Never use the names or birthdays of your loved ones.
- Do not select whole words found in the dictionary.
- Use a different password for each online application.
- Regularly change your passwords.
- Do not allow internet browsers to save your passwords.
- Do not write your passwords on your digital key.

How To End Your Session Safely

- Click on the “Disconnect” button when you want to end your session. Simply closing the
- browser window does not ensure that you have disconnected from the site.
- Empty your browser’s cache after each session.

Be Attentive When You Connect

- Always enter the address www.ubp.com manually, follow the my access link on the top right of the Home page and click on the e-Banking Asia link to enter into UBP Hong Kong
- eBanking, or directly enter the address https://ubp.pbgate.services/
- Verify that the security padlock is visible and that «https» appears in the address bar.
- Users are strongly advised to connect to only to secure or encrypted networks and not to connect to an eBanking account in public places, either on public computers or on a personal laptop over Wi-Fi.
- If you must use a Wi-Fi connection, make it more secure with password protection and use a secure program to prevent your data being intercepted by a third party.
- Notify your Relationship Manager as soon as practicable when detecting unusual activities or observations (e.g. unusual login screens, suspicious pop-up screens or abnormal Internet banking login steps)

Internet Fraud and Phishing

Phishing, the practice of using fraudulent e-mails and copies of legitimate websites to extract financial data and other personal information from unsuspecting computer users, continues to expand in sophistication and customers of financial institutions are increasingly targets of these scams. Because phishing materials often look genuine and may appear to originate from real people, organizations, institutions, and websites, the following precautions are suggested:

- Be cautious about clicking any links, opening any attachments, or downloading any files from e-mails regardless of file type or who sent them.
- Maintain your guard and read your email and SMS notifications carefully. Malicious emails may contain convincing UBP brand logos, language, with a seemingly valid email address.
- UBP will periodically contact clients through different channels such as email and phone but will never request that the client provide their electronic banking credentials on an unsolicited basis. This includes unsolicited SMS or emails asking customers to click on a link (including those email or website presented as QR code) and to enter their personal or account details into a website.
- If you receive an unsolicited email or SMS which appears to be from UBP, or are in doubt, please contact your Relationship Manger first before taking any further action. Do not click on links provided in random emails and SMS as this is how an account can be phished.