Julius Bär

E-BANKING SECURITY ADVICE

We, at Julius Baer, take Online Security very seriously and we want to do our utmost to protect our clients. Hence, we are providing you with this important security advice. While we have equipped Julius Baer e-Banking and Mobile Banking with industry standard security technology and practices to ensure that our clients are protected against fraud, you play an important role in protecting your data and account as well.

Your co-operation is essential

We strive at all times to ensure that your personal data will be protected against unauthorised or accidental access, processing or erasure. We maintain this commitment to data security by implementing appropriate physical, electronic and managerial measures to safeguard and secure your personal data. Please pay attention to the following Advice for Secure e-Banking.

1. ADVICE FOR SECURE E-BANKING

The following sections detail a few key advice to ensure online security for e-Banking and Mobile Banking.

1.1 TYPE IN THE CORRECT URL

Always access Bank Julius Baer's e-Banking by typing in the correct URL into your Browser.

For Singapore:
https://ebanking-sg.juliusbaer.com/

For Hong Kong:
https://ebanking-hk.juliusbaer.com/

Bookmark the site for subsequent e-Banking sessions. Do not click on any links or access any QR codes provided in any emails from unknown sources or search engines.

1.2 PROTECT YOUR USER ID, PASSWORD AND SECURE KEY (OTP)

Do not reply to any unsolicited emails, calls or SMS asking you to disclose any personal details, such as User ID, Password and secure key (One Time Password). Such information should be kept to yourself at all times.

Bank Julius Baer will never send you unsolicited emails or SMS and ask you to disclose or transmit personal information for e–Banking, Mobile Banking or any Password information. These include your User ID, Password and secure key (OTP). Do not share your secure key with anyone or forward it to another mobile device.

If you receive any unsolicited email, junk or chain emails, please delete them. If in doubt, please contact your Relationship Manager, reach out to the e-Channels Service Centre or visit our e-Banking webpage to report an incident

Protect your Password

It is not advisable to select easily accessible personal information such as name, telephone numbers, date of birth or any sequential numbers or letters as a Password.

Use a Password that is hard to guess (at least 8 characters, comprising of a mixture of numbers, special characters, uppercase and lowercase letters). Make sure to use different Passwords for different services.

Use a dedicated Password to access Bank Julius Baer e-Banking services. Do not use the same Password to access different online services (e.g. connection to the Internet or accessing other websites).

The Bank strongly recommends that Passwords be changed regularly

Treat your User ID, Password and secure key as confidential and protect them against misuse by unauthorised persons. In particular,

- Destroy the original printed copy of the User ID, Password and Activation Code.
- Do not store your User ID, Password and secure key unprotected in any way, including on your computer.
- Do not write down your User ID, Password and secure key on any device for accessing e-Banking or on anything usually kept with or near it.
- Do not write down or record your User ID, Password and secure key without disguising them.
- Do not allow anyone else to use your User ID, Password and secure key.
- Refrain from registering someone else's biometrics such as facial or fingerprint registration on your mobile devices if you have enabled biometrics to access the Julius Baer Mobile App.
- Refrain from supplying your Julius Baer login credentials (such as Passwords and secure key) in third-party financial aggregator applications as these applications may not be secure.
- Do not use a username that is the same or similar to the Julius Baer User ID or the same or similar Passwords, when registering for different online services.

1.3 CHECK THAT YOUR BANKING SESSION IS SECURE

When undertaking any banking activity on the Internet, you should check that the session is secure. There are two simple indicators that will tell you if your session is secure.

- The first is the use of https:// in the URL. For some browsers, such as Mozilla Firefox, the colour of the URL window changes automatically to green when you are in a secure session.
- The other indicator is the presence of a digital certificate represented by a padlock or key located at the beginning or the end of the browser's address bar of your computer screen. If you double click on this icon it should provide you with information (i.e. certificate) about the organisation with which you have entered into a secured session.

Secure Sockets Layer (SSL)

Encryption of sensitive information during online transactions is enabled by an SSL Certificate. Each SSL Certificate contains unique, authenticated information about the owner of the certificate. A Certificate Authority verifies the identity of the certificate owner when it is issued.

If you receive SSL certificate warning messages (e.g. invalid date, entrusted certifying authority, name mismatch, failed to retrieve revocation list, etc.), please quit the application. Leave a website if you suspect the website of being fraudulent and do not follow any of the instruction it may request of you. Please call the e-Channels Service Centre, inform your Relationship Manager or report the incident via our website if you encounter an SSL warning message.

1.4 KEEP YOUR COMPUTER SECURE

Use the automatic update function or perform manual updates regularly for all software – in particular operating system, antivirus software, firewall, browser including plug-ins and document viewing software. It is very important to apply all the security patches for the various software you have installed on your computer or your mobile devices either via automatic updates (e.g. Windows Update, Adobe Update, Firefox) or via manual updates.

Use a personal firewall and anti-virus software. Keep the anti-virus software up-to-date. Also regularly use relevant software to remove Spyware from your computer and mobile devices.

Disable file and printer sharing options on your computer, especially when connected to the internet.

Do not access e-Banking services through public or shared computers (e.g. at cyber cafés, public libraries or any other public sites) to avoid the risk of information being copied and abused after you leave.

Consider using private browsing modes to reduce potential leftover offline data in your computer.

1.5 CHECK YOUR NOTIFICATIONS

It is important that you promptly check the relevant notifications and account statements/advice sent as well as trading alerts, any information about the date and time of the last login to e-Banking, and Password reset notifications. If you find any irregularities, call the e-Channels Service Centre, contact your Relationship Manager or visit our e-Banking webpage to report an incident. Store your e-delivery documents such as account statements in a safe place. Ensure the regular backup of critical data and files.

1.6 LOG OFF FROM YOUR E-BANKING SESSION PROPERLY

It is important to completely log off from your e-Banking session. Simply closing the browser or tab may not immediately close the e-Banking session. Clear the cache of your browser after you have concluded the e-Banking session. Refrain from selecting the browser option for storing or retaining user ID and Password.

1.7 MOBILE BANKING SECURITY TIPS

Only install apps that are really needed and only from an official store

- Do not install applications on your mobile devices from mistrusted sources. Avoid using untrusted custom virtual keyboards.
- To avoid downloading from fraudulent websites, always download our mobile application from the official Apple App Store or Google Play store only.
- Uninstall obsolete apps that you are no longer using, every additional app constitutes a potential vulnerability.

Restrict access privileges

- Understand the permissions of mobile applications before installation and restrict access privileges.
- Be very cautious about disclosing your location data. Avoid localisation services, as hackers might abuse such information.

Secure mobile device against unauthorized access

- Enable auto-lock as well as passcode lock on your mobile devices to restrict unauthorized access.
- If possible, enable data encryption on your mobile devices.

Avoid storing any confidential data on your device or in the Cloud

- Do not save your username and Password on your mobile devices and deactivate automatic storage of Passwords in your browser and at the store as well as any such back-up to the Cloud. An automatic back-up Cloud might be convenient, but should never include any confidential information.

Only permit necessary and trustworthy connections

- Only use trusted Wi-Fi networks or service providers when connecting to Wi-Fi.
- Disable Bluetooth while not using or set your mobile devices to non-discovery mode.
- Disable any connection types you don't need while e-banking.
- Only connect your mobile device to trustworthy computers, since malicious software can also be transmitted by connection via an USB cable.
- Do not accept any connection request if you are not clear what device is trying to connect to your mobile devices.

Keep device up-to-date and clean

- Install available updates and patches for your operating systems and all apps installed in a timely manner, covering upgrades/updates of OS and other mobile applications.
- Whenever available install and update the latest anti-virus and anti-spyware software regularly on your mobile devices.
- Avoid using any jail broken or rooted mobile devices which may have security loopholes to login to Mobile Banking as it makes your device more prone to malicious software.

Stay alert

- Avoid sharing your mobile devices with anyone else and always use your own mobile device to use Mobile Banking.
- After login to Mobile Banking do not leave your mobile device unattended. Always log off completely after you have finished your Mobile banking session.
- When accessing Mobile Banking always disable screen mirroring on your mobile device.

In case of loss, act immediately

- If you lose any of your mobile devices, you should review your account transaction history through e-Banking on your desktop. If there are any suspicious transactions, please contact the e-Channels Service Centre, inform your Relationship Manager or visit our e-Banking webpage to report the incident immediately.
- Remove the respective device from the list of your bound devices.

Ensure your device is correctly reset before disposal or sale

- To remove all data from your mobile devices before donation, reselling or recycling, reset the device to its default settings.
- Unbind any devices you are no longer using or no longer have access to
- Block your account if unauthorised access is suspected or a device is lost or stolen
- For your protection, your e-Banking accounts will be blocked automatically, after a number of failed login attempts. To unblock an account, please contact the e-Channels Service Centre.

2. BEWARE OF ONLINE THREATS

2.1 SOCIAL ENGINEERING

Scammers may use social engineering to trick you into giving them your personal or financial information, especially your e-Banking credentials or trick you into performing unwanted actions. Scammers abuse their victims' good faith and helpfulness by purporting to be, for example, an employee of a trustworthy financial institution or someone you know. Phishing, phone or email scams, website impersonating or social media impersonation are just one of many examples of social engineering techniques. In general, never disclose Passwords or any other login credentials to anyone by any means, not even to someone you know.

2.2 PHISHING

Phishing may be attempted through email, SMS or a phone call and often at first sight, seem to be legitimate or appear to come from a familiar source. These types of phishing may try to persuade you to disclose sensitive information such as your User ID, Password or secure key, convince you to execute unwanted transactions, or click on malicious links or attachments.

If you fall victim, hackers may be able to steal personal information, e-Banking credentials or secure key. They might also be able to download and install malware on your computer to steal such information.

- Be careful of unsolicited emails, SMSs and phone calls and refrain from responding to them.
- Notify us of any suspicious emails that appear to originate from the bank immediately.
- Avoid clicking on links or accessing QR codes in unsolicited emails and SMSs. Always access our services through our official website. The correct links are provided in section 1.1.
- If you receive a phone call from someone claiming to be from Julius Baer, ask to call back and call the e-Channels Service Centre to verify.
- Download the Julius Baer Mobile App from the official Apple App store and Google Play store instead of using a web browser.

2.3 MALWARE

Malware or malicious software is devised to gain access to your devices without your consent and/or knowledge. There is a possibility of malware being installed by, clicking on a malicious link, opening a malicious document (e.g. in an email attachment) or installing a malicious program or app. After installation, such malware may steal your personal and financial data or utilize your device without your authorization to conduct other malicious activities.

- Beware of attachments and links received in emails and avoid opening attachments and clicking on links provided in unsolicited emails or SMSs.
- Refrain from downloading unnecessary programs or apps as these may contain malware.
- Only download the Julius Baer Mobile App from the official Apple App store or Google Play store. Do not use third-party app stores as unknown parties can modify such apps to include malware into legitimate, non-malicious apps.
- Consistently ensure that your computers and mobile devices software, firewall as well as anti-virus software are up-to-date.

2.4 THIRD PARTY CHAT SOFTWARE (I.E. WHATSAPP, ETC)

The use of third party chat software such as WhatsApp opens a new communication channel, introducing different risks. As such, please take note of the following:

- If you change your Bank-registered WhatsApp phone number – please inform the Bank accordingly via the e-Channels Service Centre.
- Do not divulge any details or information if you receive an unsolicited message through this channel.
- Always install the latest Android/ iOS updates (as well as chat software updates i.e. WhatsApp, etc) to update channel security.
- Please also do not allow persons other than yourself to access your chat channels/devices.
- If using desktop/ web versions of such Chat software, please log out when not in use.
- Please always take note of the third party Chat software's privacy policies and terms and conditions for information on how your data will be handled.

2.5 ADDITIONAL RESOURCES

Singapore's National Crime Prevention Council (NCPC) released the ScamShield app that detects incoming scam calls and text messages. NCPC also provides scam alerts to remind the public to remain vigilant. Please visit the ScamShield (https://www.scamshield.org.sg/) and Scam Alert (https://www.scamalert.sg/) websites for further details.

The Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force released the "Scameter+" mobile application that is available on the App Store and Google Play. The mobile application provides the public with a one-stop scam and pitfall search engine as well as access to crime prevention information. Please visit the CyberDefender website (https://cyberdefender.hk/) for further details.

Kindly also refer to Hong Kong Monetary Authority's website (https://www.hkma.gov.hk/eng/smart-consumers/) for more information on protecting your digital keys, security tips and educational videos.

3. IMPORTANT INFORMATION

The information expressed in this document is produced by Bank Julius Baer & Co. Ltd. (the "Bank") and the Bank may amend this document from time to time without notice as the Bank deems necessary in its sole discretion. You are advised to regularly visit the Bank's web page or contact your Relationship Manager for the Bank's latest advice on secure e-Banking.

If you suspect or become aware that any unauthorised persons have gained access to your user ID, Password, secure key, debit card, credit card, your computer or mobile devices or that any unauthorised transactions have been conducted through your accounts with the Bank, you must immediately notify the e-Channels Service Centre, verify with your Relationship Manager or visit our e-Banking webpage to report the incident.

The information in this document shall be without prejudice and in addition to the terms and conditions that apply to your account(s) with the Bank, including the terms and conditions for e-Banking.

E-Banking services mentioned in this document may not be available for all recipients in all countries. You are kindly requested to get in touch with the local Julius Baer entity in order to be informed about the services available to you.

This document shall only be for the personal use of the intended recipient and shall not be redistributed to any third party, unless the Bank gives their approval. This document is not directed to any person in any jurisdiction where (by reason of that person's nationality, residence or otherwise) such document are prohibited.