BANQUE LIBANO-FRANÇAISE

SECURITY GUIDELINES OF BANQUE LIBANO-FRANÇAISE ONLINE BANKING, POINT COM®

To ensure a secure online banking experience and safeguard your privacy, you are invited to follow the below guidelines:

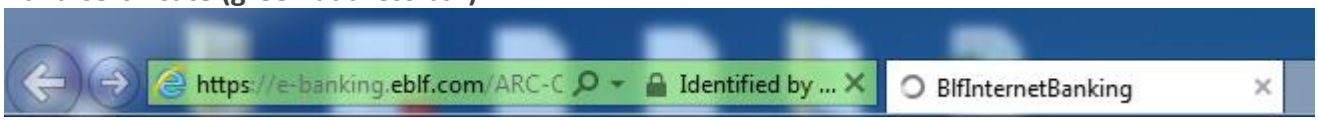
GENERAL SECURITY TIPS

- Install an antivirus program on your PC (desktop or laptop) or smart device. Keep it updated and running to constantly secure your systems and devices.
- Keep the operating systems of all your devices updated at all times to reduce the risk of unauthorized access to your personal information, malware infections and credential compromise.
- Beware of e-mails received from unknown senders and:
    - Do not open the attachments in these emails as they might contain malwares that will corrupt your device or steal your personal information.
    - Do not click on the web links in these emails as they will redirect you to sites that will download malicious content onto your PC or smart phone.
- Avoid browsing unreliable internet sites and clicking on suspicious ads and announcements as they might redirect you to other sites that contain malwares.

SECURE LOGIN

- Make sure you always access the e-banking service, Point Com®, via BLF website and not via links in e-mails you have received.
- Do not access Point Com® from public PCs (hotels, coffee shops, airports, etc.). Always use your personal devices.
- BLF does not recommend to use free public Wi-Fi access points (in hotels, coffee shops, airport lounges) to login to Point Com®.
- Before you login to BLF e-banking website, make sure its certificate is valid (refer to the below screenshots to know how to distinguish between valid and invalid certificates). In case it is invalid, do not attempt to login because you will be redirected to fake sites that seek your personal information. If this occurs, you are required to update your antivirus, scan your device for any possible malware, then try to access the site from BLF website.

Valid certificate (green address bar)



Invalid certificate (red address bar and certificate error warning)

PASSWORD PROTECTION

- We provide three layers of protection to secure your online banking experience: the User ID, the One-Time Password (via the Token device or SMS) and the PIN code. The User ID and PIN code are strictly confidential; you will need to use them every time you sign in to Point Com®. The User ID is provided to you upon subscribing to the service and signing the contract agreement, while you create the PIN code upon registration.
- Change regularly your PIN code and avoid writing it down where others can find it.
- Avoid choosing a PIN code that can be easily guessed, such as a succession of numbers, your birth date, a phone number, etc.
- After 5 incorrect login attempts (5 attempts for the PIN code and the One-Time Password via Token or SMS), the service will be automatically blocked. You would have to contact our Call Center agents on 1272 to reset your access. It is highly recommended to change your PIN code after each reset done by our Call Center agents.
- Keep the Token device in a secure place where no one can find it. Do not aimlessly press on the Token button unless you need to generate the serial number requested to login, otherwise your access will be blocked.
- If your Active ID Token is stolen or lost, you should instantly inform your branch to disable it.

PRIVACY PROTECTION

BLF will never send an e-mail asking you for confidential information such as your account numbers, credit card numbers or passwords. If you receive such e-mails, please disregard them, and it is preferable to contact our Call Center on 1272 in such cases.

AUTOMATIC LOGOUT

When you finish your e-banking session, it is recommended to log out properly by pressing the 'Log Out' button in order to end the established connection with our servers.

BROWSERS INCOMPATIBILITY

- The version of the browser you are using might not be compatible with our web pages. In this case, you may receive a message indicating that it needs to be upgraded.
- Below are the links used to update the most commonly used browsers. Choose the proper link:
    - Microsoft IE Internet Explorer: http://windows.microsoft.com/en-us/internet-explorer/download-ie
    - Google Chrome: https://www.google.com/intl/en/chrome/browser/
    - Mozilla Firefox: http://www.mozilla.org/en-US/firefox/new/
    - Apple Safari: http://support.apple.com/downloads/#safari