Corporate Internet Banking Security

What do we do to keep you safe?

Byblos Bank's Corporate Internet Banking platform was designed to protect your information and your privacy. The following are some of the security measures we have in place:

High Levels of Encryption

Any and all information exchanged between your computer and Byblos Bank's web server is secured through encryption. Encryption converts the information into a form that is unreadable as it travels across the Internet, and our Corporate Internet Banking portal meets the highest international standards. Accordingly, you must have a browser that supports 128-bit encryption to access the system.

Secure Login

In addition to your username and password, our Corporate Internet Banking system requires you to choose a secret picture. For all subsequent logins, once you have entered the username component of your login credentials, our website will identify itself to you by showing you the same picture for you to verify. The picture confirms that you have reached Byblos Bank's website and not a fraudulent one attempting to deceive you into divulging your personal information. You are then required to finish entering your login credentials by providing your password in order to gain access to the system.

Password Protection

To bolster your protection, our system will periodically request that you change your password. While changing your password, you will be shown whether your new password is considered weak, medium, or strong. Strong passwords are harder for a fraudster to guess. Please do not reveal your password to anyone, and we strongly recommend that you commit your password to memory rather than writing it down where others might find it.

Automatic Logout

You should always log out of Corporate Internet Banking when you are done. If you forget, our system will automatically log you out after a period of time.

Protecting your Privacy

In order to help us protect your personal information, you may be asked to re-enter your login credentials before gaining access to pages that contain your address, phone number, and/or login credentials. Providing these credentials will confirm your identity, ensuring that only you can see and modify sensitive information.

Fraud Protection

In order to protect you against fraudulent transactions, you also may be asked to re-enter your login credentials for any transaction that moves funds out of the Bank (e.g., a bill payment or a transfer to an external account).

What you can do to keep yourself safe?

- Always keep your virus protection software up-to-date. This will help protect you against programs that attempt to install themselves on your computer in order to capture personal information. Anti-spyware protection is also recommended to guard against the malicious programs known as "malware".

- Always keep your computer's operating system up-to- date. Check regularly for the availability of security-related patches.

- Always verify the Bank's website name in your browser. It should read "https:corporate.byblosonline.com". If any other address appears, you are not at Byblos Bank's site and should close the window.

- Never send an email that contains your personal information, including your address, account numbers, credit card numbers, or login credentials. If your email signature contains such information, you should change your signature. Email is not encrypted and can be intercepted. To send us confidential information, log into your Corporate Internet Banking account and use our Secure Message service.

- Never respond to any email that asks you to click on a link to connect to the Bank. Such emails are part of so-called "phishing" scams. Byblos Bank will never send you an email asking you to provide such personal information, and nor will we ever call you for that purpose. Please contact your Bank representative if you receive such an email or phone call.

- Never use software features that offer to remember your password. These features may provide a little convenience, but they also can reveal your password to someone else using your machine.

- Avoid doing your banking from a public computer (e.g., a library, cafe, or airport lounge).