Security recommendations for electronic communication with Silk Road Bank AD Skopje

Dear customers,

Following the determination of the Bank, our clients are in the center of our attention, Silk Road Bank advise you about security mesures and recommendations that you should apply when using the electronic services of the Bank. The bank provides three types of electronic communication with its customers:

- Through the e-banking website https://silkroad.24x7.com.mk/Retail/Account/Login

- Through the website for secure e-mail delivery https://keys.silkroadbank.com.mk

- Through the mobile application for Android and IOS Silk Road m-Bank

In order to establish effective security protection, in addition to the measures taken by the Bank, you need education and cooperation with you.

Passwords

The first step of protection is to create a complex password.

The password should not contain your personal information, surnames, important dates and easily accessible data. Also, generic words and consecutive sequences should not be used (P @ ssword, Admin, 1234567890, Administrator, user, etc.)

In order to make it easier to remember the passwords, you can define your own personal rule according to which you will create the future passwords.

Do not write down your username and password on a piece of paper that you carry with you or your mobile phone. If you need to, write them down and keep them in a safe place that only you know. It is advisable to keep the username and password in a different place, to prevent unauthorized access in case of loss or theft.

Do not use the same username and password to access other web pages, as if the password is found on any of those pages, it could be used for e-banking.

Change the password for a period of time (for example 3 months) to reduce the risk of misuse in case of theft.

Do not share the password with anyone. If any of your family members or employees need access to the services, register a separate account with a unique username and password to access it.

If you forget your password, in the case of web banking, through the following link: https://secure.24x7.com.mk/enrollment_silkroad/mk-MK/Retail/ResetAccount (forgotten password or username), you can create a new password. To change a new web banking password, you need to have a debit card in the Bank. If you have any problems call the telephone number for technical support +389 2 3289-440.

If you forget your password in case of access to the system for secure delivery of e-mail, then use the option for lost password (I lost my passphrase), and if you have problems call +389 2 3289 430.

Use of public networks and computers

Avoid using e-banking services through open and free wireless networks (airports, restaurants, shopping malls ...) unless internet access through this networks is adequately protected (WPA, WPA2, VPN or 4G).

Do not use public computer for e-banking services. Always use your own computer. However, if you have logged in to e-banking from a potentially compromised computer, change your password at the first opportunity from your computer.

Access to web banking and the system for secure delivery of emails from a verified link

- Always access e-banking services by entering the address in your browser:

https://silkroad.24x7.com.mk/Retail/Account/Login .

Never use links received by email or exposed by third parties to access the e-banking site. The most common attack that can occur is the so-called phishing attack, in which the attacker sends you a link to a fake WEB page, which is identical to the original asking you to leave your username and password and become a victim of further abuse. Always check the validity of the link and the certificate in the address bar of your browser.

If the Bank needs to send you an email with confidential content, it will be done through the PGP Web Messenger secure email delivery system. In fact, it is a separate WEB portal owned by our Bank.

Access the service for secure delivery of e-mails using the link obtained at your e-mail address and always check that the sender is paymentoperations@silkroadbank.com.mk. Also check that the subject of the message contains your account number. The link in the message should always start with: https://keys.silkroadbank.com.mk , and it contains the name of your email address.

Check out e-banking and secure email delivery system

When you have completed the usage of the web banking services and the secure email delivery system, log out and check that you have successfully logged out. Leaving an open session after you go from the computer opens the door for a potential attacker who is physically close to you to abuse your bank accounts even though they do not know your password, or to access confidential content that has been sent to you.

Do not share data

The bank will never ask you for your password to log in to e-banking services. If you receive an email asking for your password and / or username, or a message asking you to "confirm" or "update" your username, this is an attempt to steal your password / username. Do not click on the links in the email, and delete the message immediately.

The bank will never ask you to enter a payment card number, PIN, security three-digit code on the background of the card (for online transaction authorization) or other personal data as the use of web banking services does not depend on your payment card number or PIN. To use the web banking service in a strictly controlled practice, you have been given an activation code on a text message in order to activate your user profile and then create your password, known only by you.

Never provide your personal information or financial information to strangers who contact you from companies you have never contacted before and who contact you by e-mail, telephone or in writing. The same goes for agencies that present themselves as consultants, executives or marketing agencies of a company with which you already have a business relationship. The Bank will never contact you in this manner, because according to the Law on Personal Data Protection and the internal acts of the Bank your written consent is mandatory in order your contact information such as tel. number, e-mail address or home address to be given to a third party.

Monitoring of accounts and transactions

Check your transactions regularly and if you notice a transaction that you are not convinced you have authorized or does not correspond to the purchased products and services, , call the phone number immediately: +389 2 3289 440 and ask for further instructions even if it is a small amount.

If you have lost a receipt with your username or password, try logging in to e-banking services and change your username immediately. If you can not log in, report the case to the phone number: +389 2 3289 440 requesting to block access to web banking from your username and create a new password.

OS updates, antivirus and security programs

Use up-to-date antivirus software, firewalls, and security programs on your PC. It is advisable to use a quality antivirus, which in addition to viruses offers protection against other types of malware (spyware, trojans), detects malicious activity on the computer, warns and blocks visits to malicious or infected websites, etc. Choose software recommended by more trusted and independent sources.

Follow virus warnings, especially Trojans for your antivirus software. These malicious programs are usually installed automatically, by clicking on a link or opening applications that you received attached to an email or when installing pirated software.

Always use the latest version of your browser with all security updates.

Update your computer software regularly. Do not use outdated operating systems for which the manufacturer has stopped issuing security updates. This way you will ensure that your operating system, antivirus and other protection programs provide you with the best protection.

To work on your computer, and especially when using the Internet, work with a user who does not have administrator privileges.

Website identification

The web banking website of Silk Road Road Bank can be identified through an appropriate server certificate issued by DigiCert issued on silkroad.24x7.com.mk.

On the page https://silkroad.24x7.com.mk/Retail/Account/Login, next to the address field or in the lower part of the search engine (depending on the browser you use) a padlock appears on which this information can be seen.

Suspicion of theft or abuse

If you do not follow these recommendations, the so-called identity theft whereby a potential attacker who accesses your credentials may impersonate you, allowing you to access your accounts and conduct transactions without the Bank's knowledge.

In case of suspicion of theft or abuse:

- Immediately change the access password using a trusted computer;

- You can block your user account by calling +389 2 3289 440. After blocking, neither you nor the potential attacker will be able to log in to the web banking services to inspect or perform transactions;

- Check the date of the last activity in web banking.

Any attempt for access to your data by any person, in person, by phone or online, consider it an attempt at theft and report it to +389 2 3289 440. Additionally, you have the right to report the case to the Ministry of Interior and in the Directorate for Personal Data Protection.