

Security Instructions for usage of Raiffeisen ONLINE

Raiffeisenbank Bulgaria (EAD) uses the most modern security methods and tools for its online banking platform - Raiffeisen ONLINE and effectively protects your finances and gives you the convenience to bank everywhere. We encourage you to comply with the security policies described in this document to help us increase this protection. This will also lead to a significant reduction of the risk of abuse when paying with bank cards online.

Access to the Internet banking platform Raiffeisen ONLINE

- ✘ Do not use public computers (PCs in Internet cafes, libraries, etc.) to access Raiffeisen ONLINE.
- ✘ Avoid using Raiffeisen ONLINE in the presence of other people or in public places.
- ✘ If you are using wireless Internet (Wi-Fi), make sure the connection is encrypted. Any connections to public and free Internet can result in compromised user credentials (username and password).
- ✘ Access Raiffeisen ONLINE directly by typing the web address <https://online.rbb.bg> or the official site of Raiffeisenbank <http://www.rbb.bg>. Do not use automatic address completion features.
- ✘ Do not include the Raiffeisen ONLINE site in your browser's bookmarks or favorites because this way there is a risk of manipulating the saved links by unauthorized contacts (hackers).
- ✘ Always check if the Raiffeisen ONLINE web page you access is the authentic one and communication with it is secured. After loading the page, make a session security check in your browser prior to entering your username and password. The check is done as follows:

Google Chrome

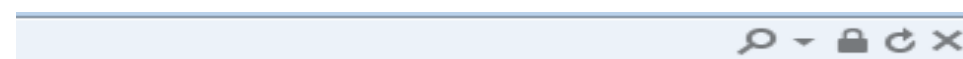
- In the left part of the address field you should see a green padlock



- Click on it
- Click the "Details"
- Click the "View certificate" button
- Select the "Certification path"
- Verify that the Certification path is consistent
"Sectigo RSA Extended Validation Secure Server CA" -> "online.rbb.bg" and the status of the certificate (Certificate status) is "OK".

Internet Explorer

- You should see a padlock on the right of the address field



- Click on it

- Click the "View certificates" button
- Select the "Certification path"
- Verify that the Certification path has the sequence "Sectigo RSA Extended Validation Secure Server CA ->" -> "Sectigo RSA Extended Validation Secure Server CA ->" online.rbb.bg "and the status of the certificate (Certificate status) is" OK ".

Edge

- In the left part of the address field you should see a green padlock

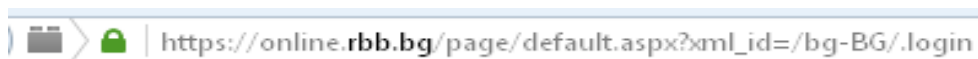


- Click on it
- Click on "Certificate (valid) Issued to Raiffeisenbank (BULGARIA) EAD [BG]Click the "More Information" button
- Choose "Certification path" tab
- Verify that the Certificate Hierarchy has the sequence "Sectigo RSA Extended Validation Secure Server CA ->" -> "Sectigo RSA Extended Validation Secure Server CA -> "online.rbb.bg" and the status of the certificate (Certificate status) is "OK ".

-

Mozilla Firefox

- In the left part of the address field you should see a green padlock



- Click on it
- In the window that opens, click on the arrow pointing to the right
- Click the "More Information" button
- Click the "View certificate" in the window that opens
- Select the "Details" tab
- Verify that the Certificate Hierarchy has the sequence "Sectigo RSA Extended Validation Secure Server CA" -> "online.rbb.bg" and the validity date (Validity Not After) is current.

- ✘ Whenever you have finished banking with Raiffeisen ONLINE, use the (Exit) button in the upper right corner of the screen before closing the browser.



Internet browsers

- ✘ DO NOT save your usernames and passwords for Raiffeisen ONLINE in your browser

- ✘ Use an Internet browser that supports a secure connection protocol TLS version 1.2 or later and versions of Internet Explorer, Edge, Mozilla Firefox, Safari, Opera, Google Chrome that receive regular updates and are not suspended from their developers to access Raiffeisen ONLINE
- ✘ Activate the Automatic updates and the Phishing filters in your browser.
- ✘ Do not install additional toolbars – ASK toolbar, Google toolbar, etc. in the browser you are using to access Raiffeisen ONLINE unless absolutely necessary. There are many cases of toolbars being used by hackers for distributing malware.

Username and password for authentication in Raiffeisen ONLINE

- ✘ Even when changing the password for the first time always choose a "strong" password, which has a minimum length of eight characters, containing lowercase and uppercase letters, numbers and special characters (*,!, &, Etc.).
- ✘ Change your password regularly (at least once every two months). The password for your internet banking must be different from the ones you use for access to your emails, accounts in social networks and others and from your name for internet banking.
- ✘ Remember your username and password for Raiffeisen ONLINE. DO NOT write them down on paper, in your mobile phone or in the computer.
- ✘ Your password should not contain names of family members, pets and company names. Do not use birthdates for a password. Do not choose dictionary words for passwords.
- ✘ Do not share your username and password with anyone, not even family members or colleagues. These are strictly personal and unambiguously define you in the system as a user. This is your identity in front of the online banking system. If someone obtains your username and password, they will gain access to the system on your behalf.
- ✘ If it is necessary that employees from your company or family members need to have access to your accounts, you as an account holder can request a separate access profile by visiting a Raiffeisenbank Bulgaria branch.
- ✘ If you change your specified contact telephone number, always inform Raiffeisenbank about the change. This way, if you need to confirm a payment order, we will be able to provide you with faster and better service. Do not give the phone number to a relative or colleague.

Additional security devices for users with active profiles

- ✘ Raiffeisen ONLINE provides system users two additional security means for transaction authorization – MTAN via SMS messages or code generated by token (hardware device or native mobile application – software token)
- ✘ Token confirmation - When authorizing payments via a token device on the device display (software or hardware) you receive details about the transfer - the last 10 digits and letters on the recipient's account, the amount of the

transfer and the currency. Always check the last 10 digits and letters of the recipient's account with the account to which you want to deposit funds - in case of difference DO NOT enter the code generated by the token to authorize the transaction and DO NOT confirm the transfer via online signature and immediately report Raiffeisenbank.

- ✘ Hardware Token – keep the token in a safe place and in a secure manner. Remember the unlock PIN and do not share it with anyone. Do not write it down on paper or on the back of the token.
- ✘ Native application for mobile devices – software token - Raiffeisen token application is available for Android and iOS operating systems. Raiffeisenbank distributes the applications for smart devices only at official stores Google Play Store (for Android) and iTunes (for iOS). Do not let the phone you use for banking to be used by others without supervision. In case you use software token with PIN do not share the last one with others and do not write it down.
- ✘ Confirmation with token - when authorizing payments with token you receive details for the transfer on the device's display (hardware or software) – the last 10 digits and letters from the account of the beneficiary, transfer amount and currency. Always check the last 10 digits and letters of the beneficiary's account you wish to send money to – in case you notice any difference do NOT enter the code generated by the token for authorizing the operation and do NOT confirm the transfer with online signing mode. Report to Raiffeisenbank immediately.
- ✘ Raiffeisen ONLINE provides the opportunity to use a group signature, in which active transactions can be confirmed by several users with various additional security tools. This increases the security of your active operations. Consider using a group signature for personal or corporate needs.

Operating system and additional software

- ✘ Always use up-to-date operating systems and software. Today most operating systems and software products can be set to automatically update. If this option is available, activate it. If the auto-renewal option is not available use only patches and updates for your operating system and software that are published on the official vendor sites. Hackers often use e-mails and fake update pages to distribute fake security patch/update announcements urging you to download patches/updates, which are malware. By using an updated operating system and software products, you reduce the chance for ill-intentioned persons to use "breakthroughs" to access your personal information.
- ✘ Different types of software that you have installed on the computer you use to access Raiffeisen ONLINE may affect the level of security of your online banking usage. Follow the information provided by vendors of the software you have installed for reported bugs and security holes in their products and apply the relevant patches, updates and fixes according to their recommendations.

- ✘ Install a personal firewall on the computer you are using for online banking to protect from unauthorized manipulations. Firewalls can be configured to send out alert message when they detect an attack from the Internet. Use automatic updates options for your personal firewall.
- ✘ Install antivirus/antimalware software on the computer you use for banking with Raiffeisen ONLINE. The antivirus software scans your files and electronic mails for viruses, Trojans and other types of malware that may allow for unauthorized users to gain control over your personal computer.
- ✘ Consider antivirus software recommended by the operating system vendor. You can find a large number of free downloadable antivirus/antimalware programs on the Internet under different names and from unknown vendors. It is very common that such programs are developed by hackers/malicious users and are distributed by spam mails or other scare tactics – as you browse a web page a pop-up or the page itself claims that it has detected that your PC is infected and you should download a specific antivirus tool in order to clean it – scareware. Very often such programs contain viruses, Trojans or other malware themselves. In other cases the program locks all the programs rendering the PC unusable until you pay some kind of license fee – ransomware.
- ✘ Most antivirus programs are automatically updated so that the new threats in the Internet are mitigated. Always use updated antivirus software.
- ✘ DO NOT install any software with unknown origin. Using cracked programs from torrent sites is also a big risk. These programs have breakthrough protection, and can be used to install malware and Trojan horses.
- ✘ We would like to draw your attention on the discontinued maintenance of the operating system Windows XP (<http://windows.microsoft.com/bg-bg/windows/end-support-help>) and the measures you should undertake to keep safe and secure.

Mobile banking through native applications

- ✘ Users can access the mobile banking system of Raiffeisenbank – Raiffeisen ONLINE through native mobile applications for smart devices – phones, tablets, etc. The applications can be used by smart devices running on Android and iOS operation systems.
- ✘ Raiffeisenbank distributes the applications for smart devices only at official stores Google Play Store (for Android) and iTunes (for iOS).
- ✘ The authentication for the mobile Raiffeisen ONLINE is carried out with the same credentials (username and password) used for the online banking system. For a more convenient and quick login, the mobile app offers the ability to set up a pin and /or biometric login when the device supports it (fingerprint for Android, FaceID, and iOS fingerprint). For this purpose, the user has to login with the username and password and then choose the preferred login method from the profile settings (My Profile menu). In case of a forgotten PIN or a biometric fingerprint reading problem, users can always choose to enter with their username and password. Only one user per device can use the PIN login option and one for biometric login. For example:
 - User "A" uses the PIN login option, user "B" uses biometric login

- User "A" uses the PIN login and biometric login. In this case, user B will not be able to set up quick login but can use a username and password. In order for the biometric login to be used, the user must have the device set up beforehand.

- ✘ In order to use the biometric fingerprint option, the user must have pre-configured their device.
 - When the device is running an Android operating system, after each change-adding or removing a biometric data in the device settings, the user must clear the mobile application's data, then re-make the appropriate pin or biometric input configurations
 - For iOS, adding or removing a biometric data in device settings does not impose any new settings in Raiffeisen ONLINE mobile app. Note that when using a biometric login and the operating system is iOS, anyone who has access to the device through a biometrics will gain access to the Raiffeisen ONLINE profile that is configured to work with biometric the device!

Raiffeisenbank Bulgaria EAD does not store or manage the biometric data!

- ✘ The mobile app supports push notifications. The users can activate the notifications he wants from their profile settings (the "Notifications" menu) after login into the mobile application. Notifications are received on the last device from which the user has logged into their Raiffeisen ONLINE account. If you need to sign up from another device, all you have to do to keep receiving notifications is to re-enter your login from your personal device. To stop receiving notifications, you can disable subscriptions from the Notifications menu.
- ✘ The additional security devices used for performing active operations through the mobile applications are MTAN via SMS and tokens. We recommend when using MTAN via SMS to receive the authorization code on a different phone number from the one in the mobile device where the application is installed.
- ✘ Consider enabling security features on your mobile devices including password, face recognition, fingerprint or other biometrics depending on the functionality of your mobile device. Enabling those features will enhance security in case of mobile device theft. Do not let the phone from which you are banking to be used by others without supervision.
- ✘ Install antivirus/antimalware software only from trusted vendors. Use the official markets for installation of antivirus/antimalware products.
- ✘ Keep the operating system of your smart device always updated. The patches/updates eliminate security vulnerabilities in operating systems. Consider vendor instructions.
- ✘ Do not use rooted and/or jail-broken smart devices for active bank operations. Rooting and jailbreaking are actions that allow you to use phone-locked features and acquire administrator rights. Acquiring administrative rights enables unauthorized persons to obtain full access on your device.

Phishing and e-mail notifications

- ✘ Fishing is a scam that encourages users of computers and other devices connected to the Internet to disclose their personal or financial information in an email or website. Users are directed to a fraudulent website where they are asked to provide personal data (for example) their username and password to access Raiffeisen ONLINE. This website looks like the real thing, but it's actually a fake copy. The information entered is then used for identity theft or unauthorized access to your internet banking. Raiffeisenbank never sends links that invite you to enter a username and password to log in to Raiffeisen ONLINE. Always enter the Raiffeisen ONLINE address in the web browser yourself - this is the only way you can be sure that you are entering your login details without sharing them with third parties.
- ✘ Some Internet browsers have built-in phishing prevention filters, and others provide this opportunity by add-ons which make these filters.
- ✘ Raiffeisenbank DOES NOT send e-mails requesting information about your credentials (username and password), bank accounts, bank cards, etc.
- ✘ Raiffeisenbank DOES NOT exchange the above stated information via e-mails.
- ✘ Raiffeisenbank DOES NOT send e-mails containing links to the bank page or online banking page.
- ✘ Raiffeisenbank DOES NOT send e-mails urging you to call a number stated within the e-mail to exchange information concerning your Raiffeisen ONLINE account.
- ✘ If you doubt the authenticity of a message do not hesitate to contact us.

If you have any questions and/or suspect any fraudulent activities, contact us at:

Phones	0700 10 000 (Vivacom); 17 21 (A1 and Telenor)
E-mail	call.center@raiffeisen.bg