

SECURITY INSTRUCTIONS FOR E-BANKING

The most important principles to be observed for secure use of e-banking.

1. Basic information on e-banking

Login

- Always enter the address for login to our e-banking portal («login.bergos.ch») manually in the address line of your browser or navigate to the e-banking portal via the Bergos AG website («bergos.ch»). Never log in via a search engine (e.g. Google) or via a link that has been sent to you by email, for example.
- Check whether there is a secure connection to the correct website:
 - Lock symbol in the address bar
 - Correct name of Bergos AG as certificate holder (click on the displayed lock symbol)
 - Correct Internet address of the login page («login.bergos.ch»)

Note: In so-called real-time phishing, customers are led to fake e-banking portals via advertisements. If a login is made on such a portal, the customer's password is accessed, which is used almost simultaneously to login to the real e-banking portal. The customer is then shown a one-time passcode on the mobile app, which the customer in turn enters in the fake e-banking portal. This allows the attacker to access the one-time passcode and gain access to the real e-banking portal. Against this background, it is particularly important to ensure that you have established a secure connection to the correct Bergos AG e-banking portal.

- Enter your username and your individual password on the login page. Your login must then be confirmed by using the Bergos Mobile App.

Protect access data

- Use complex passwords consisting of a combination of capital and lower-case letters, numbers and special characters. Avoid information that is easy to guess, such as dates of birth or names. Change the password if you suspect that it is known to other people.
- Do not write down your PIN and passwords anywhere and never disclose your personal access data.
- If you login while on the move, make sure that you enter your personal access data covertly and that nobody is looking over your shoulder. In addition, an open e-banking session should never be left unattended. This way, you do not give third parties the opportunity to misuse your data.

Logout correctly

- End the e-banking session properly by clicking on «Log out» and delete the browser history. This will remove any data temporarily stored during an e-banking session.

Protect devices

- Protect your devices with a firewall and an antivirus program and make sure that you regularly update your antivirus program, operating system, and other installed software. Activate the automatic update function whenever possible.
- Avoid using e-banking services via public WLAN networks, as these can be insecure.
- Only use trustworthy and secure devices to access your e-banking account. Avoid access from public computers or devices.

2. Rules of conduct

Beware of irregularities

- If a system interruption or an unusual message occurs, or if you are asked to execute confirmations or install software, cancel the login process and connection immediately and contact E-Banking Support without delay.

Unsolicited contact

- Always question unexpected contact and unexpected requests for payment by phone, email, or other electronic messages, and never disclose confidential information if you do not know the caller, sender, or reason for the request.
- Especially requests for payment by email or other electronic messages in which you are given bank details for a payment must always be checked with the biller. Use an official phone number or email address for this purpose and not those listed in the message.

Note: Bergos AG will never ask you to test your e-banking access, provide your access data or other confidential information, or initiate a test payment. Neither by phone call, email, or other electronic messages. If you are unsure, please contact E-Banking Support.

Suspicious emails or other electronic messages

- Fraudulent emails or other electronic messages, so-called phishing emails, are not always easy to recognize. Look out for spelling and grammatical errors, foreign characters, incorrect language, unusual tone, disclaimers, mismatched logos and design. Phishing emails tend to use urgency as a tactic to entice the recipient to act quickly without giving it enough thought. Check the sender address carefully. Often similar looking addresses are used to give the appearance of legitimacy. Check any links by moving the mouse pointer over them (without clicking). Phishing emails can pose as

legitimate sites by using similar sounding domain names. In suspicious cases, do not click on any links contained in the message, do not open any attachments, and delete the message.

- Never trust any emails or other electronic messages that seem strange to you.
- If you are unsure, please contact E-Banking Support and have the authenticity of the message confirmed. This also applies if the message appears to come from Bergos AG.

3. E-banking on mobile devices

- Enter your username and your individual password in the Bergos Mobile App.
- Only install the mobile app from the official stores.
- Always activate an individual lock code on your mobile devices.

4. E-Banking Support

In the event of unusual circumstances or uncertainties, please contact E-Banking Support immediately.

Phone: +41 44 284 21 37

Email: ebanking@bergos.ch
