AccessBank
Your accessible European bank

myAccess - recommendations for safer internet banking

1) **Use a Strong Password**. Come up with a complex password containing letters and numbers that will be easy to remember and difficult to guess for others. If your password for **myAccess** is the same password as on another website, email or social networks, then it is easy to crack. AccessBank pays great attention to the security of your passwords for its side, but we cannot vouch for the other sites. We recommend to come up with unique password for **myAccess** so that you do not use it in anywhere else. Your Bank strongly recommends changing your password at regular intervals. And do not forget: a good password – is 90% of the security of your money.

2) **Keep your password confidential.** The safest place to store your password - your memory. Do not tell anyone and do not share personal information. Do not write down your password on **myAccess**. Do not save the password of **myAccess** in the browser. The best way to remember a password - enter it on a regular basis when entering **myAccess**. Visit **myAccess** more often to make payments and track the money. Try not to use questionable places for working with **myAccess** (Internet cafes and etc.). Just keep the password confidential at all times.

3) **Anti-Virus.** Use licensed anti-virus software and update it regularly. A good antivirus protects against spyware, encrypts your passwords and self eliminates security threats. If you have used the mobile Internet on the phone, it certainly keeps your personal data. Use Antivirus for smartphones, to protect them. For additional protection, you may use the Internet Security. In addition to the functions of anti-virus tools offer secure payments (isolated virtual environment for online transactions). And do not forget to promptly install security updates of the operating system.

4) **Watch for the SMS.** We will send you messages about each transaction. Once you see an SMS with the operation that you did not commit, immediately call the bank. Put your electronic signature (AsanImza) only for orders you expect or have initiated yourself.

5) **Beware of unsolicited emails or phone calls.** You might be asked for PINs or passwords – your bank or the police would never ask for these in full. If someone calls you up on behalf of your bank and asks you to provide personal data and/or to sign electronically, refrain from taking any action at all, for your bank will never ask you to provide this kind of information. AccessBank will never ask for your confidential information via phone or email. So whether you get an apparent phone call from the bank or an email requesting your details, do not give out your login information.

6) Use your login ID and password only on the official login page of the bank, which should be a secure website. Look for "https://" in the URL when logging in; it means that the website is secure.

7) **Regular Statements check.** Check your statements of account at regular intervals.

8) If you suspect someone has access to your page, logon to **myAccess** to change your Password and immediately contact the Bank