20.11.2020

SECURITY PROCEDURES

MAGYAR BANKHOLDING ZRT.

Security plays an extremely important role in managing our finances, and for this reason the information technology systems of Magyar Bankholding Zrt. are constantly under development to ensure the constant availability of the data and the functionality of the systems, as well as an adequate level of protection of the personal data processed in such systems at all times in accordance with the requirements of individual services.

In view of the above, when building our information technology systems we rely on high performance and highly reliable state-of-the-art information technology and security system components that we apply under stringent development and operational protocols. We constantly monitor and analyze any potential threats which enables us to apply risk-proportionate measures at all times so that we can ensure a high level of data protection and data security in our systems.

Our company applies various technological assets and organizational measures to protect our information technology systems in light of the business aims and protection purposes and we utilize multi-layer antivirus and anti-malware solutions, too. Our systems to be protected are operated in a manner that allows us to inspect unauthorized activities and identify those responsible. Our company strengthens the security of the systems prior to their deployment in every case.

To protect our systems, we strive to preserve the functionality, availability, confidentiality, integrity, credibility of the components and data thereof, which we consider to be of utmost importance. In addition to this, we pay special attention to access control, data protection and secrecy, operational security, and we apply adequate technical and organizational measures to enforce and implement these.

To handle extraordinary events disrupting the continuity of service, we have in place business continuity and emergency response plans which ensure to maintain operational conditions even under extraordinary circumstances.

To manage the risk of data leakage, and proportionately to the security risks, we operate a comprehensive solution that supports security procedures centrally monitoring potential channels, we apply monitoring measures, and to manage any data breach we apply procedures that ensure that the detection, inspection and remediation of the impacts of incidents are conducted as efficiently as possible.

With our data security and information security activities we aim to ensure the security of the data, i.e. the confidentiality, integrity, credibility and availability of the data, while data protection and secrecy ensure that the data to be protected remains protected. We have implemented and maintain adequate technical and organizational measures to protect the data that is under a data protection obligation by law or that we have deemed to be protected within our authority (professional and state secrets; bank, securities, fund and trade secrets; personal data, etc.).

Your cooperation, your careful and cautious actions as well as the high level of security of the devices that you use are all indispensable to maintain the level of security we have achieved to ensure that fraudsters are denied the opportunity of a successful attack.

Useful tips for banking activities:

- We recommend that the data you provide to the clerk should be limited to the scope and quality required for your identification.
- Do not throw away documents containing your personal data allowing your identification or related to banking issues (contracts, account balance, etc.), keep them locked away to prevent access to them by unauthorized parties.
- We would like to advise you that banks never request client identifiers, login passwords, PIN codes, bank card details via e-mails, telephone or SMS.
- When you are using electronic banking services, check the authenticity of the website. In genuine websites of banks and other financial institutions, a lock icon is displayed in the footer of the browser and in the address bar at the top as a sign of a secure connection.
- If you ever experience a display out of the ordinary, a weird wording or identification request, terminate the Internet connection with that website immediately and contact the customer service of the bank.
- You may protect against malware by purchasing and properly installing legitimately licensed versions of the software you use on your device.
- Always have active antivirus protection on your computer.
- Beware of links received in unwanted e-mails, popup windows or in advertisements as these may redirect to fake or fraudulent websites.
- Always select a strong password and never use the same for every website.
- Regularly check the movement on your bank account to see if debits of unknown origin have been initiated.