Garanti BBVA Online Security

When it comes to online shopping, payments or money transfer, there is nothing more important than the security of your information and bank transactions. That is why on your Garanti BBVA Online account you have a special menu dedicated to security settings, so that you can control them better.

You can access online the security definitions through the “Security settings” option from the “Settings” menu. The security settings contain five options:

Defining accounts and cards

You can define the accounts and cards that you wish to have transactions blocked through Garanti BBVA Online. You can also choose to never display them.

Cash transfer e-mail alerts

You can define a cash transfer limit (transfers above a certain amount) for Garanti BBVA - Garanti BBVA transfers as well as Garanti BBVA - Other banks, performed through Internet banking for which you will automatically receive an e-mail alert.

We also advise you to consult and keep in mind the following preventive security measures:

Make sure your e-mails are received from a verified source

Garanti BBVA will NEVER ask you for sensible information, like passwords, through e-mail. If you ever receive an email that asks for information regarding Garanti BBVA or passwords, please contact us immediately through our Customer Communication Center 0800 80 1234 (free of charge from any fix network) or 021 200 9494 (regular charge from any network), available 24/7. There are also viruses that spread through e-mail. If you receive an e-mail from an unknown or dubious sender, please delete it without opening it or reading it.

Manually enter the “www.garantibbva.ro” address in your browser.

Anytime you wish to access Garanti BBVA Online, MANUALLY insert “www.garantibbva.ro” in the address bar of your browser and then click the link from the page. This is the safest way to protect you against “phishing” - someone’s attempt to confuse you by masquerading as Garanti BBVA, in order to obtain sensible information.

Keep your personal information confidential

Never give away personal information as your date of birth, ID number, etc.

This type of information will only be asked if you ever call our Customer Communication Center 0800 80 1234 (free of charge from any fix network) or 021 200 9494 (regular charge from any network), available 7/7 from 9 am to 10 pm, with the purpose of activating the Internet Banking service.

Garanti BBVA will NEVER ask for your mother's maiden name - but only a few containing letters. If you believe that someone attempted at the safety of your personal information please contact us as soon as possible at Customer Communication Center 0800 80 1234 (free of charge from any fix network) or 021 200 9494 (regular charge from any network) available 24/7.

Use passwords that are hard to guess

Protect your Computer

First of all, if you are using Microsoft Windows, you should go to http://update.microsoft.com, and download and install all the recommended security updates and patches.

You can protect your computer against viruses or malware by regularly using 3 types of software: an antivirus, an anti-spyware application and a firewall. There is also a broad variety of software that offers all these three forms of protection, but you can choose as well from all the commercially available options. Some of them include:

Antivirus software [1]*:

There are a number of web sites that offer free virus scanning services:

Trendmicro House Call Kaspersky Virus Scanner Panda Software Active Scan

Antivirus software that you can install on your Computer*:

Panda Software McAfee VirusScan Norton AntiVirus Grisoft AVG Anti Virus

Anti-spyware/anti-malware software* (protects you against websites that try to collect information about the way you use the Internet):

Spybot S&D (free)

Lavasoft Ad-Aware SE Personal Edition (free)

McAfee AntiSpyware

Firewalls* (software that prevents the unauthorized access when you are online, blocking access to certain applications from your computer):

Zone Alarm (free)

Norton Internet Security

McAfee Firewall Plus

*The links displayed below are not associated in any way with the Garanti BBVA website and are included just as simple suggestions. Garanti BBVA is not held responsible for any damage

caused by any software downloaded from the specified links or for damages caused to your system, as well as for your level of security provided by the specified software.

Garanti BBVA does not provide support for any of the software or derivate that is accessed through the links below

Use only computers that are considered safe

In order to access Garanti BBVA Online, NEVER use computers that have access to the open public (ex. internet cafes) or any other computer that does not use an up to date antivirus software.

In order to ensure the security and confidentiality of your information and transactions we rely on three solid pillars:

Authentication that ensures access to transaction only to authorized clients.

Before a client can perform online transaction through Garanti BBVA Online, he has to go through all the four security verifications:

- Client ID: a unique number that is used to identify every Garanti BBVA client
- The ciframatic PIN: a 4 digit code required in order to use the Ciframatic (after 5 consecutive attempts the Ciframatic is automatically locked)
- The code generated by the Ciframtic: a unique cipher, always different, containing 6 digits generated by the Ciframatic
- The password: a key word that the user will have to specify at every attempt to access Garanti BBVA Online.

The protection of information concerns the assurance of integrity and confidentiality of information. The traffic between the user and the bank is encrypted, and the integrity and confidentiality are protected through the Secure Sockets Layer (SSL). The SSL protocol is accepted by most web servers and browsers. It decodes information transmitted via SSL only at the specified recipient address. Before the information is sent it is automatically encrypted in order to be decoded only by the specified recipient. The verification takes place at both ends of the connection, ensuring the integrity and confidentiality of information and transactions. The strength of the encryption used in transmitting information depends on the length of the cipher in use. The length of this cipher is especially important for protecting information, and the SSL uses cipher with lengths of 40 and 128 bit. 128 bit encryption contains 2128 (3.40 * 1038, o number with 39 digits) possible combinations, making it impossible to crack the cipher.