Important aspects related to security

At BBVA, we are aware of the need to **guarantee security** during the transfer of data between the bank and our customers. This is why we have the highest security measures to ensure the **confidentiality of communications.**

Always ensure that your data is entered on a **secure page.**

SECURITY STANDARDS

It is important that you follow the following **security standards** whenever personal data is requested from you over the Internet:

1. Make sure the **connection** is established through a **secure server** by checking some of the following:

- The address (URL) of the server, since the address of a secure server starts with https and not http.
- A sign in your browser, which is located in one of the bottom corners of your window: a **whole key** (instead of being broken, like for any non-secure server) or a **closed padlock** (instead of being open, like for any non-secure server).

2. **Check** the page's **security certificates:**

- To do so, click on the padlock icon that appears when you access a secure area in the bottom right of your browser, and make sure the certificate's expiry date and domain are currently valid. Among the details provided, you will find the sender, the validity period and who the certificate was issued by.

In order for the following measures to be effective, it is necessary to use the most recently updated versions of the following browsers:

- Internet Explorer
- Firefox
- Chrome

In addition, the website has been optimized for a screen resolution of 1280 x 800 pixels or higher, for a better display.

SECURE SERVER

Transactional service systems operate on a secure server that uses the **SSL** (Secure Socket Layer) protocol, which is always activated upon entry into the service system. The server sends **the data encrypted** using 128-bit algorithms, which ensure that it is **only intelligible to the customer's computer** and **the bank's server.**

By using the SSL protocol, we guarantee:

- That the customer communicates their data to BBVA's server center.
- That between the customer and BBVA's server center, the data is encrypted during transfer, thus preventing it from being read or manipulated by third parties.

ACCESS TO BBVA.BE

At BBVA, we recommend all our users to follow these simple tips to maintain absolute security of their session through our remote banking service.

To close your session on BBVA.BE, you should always use the "Logout" button in the BBVA.BE toolbar and click "OK" in the window that will then appear.

This way you will have closed your BBVA.BE session securely and the next time you connect to BBVA.BE, your user number and access password will be requested again.

If you do **not log off properly**, the server will only consider the session closed once the set time-out period has expired, which will activate the **automatic disconnection.** If you change Internet pages without following these steps, it will be possible to directly access your personal space on BBVA.BE without entering your access passwords while the period of time required for automatic disconnection has not elapsed.

CACHE MEMORY

The browser's cache memory allows almost immediate access to web pages that you have visited recently.

Sometimes, this possibility can cause some **minor incidents** in the correct operation of the pages. It is possible that through your personal computer, **the latest version displayed is the last version stored in the cache** and not the latest version stored on the server of this website.

To avoid these problems, we recommend that you check in your browser the **content update option each time you visit the page** and that you delete all files in the **temporary internet files** folder on a regular basis.

SECURITY OF YOUR PASSWORDS

Advice

- **Do not share** the passwords you use on BBVA.BE with anybody.
- The username and the access password should be different. This way, it will be more difficult for a third party to know them and to guess them.

- If you think someone has found out your password, you must change it as soon as possible.

STORAGE OF PASSWORDS ON COMPUTERS

- Currently, browsers offer the option to **save codes and passwords** for Websites that request them, the latter being stored in your computer's memory. **This practice,** although it makes access to the sites that request the username and password easier, is strongly **discouraged** when the passwords stored are those of banks or other services which, if lost or stolen, can cause **serious losses to the users**.
- At BBVA, we recommend that you **do not save any of your access passwords** to our remote banking service on your computer. Your computer can be subject to certain **attacks** that can **send the passwords to other** computers connected to the Internet.

To **clear the passwords stored** on a computer, simply follow a series of simple steps that you can consult in **your browser's help manual**.

PREVENTION AND DETECTION OF VIRUS ATTACKS

Viruses are software whose objective is **to be installed** on a user's computer **without them giving their permission and/or without their knowledge.** There are several types of virus, but they all have in common that they spread and disseminate, within the same computer and across the network.

It is easy to unknowingly contribute to the spread of a virus, by transferring emails containing virus-infected attachments. **The collaboration of all** Internet users is critical to **prevent the spread** of viruses across the network.

There are several types of files that can be infected by a virus: we recommend that you do not trust file extensions such as .exe, .com, .bat and that **only run** on your personal computer **files** from a **trusted** sender.

We recommend you **not to download** to your computer **files that have not been verified and certified** and **not to open emails to unknown recipients**.

PRECAUTIONS

- Set the **security of the system and Internet connection** properly and regularly check the connection security level. Do not change your computer's security settings, unless you have the proper knowledge. In this case, set your computer and all your software to have the highest possible levels of security.
- Make sure you always keep your operating system, browser and the software you use regularly **updated**.
- Install a **firewall** and an **anti-virus** program and make sure they are regularly updated.
- Perform regular file **backups**.
- If you use flat-rate **bundle** connections (for example, ADSL and cable), **turn off your computer** once your session is closed to avoid exposing your computer to possible attacks.
- Make sure the web pages on which you must enter confidential details are **secure:** with the padlock and key icons and whose address begins with https.
- Before selecting a **link** on a Web page, **make sure** it sends you to the desired address. It is also common to include links in an email that appear to link a legitimate website but that actually link to a website that has nothing to do with the company the message comes from, if they are examined more thoroughly. Remain alert even when the design of the website looks legitimate.
- Pay special attention and caution when **downloading software:** if in doubt, do not allow downloads on sites that you do not completely trust
- Set your **email** to only receive messages in text format. Do not run an attached file from an email that has been sent to you. Try saving the file to your hard drive and if it is infected, your anti-virus will detect it. Refuse files from chats or chat groups that you did not request beforehand. Encrypt the most important messages and files.

DATA PROTECTION

At BBVA, **we guarantee the protection of our customers' data.**

The seal of the Spanish Association of Electronic Certification (ACE) awards us the position of **first financial entity to** adhere to its **Code of Ethics of data protection on the Internet.**

The website of BBVA (Banco Bilbao Vizcaya Argentaria) in Belgium, at www.bbva.be, does not automatically recognize any data regarding the identity of visitors to its pages. For remote banking services, in order **to guarantee the security and confidentiality** of transactions, the user must first **identify and authenticate themselves** on the system by **entering access passwords.** In the case where the user requests information about our services or products or wishes to follow a complaints or impact assessment procedure, by sending forms that reside on BBVA's web pages, it will be necessary in all cases to collect personal data essential to enable us to respond to their request.

All data is transferred in absolute confidentiality and **is not accessible by third parties** for any purposes other than those for which they were requested. For further information or personal comment regarding the exercising of rights of access, cancellation, rectification or opposition provided for by Belgian law on personal data protection, you can contact us at:

bbvabe@bbva.com, by telephone on +32 (0) 2 512 32 62 or by mail at the address BBVA, succursale en Belgique, Customer Services, Avenue des Arts 43, 1040, Bruxelles.