BBVA

Creating Opportunities

Security in BBVA Net cash

Client solutions

May 2018

Introduction

The new possibilities provided by the rapid evolution of the Internet are evident. Possibilities that allow us at BBVA Net cash to complete, day by day, our complete range of online services and, at the same time, open the doors to the development of new forms of fraud and swindling that are increasingly advanced.

At BBVA Net cash, we are aware of these threats and we are constantly vigilant and work to take extreme precautions to ensure that you can continue to operate securely. In this document, we have compiled all the initiatives implemented by BBVA to protect both your data and access from intruders. You will also find a number of recommendations that you should take into account to help make your internet connections and online operations secure.

1. Measures from BBVA

1.1 Service / User administration

BBVA Net cash is a **multi-user application**. It has different user profiles that the company can assign to its employees **based on its operational structure**.

A specific profile, the **administrator**, defines and manages the company's users in BBVA Net cash. There can be one or more administrators with different delegation powers (without powers or with joint - several or joint 2/3/4).

Each user is assigned a profile that is defined at the highest level of detail. In the case of authorizing operations, the options are:

01	No signer	Cannot approve operations
02	Representative	This can be joint and several or joint
03	Auditor	This individual can even stop fully signed orders until they have their permission

This structure allows **the user circuit to be as restrictive as the company wishes**, in order to guarantee, at all times, that each one of them:

- Accesses only the services and accounts defined by the administrator.
- Can only perform inquiries and operations as authorized by the administrator.
- Has the power to authorize operations (or not).
- Has a cash limit depending on the operations and account, as per the administrator's decision.
- Only administrators can view their profile as well as a list of users defined in their entity, their profiles, access to services and assigned powers.

1.2 Service / Activity control

Users can monitor the entity's operations in BBVA Net cash through:

- The <**Statistics>** module (*Signatures and files>Statistics*): consultation of the operations carried out in a given period.
- The **<Audit>** option (*Signatures and files>File signatures and monitoring*): control of the operational activity of each user of the entity.
- The **<User audit>** option (*Administration>Audit*): reflects what actions each of the administrators has taken within the user circuit.

1.3 Service / User credentials

BBVA Net cash uses two-factor authentication, which basically consists of **including a device**, token, to validate in the user and transaction signature circuit. Consequently, the system will prompt the user to enter a (single-use) six-digit security code generated by their device. This device may be physical or can be installed on your cell phone (by downloading the BBVA Net cash app*).

*Android/iOS Environments. Should you have a BlackBerry/Windows Mobile device, you must download the BBVA Token app.

If necessary, BBVA provides a special model of physical token enabled for users with visual impairment.

- Although the passwords do not expire, we recommend that you change them every month.
- **Password size is** 8 alphanumeric **characters** to make it difficult for third parties to deduce by testing options.
- Passwords are stored **in irreversible encryption** in specialized user and identity management systems so that no one can obtain or deduce them.

Requirement to change the password on first login: to prevent someone from impersonating the user, you are required to change your password the first time you log in to BBVA Net cash.

Blocking users:

- If the user or activation key is entered **incorrectly** five times in a row, the reference in BBVA Net cash reference will be blocked and cannot be activated until BBVA generates a new activation key.
- In the case of the password, after three failed attempts, the user is blocked.
- If the security code generated by the user's security device is incorrectly entered five times in a row, the user is blocked from BBVA Net cash.
- The user administrator has the autonomy to block access to users in their entity, so if an employee leaves the company, **access can be immediately revoked.**

1.4 Service / Identification and authentication

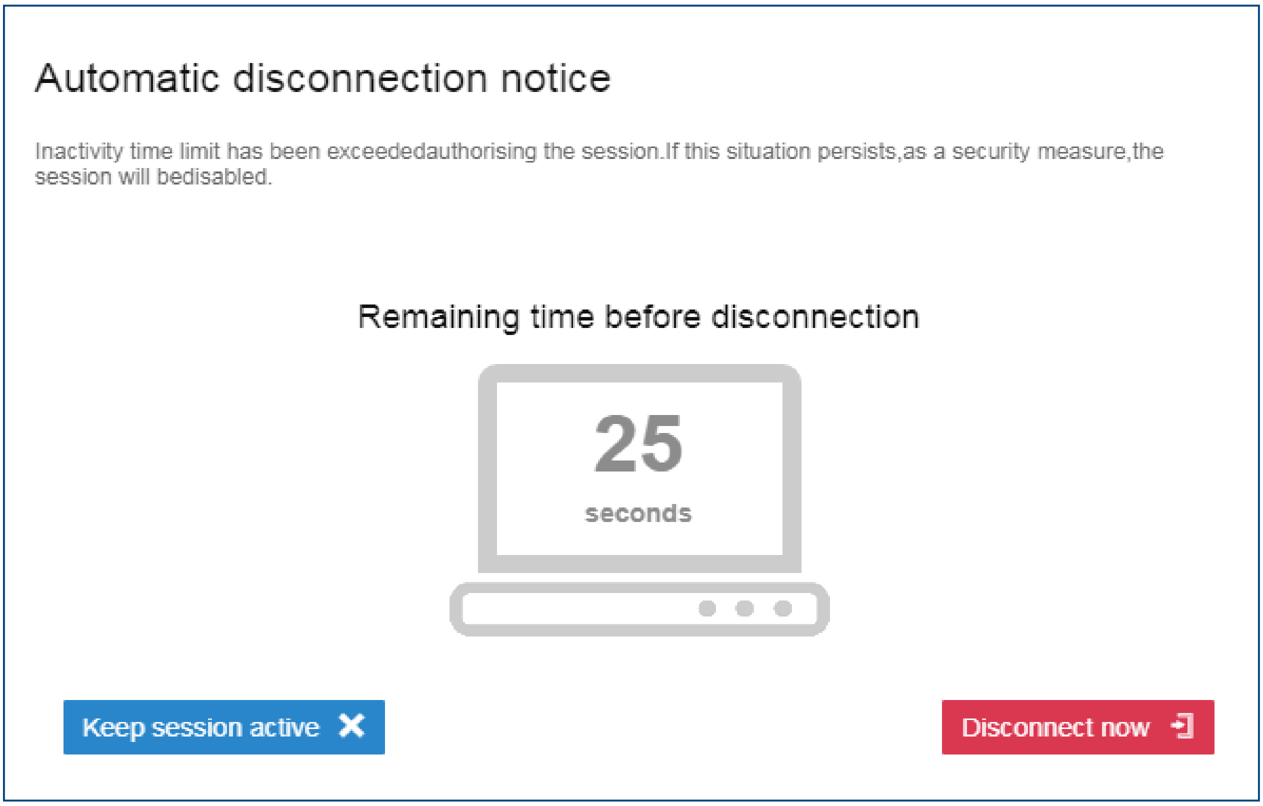
Traceability of transactions: the accesses and transactions carried out are reflected in **automated operation logs** that include the operation carried out, the date and time of the operation and the user who carried it out, allowing the validity of the registered operations to be determined.

Last connection information:

- If the user logs in for the first time, BBVA Net cash will inform them of this.
- In subsequent logins, BBVA Net cash will show the date and time of the last login.

Cookies are only active during the session: cookies placed on the user's operating system, which are required to securely browse any website, are only active when logged on to BBVA Net cash and **are deleted when the user logs off the application.**

Automatic logout: as an additional security measure, after 10 minutes of inactivity in BBVA Net cash, the user is logged out and disconnected from the system.



Automatic disconnection notice

Inactivity time limit has been exceededauthorising the session.If this situation persists,as a security measure,the session will bedisabled.

Remaining time before disconnection

1.5 Service / Compliance with national and international regulations

BBVA complies in all its services with the rules and regulations of the countries in which it operates. BBVA's commitment to these regulations is set out in the Code of Conduct, which is compulsory for all employees.

1.6 Technology / Confidentiality and Integrity

Of all user credentials:

- All user transaction passwords are stored **in irreversible encryption** in specialized user and identity management systems so that no one can obtain or deduce them.
- BBVA's operating procedures do not require anyone at the Bank to have the transaction passwords of its customers, so **no one knows them or will ask for them personally.**

Of communications:

- Communications from BBVA's transactional and remote banking services are encrypted by means of **SSL protocol** to preserve the confidentiality and integrity of online communications.
- The certificates used by BBVA to provide this service are generated by **Verisign Inc.**
- In addition, the sensitive communications that take place in BBVA's internal networks are adequately protected according to the operating environment and the protocol used.

Of the information:

- The information stored in the internal systems and databases is protected by different security systems allowing for **access only to authorized employees.**
- BBVA has an automated system for managing access privileges to information that guarantees controlled and restricted access to authorized personnel.

1.7 Technology / Physical Security of Data Processing Centers

BBVA's Data Processing Centers are equipped with extensive **physical security measures** to protect data processing systems, which include the following:

- CPD Tier IV Gold in operational sustainability.
- Individualized access control to the premises and the different technical rooms, equipped with systems for the detection of dangerous elements.
- Teams providing physical and video surveillance of the perimeter and inside of the facilities on a 24x7 basis.
- Specific detection and protection systems against intrusion, fire, flood, supply failure and other catastrophic events.

In addition, having two fully operational Data Processing Centers, **BBVA guarantees the safeguarding and recovery of information**, if necessary.

1.8 Technology / Security architecture

In order to achieve optimal security in the design of its systems, BBVA has a specific security architecture especially for those who provide online services to their customers.

Specifically, and to minimize the level of exposure to the Internet, only the presentation layer (which performs the functions of user authentication, authorization of access to web applications and secure session control) is kept exposed through a reverse security proxy.

1.9 Technology / Specific protection systems

Firewalls and antivirus and anti-intrusion systems that are always up-to-date:

- BBVA **segregates its networks** and systems with **several levels of firewalls**.
- Furthermore, BBVA's internal systems are permanently protected through **anti-malware and intrusion detection systems**.
- Both types of systems are managed on a 24x7 basis and are **constantly updated**, which makes it possible to prevent the action of new threats on a permanent basis.
- All surveillance, alert and security response **systems** against possible frauds are **monitored and supervised** by a team of specialists on a 24x7x365 basis at the Data Processing Center facilities.

Activity logs for all components: BBVA's remote banking systems and applications have logs of all critical components that support services for detecting fraud attempts and forensic analysis of suspicious or fraudulent activities or transactions.

Periodic review of the service applying the latest attack techniques: the systems that support remote banking services are periodically reviewed using vulnerability analysis tools.

Internal and external audits: BBVA's systems and processes are subject to periodic security audits both by the independent Audit department and by specific external audits or audits associated with financial or compliance audits.

2. Actions you need to take: recommendations

2.1 Protecting your user credentials

- Use **complex and difficult to deduce passwords**, which contain a mix of lower case and upper case characters and numbers.
- **Don't share** your **passwords** with anyone. Passwords are secret and should be known only to their owner.
- **Don't write your password down** on post-it notes or notebooks; **memorize it and use specialized password managers**. You can find these kinds of free programs at www.osi.es.
- **Disable** the **save password** option on your **browser.** It's securer to enter it every time you log on.
- **Change** your passwords periodically. If you suspect that someone has been able to guess your password, you should change it as soon as possible.
- **Do not use the same password in different** services (email, Evernote, other banks, etc.)
- Your physical security device is **personal and non-transferable.**
- If you receive a message requesting your personal passwords, **do not provide any information** and contact BBVA Net cash customer service immediately:

  91 224 98 02/902 33 53 73

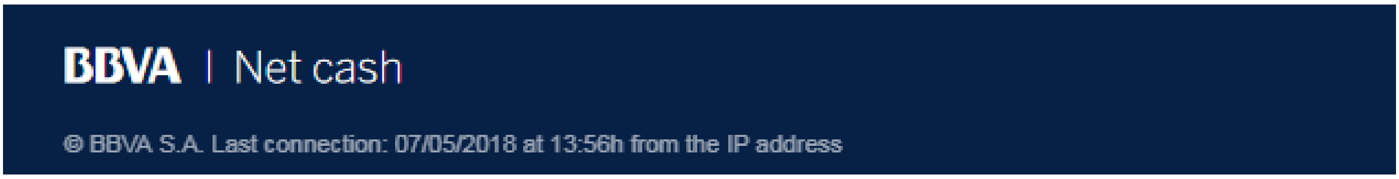
2.2 Protecting your computer

- Keep your **operating system and browser version** permanently updated with the corresponding patches to protect you from possible cracks or errors detected.
- **Configure** your computer and all its programs with the **highest levels of security**.
- Install a **firewall and keep it active and always up to date.**
- Install **anti-malware programs and keep them up to date and active**. Verify the documents received from the outside with the antivirus.
- Regularly **back up** your files.
- **Avoid downloads from unknown websites**, as they may contain viruses or spyware.

- **Don't connect** any **external device** to your devices **if you don't know where it came from**, such as flash drives, hard drives and unknown cellphones.
- Regularly clean **cookies and temporary files**.
- Download programs and apps only from **official websites.**
- Set an **unblocking pattern** on your cell phones and tablets so they can't be accessed by third-parties.

2.3 Secure Internet access and browsing practices

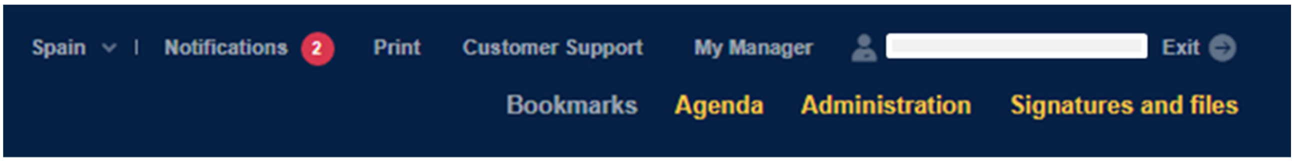
- On **shared computers** or if you're connected to a **public Wi-Fi**, **do not access pages** that need your username and password. **Don't provide personal data either** such as postal address, phone number, etc.
- Avoid connecting to sites with private content from **public computers.**
- **If you have to enter your credentials**, check that the address (URL) of the server begins with **https**, which means that you are accessing a secure server.
- Another indication that the **server is secure** is the presence of a **closed padlock** (instead of being open, like on any non-secure server) to the left or right of the address (URL).
- **Check the security certificates** of the page you are on by clicking on the padlock icon that appears when accessing a secure area, or on the certificate in the browser bar, and check that the expiry date and domain of the certificate are up to date. The detailed information includes the issuer (Verisign), the period of validity and who the certificate was issued to (BBVA).
- **Do not use the "autofill password" option in your browser.** If enabled, the passwords you enter on the website are stored on your computer and when you re-enter your username, the password field is automatically filled in. On a shared computer, this option may cause someone to use your personal passwords.
- **Check the time and date of your last login.**



BBVA | Net cash

© BBVA S.A. Last connection: 07/05/2018 at 13:56h from the IP address

- To end your BBVA Net cash session securely, **use the <Exit> button** that appears in the upper right-hand corner.



3. Most frequent viruses and attacks

Computer viruses are programs whose purpose is to install themselves on a user's computer without their permission or knowledge. There are several types of viruses, but all of them tend to share the property of propagating and spreading in the computer itself via the Internet.

It's easy to inadvertently contribute to spreading viruses by resending emails containing infected attachments. The collaboration of all Internet users is essential to avoid them spreading.

There are different types of viruses and some of the most notable include:

Phishing: this consists of sending an email purporting to be from a well-known organization and requesting the user's data (address, bank details, passwords, etc.) To provide this data, the user is in most cases required to follow a link that appears in the email and enter the requested information once on the bogus page.

The basic scheme of operation is as follows:

1. A mass message (spam) is sent informing that BBVA Net cash users must confirm their access data.
2. The message includes a link to a page from which you must confirm the data. Sometimes the link starts downloading malware.
3. The user accesses the link that leads to a "similar" page to the real BBVA Net cash and, in all confidence, enters his or her details.
4. Since the page is fake and controlled by the scammers, they are the ones who actually receive the user's data, and once in possession of these details, they have free access to the affected user's live account.

Even though BBVA will never ask you for your BBVA Net cash passwords and signature by email, here are some tips for recognizing these types of attacks:

- Sometimes the logo appears distorted or stretched. In addition, there are often misspellings, or they contain expressions that have fallen into disuse.
- They refer to you as "Dear customer" or "Dear user" instead of including your real name.
- They warn you that your account/e-banking service will be closed unless you reconfirm your login information immediately.
- The tone of the email is threatening.
- The text refers to "security commitments" or "security threats" and requires immediate action.

- The URL is not https:// and the security padlock does not appear in the lower browser bar. Fake links include this icon inside the window to fool you.

Ransomware: this is a lucrative method of technology crime. Usually concealed as "parcel delivery services" or any other credible excuse, they are propagated via email with links that enable programs to be installed or infected files to be downloaded. This virus blocks access to computer information and demands a ransom that will supposedly provide the key to decrypt the information.

Here are a few tips to protect yourself from ransomware:

- Do not follow links or download email attachments that you think are suspicious.
- Only use legitimate software and keep it up to date.
- Always have an antivirus installed and updated.
- Make frequent backups. If you become infected, you can retrieve the information without paying the ransom.

Trojans: these are introduced into personal computers by being embedded within a program. They transform the computer's behavior so that everything that's done on it can be seen from the delinquent's computer.

To prevent infection by a Trojan horse, you should follow the same instructions as we have discussed with ransomware above:

- Do not follow links or download email attachments that you think are suspicious.
- Only use legitimate software and keep it up to date.
- Always have an antivirus installed and updated.

Hoaxes: these are emails conveying certain false rumors with the sole aim of transmitting and increasing the low-quality information circulating on the Internet. They are generally not very harmful and are easy to eliminate.

To prevent these attacks, follow the recommendations we are giving you and report any suspicious situation or communication you receive: **91 224 98 02** / **902 33 53 73**

Based on this communication, BBVA Net cash's customer service department will implement the established fraud protocol: a team of specialists will analyze the case. If the suspicion is confirmed, you will be recommended to:

- Format your hard drive.
- Install updated anti-malware.
- Keep your computer software up to date.

In all confirmed cases, the password of the user concerned will be changed.