Tips and preventive measures to limit the risk of loss of sensitive data through phishing campaigns and/or device infections caused by malware and trojans

1. Security best practices for smartphones

- Use complex passwords, even to unlock and access the smartphone (see Section 3).
- Configure automatic lock of the smartphone (by time or by inactivity).
- Activate Biometric access.
- Regularly back up the content of the smartphone to preserve important data.
- Avoid using unofficial smartphone retailers or repairers.
- Install original software only.
- Maintain actualized the smartphone software.
- Maintain actualized the application versions.
- Be careful with messages (SMS or email) as well as calls from unknown numbers or unreliable sources where personal data is requested, either by phone or via links where the domain is not clearly and evidently identifiable.
- Properly configure the device using the operating system options to prevent the installation of applications from unknown sources.
- In case of theft of the device, report it to BBVA and call the relevant operator to block the SIM and the smartphone. If you have the "Remote Information Deletion" service, it is recommended to use it.
- Do not activate the Bluetooth of the mobile phone unless necessary and avoid connecting to unknown Bluetooth devices.
- Always request authorization when someone attempts to connect to your device.
- Ensure that Bluetooth is in "Hidden" mode and avoid pairing Bluetooth devices in public places as various types of attacks (e.g., Bluejacking, Bluebugging, Bluesnarfing) occur through this communication channel.
- Activate Internet connections via WiFi only if necessary and avoid connecting to unknown access points as all information, including confidential ones such as conversations, passwords, bank

details, etc., can be intercepted by the owner of the access point through which you are trying to connect to the Internet.

- Disconnect or log out from web services that require a password before closing the browser.
- When the operating system notifies the availability of a new version of the system itself or new updates of the applications installed on the device, accept and install them as they often add functionalities and fix security flaws, preventing possible infections due to the presence of vulnerable applications on the phone.
- If you wish to dispose of the smartphone, it is advisable to erase its content first to prevent third parties from accessing the information saved on it, such as contacts, SMS, photos, email accounts, applications that give access to social networks, online stores or payment gateways, cache, and passwords stored in the browser. It is recommended to reformat the device and, if the operating system allows it, use the factory reset function (restore and delete).
- Distrust emails requesting biometric data through sending photos or videos.
- Install a mobile antivirus/ antimalware.
- Activate the remote localization, remote block and remote erase in case of device lost or stolen.

2. What to do when the device is infected or suspected to be infected

- Analyze the presence of anomalous files or folders using an antivirus to identify and eliminate any viruses present on the device.
- Make an antivirus/ antimalware device scan.
- Since the antivirus is not always able to detect all types of malware or trojans, it is recommended to return the device to its original factory state.
- Change the access credentials to the applications installed on the device before formatting it and restoring it to its factory state.
- Check the applications you want to reinstall on the device, ensuring they are necessary, come from official app stores, and are released by recognized developers; also ensure that these applications only require permissions related to the device and personal information strictly necessary for the functioning of such applications.

3. Passwords

- Before defining new passwords for the applications, scan the device using an antivirus to detect the presence of malware or trojans that might be installed on the device.
- Passwords should be at least eight characters long. The longer the password, the harder it will be to decipher, and the more security it will offer.
- Previously used passwords should not be reused.
- Form passwords with a combination of alphabetical characters (combining uppercase and lowercase letters), digits, and special characters (@, ¡, +, &).
- Use different passwords depending on the use (for example, do not use the same password for an email account as for accessing banking services).
- A good method to create a complex password is to think of an easy-to-remember phrase and shorten it by applying some simple rule.
- Passwords should be changed regularly.
- The password should not contain the account username or other easily identifiable personal information (birthdays, names of children, spouses, etc.). Also, avoid adjacent letter series on the keyboard (qwertz) or in alphabetical or numerical order (123456, abcde, etc.).
- Avoid passwords containing words existing in a language (e.g., "field"). One of the most well-known attacks to crack passwords consists of testing every word in a dictionary and/or commonly used words.
- Passwords should not be stored in a public place or within reach of third parties (on the table, written on paper, etc.).
- Do not share passwords over the Internet (via email) or by phone. Specifically, be wary of any email that requests them or indicates that you should visit a website to verify them: it is almost certainly a fraud.
- Use biometric access, biometric authentication or any official Second factor authentication.