BNP PARIBAS

10 rules of safe electronic banking

#BankDobrychDecyzji

10 RULES OF SAFE ELECTRONIC BANKING

01 Check website address and encryption

Do not click on or use:

- links in emails or text messages of unknown origin and links found on unverified websites;
- browser features such as: auto-complete forms, password or session memorisation.

Check:

- the certificate before each attempt to log into the system – this will allow you to verify server authenticity.

02 Read security communications

- Carefully read the security messages on the login page, the screens that appear after logging in, and the messages in your internal mail. There you will find information about current threats and possible social engineering attacks
- Report suspicious text messages to the nationwide, 24/7, toll-free **CERT number 8080**. This will allow suspicious numbers to be added to the blocked number database.

03 Protect private data

Bank employees **never ask you for:**

- Your banking login or password, installation of additional software, remote access to your computer or phone, full card number and CVV/CVC code, BLIK code, transfer, deposit or withdrawal of money at an ATM or bank branch.
- If you are asked any of these, please report **to the phone number available 24/7:** +48 22 548 29 40 (operators' charges apply).

04 Use Behavioural Protection

- This is a modern, free service that further enhances the security of funds on your account. The activation is straightforward and can be done both in GOonline and GOmobile app. *Personal Profile Settings --> Security --> Behavioural Protection --> Accept*

05 Take care of the safety of your computer

- Use antivirus or anti-spyware
- Remember to install patches and updates recommended by software manufacturers, including your operating system and security software.
- Install legal software from trusted sources.
- Do not use public, open Wi-Fi networks. Avoid logging into electronic banking systems from publicly accessible computers, such as those at airports or cafes.

06 Check your instructions and set limits

- Always make sure that the SMS message with the authorization code matches the transaction you are performing (e.g., confirm with the invoice details – account number/transaction amount).
- In the case of authorization by electronic signature or token, remember to verify the transaction details. Ensure that they are consistent with the transaction you are performing.
- Set secure limits for daily BLIK transactions, payment cards, cash withdrawals, and transfers. Attempts at suspicious large transfers and withdrawals will not be executed.

07 Take care of the safety of your passwords

- Strong password: contains at least 15 characters, upper- and lower-case letters, special characters (@#ś&!), and digits (1, 3, 7, 0). It can be a sentence equivalent or a sentence.
- The password should only be known to the user and stored securely.
- A bank employee will never ask you to provide your login or password.
- If you log in using a masked password, remember that the bank does not need your full password, except when changing your password to a new one. Only enter selected characters from the password when logging in.
- If you log in using an electronic signature, do not share your USB cryptographic device or cryptographic card, on which your keys and PIN code are stored, with anyone.

08 Check your login data

- Check the dates of your last logins, both successful and failed. If these dates do not correspond to your activity, you should be concerned. This may mean that someone else has gained access to your account.

09 Do not ignore system notifications

- Set up automatic email or SMS notifications for every successful or unsuccessful login, system access block, and account charges exceeding the declared amount. Thanks to these notifications, you will have control over the activity on your bank account.

10 Log out of the system

- Always log out. To do that, click the logout icon in the top right corner. Do not close the browser window without logging out of the internet banking.

More information on security is available on our website
www.bnpparibas.pl/bezpieczenstwo