10 rules for secure online banking for companies

#BankOfMindfulDecisions

10 RULES FOR SECURE ONLINE BANKING

01 Use two-factor authentication

- By enabling two-factor authentication, even if someone learns your password, they will not be able to access your account without the second factor, i.e. an SMS password.

02 Protect your private information

Bank employees will never ask you for:

- your banking login or password,
- installing additional software,
- remote access to your computer/phone,
- your full card number and CVV/CVC code,
- your BLIK code,
- making a transfer,
- depositing or withdrawing money at an ATM or bank branch.
- Report such an incident to the 24/7 phone line on :
  +48 22 548 29 40 (calls will be charged at your operator's rate).
- Report suspicious SMS messages to the nationwide 24/7 toll-free **CERT** number 8080 - this will allow suspicious numbers to be added to the blocked call database.

03 Read security messages

- Carefully read the security messages on the login page, on the screens you see after logging in, and on the bank's website. These provide information about current threats or possible social engineering attack attempts.

04 Keep your passwords safe & secure

- Strong password: contains at least 15 characters, upper and lower case letters, special characters (@#ś&!), numbers (1, 3, 7, 0). It can be a nominal sentence or a sentence.
- The password should only be known to the user and should be kept safe & secure.
- A bank employee never asks for a login or password.
- If you log in using a masked password, remember that the bank does not need your full password, except to change your password to a new one. When logging in, enter only selected characters from your password.
- If you log in using an electronic signature, do not provide anyone with a USB flash drive or a USB cryptographic device or the cryptographic card on which your keys and PINs are stored.

05 Keep your computer safe & secure

- Use anti-virus or anti-spyware software.
- Keep up with patches and updates recommended by software vendors, including the system and software securing your computer.
- Install legitimate software from verified sources.
- Avoid logging into online banking systems from publicly accessible computers, such as those at airports or coffee shops.
- Do not use public, open WiFi networks.

06 Check website address - encrypted connection

Do not use:

- links in emails or SMS messages of unknown origin and links from unverified websites,
- browser features such as autocomplete forms, password and session saving.

Verify:

- the security certificate before each attempt to log in to the system to check the authenticity of the server.

07 Verify given instructions and set safety limits

- Always check whether the SMS message with the authorisation code is consistent with the transaction you are making (e.g. confirm with the invoice details - account number / transaction amount).
- If the authorisation is made with an electronic signature or token, remember to verify the transaction details. Make sure they are consistent with the transaction you are making.
- Set safe limits for daily transfers, payment cards and cash withdrawals. Attempts at suspicious large transfers and withdrawals will then not be processed.

08 Check login details

- Check the dates of your last logins, both successful and unsuccessful. These dates should correspond to your activity, otherwise it could mean that an unauthorised person has gained access to your banking environment. If in doubt, report the situation to the bank's helpline.

09 Use system notifications

- Set up automatic email or SMS notifications for each successful or unsuccessful login, blocked access to the system and debits above a declared amount. These notifications will keep you in control of your bank account.

10 Always log out of the system

- Always log out of the e-banking system. To do this, click on the ‘Logout ’ icon in the top right-hand corner.
- Do not close the browser window or the application without first logging out of the system.

You can find more safety information on our website
www.bnpparibas.pl/bezpieczenstwo

BNP Paribas Bank Polska Spółka Akcyjna z siedzibą w Warszawie przy ul. Kasprzaka 2, 01-211 Warszawa, zarejestrowany w rejestrze przedsiębiorców Krajowego Rejestru Sądowego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr. KRS 0000011571, posiadający NIP 526-10-08-546 oraz kapitał zakładowy w wysokości 147 799 870 zł, w całości wpłacony.