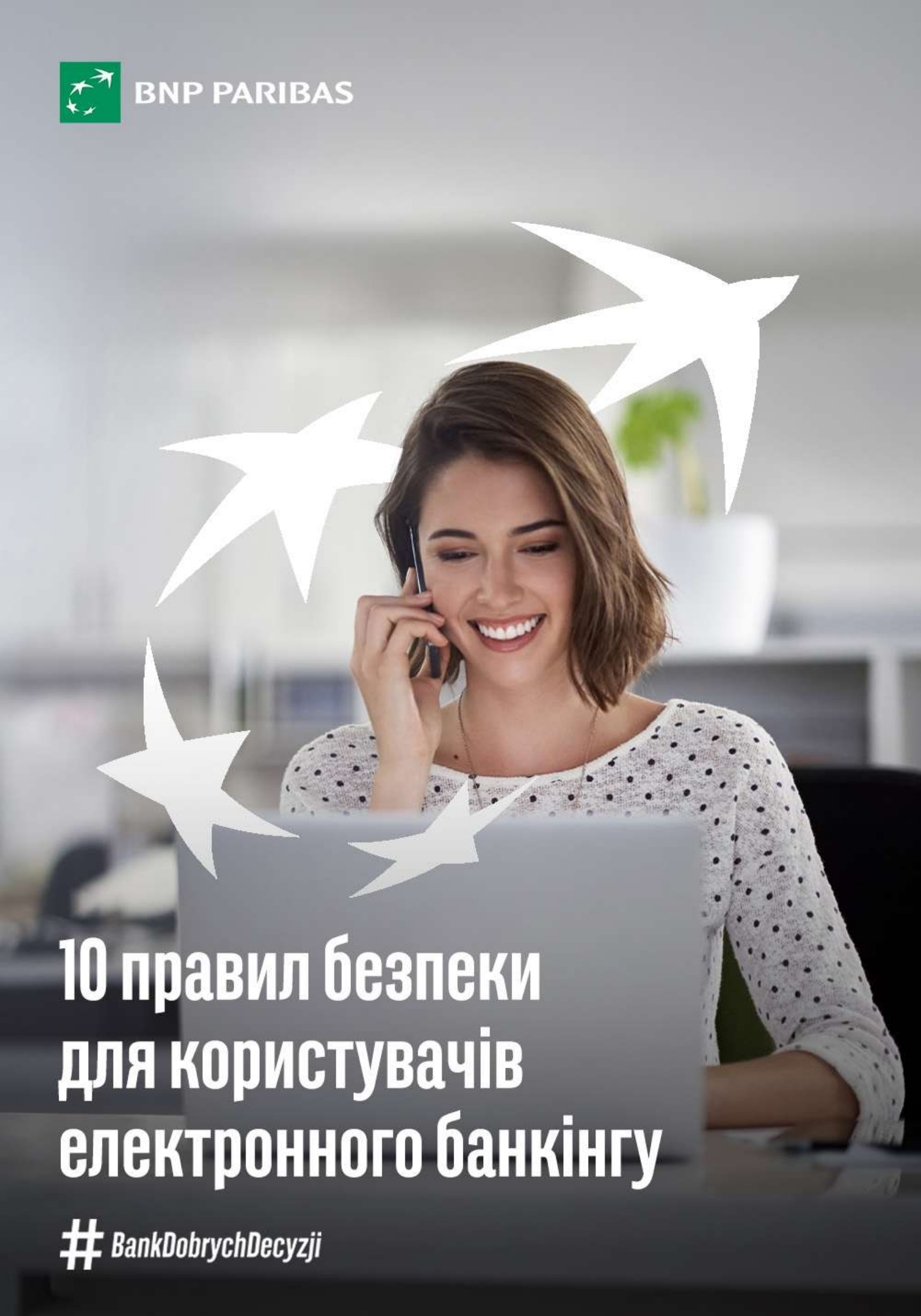
BNP PARIBAS



10 правил безпеки для користувачів електронного банкінгу

#BankDobrychDecyzji

10 ПРИНЦИПІВ БЕЗПЕЧНОГО ЕЛЕКТРОННОГО БАНКІНГУ

01 Перевіряйте адреси вебсайтів і шифрування з'єднання

Не використовуйте:

- посилання в електронних листах або текстових повідомленнях невідомого походження та посилання з неперевірених вебсайтів;
- функції браузера, такі як автозаповнення форм, запам'ятовування паролів і сеансів.

Перевіряйте:

- сертифікат перед кожною спробою входу в систему - це дозволить вам перевірити справжність сервера.

02 Читайте безпекові повідомлення

- Уважно читайте безпекові повідомлення на сторінці входу в систему, на екранах, які з'являються після входу, і в повідомленнях у вашій внутрішній пошті. Там ви знайдете інформацію про поточні загрози або можливі спроби атак, що базуються на соціальної інженерії.
- Повідомляйте про підозрілі текстові повідомлення на загальнонаціональний цілодобовий безкоштовний номер **CERT 8080** - це дозволить додати підозрілі номери до бази даних заблокованих номерів.

03 Захищайте приватні дані

Співробітники банку ніколи не просять:

- Ваш банківський логін або пароль, встановлення додаткового програмного забезпечення, отримання віддаленого доступу до комп'ютера або телефону, повний номер картки та CVV/CVC-код, введення BLIK-коду, здійснення переказу, поповнення або зняття грошей у банкоматі чи відділенні банку.
- Повідомляйте про такі випадки за номером, який працює в режимі 24/7: +48 22 548 29 40 (вартість дзвінка згідно з тарифом оператора).

04 Використовуйте поведінковий захист

- Це сучасна безкоштовна послуга, яка додатково підвищує безпеку коштів на вашому рахунку. Активація проста і може бути здійснена як в GOonline, так і в додатку GOmobile: *Налаштування особистого профілю --> Безпека --> Поведінковий захист --> Прийняти*

05 Дбайте про безпеку свого комп'ютера

- Використовуйте антивірусне або антишпигунське програмне забезпечення.
- Стежте за виправленнями та оновленнями, рекомендованими виробниками програмного забезпечення, включно з системним та безпековим програмним забезпеченням для вашого комп'ютера.
- Встановлюйте легальне програмне забезпечення з перевірених джерел.
- Не використовуйте публічні, відкриті мережі Wi-Fi. Уникайте входу в системи електронного банкінгу з загальнодоступних комп'ютерів, наприклад в аеропорту або в кафе.

06 Перевіряйте доручення, які подаєте, і застосовуйте ліміти

- Завжди перевіряйте, чи відповідає SMS-повідомлення з кодом авторизації транзакції, яку ви виконуєте (наприклад, чи збігаються дані з рахунку-фактури з номером рахунку / сумою операції).
- Під час авторизації за допомогою електронного підпису або токена не забувайте перевіряти деталі транзакції. Переконайтеся, що вони відповідають транзакції, яку ви проводите.
- Встановіть безпечні ліміти для щоденних транзакцій BLIK, платіжних карток, зняття готівки, переказів. У такому разі спроби підозрілих переказів на великі суми і зняття коштів не відбудуться.

07 Дбайте про безпеку паролів

- Надійний пароль містить щонайменше 15 символів, великі та малі літери, спеціальні символи (@#¶&!), а також цифри (1, 3, 7, 0). Це може бути еквівалент речення або речення.
- Пароль повинен бути відомий тільки користувачеві і зберігатися в надійному місці.
- Працівник банку ніколи не запитує логін чи пароль.
- Якщо ви входите в систему за допомогою прихованого пароля, пам'ятайте, що банку не потрібен ваш повний пароль, окрім операції зі зміни старого пароля на новий.
- Під час входу в систему вводьте лише вибрані символи з пароля.
- Якщо ви входите в систему за допомогою електронного підпису, нікому не передавайте криптографічний носій USB або криптографічну картку, на якій зберігаються ваші ключі та PIN-код до них.

08 Перевіряйте дані для входу

- Перевіряйте дати останнього входу до системи - як успішного, так і ні. Якщо ці дати не відповідають вашій активності, це повинно вас насторожити. Це може означати, що до вашого рахунку отримав доступ хтось інший.

09 Не ігноруйте системні сповіщення

- Налаштуйте автоматичне сповіщення електронною поштою або SMS-повідомленням про кожен успішний або неуспішний вхід, заблокований доступ до системи та списання коштів понад заявлену суму. Ці сповіщення допоможуть вам контролювати активність на вашому банківському рахунку.

10 Виходьте з системи

- Завжди виходьте з системи. Для цього натисніть на піктограму «Вихід» у верхньому правому куті. Не закривайте вікно браузера, не вийшовши з системи електронного банкінгу.

Більше інформації про безпеку - на нашому вебсайті
www.bnpparibas.pl/bezpieczenstwo