Правила безпеки в застосунку bank.kd

Оновлені стандарти безпеки для клієнтів АТ "БАНК КД".

1. Доступ та паролі

- **Налаштуйте біометрію.** Використовуйте FaceID або TouchID для входу в застосунок — це безпечніше та швидше за введення пароля вручну.
- **Створюйте надійні паролі.** Якщо використовуєте пароль, він має бути унікальним. Для безпечного зберігання використовуйте спеціальні програми — менеджери паролів (наприклад, Apple Keychain, Google Password Manager).
- **Блокуйте екран смартфона.** Встановіть PIN-код, графічний ключ або біометрію на розблокування самого телефону.

2. Захист від шахраїв (Соціальна інженерія)

- **Банк ніколи не просить паролі.** Ні в телефонній розмові, ні в SMS, ні в месенджерах ми не вимагаємо назвати ваш пароль від bank.kd, PIN-код картки або тризначний CVV-код.
- **Не переходьте за підозрілими посиланнями.** Якщо ви отримали повідомлення про "блокування рахунку" чи "виграш" із посиланням — ігноруйте його.
- **Уникайте публічного Wi-Fi.** Не проводьте фінансові операції через відкриті мережі в кафе чи метро без використання VPN.

3. Контроль та управління

- **Керуйте лімітами.** Встановіть у bank.kd обмеження на суму інтернет-покупок та зняття готівки. Збільшуйте їх лише за потреби.
- **Оновлюйте застосунок.** Завжди встановлюйте останні оновлення операційної системи вашого смартфона та застосунку bank.kd, щоб мати актуальний захист від вразливостей.

Що робити в разі небезпеки?

Якщо ви загубили телефон, помітили підозрілі транзакції або випадково передали свої дані третім особам:

1. **Заблокуйте свої картки в застосунку bank.kd**.
2. **Негайно зателефонуйте на гарячу лінію АТ «БАНК КД»:**

    • **0 800 501 808** (цілодобово, безкоштовно зі стаціонарних та мобільних телефонів у межах України)

    • **+38 044 593 10 20** (цілодобово, для дзвінків в межах України та міжнародних дзвінків згідно зі стандартними тарифами)

Правила безпеки при використанні платіжних карток

1. Захист даних картки (заборонено)

- **Нікому не повідомляйте:** ПІН-код, CVV-код (три цифри на звороті), одноразові коди з SMS або пароль до застосунку bank.kd. Співробітники банку ніколи не запитують ці дані.
- **Не зберігайте дані відкрито:** Не записуйте ПІН-код на картці або в нотатках телефону.
- **Не передавайте третім особам:** Навіть родичам чи друзям.

2. Безпека платежів

- **Керуйте лімітами:** Встановіть індивідуальні ліміти на інтернет-оплати в застосунку bank.kd.
- **Перевіряйте сайт:** Використовуйте лише перевірені інтернет-магазини. Не вводьте дані картки на сайтах, де пропонують "виплати", "допомогу" або занадто низькі ціни.

3. Дії при загрозах

Миттєве блокування: Якщо ви втратили картку, помітили підозрілу транзакцію або ввели дані на сумнівному сайті — негайно заблокуйте картку через застосунок або за телефонами:

- **0 800 501 808** (цілодобово безкоштовно зі стаціонарних та мобільних телефонів у межах України)
- **+38 044 593 10 20** (цілодобово для дзвінків в межах України та міжнародних дзвінків згідно стандартних тарифів)

4. Робота з банкоматами

- Якщо банкомат виглядає пошкодженим або має сторонні пристрої на клавіатурі/картоприймачі — не користуйтеся ним.
- Не приймайте допомогу від сторонніх осіб під час проведення операцій.

Обережно, фішинг: Як захистити свої гроші в інтернеті

Фішинг — це створення шахраями підроблених сайтів (магазинів, сервісів поповнення, банків), які виглядають як справжні, щоб вкрасти дані вашої картки.

Головне правило безпеки

АТ «БАНК КД» ніколи не телефонує та не пише клієнтам із проханням продиктувати або ввести на сайті:

- Пароль від застосунку bank.kd.
- PIN-код картки.
- CVV-код (три цифри на звороті).
- Одноразові коди з SMS.

Як розпізнати шахрайський сайт

1. **Звертайте увагу на посилання.** Шахраї змінюють 1-2 літери в назві відомих сайтів.
2. **Не переходьте за посиланнями з повідомлень.** Якщо вам надіслали SMS, повідомлення у Viber/Telegram або email із пропозицією отримати "виплату", "допомогу" або сповіщенням про "блокування рахунку" — це шахраї.
3. **Ігноруйте наднизькі ціни.** Сайти, що пропонують перекази з нульовою комісією або товари за нереалістично низькими цінами, створюються для збору карткових даних.

Що робити, якщо ви ввели дані на підозрілому сайті?

Шахраї списують кошти миттєво. Якщо ви зрозуміли, що передали дані картки або пароль стороннім:

4. **Негайно заблокуйте картку в застосунку bank.kd**.
5. **Зателефонуйте до служби підтримки АТ «БАНК КД» за номерами:**

    • **0 800 501 808** (цілодобово безкоштовно зі стаціонарних та мобільних телефонів у межах України)

    • **+38 044 593 10 20** (цілодобово для дзвінків в межах України та міжнародних дзвінків згідно стандартних тарифів)