



ПАМ'ЯТКА ПО БЕЗПЕЦІ

Звертаємо Вашу увагу на те, що на ринку банківських послуг почастишали випадки фішингу.*

АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ» (надалі – Банк) просить своїх клієнтів бути особливо уважними і пам'ятати, що:

- Банк НІКОЛИ не вимагає від своїх клієнтів повідомляти конфіденційну інформацію, таку як ПІН-код, CVV-код, паролі і ключі;
- дзвінки, листи або СМС-повідомлення з проханнями надіслати/повідомити Ваш номер карти, ПІН-код, пароль та іншу конфіденційну інформацію, навіть отриману з адреси, зовні схожої на офіційну адресу Банку, є спробою шахрайства і жодного відношення до АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ» не мають. Переконливе прохання — не відповідати на подібні запити!

АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ» наполегливо рекомендує Вам дотримуватися наступних правил безпеки, щоб захистити себе від шахрайства:

- ні за яких обставин не повідомляйте реквізити Вашої карти та іншу конфіденційну інформацію третім особам;
- перевіряйте операції у Виписці по картковому рахунку;
- при введенні інформації з карти для оплати в мережі Інтернет необхідно переконатися в тому, що використовується захищене SSL з'єднання (використання протоколу <https://>, дійсного сертифікату шифрування відкритого сайту). У більшості популярних інтернет-браузерів таке з'єднання візуально позначається зображенням замочка біля адресного поля, при натисканні на яке можна дізнатися деталі (тип з'єднання, шифрування, інформацію про сертифікат);
- не користуйтеся сторінками підозрілих і маловідомих компаній;
- для переходу за допомогою посилання, яке надійшло Вам електронним листом, самостійно введіть його в адресне поле браузера;
- використовуйте ліцензійне програмне забезпечення (Інтернет-браузер, операційну систему, антивірусне ПЗ тощо).

Якщо Ви підозрюєте, що стали жертвою фішингу:

- змініть паролі або ПІН-коди у всіх своїх онлайн-акаунтах, які могли бути скомпрометовані;
- зверніться безпосередньо до Банку або інтернет-магазину. Не переходьте за посиланням у фішинговому повідомленні;
- якщо Вам стало відомо про шахрайський доступ до рахунків, заблокуйте їх;
- активуйте послугу СМС-інформування («GSM-банкінг») для своїх карткових рахунків.

При виникненні будь-яких запитань або підозр негайно телефонуйте фахівцям цілодобового Контакт-центру за телефоном: 0 800 210 804 (безкоштовно з усіх телефонів по Україні).

За будь-якої підозри щодо несанкціонованого доступ або зміну клієнтської інформації в системі дистанційного обслуговування – терміново повідомте про це Контакт-центр Банку для блокування облікового запису у відповідній системі дистанційного обслуговування для попередження можливих фінансових втрат.

**Фішинг (англ. phishing, від fishing — рибалка, вивуджування) – це вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів — номерів карт, CVV-коду (3 цифри на зворотному боці карти), ПІН-коду, логінів і паролів за допомогою шахрайських запитів електронною поштою, телефонних дзвінків, розсилки фальшивих СМС-повідомлень нібито від імені Банку.*