

1. ДІЇ ПРИ ВТРАТІ, КРАДІЖЦІ АБО КОМПРОМЕТАЦІЇ КАРТКИ (КОЛИ ДАНІ КАРТКИ СТАЛИ ВІДОМІ ТРЕТІМ ОСОБАМ)

- У випадку втрати, крадіжки або компрометації картки необхідно негайно зателефонувати до Клієнтської підтримки Банку за телефонами **+38(044) 290-93-10** (для дзвінків з-за кордону. Вартість дзвінків згідно з тарифами Вашого оператора) та/або **0 800 505 555** (для безкоштовних дзвінків у межах України) для блокування картки.

Рекомендуємо внести вищезазначені номери телефонів у телефонний довідник, щоб номер телефону Контакт-Центру (клієнтської підтримки) завжди був у Вас під рукою.

- Для випуску нової картки необхідно звернутись до найближчого **відділення** АТ «ЄПБ».

Нагадуємо!

До моменту блокування картки Ви несете повну фінансову відповідальність по всіх операціях, здійснених із використанням втраченої, викраденої або скомпрометованої картки.

2. УНИКНЕННЯ ВИПАДКІВ ПІДВИЩЕНОГО РИЗИКУ ЗБИТКІВ ДЛЯ КОРИСТУВАЧА ЕЛЕКТРОННОГО ПЛАТІЖНОГО ЗАСОБУ.

Персональний ідентифікаційний номер (ПІН-код) – це чотиризначний код, який шляхом SMS Банк надсилає на зазначений номер фінансового телефону власнику платіжної картки.

Банк рекомендує:

- Якщо ПІН-код не зручний для запам'ятовування, змініть його в банкоматі АТ «ЄПБ»;
- Ніколи не записуйте свій ПІН – запам'ятайте його. Ні в якому разі не записуйте ПІН-код на самій картці, а також не зберігайте платіжну картку та ПІН-код разом;
- Нікому не передавайте картку та не розголошуйте ПІН-код (в т.ч. родичам, співробітникам банків та правоохоронних органів, касирам підприємств торгівлі та сервісу) – це гарантія безпеки Ваших коштів;
- Якщо Ви хочете надати комусь із Ваших близьких доступ до свого поточного рахунку, замовте додаткову картку на його/її ім'я.

3. ФІШИНГОВІ ВЕБСАЙТИ.

Фішинговий сайт — це шахрайський веб ресурс, який виманює реквізити платіжних карток під виглядом надання послуг, що не існують (наприклад, поповнення мобільного рахунку, переказів з картки на картку), або веб-ресурс організації, якій користувач довіряє (наприклад, клон знаменитих надавачів платіжних послуг), що має на меті збір реквізитів платіжних карток для подальшої крадіжки грошових коштів з рахунків держателів платіжних карток. Усі фішингові сайти надають неіснуючі послуги з поповнення мобільного рахунку та переказу коштів з картки на картку.

З більш розширеною та детальною інформацією про фішинг можна ознайомитись на офіційному вебсайті провідного розробника програмних продуктів для захисту від зловмисного коду – компанії ESET: https://eset.ua/ua/support/entsiklopediya_ugroz/fishing

Для боротьби з фішингом Українська міжбанківська асоціація членів платіжних систем ЕМА, яка за підтримки Державного департаменту США реалізує в Україні Національну програму сприяння безпеці електронних платежів і карткових розрахунків SafeCard, створила та регулярно оновлює список виявлених фішингових сайтів. Ознайомитися з переліком сайтів, які становлять небезпеку, може кожен інтернет-користувач на офіційному ресурсі ЕМА.

- «Чорний список сайтів»: <https://www.ema.com.ua/citizens/blacklist/>;
- перевірені платіжні сервіси: <https://www.ema.com.ua/citizens/whitelist/>;
- посилання на офіційні сторінки учасників Української міжбанківської асоціації членів платіжних систем ЕМА (банки, платіжні системи): <https://www.ema.com.ua/about/members/>

Для унеможливлення потрапляння клієнтів банків на фішингові вебсайти Національний банк України на своєму офіційному Інтернет-представництві розмістив перевірений перелік вебсайтів банків України з яким можливо ознайомитися за посиланням: <https://bank.gov.ua/ua/supervision/institutions>

Банк рекомендує

щодо використання платіжної картки для оплати товарів та послуг у мережі Інтернет

- Відкрийте окрему картку для оплати товарів та послуг у мережі Інтернет та зараховуйте на неї необхідні кошти безпосередньо перед здійсненням платіжної операції;
- Здійснюйте покупки на сайтах, у надійності яких Ви впевнені. Для перевірки репутації вебсайту зверніть увагу на наявність наступної інформації:
 - ✓ правила захисту конфіденційної інформації – веб-сайт, що заслуговує на довіру, завжди розміщує інформацію про правила, які гарантують клієнтам захист персональних даних при здійсненні on-line операцій;
 - ✓ інформація про замовлення – переконайтесь, що Вам відомо всю інформацію про здійснене замовлення, у тому числі дату доставки, гарантійні зобов'язання та правила відмови від товару;
 - ✓ інформація про магазин – переконайтесь, що Вам відома поштова адреса фірми та номери її телефонів.
- Не використовуйте картку на сайтах без кодування даних. Адреса сайту повинна починатися з «**https**», а не з «**http**»;
- Не слід вводити дані ПК на веб-сайтах, які пропонують участь у різноманітних акціях з подальшою виплатою нагороди на ПК, так як більшість з них створені для незаконного збору інформації та подальшого шахрайського використання;
- Ні в якому разі не використовуйте ПІН-код при здійсненні операцій у мережі Інтернет;

- У разі необхідності зміни добових лімітів по сумі і по кількості операцій - держателю платіжної картки необхідно звернутися до Клієнтської підтримки Банку за телефоном **+38(044) 290-93-10** (для дзвінків з-за кордону. Вартість дзвінків згідно тарифів Вашого оператора) та/або **0 800 505 555** (для безкоштовних дзвінків у межах України).