**Безпечне користування карткою, в т.ч. рекомендації щодо уникнення випадків підвищеного ризику збитків**

Фішинг – це поширений вид інтернет-шахрайства, мета якого - під різними приводами отримати у довірливих користувачів мережі конфіденційні персональні дані (логіни, паролі в інтернет-банкінг, повні реквізити платіжних карток, тощо).

Шахраї створюють сайти-клони, які дуже схожі або повністю копіюють [дизайн](https://uk.wikipedia.org/wiki/%D0%94%D0%B8%D0%B7%D0%B0%D0%B9%D0%BD) відомих ресурсів, наприклад, для грошових переказів, поповнення мобільного телефону, тощо. На таких сайтах злочинці пропонують послуги з більш привабливими умовами. Всі фішингові сайти надають неіснуючі послуги, вони створюються лише з метою збору конфіденційної інформації, яку шахраї використовують в своїх цілях.

Завжди звертайте увагу на адресу інтернет-сайту, на якому Ви бажаєте розрахуватися карткою, вона  повинна  починатися з https:// та містити значок замочка "https://bank.gov.ua/admin_uploads/article/Lock.jpg".

Для максимальної безпеки при розрахунках в мережі Інтернет відкрийте окремий рахунок ( Інтернет-картку ), на який зараховуйте кошти безпосередньо перед здійсненням платіжної операції та в розмірі, необхідному для здійснення розрахунку.

Нікому не повідомляйте реквізити картки (трьохзначний номер на звороті картки, термін дії картки, PIN-код до платіжної картки, ім’я та прізвище власника ).

Для оперативного контролю за коштами на Вашому рахунку замовте послугу SMS-банкінгу.

Купуйте онлайн або сплачуйте за сервіси тільки на перевірених сайтах.

Останнім часом почастішали випадки телефонного шахрайства. Зловмисники постійно придумують нові схеми обману. Аферисти представляються працівниками банків, загрожують блокуванням карт або ж розповідають про неіснуючі борги, за які на вас можуть подати в суд. Ніколи не слід піддаватися паніці і перераховувати кудись гроші , адже всі схеми базуються на простому психологічному тиску.

Не надавайте персональну інформацію та/або реквізити Вашої картки у відповідь на будь-які електронні листи. Ні в якому разі НЕ переходьте на запропоновані у цих листах Інтернет-адреси.

**Важливо!**

Національний банк України ніколи та за жодних обставин не телефонує клієнтам банків.

Працівники банків не запитують:

* PIN-код до платіжної картки;
* трьохзначний номер на звороті картки;
* коди підтверджень платежів;
* термін дії картки;
* паролі до Інтернет-банкінгу.

Перелік сайтів, які становлять небезпеку, можна перевірити на офіційному ресурсі ЕМА в розділі «**Чорний список сайтів**»:  
<https://www.ema.com.ua/citizens/blacklist/>

**Довідник банків**

<https://bank.gov.ua/supervision/institutions>

За будь-якої підозри, що дані Вашої платіжної картки стали відомі стороннім особам – терміново сповістіть про це Контакт-центр Банку та заблокуйте картку для попередження можливих фінансових втрат.

**Телефонуйте до Контакт-Центру 0-800-30-45-45 (безкоштовно зі стаціонарних та мобільних телефонів України).**