

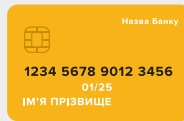


## Тримайте в секреті!

Тризначний  
номер на звороті  
картки

Пароль  
до інтернет-  
банкінгу

Коди банків  
та мобільних  
операторів

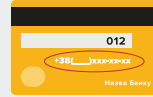


Можна  
повідомити лише  
**16-значний номер**  
картки!

## Телефонують зі служби безпеки банку?

**Радять переказати гроші  
на "безпечний рахунок" або прив'язати  
картку до іншого телефонного номера  
через кібератаку?**

Це шахраї!  
Припиніть розмову та зателефонуйте  
до банку за номером, що вказаний  
на звороті картки



## Шахраї пропонують соцвиплати від імені держави, міжнародних організацій, банків та благодійних фондів

**Створюють шахрайські сайти,  
схожі на справжні**

Отримуйте інформацію  
про соцвиплати лише  
на офіційних сайтах.  
Не переходьте за посиланнями  
з sms та месенджерів



## Просять ввести логін та пароль до особистих сторінок у соціальних мережах?

**Налаштуйте двофакторну  
автентифікацію  
всюди, де це можливо**

Можливо, це шахраї  
намагаються отримати доступ  
до вашого акаунту



## Роботизоване голосове меню просить повідомити:

**смс-код від банку, три цифри на звороті картки, логін та пароль від інтернет-банкінгу?**

Припиніть розмову, це витівки шахраїв!



## Купуйте та платіть на безпечних сайтах!

**Перевіряйте правильність назви сайтів, на які переходите та де вводите свої персональні дані**

Адреси справжнього та шахрайського сайту можуть бути схожі, за винятком одного чи кількох символів



## Дзвінки та sms-повідомлення від шахраїв можуть виглядати, наче від справжнього банку

**Шахраї підмінюють номер телефону та імітують дзвінки, sms-повідомлення від банків**

Це прийом аферистів, щоб виманити конфіденційну інформацію та отримати доступ до рахунків



## Автомобілі, дрони, військова техніка та амуніція

**Такі товари шахраї "продають" онлайн. Отримують передоплату, а потім зникають!**

Обирайте лише перевірені ресурси для онлайн-покупок, надавайте перевагу післяплаті за послуги

