

Інформаційні матеріали до Дня безпечного інтернету

 беремо
і навчаємо



Лютий 2026

Що таке фрод і чому це стосується тебе?



Шахрайство (або **фрод**) в інтернеті - це будь-яка спроба виманити ваші гроші, паролі або особисті дані через мережу.

Чому ти в зоні ризику?



- Ти часто купуєш ігри, скіни або підписки.
- Ти активно користуєшся соцмережами.
- Ти шукаєш способи заробити перші гроші онлайн.

Анатомія банківської картки

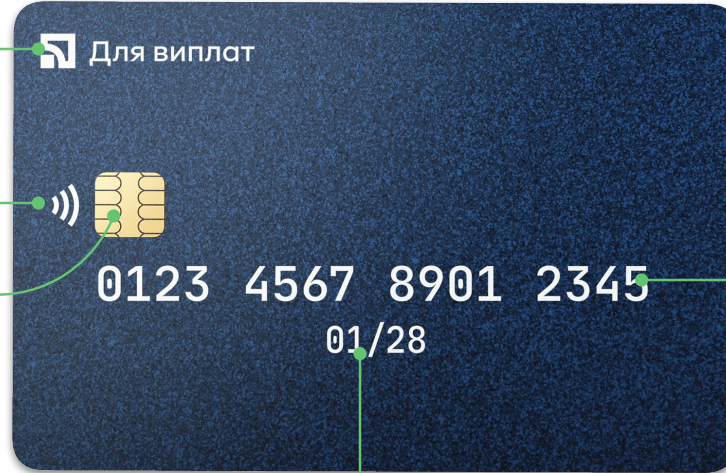
Лицьова сторона

Найменування/лого
банку чи іншого емітента

Для виплат

**Знак безконтактної
оплати**

Контактний чип -
вбудований мікропроцесор,
що є носієм платіжних даних
і в зашифрованому вигляді
значно підвищує безпеку
здійснення платіжних
операцій.



Номер картки - складаються з 16 цифр (4 групи по 4 цифри). Комбінація з перших шести - вказує на платіжну систему та емітента картки. Перша цифра - вказівка на платіжну систему. Наприклад, номер платіжної картки починається з 4 - Visa, 5 - MasterCard. Решта п'ять цифр позначають емітента, що випустив вашу платіжну картку.

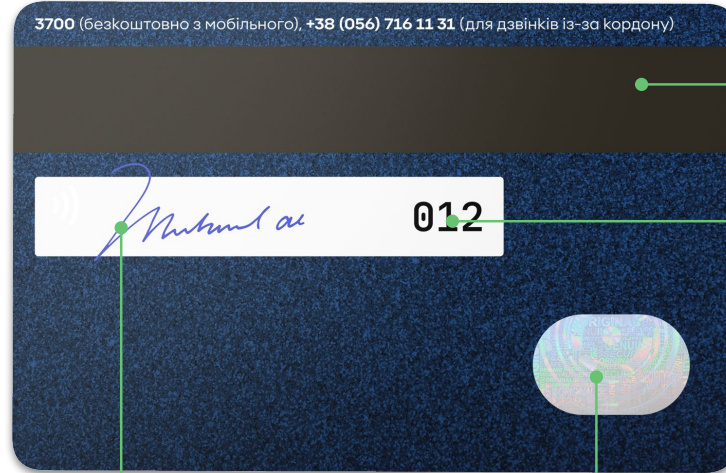
Термін дії платіжної картки. Платіжна картка має термін дії, але рахунок, до якого вона випущена, – безтерміновий. У разі завершення терміну дії платіжної картки емітент може здійснити її перевипуск, випустити нову платіжну картку до рахунку або продовжити термін дії платіжної картки.

Анатомія банківської картки

Зворотня сторона

Контакти банку

Адреса й телефон банку, за яким ви можете в будь-який час зв'язатися з банком, щоб отримати кваліфіковану допомогу.



Магнітна стрічка

Зберігає в зашифрованому вигляді ключ доступу до вашого рахунку.

CVV-код

Номер із трьох цифр у верхній правій частині смуги для підпису.

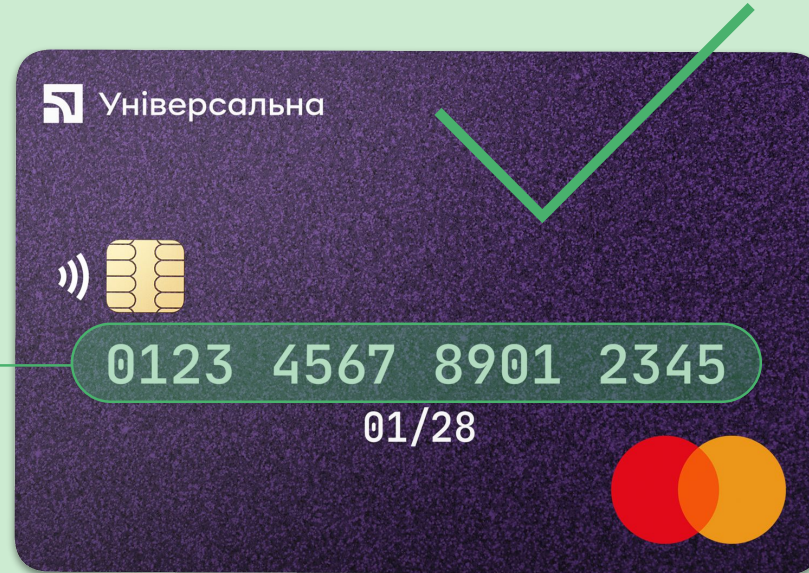
Місце для підпису

Підпис власника, щоб ніхто не міг скористатися карткою.

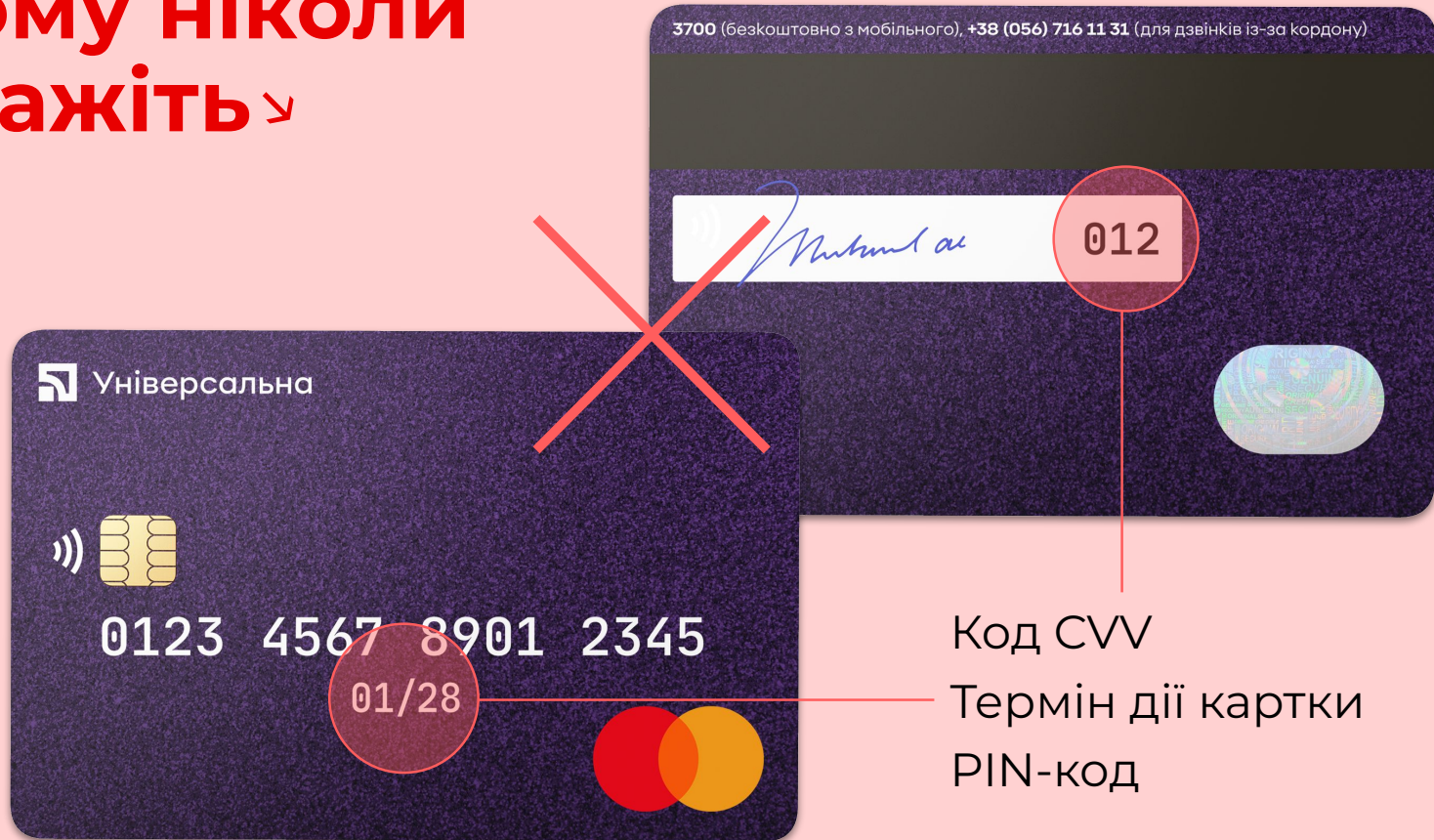
Захист - захисна голограма й логотип гарантують, що ви тримаєте в руках справжню картку.

Можна повідомляти ➤

16-ти значний
номер карти



Нікому ніколи не кажіть ↘





Фішинг («Перейди за посиланням»)

ДІІ ШАХРАЯ

- «Для оформлення безпечної доставки ОЛХ, **перейди за посиланням**»
- «Отримай виплату від держави/ООН»
- «Твій аккаунт буде заблоковано, **підтвердьте дані**»

Ви переходите за посиланням на сайт, який один-в-один схожий на Instagram, OLX або банк, і вводите там свої дані. Отримуючи доступ до ваших даних, шахраї мають доступ до ваших коштів

ЯК ЗАХИСТИТИСЯ

- ➔ Дивись на адресу сайту: Шахраї змінюють назву сайту, часто це може бути навіть одна або декілька літер (наприклад, **olx.ua** перетворюється на **olx-dostavka.net**).
- ➔ Користуйся офіційними застосунками: Не вводь дані картки на сторонніх сайтах, на які ви переходите з повідомлення.





АГЕНТ 3700

Ввести пароль Privat24?



Миттева грошова
винагорода!



Дзвінок з банку

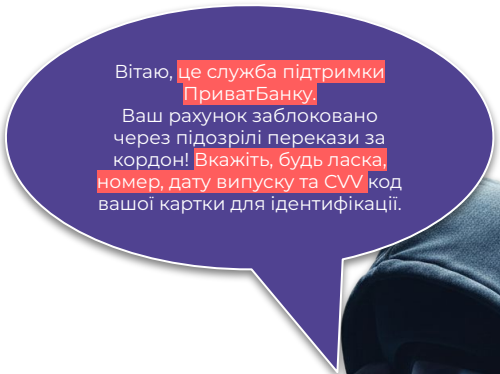
(«Алло, це безпека банку!»)

ДІЇ ШАХРАЯ

- каже, що з картки прямо зараз намагаються списати гроші, або хтось намагається змінити номер телефону. Щоб «зупинити операцію», просять назвати код із SMS або CVV-код;
- повідомляє, що картка заблокована, пропонує переказати кошти на іншу картку;
- пропонує продовжити дію кредитної картки або підвищити кредитний ліміт на ній;
- повідомляє, що у зв'язку з військовими діями потрібно оновити чи підтвердити ваші дані, бо картки будуть заблоковані

ЯК ЗАХИСТИТИСЯ

- Справжній банк ніколи не питає коди з SMS, паролі до застосунку або CVV.
- Якщо виникають сумніви - поклади слухавку і сам перетелефонуй за офіційним номером банку, який вказаний на твоїй картці.
- Нікому не вір на слово, навіть якщо на екрані висвічується назва банку (номери можна підмінити)



Вітаю, це служба підтримки ПриватБанку.
Ваш рахунок заблоковано через підозрілі перекази за кордон! Вкажіть, будь ласка, номер, дату випуску та CVV код вашої картки для ідентифікації.





«Дзвінок з банку в месенджер»

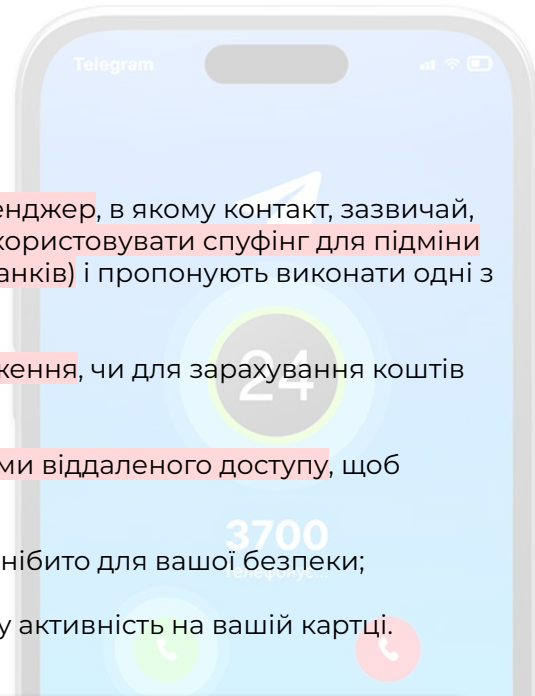
ДІЇ ШАХРАЯ

Шахраї телефонують клієнту через месенджер, в якому контакт, зазвичай, підписаний як ПриватБанк, (можуть використовувати спуфінг для підміни номера телефону та імітувати SMS від банків) і пропонують виконати одні з перелічених дій:

- провести транзакції для ніби збереження, чи для зарахування коштів на інші карткові рахунки;
- встановити на ваш пристрій програми віддаленого доступу, щоб отримати доступ до ваших даних;
- перевести кошти на інший рахунок, нібито для вашої безпеки;
- заблокувати рахунок через підозрілу активність на вашій картці.

ЯК ЗАХИСТИТИСЯ

- Банк ніколи не телефонує клієнтам через месенджер! Перевірити дзвінок від банку можна у Приват24. Завжди будьте на зв'язку зі своїм банком!





Злом соцмереж

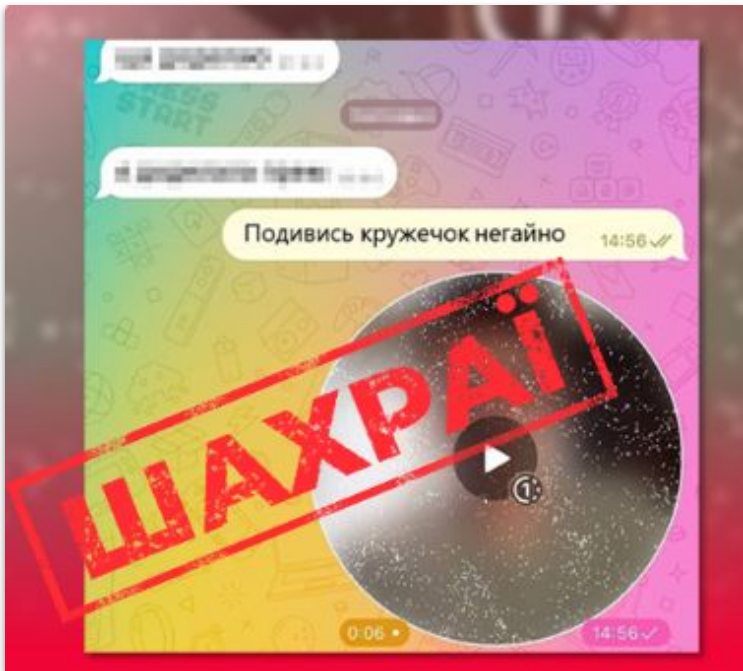
(«Друже, позич до вечора»)

ДІЇ ШАХРАЯ

- «Привіт! Виручи, будь ласка, терміново треба 500 грн на ліки/інтернет, скину завтра».
- «Проголосуй за мене в конкурсі». Після кліку твій аккаунт теж зламують, і від твого імені починають розсилати такі ж прохання.
- За допомогою використання технології Deepfake, записує голосове, або відео повідомлення.

ЯК ЗАХИСТИТИСЯ

- Подзвоніть другу: Найшвидший спосіб перевірити - просто набрати його номер.
- Контрольне запитання: Запитайте друга про те, що знаєте тільки ви двоє (наприклад: «Як звали нашого вчителя в 1 класі?»).
- Двофакторка - це мастхев: Увімкніть двоетапну перевірку в налаштуваннях (код на пошту або в застосунок-автентифікатор).





Фейковий заробіток

(«Робота для підлітків 2000 грн/день»)

ДІЇ ШАХРАЯ

За обіцяну винагороду слід поставити 5-6 лайків, написати кілька коментарів, чи здійснити бронювання готелів за свої кошти, які шахраї обіцяють повернути разом із винагородою.

Спочатку шахраї виплачують незначні суми від 100 до 500 гривень, щоб увійти в довіру.

Далі - суми вкладів збільшуються, а «роботодавці» перестають виходити на зв'язок.



ЯК ЗАХИСТИТИСЯ

- Головне правило: Робота - це коли гроші **платять ТОБІ**, а не коли **ТИ платиш** за можливість працювати.
- Перевіряйте роботодавця: Якщо в компанії **немає сайту, офісу**, а все спілкування йде тільки в анонімному чаті - **це шахрайство**.



Оренда картки або акаунту («Стань нашим партнером: 1000 грн за доступ до твого банку») ДІЇ ШАХРАЯ

Вам пропонують легкі гроші (наприклад, 500–1000 грн) просто за те, що ви дозволите покористуватися своєю картою або доступом до банківського додатка.

ЧОМУ ЦЕ НЕБЕЗПЕЧНО:

- **Ви стаєте співучасником:** Через вашу карту можуть відмивати гроші, вкрадені у пенсіонерів або отримані від продажу заборонених речовин.
- **Блокування назавжди:** Банки можуть розірвати з вами відносини, і ви більше ніколи не зможете відкрити рахунок, щоб отримувати заробітну плату чи взяти кредит у майбутньому.
- **Кримінальна відповідальність:** За отримання незаконних коштів передбачена кримінальна відповідальність

ЯК ЗАХИСТИТИСЯ

Ваша картка - це як ваш паспорт.
Нікому не передавайте її в руки та не давайте паролі від застосунку.
Легких грошей за «оренду картки» не існує без криміналу.

беремо
і робимо

гроші

рахунок

фінанси

безпеку платежів

кіднотвдіальність

фінансова безпека

Не ставай дропом





Схема («Встановіть застосунок»)

ДІЇ ШАХРАЯ

- Створюють фейкові мобільні застосунки для «зарахування допомоги» чи «отримання коштів» за товар, в які ви самі вводите реквізити платіжної картки.
- Пропонують встановити застосунки, що завантажують віруси, які отримують доступ до онлайн-банкінгу або криптогаманця.
- Видають себе за співробітників банку та змушують клієнтів встановлювати підроблений застосунок, отримуючи доступ до особистих даних і коштів.

ЯК ЗАХИСТИТИСЯ

Завантажуйте файли лише з офіційних або довірених джерел:

- для Android - з Google Play,
- для Apple - з App Store.

Перевіряйте смартфони на віруси.





Продаж неіснуючих товарів

(«Останні кросівки зі знижкою 70%, тільки повна передплата»)

ДІЇ ШАХРАЯ

Магазини з крутими фото та низькими цінами.

Після того, як ви скидаєте гроші на карту, продавець зникає та блокує вас.

ЯК ЗАХИСТИТИСЯ

Використовуй накладений платіж (оплата при отриманні).

Перевіряй дату створення сторінки та відгуки щодо продавця на незалежних ресурсах.



Фіктивні виграші

(«Вітаємо! Ви стали переможцем Giveaway, сплатіть лише доставку»)

ДІЇ ШАХРАЯ

- Надсилає повідомлення про **виграш у конкурсі**, в якому ви не брали участь.
- Підкидає повідомлення у соцмережах на сайт, де ви бачите свій номер мобільного серед «переможців».
- Телефоную та повідомляє, що **для отримання призу необхідно оплатити** «мито» або «кур'єра».

ЯК ЗАХИСТИТИСЯ

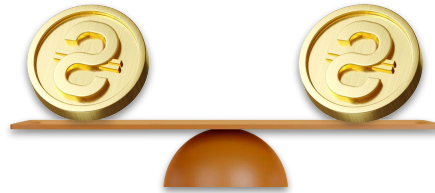
- Безкоштовний приз не потребує попередніх оплат.
- Якщо просять гроші за «активацію виграшу» - видаляйте повідомлення.

Поради з безпечних онлайн-покупок



КРАЩЕ ВІРТУАЛЬНО

Користуйтеся
віртуальною картою
для покупок онлайн



ТІЛЬКИ ПОТРІБНА СУМА

Перераховуйте
на віртуальну картку тільки
ту суму, яка необхідна
для покупки



ТРИМАЙТЕ В СЕКРЕТІ

Тризначний номер на
звороті картки - CVV-код.

Коди банків та
мобільних операторів.

Паролі до інтернет-
банкінгу

Захист від шахрайства: перевірка та запобігання



ЯК ПЕРЕВІРИТИ ЧИ ТЕЛЕФОНУВАВ БАНК

У застосунку Приват24 натисніть на значок чоловічка у правому верхньому куті, далі виберіть меню «Комунікації» → «Дзвінки» → «Перевірити номер телефону».

ПЕРЕВІРЕНА ІНФОРМАЦІЯ

Черпайте інформацію лише з перевірених джерел!

Як працює банк в умовах воєнного стану:

privatbank.ua/help.

Новини ПриватБанку:

privatbank.ua/news.

ТРИМАЙТЕ ЗВ'ЯЗОК

Завжди будьте на зв'язку з банком - тут завжди допоможуть порадою та дією.

Захистіть свій телефон!



ФІНАНСОВИЙ ТЕЛЕФОН

Не використовуйте його у соцмережах, в оголошеннях тощо.

ФІНАНСОВИЙ НОМЕР

Ідентифікуйте його у свого мобільного оператора та відключіть можливість віддаленого перевипуску SIM-картки.

ЯКЩО ВИ БАЧИТЕ ОЗНАКИ ЗМІНИ SIM-КАРТКИ

- Негайно зверніться до мобільного оператора, щоб зупинити перевипуск та повернути номер.
- Зверніться до банку, щоб заблокувати картки, рахунки та доступ до Інтернет-банку.

ПАРОЛЬ НА ВХІД ДО ТЕЛЕФОНУ

Встановіть пароль або ПІН-код, або відбиток пальця, чи розблокування за обличчям. Використовуйте будь-який метод блокування екрану!

SMS-ПАРОЛІ

Ніколи, нікому не повідомляйте SMS-паролі від мобільного оператора.

Остерігайтеся **шахраїв!**

Пам'ятайте: шахраї не вигадують нічого нового.
Вони використовують однакові емоційні
«відмички» до людського мозку та прогалини
у фінансовій грамотності



ДОВІРА



СТРАХ



ПОСПІХ

НОРМ



чи

СТРЬОМ



1. Ваш знайомий просить в інстаграм позичити 500 гривень до вечора. Переслати кошти, не позвонивши клієнту. **СТРЬОМ** 
2. Подруга просить проголосувати за неї в конкурсі. Перейти за посиланням та ввести персональні для авторизації. **СТРЬОМ** 
3. Встановити індивідуальні ліміти на операції з платіжною картою **НОРМ** 
4. Вам телефонує співробітник банку, і просить назвати пін код картки **СТРЬОМ** 
5. Знайомий пропонує заробити 1000 гривень за передачу йому картки в оренду. **СТРЬОМ** 
6. Ви продаєте товар на OLX і покупець просить перейти для спілкування в месенджер. **СТРЬОМ** 
7. Увімкни в усіх соцмережах та пошті двофакторну аутентифікацію **НОРМ** 

Що робити, якщо ви все ж стали жертвою шахрайства?

Не панікуйте і не соромтесь. Навіть досвідчені дорослі іноді потрапляють у пастки.



1. **Негайно заблокуйте картку.** Зробити це можна **через застосунок банку або зателефонувати на гарячу лінію** (номер завжди є на зворотній стороні картки).
2. **Повідомте батьків.** Вони **допоможуть** юридично та **підтримають**.
3. **Змініть паролі.** Якщо ви вводили дані на фейковому сайті, **терміново міняйте паролі на пошті та в соцмережах**.
4. **Зверніться до Кіберполіції.** Напишіть заяву на сайті cyberpolice.gov.ua. Це допоможе заблокувати рахунки злочинців.



**Є питання? -
запитуйте,
будь ласка!**

