# [Продаж товару в Інтернеті](https://stopfraud.gov.ua/cybersecurity-in-life/fishyngovi-qr-kody-v-gromadskyh-mistsyah-kiberpolitsiya-zasterigaye-vid-shahrayiv-i1126)

*Купив собі новий телефон, попередній виставив на продаж на одній із дошок оголошень. Мені телефонує покупець, просить реквізити для оплати та каже що зробить повну оплату наперед що б уникнути комісії накладеного платежу при доставці Новою поштою. Одразу ж мені телефонує невідомий номер, представляється працівником банку і намагається вивідати у мене платіжну інформацію по моїй картці під приводом зарахування мені коштів від юридичної особи. Після чого з моєї картки списалися всі кошти.*



Псевдопокупець може запитати реквізити картки для оплати за ваш товар на дошці оголошень і назвати час здійснення переказу або щось подібне.

У цей час напарник зловмисника під виглядом працівника служби безпеки банку може зателефонувати вам і сказати, що для зарахування грошей необхідно вчинити якусь дію, наприклад "активувати платіжну картку".

Таким чином шахраї будуть намагатися вивідати у вас реквізити та інші дані по вашому рахунку.

Пам’ятайте:

❌ Не повідомляйте стороннім особам інформацію по картці або дані, що можуть бути використані для підтвердження платежів.

❌ Не виконуйте жодних операцій з "верифікації" карти.

✅ У разі сумнівів – телефонуйте до банку за телефоном, вказаним на звороті картки та уточніть інформацію.

✅ Безпека збереження коштів та користування рахунками починається з Вас.

*На замітку:*

* *Твоя безпека — твої секрети. Не розголошуй дані!*
* *Служба банку не питає паролів та кодів!*
* *Телефонний "покупець"? Можливо, це шахрай!*
* *Ніколи не активуй фейкові платежі!*
* *Шахраї працюють у парі — будь напоготові!*