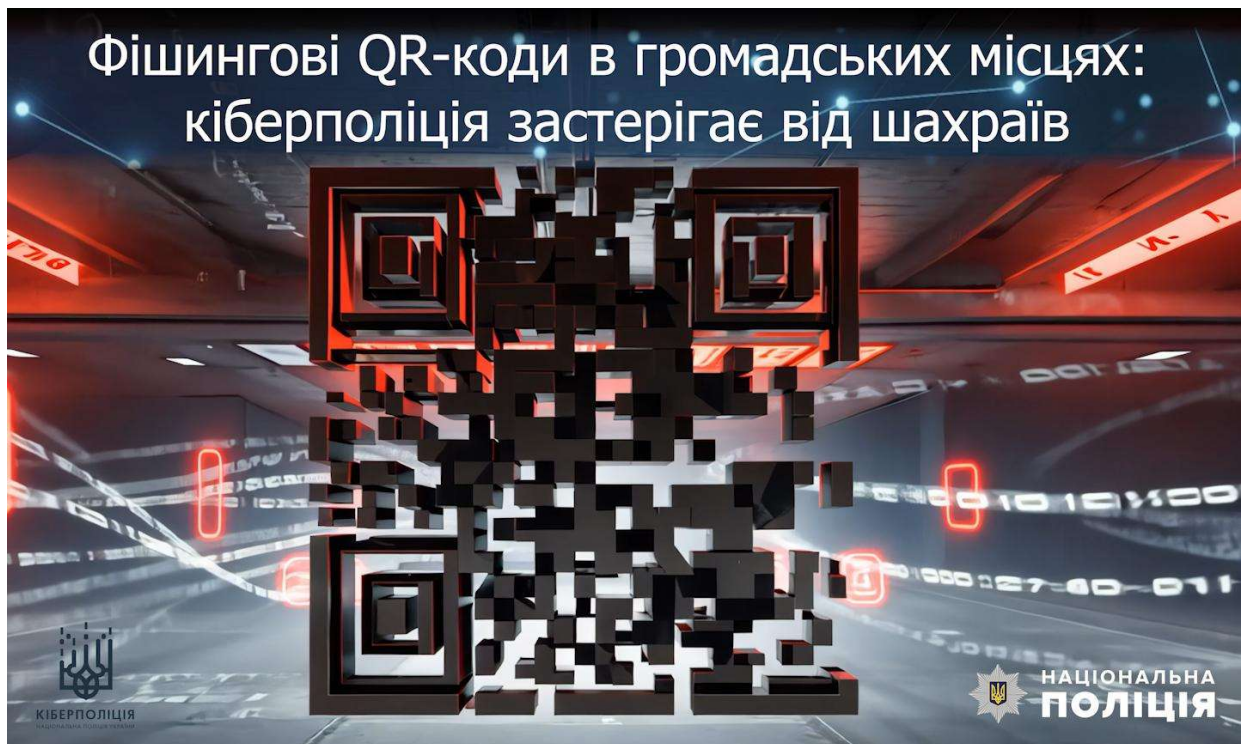


Фішингові QR-коди в громадських місцях: кіберполіція застерігає від шахраїв

В Україні знову активізувалася шахрайська схема, пов'язана з підміною QR-кодів у загальнодоступних місцях. Зловмисники використовують фішингові сайти, щоб отримати дані банківських карт громадян.



Шахраї підмінюють QR-коди на офіційних інформаційних табличках або просто розміщують їх в громадських місцях. Скануючи такі коди, користувачі потрапляють на підроблені сайти, що імітують реальні онлайн-сервіси. У результаті зловмисники можуть отримати доступ до банківських даних і викрасти кошти.



Найчастіше такі випадки трапляються у місцях, де люди активно використовують QR-коди для швидких оплат: під час паркування, оплати громадського транспорту, входу на заходи чи здійснення благодійних внесків.

Візуально відрізнити якісно підроблений код від справжнього дуже складно, тому головна порада – завжди перевіряти адресу сайту перед введенням будь-яких конфіденційних даних.

Щоб уберегтися від шахраїв, варто дотримуватися кількох правил:

- скануйте QR-коди лише з надійних джерел – уникайте кодів, розміщених на випадкових наклейках, листівках або рекламних оголошеннях.
- перед скануванням перевіряйте наклейку – звертайте увагу на можливі сліди підробки (додатковий шар, нерівні краї, інший шрифт).
- використовуйте функцію попереднього перегляду посилання – більшість смартфонів дозволяють побачити URL перед переходом.
- завжди звертайте увагу на веб-адресу після переходу за QR-кодом – навіть якщо сайт виглядає переконливо, будь-які відмінності в домені можуть бути ознакою шахрайства.
- Перевіряйте наявність захищеного з'єднання (<https://>) – якщо сайт не має сертифіката безпеки, вводити на ньому будь-яку інформацію небезпечно.
- Не вводьте банківські дані на невідомих сайтах та без необхідності.
- Якщо ви виявили підозрілий QR-код – повідомте адміністрацію закладу, службу підтримки або правоохоронні органи.
- Використовуйте віртуальні або тимчасові картки для онлайн-платежів – це

допоможе уникнути значних фінансових втрат у разі витоку фінансових даних картки.

Якщо ви стали жертвою шахрайства - негайно зверніться до банку для блокування картки та подайте електронне звернення до кіберполіції за посиланням <https://ticket.cyberpolice.gov.ua>.