СЦЕНАРІЇ ШАХРАЙСТВ

№1 «Не розголошуй SMS-код мобільного оператора»

Фінансовий номер телефону – це номер мобільного, який прив'язаний до банківських рахунків. А отже це гарна нажива для шахраїв.

Як шахраї можуть вкрасти фінансовий номер?

Жертві телефонує шахрай під маскою працівника мобільного оператора. Пропонує перейти на нові поліпшені стандарти зв'язку. Для підтвердження потрібно лише назвати код з SMS.

Що ж це за код?

Насправді, це пароль для входу в персональний кабінет жертви на сайті мобільного оператора. Шахрай швиденько здійснює віддалений перевипуск SIM-картки. З цього моменту SIM-картка жертви не працює, а фінансовим номером телефону розпоряджається шахрай.

Шахрай має змогу отримати доступ до:

- телефонної книги та SMS
- аккаунтів в соціальних мережах
- bank-ID, Google Account (ICloud), електронної пошти

Зрештою шахрай може:

- вкрасти гроші з банківських рахунків
- оформити онлайн-кредити
- від імені жертви просити грошей у друзів в соціальних мережах

Як цього не допустити:

- тримати в секреті SMS-пароль мобільного оператора
- зареєструвати SIM-картку на свій паспорт або перейти на контракт з мобільним оператором.

№2 «Небезпечні покупки»

70 % випадків шахрайства складає соціальна інженерія та шахрайство в інтернеті, тому, якщо купуєш онлайн, дотримуйся правил платіжної безпеки та дізнавайся більше про шахрайські схеми.

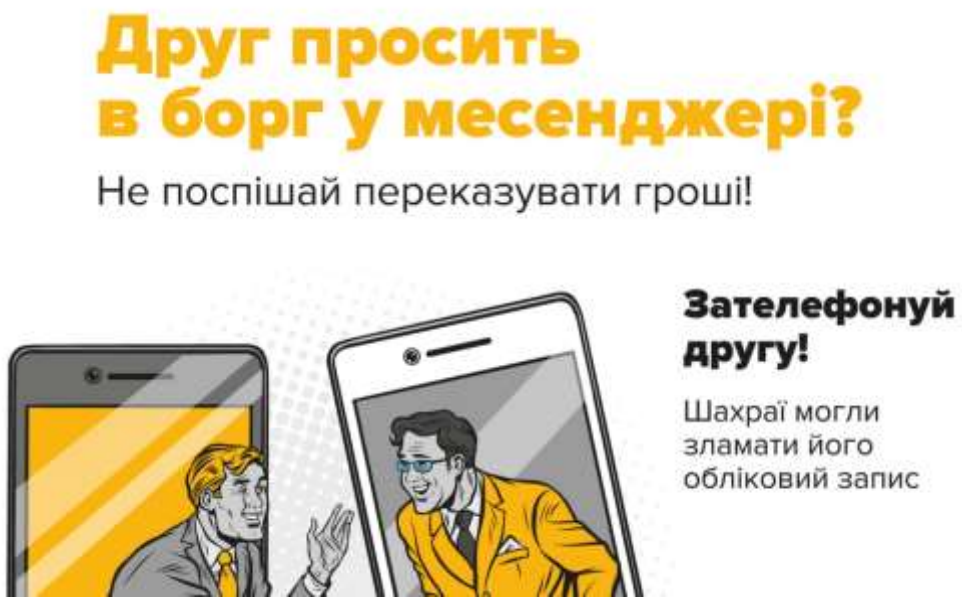
Ось одна із них:

Особа вирішила купити щось на торгівельному майданчику.
Знайшла потрібний товар та вийшла на зв'язок з продавцем.
Продавець замість того, щоб обговорювати деталі угоди в особистому кабінеті, несподівано пропонує перейти в месенджер, де продовжується розмова про товар. Псевдопродавець може надсилати додаткові фото товару і підтримувати розмову про товар.
Коли час приходить платити, надає посилання для оплати, яке веде на фішинговий сайт. Вже на фішинговому сайті жертва, вводить реквізити картки: номер, термін дії, трьохзначний номер картки та код з SMS. Шахраї зчитують цю інформацію та крадуть гроші з картки.

Що робити, щоб цього не сталося?

- Оговорювати деталі тільки в особистому кабінеті.
- Бути уважним до сайтів, де купуєте та оплачуєте товар.
- Сайти, які приймають онлайн-платежі мають бути захищеними, для цього в назві адреси вони мають містити https:// та значок «замочок»
- На сайті мають бути значки захисту онлайн-покупок від платіжних систем – Verified by Visa та MasterCard SecureCode.
- А краще за все використовувати наложений платіж.

№3 «Друг просить у борг»



Якщо стандартні розсилки від магазинів, банків, мобільних операторів тощо ми можемо пропустити повз, то повідомлення від друзів ми ніколи не ігноруємо.

Шахраї вирішили скористатись і цим.

Отже, ділимося розповсюдженою шахрайською схемою в соціальних мережах.

Шахраї зламують сторінку жертви в соціальних мережах, наприклад Facebook чи Instagram, або ж Telegram.
Розсилають всім підписникам, контактам однакові повідомлення наступного характеру:

«Привіт! Позич, будь ласка, гроші до завтра! Дуже треба!»
Суму шахраї зазначають різну.

Що робити, якщо отримали таке повідомлення?

Звичайно, подібна ситуація може статися з кожним. І у друга могло виникнути скрутне становище. Але, перш ніж позичати гроші:

- Перетелефонуйте другу.

За номером, який ви точно знаєте, а не на той, що вказаний на сторінці в соціальних мережах. Бо якщо шахрай зламав сторінку, то міг змінити номер телефону в профілі жертви.

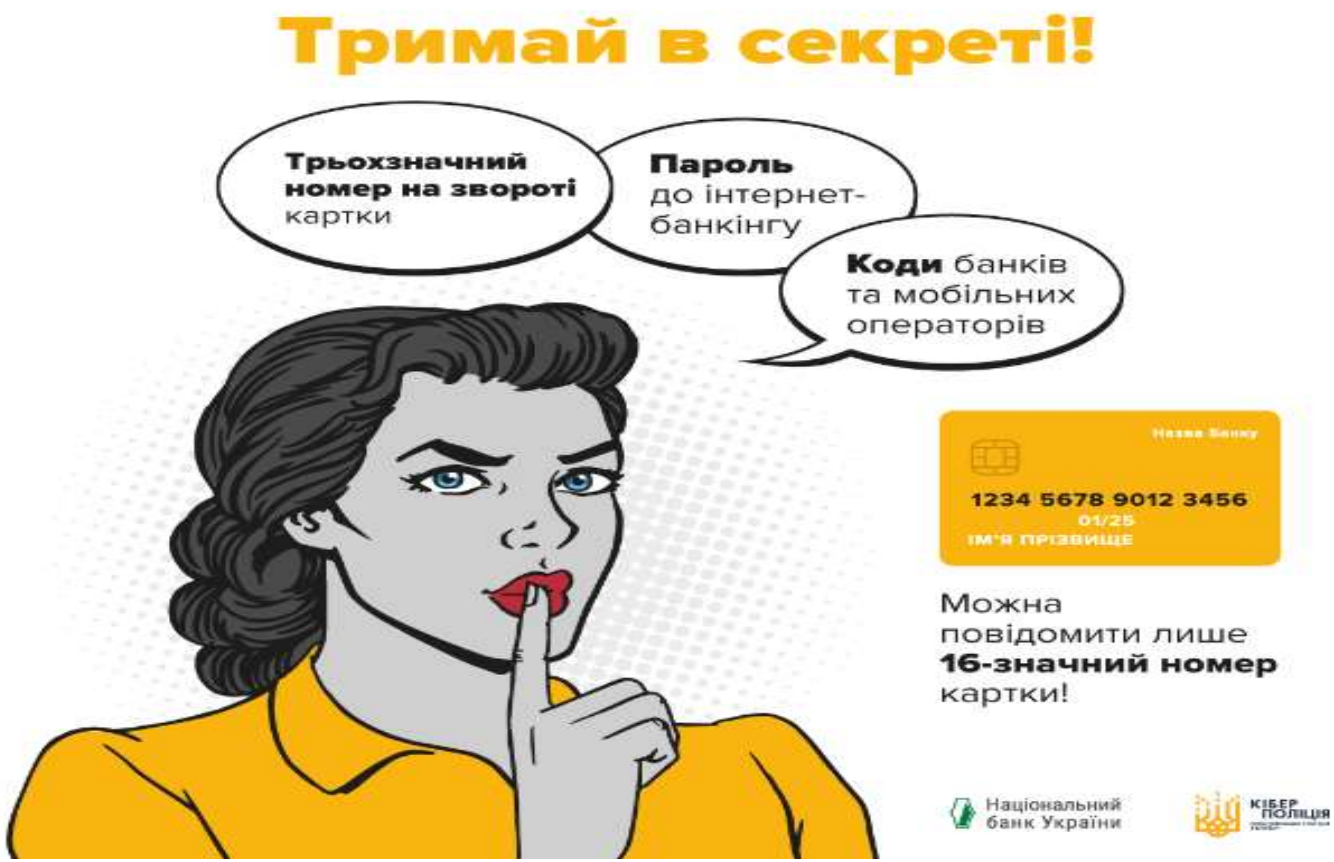
- Запитайте друга те, що можете знати тільки ви.

Не завжди є можливість подзвонити, чи можливо ви давно не спілкувалися і номеру телефону у вас немає. Таке питання одразу викриє шахрая.

- Напишіть спільним друзям в соціальних мережах чи не отримували вони подібних повідомлень від друга. Шахраї, як правило, одночасно роблять розсилку на всіх підписників зламаної сторінки.

А щоб такого не трапилося з Вами, створюйте складні та унікальні паролі для кожного облікового запису.

№5 Сценарій шахрая «Псевдо-покупець»



Що можна повідомляти про свою картку **- тільки 16-значний номер картки.**

Все інше, то велика таємниця. Шахраї під різними хитрощами намагаються виманити у своїх жертв більше інформації.

Ось, яку схему придумали шахраї!

Продавець виставляє на безкоштовній дошці оголошень на продаж товар (часто це дитячі товари).
Продавцю телефонує псевдо-покупець, який сам пропонує здійснити повну передоплату. Шахрай нібито хвилюється, щоб продавець не продав товар іншому.
Просить у покупця швиденько для здійснення переказу надати:
номер картки, термін дії, трьохзначний номер на звороті картки, SMS-код від банку.

Але це пастка! Пам’ятай! 16-значний номер картки – це все, що потрібно знати, щоб перерахувати гроші на картку.

Як вберегтися?

№6 Пройди опитування-виграй Iphone

Шахраї створюють сайти, які дуже схожі на сайти відомих кампаній.

Розміщують подібні оголошення:

- пройди опитування та отримай грошову винагороду або
- пройди опитування та візьми участь розіграші iPhone.

Завдання просте: потрібно відповісти на 5-10 нескладних запитань.

Суть запитань: оцінити рівень сервісу, вказати товари чи послуги яким ви надаєте перевагу, зазначити вік, стать тощо.

Після пройденого опитування система показує, що ви то самий щасливчик, який виграв iPhone. Або ви «заробили» декілька тисяч.

І тут починається найцікавіше:

- щоб отримати гроші потрібно сплатити комісію;
- виграш – 10 000 тисяч, а комісія – всього 100 грн;
- жертві не шкода, вона платить;
- потім ще треба заплатити податки, військовий збір тощо (список таких комісій безкінечний);
- жертва платить, поки є гроші або поки не прийде осяяння, що це звичайна афера.

● Не вірити в халяву.

● Не висилати жодних документів та не вказувати секретних реквізитів, кодів, паролів.

● Податки та збори порядна кампанія, яка проводить розіграш бере на себе або такі платежі вираховуються з виграшу.

№7 Селфі з паспортом

Чули ви таке, що за працевлаштування треба платити?
Виявляється, що треба! Тільки не справжнім роботодавцям, а – шахраям.

● Шахраї розміщують вакансії.

● Заманюють людей привабливими умовами та відсутністю кваліфікації.

● Коли людина погоджуються на роботу, просять заплатити страховий внесок.

● Як результат, людина без роботи і без грошей.

Але страховий внесок, це далеко не все.
Шахраї просять надати селфі з паспортом, а потім набирають онлайн-кредитів на своїх жертв. Замість страхового внеску «йдуть на поступки» і просять повні реквізити картки. Звичайно ж, щоб вкрасти з неї гроші.

Як захиститися?

● Ніколи не платити за працевлаштування наперед.

● Берегти свій паспорт. Не надсилати селфі з документам незнайомим особам.

● Тримати реквізити картки в секреті. Повідомляти можна лише 16-значний номер картки.

● Є необхідність надіслати копію паспорту? На копії зазначайте дату, підпис та назву компанії до якої надсилаєте копію документа.

Як не потрапити в пастку?

● Користуватися безпечними платіжними сайтами.

● Не переходити за посиланнями від сторонніх осіб.

№8 Шахраї на сайтах онлайн-знайомств

Шахраї реєструються на сайтах онлайн-знайомств та полюють там на своїх жертв. Мішенню шахрая можуть стати як чоловіки, так і жінки.

Розглянемо сценарій, де жертва – чоловік:

● шахрай створює профіль з приваблими жіночими фото;

● грайливо пише парубку та майже одразу пропонує зустрітись;

● місце зустрічі – кінотеатр для двох.

Жертва в захваті від такої ініціативи. Зовсім нічого не підозрює.

Шахрай пропонує кавалеру забронювати квитки та скидає посилання на сайт кінотеатру.

Звичайно, сайт шахрайський.

Парубок платить, лишається без грошей і без побачення.

І добре, якщо вартість квитків буде єдиною втратою жертви.

Можуть бути такі сайти, які зчитують реквізити карток.

Плакат №13 Мобільний інтернет чи WI-FI у незнайомих місцях

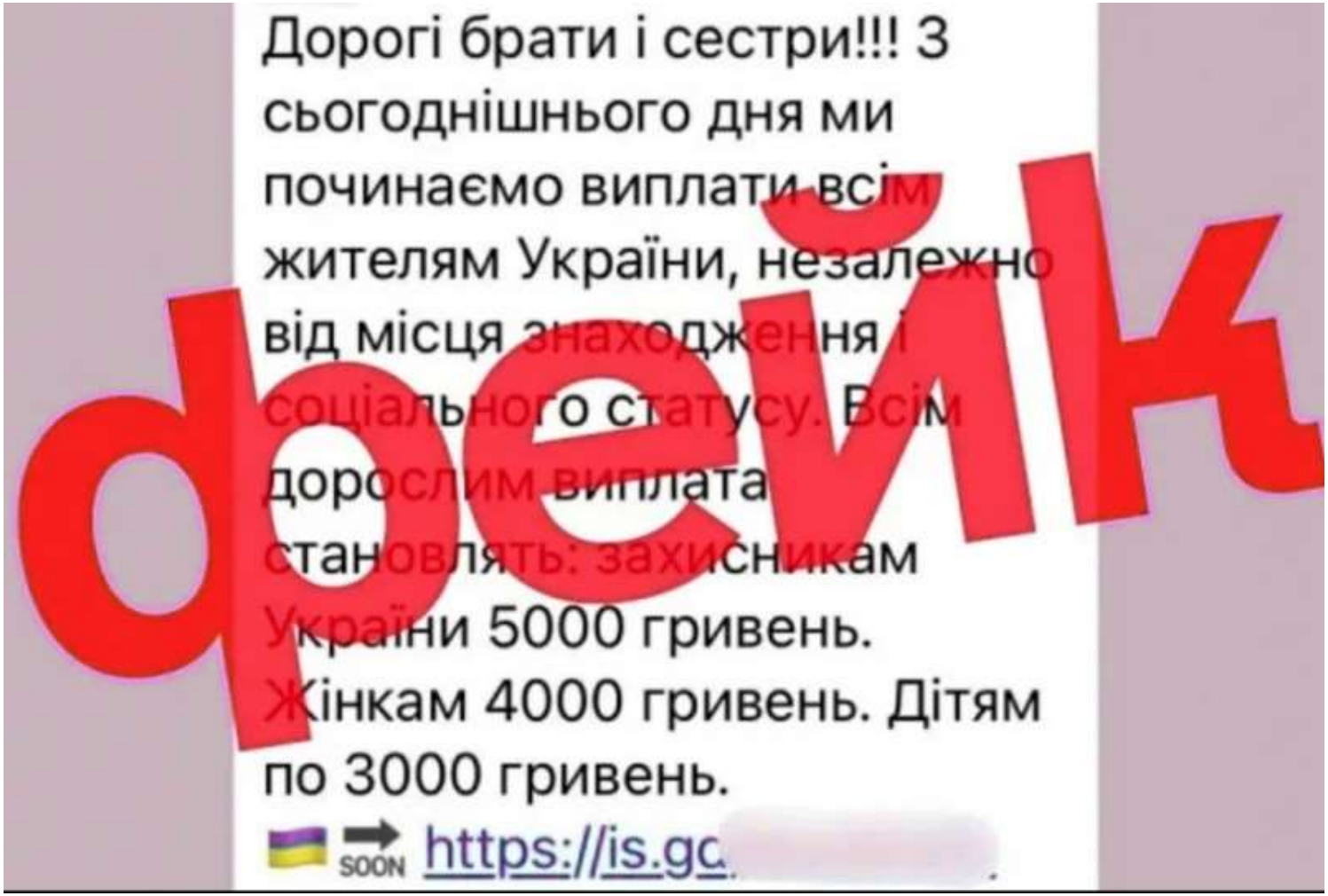
Надавай перевагу інтернету від мобільного оператора перед загальнодоступною мережею Wi-Fi!

Шахраї можуть створювати дублікати загальнодоступних мереж Wi-Fi та, перебуваючи в одній мережі з тобою, перехоплювати дані банківських карток, паролі та повідомлення.

Дотримуйся порад, щоб не потрапити до рук шахраїв.

1. Не здійснюй банківські операції, коли підключений до загальнодоступної мережі Wi-Fi.
2. Не використовуй мережі Wi-Fi, що просять авторизуватися за номером телефону, електронною поштою або через соцмережі: цим можуть скористатися зловмисники.
3. Вимкни опцію автоматичного підключення до загальнодоступних мереж Wi-Fi.

Краще завжди користуйся інтернетом від мобільного оператора!



СУМНІВНІ ВИПЛАТИ!!!!

Чергова схема шахраїв - «допомога» від ООН. У месенджері Telegram або Фейсбук, чи будь-якій іншій соціальній мережі можуть з’являтися посилання на отримання допомоги від ООН чи будь яких інших організацій.

Жертва вводить свої реквізити для онлайн-банкінгу. Після цього з її рахунку зникають гроші.

У поліції нагадують — аби не стати жертвою шахраїв, слід не переходити за сумнівними посиланнями та залишати дані свої банківських карток. Також радять отримувати інформацію тільки з офіційних джерел. Для злочинних дій шахраї створюють фейкові сторінки різних організацій, як от ООН, Червоного хреста, благодійних фондів та банків.