ШК ЄМА UKR EXIM BANK

УГОН SIM-КАРТКИ

Шахрайство з перевипуску SIM-картки без відома її власника

Мета шахраїв:

BankID Google Account sms iCloud

Доступ до ваших банківських рахунків, BankID, Google акаунта, пошти, Viber, облікових записів у соцмережах та месенджерах, фото та відео із подальшою крадіжкою ваших коштів або шантажу.

- крадіжка грошей з ваших рахунків
- оформлення кредитів від вашого імені
- крадіжка приватної інформації
- шантаж
- крадіжка цифрової особистості
- «розвод» ваших друзів від вашого імені
- крадіжка персонажів онлайн-ігор
- крадіжка криптовалюти

Шахрай перевипускає SIM-картку, звернувшись до мобільного оператора з повідомлецнням про крадіжку телефону…

- **відповівши на ідентифікаційне питання про «останні дзвінки»,** які шахрай попередньо сам і зробив, або **надавши PUK-код;**
- **через особистий кабінет мобільного оператора,** який шахрай реєструє сам, одночасно виманюючи у жертви SMS-код оператора;
- **надавши скан-копію або фальшивий паспорт** жертви у магазині оператора.

Ваша SIM-картка перестала працювати:

- **Негайно змініть пароль до Інтернет-банку!**
- **Негайно зверніться до банку**, заблокувавши картки, рахунки та доступ до Інтернет-банку. Зверніться в усі банки, в яких маєте рахунки! Дуже важливо чітко пояснити банківському співробітнику про перевипуск SIM-картки шахраями.
- **Негайно зверніться до мобільного оператора** та виконуйте його інструкції. Якщо оператор не повертає номер відразу, вимагайте блокування обох SIM-карток (старої і нової) до закінчення розгляду справи.
- **Негайно заблокуйте акаунти в усіх інших фінансових сервісах** до яких прив'язані ваші картки. Заблокуйте доступ до персональних кабінетів компаній мікрофінансових позик.

Якщо ви отримали повідомлення про заплановану оператором заміну сімки:

- **Виконайте усі вище наведені поради, але у першу чергу зателефонуйте до мобільного оператора і зупиніть перевипуск SIM-картки**.

Як запобігти:

- **Перейдіть на «контракт»** або, як мінімум, **прив'яжіть pre-paid номер до свого паспорта.**
- **Відключіть можливість віддаленого перевипуску SIM-картки.**
- **Створіть унікальні паролі** до Інтернет-банку, мобільних платіжних додатків та електронної пошти.
- **Власноруч зареєструйтеся в онлайн-кабінеті мобільного оператора.** Нікому і ніколи не передавайте SMS-коди мобільних операторів, PUK-код, серійний номер SIM-картки, кодове слово та номери телефонів абонентів,з якими ви спілкуєтесь.
- **Не світіть фінансовий номер** у соцмережах, на дошках оголошень тощо.
- **Обережно в соцмережах!** Не додавайте у «друзі» незнайомців, навіть якщо це друзі ваших друзів. Не світіть номер телефону та день народження.