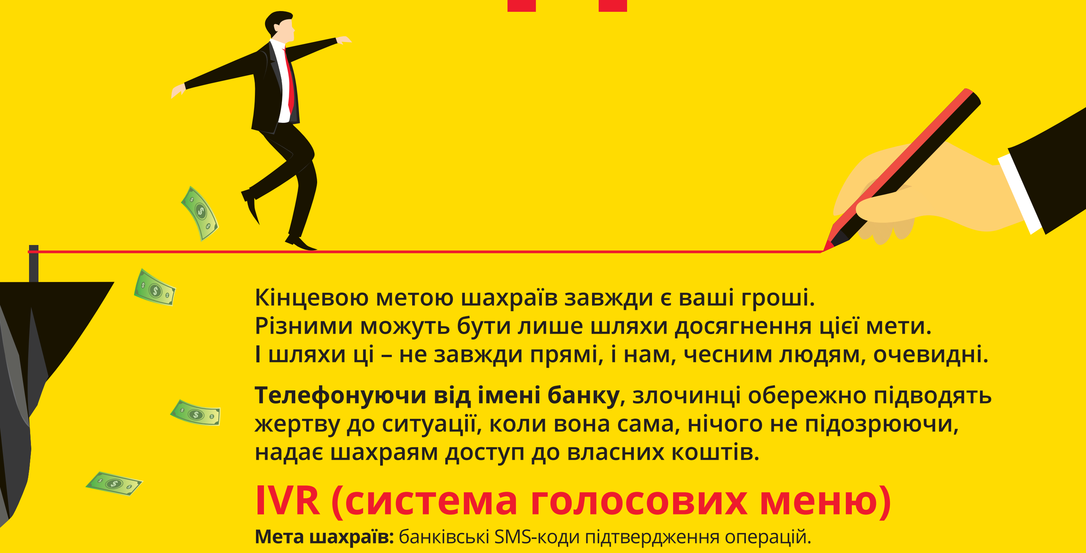
«БАНК» НА ДРОТІ



Кінцевою метою шахраїв завжди є ваші гроші.
Різними можуть бути лише шляхи досягнення цієї мети.
І шляхи ці – не завжди прямі, і нам, чесним людям, очевидні.

Телефонуючи від імені банку, злочинці обережно підводять жертву до ситуації, коли вона сама, нічого не підозрюючи, надає шахраям доступ до власних коштів.

IVR (система голосових меню)

Мета шахраїв: банківські SMS-коди підтвердження операцій.

Схема: просять переключитися на IVR та ввести код у тоновому режимі, зчитуючи (підслуховуючи) набрані цифри.

Результат: шахраї отримують коди для входу у Інтернет-банк, або проведення інших операцій з платіжною карткою жертви.

Віддалений доступ (Remote desktop)

Мета шахраїв: здійснювати платежі зі смартфону жертви на власну користь.

Схема: назвавшись співробітником служби безпеки банку, повідомляють, що смартфон заражений вірусом, та надають посилання для завантаження програми віддаленого доступу.

Результат: шахрай отримує доступ до смартфону жертви і можливість здійснювати платежі на власну користь.

«Безпечний» рахунок

Мета шахраїв: змусити жертву перерахувати гроші на рахунок злочинців.

Схема: повідомляють жертві, що її рахунок і гроші на ньому у небезпеці, наказуючи зробити негайний переказ усіх коштів на «безпечний рахунок» або зняти їх у банкоматі (з функцією cash in) та одразу внести на «безпечний рахунок».

Результат: жертва самостійно перераховує кошти на рахунок шахрая.

Операція «Переадресація»

Мета шахраїв: отримати доступ до усіх вхідних дзвінків та СМС жертви.

Схема: Просять набрати на телефоні послідовність символів, яка у дійсності є USSD-командою мобільному оператору на переадресацію усіх вхідних дзвінків жертви на номер шахрая.

Результат: СМС-повідомлення з кодами від банку відтепер надходитимуть шахраям.

ЗАХИСТ

Покладіть слухавку та самостійно зателефонуйте до банку

Телефонуйте за номером, що зазначений на звороті вашої картки

Не розголошуйте секретних реквізитів та паролів

Не розголошуйте жодних реквізитів вашої картки (за винятком її номера), а також банківські SMS коди та паролі мобільних операторів

Не встановлюйте жодних програм на прохання телефоном

Ніколи не встановлюйте жодних програм чи застосунків з функціоналом віддаленого доступу на прохання банківських співробітників

Обережно з USSD-командами

Не виконуйте USSD-команди на телефонні вимоги банківських співробітників

Не переказуйте кошти на прохання співробітників банку

За жодних обставин не переказуйте на прохання банківських співробітників ваші кошти на будь-які інші рахунки та рахунки третіх осіб

Вірити не можна нікому!

Ви ніколи не можете бути впевнені, хто насправді на іншому кінці

ЕМА