МЕТОЮ ХАКЕРА МОЖЕТЕ БУТИ ВИ!

ČESKÁ BANKOVNÍ ASOCIACE

POLICIE ČESKÉ REPUBLIKY

УВАГА! ХТОСЬ ВІД ІМЕНІ ВАШОГО БАНКУ АБО ПОЛІЦІЇ ЧЕСЬКОЇ РЕСПУБЛІКИ ПРОСИТЬ ВАС НАДАТИ ДОСТУП ДО ДАНИХ В ІНТЕРНЕТ-БАНКІНГУ АБО ДО ДАНИХ ВАШИХ ПЛАТІЖНИХ КАРТОК? АБО ЗДІЙСНИТИ ПЛАТІЖНУ ОПЕРАЦІЮ ЧЕРЕЗ НЕМИНУЧУ АТАКУ НА ВАШ ОБЛІКОВИЙ ЗАПИС?

НЕ РЕАГУЙТЕ, ЦЕ ШАХРАЙ! НЕГАЙНО ЗВ'ЯЖІТЬСЯ З БАНКОМ АБО ЗАТЕЛЕФОНУЙТЕ ЗА НОМЕРОМ 158!

#ФІШИНГ #ВІШИНГ

5 ПОРАД ЩОДО ЗБЕРЕЖЕННЯ ВАШИХ ГРОШЕЙ

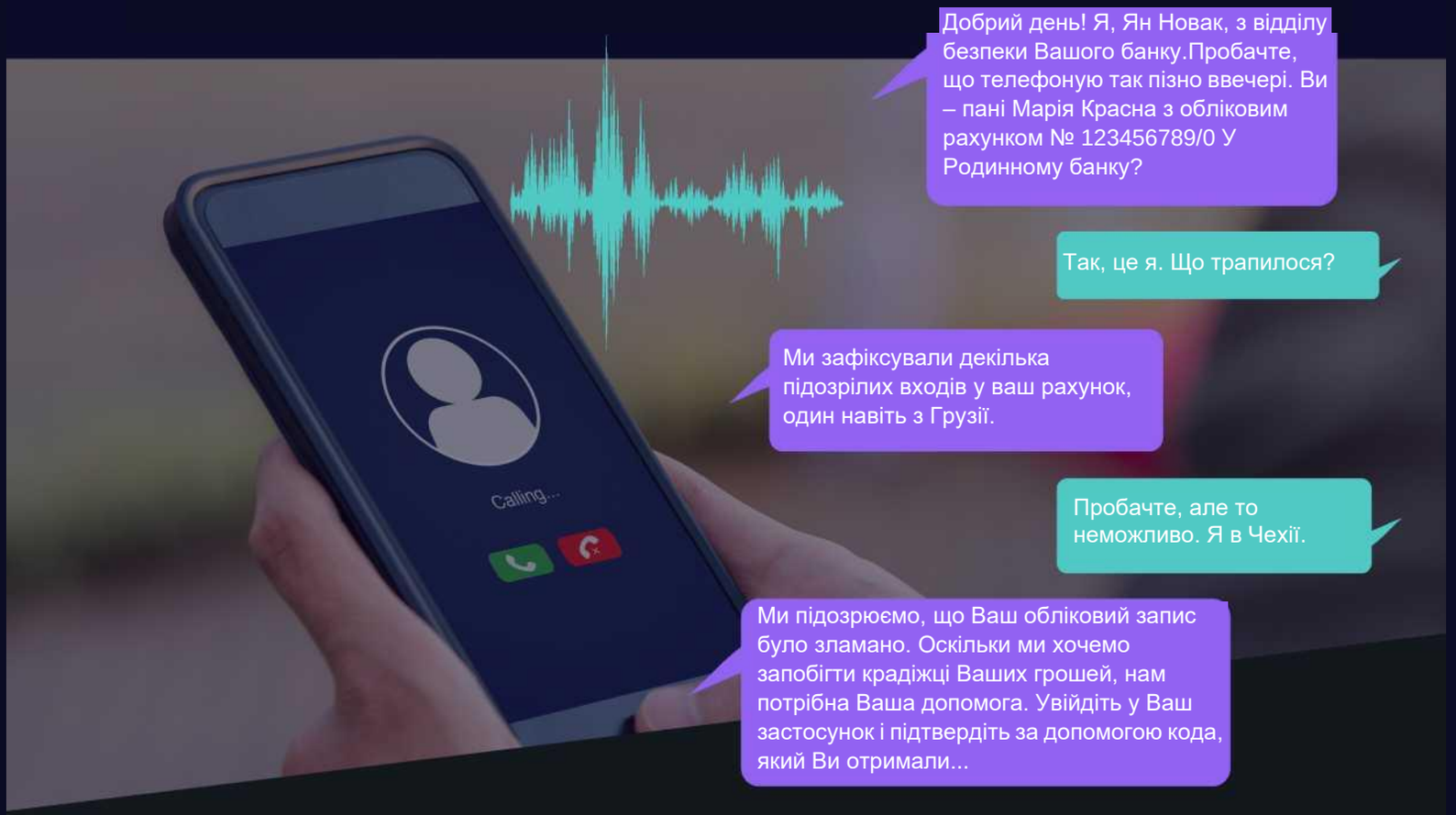
1. Ніколи ні з ким не діліться своїми реєстраційними даними в інтернет-банкінгу або номерами платіжних карток. Банки не запитують про них, а також не надсилають повідомленнями або електронною поштою посилання на веб-сайти, де вони потрібні!

2. Не відповідайте на телефонні дзвінки, електронні листи або повідомлення, коли хтось намагається маніпулювати вами в ситуації, коли ваші кошти знаходяться під загрозою, і вам потрібно вжити подальших заходів, щоб врятувати їх. Якби ваші гроші були в небезпеці, банк вже давно б відреагував без вас.

3. Власником вашого рахунки є лише ви. Не вводіть і не підтверджуйте в застосунку платежі, які вам хтось диктує по телефону, не повідомляйте і не пересилайте нікому коди підтвердження з СМС. А також не надавайте нікому віддалений доступ до вашого комп'ютеру.

4. Оновіть програмне забезпечення та антивірус. Навіть в телефоні!

5. У разі виникнення сумнівів завжди звертайтеся до свого банку або телефонуйте за номером 158. Майте на увазі, що зловмисник може імітувати будь-який номер телефону (так званий спуфінг) або електронну пошту, включаючи ваш банк.



#ФІШИНГ – шахрайські повідомлення, електронні листи

#безпечні банки

#ВІШИНГ – дзвінки фальшивих працівників банку