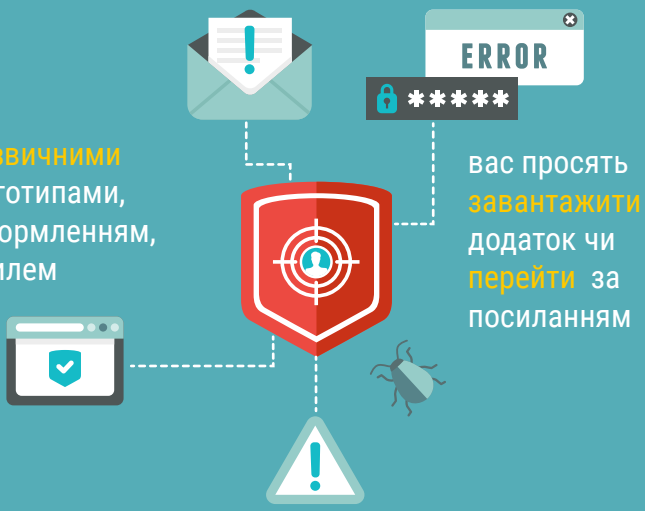
«ЦЕ З БАНКУ»: ФІШИНГ

Фішинг: електронні листи від шахраїв, які хитрощами вивідують особисту, фінансову або конфіденційну інформацію.

ЩО ВІДБУВАЄТЬСЯ?

Прийшов лист:

на перший погляд схожий на листи, які регулярно надходять із банку



зі звичними логотипами, оформленням, стилем

вас просять завантажити додаток чи перейти за посиланням

формулювання свідчать, що справа нагальна

ЯК ДІЯТИ?

- **Оновлювати програмне забезпечення**, зокрема, браузер, антивірус, операційну систему.
- Особливо **пильнувати**, якщо «з банку» вимагають таємну інформацію (скажімо, ваш пароль до системи «Клієнт-Банк»).
- **Ретельно вивчити лист**: порівняти адресу з попередніми справжніми листами з банку. Зважати на помилки в правописі.
- **Не відповідати на підозрілі листи**, натомість пересилати їх у банк, вводячи його адресу вручну.
- **В жодному разі не тиснути на посиланнях та не завантажувати додатки** — вводити адреси в браузері вручну.
- У разі сумніву, **перевірити** відомості на сайті або зателефонувати в банк.

Кіберзлочинці покладаються на зайнятість жертв: на перший погляд фальшиві листи схожі на справжні.

#CyberScams

Обережно з мобільними пристроями! Спробу фішингу важче виявити на маленькому екрані телефону та планшеті.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | EMA

«ЦЕ З БАНКУ»: СМІШИНГ

Смішинг (від слів «СМС» та «фішинг»): шахраї надсилають текстові повідомлення, щоб вивідати особисту, фінансову або конфіденційну інформацію.

ЩО ВІДБУВАЄТЬСЯ?

Надходить СМС з вимогою перейти за посиланням чи перетелефонувати на певний номер, щоб «перевірити» або «відновити» рахунок.
Але... посилання веде на підроблений сайт, а з номера відповідає шахрай, що видає себе за співробітника компанії.

ЯК ДІЯТИ?

- Якщо надійшло несподіване СМС, **не відкривайте посилання, додатки, зображення**, спершу перевірте, хто його прислав.
- **Зберігайте спокій!** Не кваптеся, перевірте все до пуття, перш ніж якось реагувати.
- **Не відповідайте на СМС**, де вимагають PIN, пароль до системи «Клієнт-Банк» чи облікові дані.
- Відповіли на СМС, надали банківські реквізити, а потім запідозрили, що це смішинг? **Негайно повідомте про це банк!**

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | EMA | #CyberScams

«ЦЕ З БАНКУ»: ВІШИНГ

Вішинг (від слів Voice у значенні «голосовий зв'язок», і Phishing, фішинг): шахрай телефонує й переконує жертву повідомити особисту, фінансову чи конфіденційну інформацію або переказати гроші.

ЯК ДІЯТИ?

- **Стерегтися** непроханих дзвінків.
- **Спитати, з якого номера телефонують**, і сказати, що ви перетелефонуєте.
- Для перевірки **дізнатися номер названої організації** та зателефонувати туди за цим номером.
- **Не використовувати номер, повідомлений людиною, яка дзвонила** (може бути підробний чи фальшивий).
- Шахраї можуть знайти ваші дані в Інтернеті (зокрема, соцмережах). Знання цих даних — **не доказ, що телефонує не шахрай**.
- **Не повідомляйте** реквізити та PIN-код платіжної картки чи пароль у системі «Клієнт-Банк». Працівники банків цього не вимагають.
- **Не переказуйте нікому гроші** на вимогу телефоном.
- Дзвінок видався шахрайським? **Повідомте в банк**.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

EMA

#CyberScams