БАНКОВИ ФИШИНГ ИМЕЙЛИ

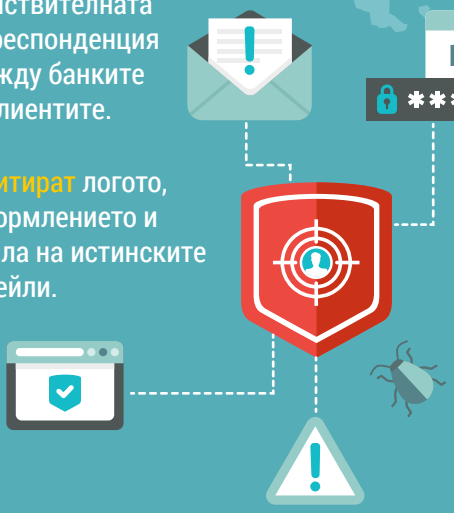
Фишинг означава измамни имейли, които целят получателите да споделят своята лична, финансова или информация, свързана със сигурността.

КАК РАБОТИ ИЗМАМАТА?

Тези имейли:

могат да изглеждат идентични с действителната кореспонденция между банките и клиентите.

имитират логото, оформлението и стила на истинските имейли.



искат от вас да изтеглите приложен документ или да кликнете върху линк.

използват език, който създава усещане за неотложност.

КАКВО МОЖЕТЕ ДА НАПРАВИТЕ?

- **Актуализирайте софтуера си редовно,** включително браузъра, антивирусната и операционната система.
- **Бъдете особено бдителни,** ако имейл от "банката" изисква от вас чувствителна информация (например, паролата за онлайн банкиране).
- **Разгледайте внимателно имейла:** сравнете адреса с предишни реални съобщения от вашата банка. Проверете за лош правопис и граматика.
- **Не отговаряйте на подозрителен имейл,** вместо това го препратете на банката си, като сами въведете имейл адреса.
- **Не кликвайте върху линка и не изтегляйте прикачения файл,** вместо това въвеждайте ръчно адреса в браузъра си.
- Когато се **съмнявате**, проверете на уеб сайта на вашата банка или й се обадете.

Киберпрестъпниците разчитат на това, че хората са заети; на пръв поглед, тези подправени имейли изглеждат истински.

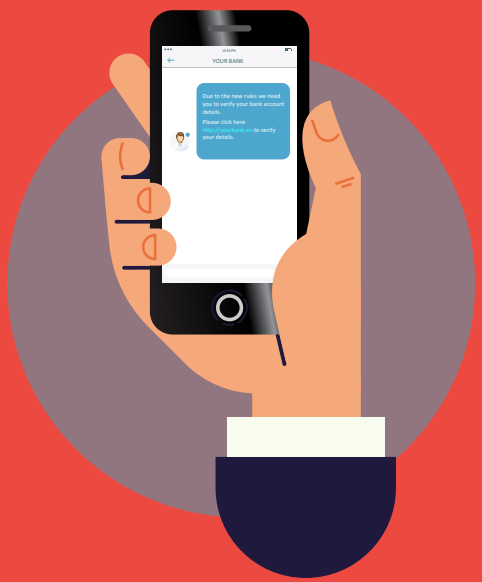
#CyberScams

Внимавайте, когато използвате мобилно устройство. Може да е по-трудно да забележите опит за фишинг през вашия телефон или таблет.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | Асоциация на банките в България

БАНКОВИ ФИШИНГ SMS-И

Смишинг (комбинация от думите SMS и Фишинг) е опит за измама, чрез която да бъде получена лична, финансова или свързана със сигурността информация чрез текстово съобщение.



КАК РАБОТИ ИЗМАМАТА?

Текстовото съобщение обикновено изисква от вас да кликнете върху линк или да се обадите на телефонен номер, за да "потвърдите", "актуализирате" или "активирате" профила си. Но ... линкът води до фалшив уебсайт и на телефонния номер отговаря измамник, който се представя, че е от реална компания.

КАКВО МОЖЕТЕ ДА НАПРАВИТЕ?

- **Не кликвайте върху линкове, прикачени файлове или изображения,** които получавате в непоискани текстови съобщения, без първо да проверите изпращача.
- **Не бързайте. Отделете време и направете необходимите проверки, преди да отговорите.**
- **Никога не отговаряйте на текстово съобщение,** което изисква вашия ПИН или паролата ви за онлайн банкиране или други данни за идентификация.
- Ако смятате, че може да сте отговорили на измамно смишинг съобщение и да сте предоставили банкови данни, **незабавно се свържете с банката си.**

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

Асоциация на банките в България

#CyberScams

БАНКОВИ ВИШИНГ ОБАЖДАНИЯ

Вишинг (комбинация от английските думи за Глас и Фишинг) е телефонна измама, при която измамниците се опитват да накарат жертвата да разкрие лична, финансова или свързана със сигурността информация или да им преведе пари.

КАКВО МОЖЕТЕ ДА НАПРАВИТЕ?

- **Пазете се** от нежелани телефонни обаждания.
- **Вземете номера, от който ви се обаждат** и кажете, че ще им върнете обаждането.
- За да потвърдите самоличността им, **потърсете телефонния номер на организацията**, от чието име се представят и се свържете с тях директно.
- **Не потвърждавайте самоличността, като използвате номера, който са ви дали** (може да бъде фалшив или подправен номер).
- Измамниците могат да намерят основната информация за вас онлайн (например, социални мрежи). **Не допускайте, че разговорът е автентичен**, само защото имат такава информация за вас.
- **Не споделяйте** ПИН кода на вашата кредитна или дебитна карта или паролата си за онлайн банкиране. Вашата банка никога няма да ви поиска такива данни.
- **Не превеждайте пари** на друга сметка по тяхно искане. Вашата банка никога няма да поиска да го направите.
- Ако смятате, че обаждането е фалшиво, **уведомете вашата банка.**

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

Асоциация на банките в България

#CyberScams