БАНКОВИ ФИШИНГ ИМЕЙЛИ

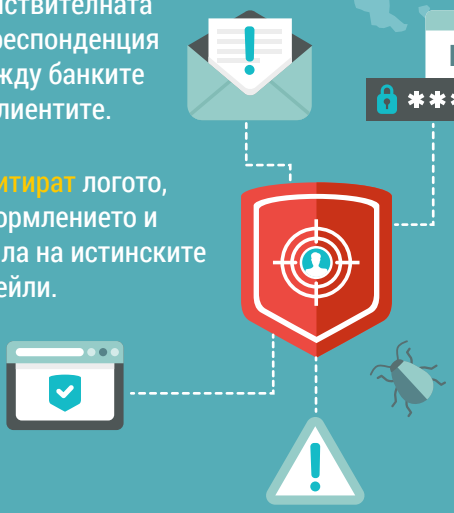
Фишинг означава измамни имейли, които целят получателите да споделят своята лична, финансова или информация, свързана със сигурността.

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