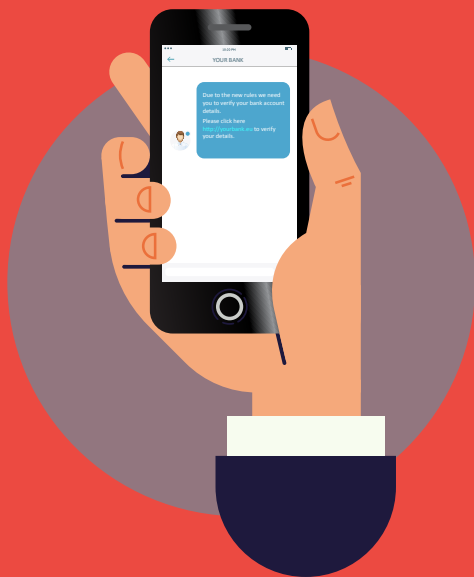


## БАНКОВИ ФИШИНГ SMS-И

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 кликайте 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.**