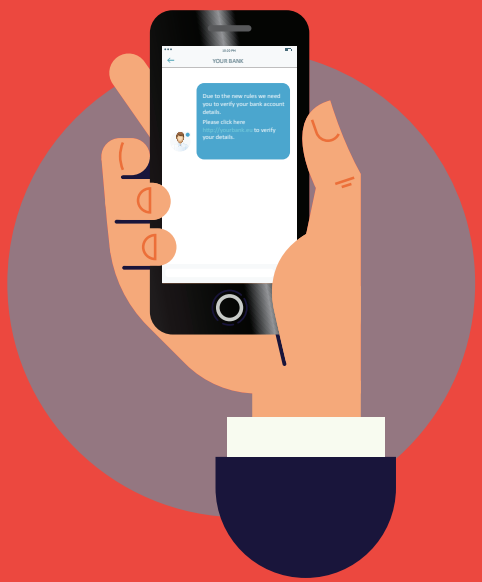
SMS-JI Z LAŽNIM PREDSTAVLJANJEM BANK

Pošiljanje SMS-jev z lažnim predstavljanjem (angl. »smishing«) je način, s katerim poskušajo sleparji prek sporočila SMS pridobiti osebne, finančne ali varnostne podatke.



KAKO DELUJE?

V sporočilu SMS bo običajno zahteva, da kliknete povezavo ali pokličete telefonsko številko, da »potrdite«, »posodobite« ali »znova aktivirate« svoj račun. Vendar pa povezava vodi na lažno spletno mesto, telefonska številka pa je od sleparja, ki se predstavlja kot verodostojno podjetje.

KAJ LAHKO STORITE?

- **Ne klikajte povezav, prilog ali slik**, ki jih prejmete v nezahtevanih sporočilih SMS, ne da bi prej preverili pošiljatelja.
- **Ne hitite.** Vzemite si čas in preverite vse potrebno, preden se odzovete.
- **Nikoli ne odgovarjajte na sporočilo SMS**, ki zahteva vaš PIN, geslo za spletno banko ali kakršne koli druge varnostne poverilnice.
- Če menite, da ste morda odgovorili na lažno predstavljanje prek sporočila SMS in razkrili svoje bančne podrobnosti, **se takoj obrnite na svojo banko.**

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLICIJA

si·cert Nacionalni odzivni center za kibernetsko varnost

#CyberScams