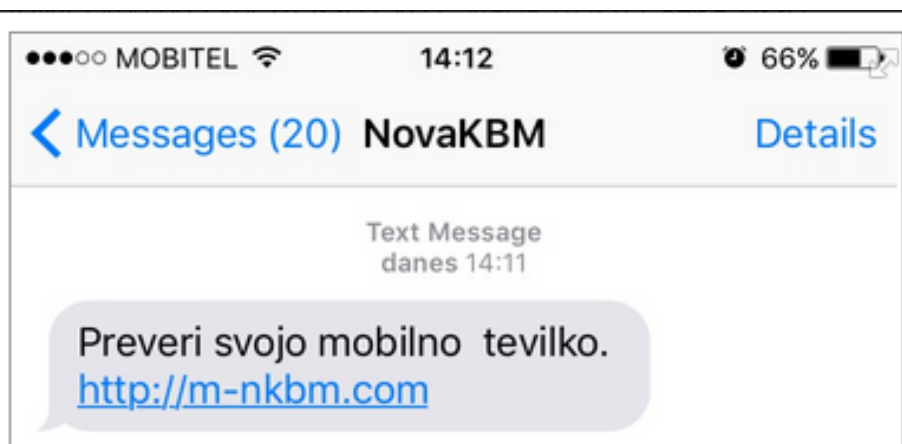


Prikaz poteka poskusa spletne prevare preko ponarejenega SMS sporočila

KORAK 1: Na svoj mobilni telefon prejmete ponarejeno SMS sporočilo:



Slika 1: Ponarejeno - lažno SMS sporočilo

Zaznali smo tudi vsebino SMS sporočila v »polomljeni« slovenščini:

"Preverite, ali številko mobilnega telefona: <http://m-nkbm.com>"

POMEMBNO:

Takšno besedilno ali slikovno SMS sporočilo je ponarejeno. Takoj ga izbrišite!

KORAK 2: Klik na ponujeno povezavo vas pripelje na lažno spletno stran:



Slika 2: Prikaz lažne vstopne spletne strani na mobilnem telefonu



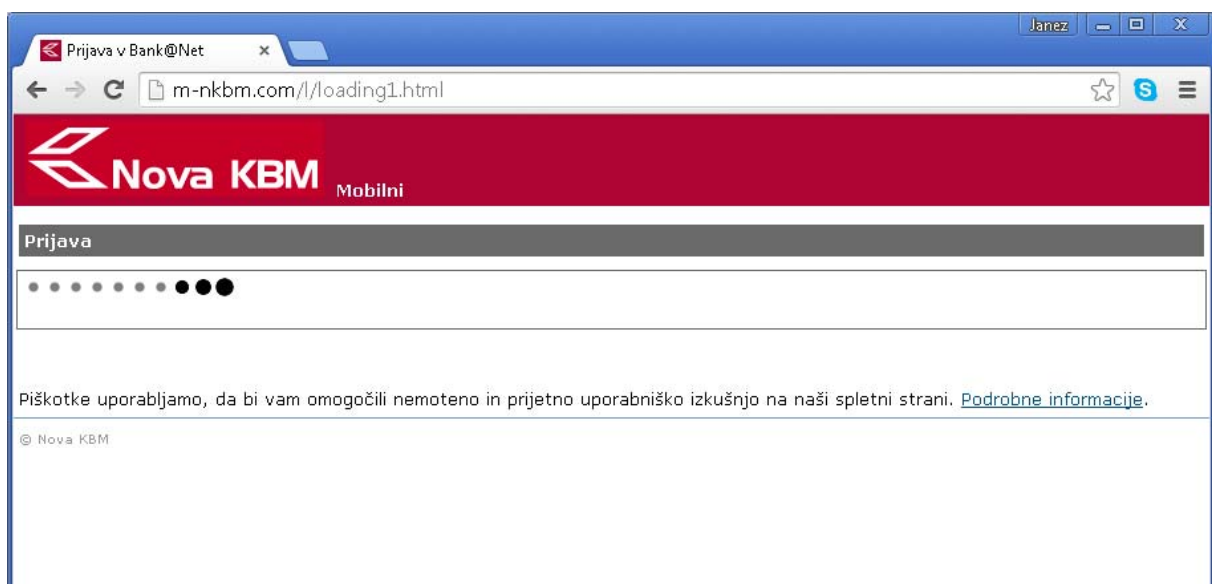
Slika 3: Prikaz lažne vstopne spletne strani v brskalniku

KORAK 3: Po vpisu vstopnih podatkov je zahtevan vpis telefonske številke.



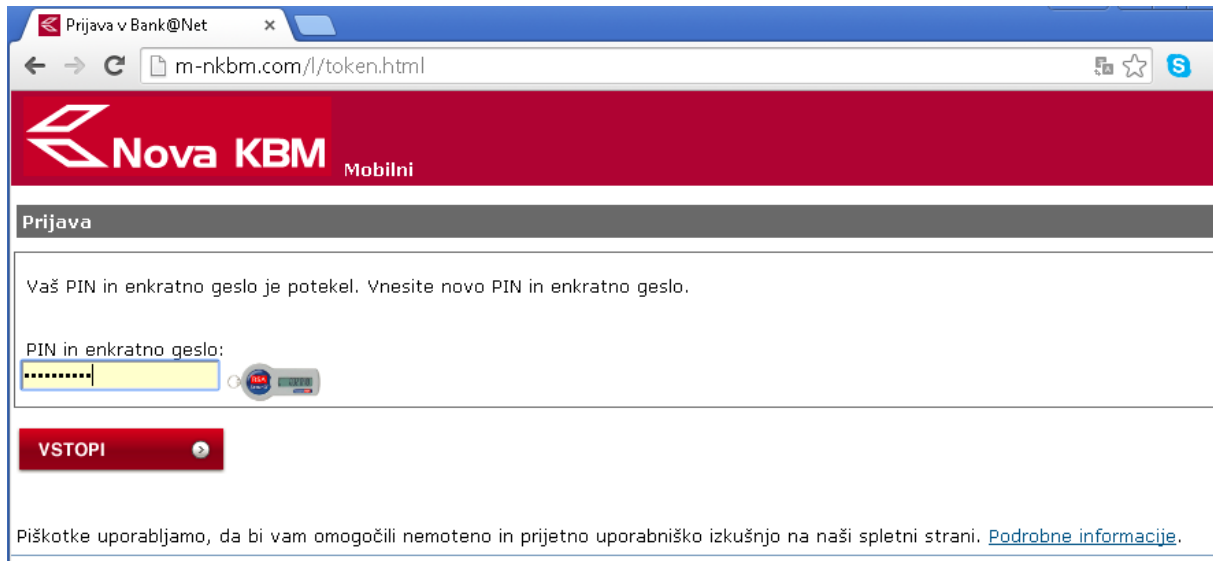
Slika 4: Prikaz lažne strani za vpis telefonske številke

KORAK 4: Nekaj trenutkov je prikazana vsebina, ki spominja na 'nalaganje strani' (tekoče pike):



Slika 5: Lažno 'nalaganje strani'.

KORAK 5: Pojavi se stran, ki vas poziva k ponovnemu vpisu PIN in enkratnega gesla



Slika 5: Poziv k ponovnemu vpisu PIN in enkratnega gesla.

POMEMBNO:

Če naredite vse zgoraj opisane korake, lahko v nadaljevanju pride do zlorabe spletne banke.

KAKO RAVNATI?

1. Lažno sporočilo takoj izbrišite.
2. V prijavnih poljih ne vpisujte identifikacijskih podatkov: uporabniško ime, PIN, enkratno geslo...
3. Če ste podatke vpisali in se prijavili v ponarejeno spletno banko, o tem obvestite na: spletneprevare@nkbm.si ali pokličite na telefonsko številko 02 229 2760 (vsak delovnik med 7. in 22. uro), kjer bomo uredili ustrezno rešitev za vas.
4. V spletno banko Bank@Net se prijavljajte izključno prek naše spletne strani www.nkbm.si.
5. Pred potrjevanjem vedno preglejte spisek plačil, ki jih potrjujete, saj so med njimi lahko tudi ponarejena plačila.

VEČ INFORMACIJ:

- e-pošta: spletneprevare@nkbm.si ali bankanet@nkbm.si
- telefon: 02 229 2760 (vsak delovnik med 7. in 22. uro)
- Skype: NovaKBM.Bankanet