

## POZOR: Zaznali smo lažna elektronska sporočila

Spoštovani,

obveščamo, da smo zaznali nove primere Phishing napadov, ki so usmerjeni na uporabnike spletne banke Addiko EBank, pri čemer potencialne žrtve prejmejo elektronsko sporočilo s povezavo na lažno spletno stran, ki je kopija prijavnih strani za vstop v spletno banko Addiko EBank za občane.

Če uporabnik vpiše prijavne podatke (uporabniško ime in enkratno geslo) na lažni spletni strani, jih napadalci lahko uporabijo za prijavo v spletno banko Addiko EBank in v imenu uporabnika oddajo plačilni nalog. Spletna banka nato v naslednjem koraku uporabniku za potrditev plačila pošlje sporočilo SMS z varnostno kodo. Vpis te kode v drugem koraku na lažni spletni strani zahtevajo tudi napadalci, ki jo v primeru, da jo uporabnik tudi vpiše, sami vpišejo v spletni banki in s tem potrdijo goljufivo transakcijo.

To pomeni, da če se SMS koda vpiše v spletni obrazec, se s tem dejansko avtorizira plačilo, ki so ga napadalci po pridobitvi prijavnih podatkov vnesli v spletno banko.

**Opozarjamo, da za prijavo v spletno banko Addiko EBank ni nikoli zahtevan vpis SMS kode, ampak izključno uporabniško ime in enkratno geslo.**

Dodatno svetujemo, da nikoli ne dostopate do spletne banke preko spletnih povezav prejetih preko elektronske pošte ali SMS sporočila, ampak vedno z vpisom spletnega naslova v spletni brskalnik oz. preko shranjenega zaznamka v vašem spletnem brskalniku.

Slike prijavnih obrazcev na lažni spletni strani:

Prijava v Addiko EBank in Addiko Business EBank

Addiko EBank

OBČANI

Prijava z uporabniškim imenom in geslom

Uporabniško ime

Geslo

Prijava

Demo

Prijava v Addiko EBank in Addiko Business EBank

Addiko EBank

OBČANI

Vnesite SMS kodo, poslano na vašo številko mobilnega telefona.

SMS koda

Prijava

Demo

S spoštovanjem,

Addiko Bank d.d.