URSIV opozarja na phishing kampanjo, ki zlorablja podobo OTP banke in URSIV-a

4.6.2026 - | gov.si

Urad Republike Slovenije za informacijsko varnost (URSIV) opozarja na lažna elektronska sporočila, ki se predstavljajo kot obvestila OTP banke. Kampanja je usmerjena predvsem v poslovne uporabnike spletnega bančništva in uporabnike poziva k domnevni nujni varnostni obnovi oziroma aktivaciji računa.

Po kliku na povezavo v sporočilu se uporabniku odpre lažna spletna stran, ki zlorablja grafično podobo OTP banke in se lažno predstavlja kot stran, povezana z URSIV-om. Uporabnike poziva k vnosu elektronskega naslova in telefonske številke ter jih vodi skozi večstopenjski postopek, s katerim skušajo napadalci pridobiti podatke za dostop do spletne banke.

Gre za napredno obliko phishing napada, pri katerem napadalci z uporabo lažnih elektronskih sporočil, spletnih strani in telefonskih klicev skušajo pridobiti podatke za prijavo v spletno banko ter podatke za potrjevanje transakcij. Takšni napadi lahko povzročijo veliko finančno škodo podjetjem in drugim organizacijam.

Posebnost tovrstnih napadov je, da jim pogosto sledi telefonski klic osebe, ki se predstavlja kot uslužbenec banke. Ker lažna spletna stran uporabniku predhodno sporoči, da ga bo kontaktiral predstavnik banke, žrtev tak klic pričakuje in ga zato težje prepozna kot prevaro. Napadalci pri tem pogosto uporabljajo slovenske telefonske številke ali ponaredijo prikaz telefonske številke, tako da se na zaslonu telefona izpiše prava številka banke.

Uporabnike pozivamo, da pred vnosom osebnih ali prijavnih podatkov vedno preverijo naslov spletne strani in pošiljatelja elektronskega sporočila. Banke in hranilnice uporabnikov ne pozivajo prek elektronske pošte ali SMS-sporočil, da morajo zaradi domnevnih varnostnih razlogov, grožnje blokade računa ali drugih nujnih okoliščin prek povezav v sporočilih vnesti gesla, potrditvene kode ali druge občutljive podatke.

Če prejmete takšno sporočilo, ga obravnavajte kot sumljivo in se za preverjanje informacij obrnite neposredno na svojo banko prek uradnih kontaktnih podatkov. Če ste na lažni spletni strani že vnesli svoje podatke ali ste sledili navodilom oseb, ki so se predstavljale kot predstavniki banke, nemudoma kontaktirajte svojo banko in preverite morebitne nepooblaščene aktivnosti na računu. Takšna sporočila posredujte tudi pristojni CSIRT skupini (SI-CERT ali SIGOV-CERT).

https://www.gov.si/novice/2026-06-04-ursiv-opozarja-na-phishing-kampanjo-ki-zlorablja-podobo-otp-banke-in-ursiv-a