ZBS | Združenje bank Slovenije

Obvestilo za javnost

Zaznani novi poskusi spletnih prevar

Banke in hranilnice, članice Združenja bank Slovenije, v zadnjem času opažajo porast poskusov spletnih prevar, predvsem t.i. phishinga (spletno ribarjenje). Goljufi prek elektronske pošte ali SMS-sporočil pošiljajo lažna sporočila s ciljem pridobiti občutljive podatke. Pri tem se usmerjajo na tarče z veliko uporabniki – npr. družbena omrežja, priljubljene spletne portale in trgovine, e-poštne storitve in storitve v oblaku, dostavne službe ter banke in hranilnice.

V Združenju bank Slovenije zato strankam bank in hranilnic svetujemo dodatno previdnost pri poslovanju v spletnih ali mobilnih bančnih aplikacijah, pri spletnih nakupih in poslovanju s plačilnimi karticami.

Kako prepoznamo phishing?

Phishing je omrežni napad, katerega cilj je pridobitev različnih osebnih in občutljivih podatkov. V večini primerov gre za krajo uporabniških imen in gesel ter podatkov o kreditni kartici, ki se običajno začne prek elektronske pošte, zadnje čase pa vse bolj tudi prek SMS-sporočil ali s pomočjo telefonskih klicev. Sporočila so običajno poslana s **sumljivih elektronskih naslovov**, pogosto so zapisana v **tujem jeziku ali v nepravilni slovenščini**. Vsem je skupno to, da prejemnika nagovarjajo h **kliku na povezavo v sporočilu**, običajno pod krinko nekega nepredvidenega dogodka, ki zahteva hitro ukrepanje. Primer: pod pretvezo, da sporočilo pošilja banka ali hranilnica, vas obvestijo, da je vaš račun ogrožen ali zaklenjen oz. blokiran in da je zato treba klikniti na priloženo povezavo ter tam potrditi ali zavrniti transakcijo. Povezava v resnici vodi na **lažno spletno stran**, ki zahteva vpis uporabniškega imena, gesla in drugih osebnih podatkov. Sporočilo običajno vsebuje **grafične elemente in podobo ciljane storitve**, npr. mobilnih ali spletnih bank.

Seveda gre za **lažne povezave** in **lažna sporočila,** zato je najbolje takšna sporočila **izbrisati** in **nanje ne odgovarjati**.

Kaj pa, če ste na lažno povezavo že kliknili?

Če ste povezavo že odprli in:

- vnesli podatke za vstop v spletno ali mobilno aplikacijo vaše banke, je dostopno geslo najbolje takoj **preventivno zamenjati;**
- vnesli podatke svoje bančne kartice, je najbolje **kartico nemudoma blokirati,** kar storite s klicem na telefonsko številko kartičnega servisnega centra banke, ki je zapisana na hrbtni strani vaše kartice, ali s klicem na kontaktni center banke ali hranilnice.

Če ste v vaši spletni ali mobilni banki morebiti že potrdili kakšen plačilni nalog, ki so ga vnesli goljufi, o tem nemudoma obvestite svojo banko ali hranilnico.

PR koordinacija aleksandra.zibrat@zbs-giz.si
tel.: 01 24 29 758, 031 716 589
www.zbs-giz.si

Uporabniki spletnih ali mobilnih aplikacij moramo biti namreč še posebej pozorni tudi pri potrjevanju zahtev za plačilo – **potrdite le zahteve za plačilne naloge, ki ste jih v bančno aplikacijo vnesli sami**.

Ne pozabite!

Banke ali hranilnice od vas nikoli ne bodo zahtevale, da vnašate svoje prijavne podatke ali podatke o karticah v spletne povezave, poslane prek elektronskih ali SMS-sporočil – to je lahko prvi znak, da gre za prevaro. Če niste prepričani o verodostojnosti prejetega sporočila, raje to preverite pri svoji banki ali hranilnici.

Več o tem, kakšne trike uporabljajo spletni goljufi, da bi se dokopali do vaših podatkov, lahko preberete na spletni strani slovenskega nacionalnega odzivnega centra za kibernetsko varnost SI-CERT na naslovu: Spet o phishingu - Varni na internetu.

Združenje bank Slovenije
Ljubljana, 27. januar 2022

PR koordinacija aleksandra.zibrat@zbs-giz.si
tel.: 01 24 29 758, 031 716 589
www.zbs-giz.si