

## Obvestilo o poskusih zlorab plačilnih kartic

Spoštovani,

obveščamo vas, da zaznavamo vse pogostejše poskuse zlorab plačilnih kartic (t. i. phishing napadi), ki ciljajo na uporabnike, ki prodajajo izdelke prek spletnih malih oglasov.

Po oddaji malega oglasa prodajalca po SMS-sporočilu ali prek mobilnih aplikacij za sporočanje (npr. Viber, WhatsApp, Messenger itd.) kmalu kontaktira potencialni kupec, pri čemer uporabi lažni profil v aplikaciji. Osebo, ki je poslala sporočilo, zanima, ali je oglas še aktualen, nato se po še nekaj komunikacije odloči za nakup in predlaga dostavo prek kurirske službe (GLS, DPD, UPS, Pošta Slovenije itd.) in pošlje spletno povezavo (»link«), prek katere naj bi z vpisom podatkov o plačilni kartici prodajalec prejel plačilo za prodajani izdelek.

Potrditev spletne povezave prejemnika sporočila preusmeri na lažno spletno stran, kjer naj bi vnesel osebne podatke in podatke o plačilni kartici, za tem pa vnos in izvršitev transakcije potrdil z uporabo močne avtentikacije z uporabo storitve Rekono (Rekono OnePass – vnos PIN ali uporaba biometrične avtentikacije za vstop v aplikacijo in potrditev transakcije – ali Rekono SMS OTP – vnos enkratnega gesla, ki ga imetnik kartice prejme prek SMS-sporočila na svoj telefon, in potrditev transakcije), ki jo imetnik kartice uporablja za potrjevanje spletnih plačil. Med postopkom vnosa osebnih podatkov in podatkov o plačilni kartici napadalec celo nudi podporo uporabniku in ga vodi čez postopek. Pri tem ta lahko navaja različne razloge, zakaj je treba vnesti podatke o kartici, in lahko še posebej poudarja, da s potrditvijo transakcije ne bo izvedena obremenitev, temveč odobritev.

Če imetnik kartice sledi napotkom in jih upošteva, s potrditvijo transakcije z močno avtentikacijo z uporabo storitve Rekono nevede potrdi transakcijo, ki bremeni njegov račun oziroma plačilno kartico v znesku, ki je praviloma lahko tudi precej višji od zneska, ki naj bi ga prejel za prodano blago.

Ker je plačilo potrjeno z močno avtentikacijo, je uspešnost reklamacijskega postopka otežena ali celo nemogoča.

Svetujemo vam, da ste pozorni in pazljivi ob uporabi in posredovanju podatkov o svoji plačilni kartici in enkratnega gesla, ki ga uporabljate za potrjevanje spletnih plačil.

V primeru, da ste po potrditvi spletne povezave na lažni spletni strani vnesli svoje podatke in to tudi potrdili z vnosom enkratnega gesla, nemudoma kontaktirajte banko na telefonsko številko: 01 589 57 00.

Lep pozdrav.

BKS Bank AG, Bančna podružnica

Ljubljana, 9. 6. 2023