HNB FINANCIJSKA PISMENOST

PRIJEVARE POVEZANE SA SOCIJALNIM INŽENJERINGOM

ZAŠTITITE SE

Socijalni inženjering obuhvaća niz tehnika kojima napadač iskorištavanjem ljudskih pogrešaka i slabosti utječe na žrtvu kako bi je prevario, odnosno naveo da učini nešto što nije u njezinu interesu. Posljedice takve prijevare najčešće su ostvarivanje nelegalne imovinske koristi, pristup povjerljivim informacijama ili drugim resursima koje napadač može zloupotrijebiti.

Donosimo nekoliko savjeta o tome kako se zaštititi od uobičajenih oblika online socijalnog inženjeringa.

Prijevare ulaganja / dobrotvorne organizacije

Obećava vam se brza i laka zarada. Ponuda koju ste dobili zvuči predobro da bi bila istinita. Osim toga, dobili ste molbu za donaciju u dobrotvorne svrhe.

Provjerite izvor informacija i na vrijeme se raspitajte kome uplaćujete svoj novac!

Prijevare s računima

Prijatelji, klijenti ili dobavljači navode vas da platite buduće račune na drugi račun za plaćanje.

Javite se izravno osobi koja vam je uputila zamolbu i provjerite razloge izmjene broja računa! Može se raditi o lažnom računu.

Budite osobito oprezni u vezi s tim kome upućujete instant plaćanja ako primatelja plaćanja određujete prema broju telefona, e-adresi ili OIB-u.

Krađa identiteta

Putem društvenih mreža, telefonskim pozivom, porukom ili e-poštom nepoznate osobe koje se lažno predstavljaju kao zaposlenici određene institucije nude vam razne pogodnosti, za čiju im realizaciju trebaju vaši osobni podaci ili financijske informacije.

Nikome ne otkrivajte osobne podatke, podatke s kartice ili PIN!

Krivotvorene mrežne stranice

Lažnom porukom poslana vam je poveznica koja vas navodi da se spajate na svoju banku, ali u stvarnosti se spajate na lažnu stranicu koja ima postavljenu drukčiju pristupnu adresu. Unosom podataka prevaranti će prikupiti vaše osobne podatke ili podatke s kartice.

Internetskom bankarstvu i servisima za plaćanje uvijek pristupajte izravno, a ne preko poveznice! Nakon što upišete podatke i autorizirate transakciju 3Dsecure kodom koji će vam poslati banka, iznos će biti plaćen.

Krađa kartičnih podataka

Pri kupnji ili prodaji robe preko oglasa osoba s kojom dogovarate kupoprodaju traži od vas sve podatke s kartice, uključujući CVV/CVC broj s poleđine kartice kojim se može odobriti plaćanje.

Nikome ne ustupajte podatke koji se nalaze na kartici, posebice ne CVV/CVC broj! Nikada ne šaljite nepoznatima fotografije svoje platne kartice! Za uplatu na vaš račun dovoljan je samo vaš IBAN i nijedan drugi podatak s vaše kartice.

O različitim rizičnim ponašanjima na internetu, kao što su korištenje jednostavne lozinke ili neprovjeravanje izvora informacija, informirajte se i na stranicama Nacionalnog CERT-a, tijela za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj (https://naivci.hr/#Uvod).

Ukratko

Ne nasjedajte na primamljive online ponude u kojima se nudi velika i laka zarada. **Ne uplaćujte novac nikome bez prethodne provjere** zatražene transakcije i onoga koji ju traži. **Ne pristupajte internetskom bankarstvu i servisima za plaćanje preko poveznica**. **Ne ustupajte nikome podatke** s platnih kartica kao ni osobne podatke.

HRVATSKA NARODNA BANKA

Trg hrvatskih velikana 3, 10000 Zagreb
www.hnb.hr