CROATIA BANKA	**Podizanja svijesti o informacijskoj sigurnosti klijenata CROATIA banke**
Tema: Socijalni inženjering	

Socijalni inženjering je skupni naziv za niz tehnika pomoću kojih zlonamjerni pojedinac, iskorištavanjem ljudskih pogrešaka i slabosti, utječe na druge kako bi ih naveo da učine nešto što nije u njihovom interesu. Socijalni se inženjering najčešće koristi u svrhu otkrivanja povjerljivih informacija ili dobivanja pristupa nekim drugim resursima do kojih napadač inače ne bi mogao doći.

Napadači se često služe ovom tehnikom jer im za uspješan napad nije potrebno složeno probijanje korisnikove sigurnosne zaštite, korištenje ranjivosti njegovog softvera i sl.

Napadači uvijek žele ostaviti **dojam legitimnosti**, odnosno **uvjerljivosti**. Tako npr. u porukama elektroničke pošte često navedu neki poznati podatak o korisniku kao što su ime, prezime, datum rođenja i sl. Napadači u nekim slučajevima šalju i veću količinu poruka kako bi stekli **povjerenje** ciljanih korisnika i nagnali ih da učine ono što oni žele. Napadači se mogu usmjeriti prema prikupljanju detaljnih informacija vezanih uz zasebnog korisnika kao i prikupljanju osnovnih informacija o velikom broju korisnika.

Socijalni inženjering najčešće susrećemo u 3 različita oblika:

- **phishing** - odnosi se na slanje poruka s izvora koji djeluje pouzdano u svrhu dobivanja raznih informacija (npr. poruka „od strane banke“ u kojoj se zahtjeva dostava broja kreditne kartice, zahtjev za dostavom osobnih podataka poslan „od strane Porezne uprave“ i sl.),
- **vishing** - podrazumijeva sakupljanje informacija putem telefona, često uz lažiranje broja pozivatelja,
- **impersonation** - uključuje dobivanje pristupa informacijama i utjecaja korištenjem lažnog identiteta.

Umanjiti mogućnost uspješnog provođenja socijalnog inženjeringa možemo tako što ćemo se upoznati s vrijednostima podataka, te provjeravati identitet osoba s kojima stupamo u kontakt putem maila i Interneta. **S povjerljivim podacima potrebno je postupati odgovorno i promišljeno te smireno djelovati u potencijalno nesigurnim situacijama** (npr. unutar phishing poruka često se zahtjeva žurna reakcija korisnika što povećava vjerojatnost da korisnik nepromišljeno reagira).

Važno je osvijestiti činjenicu kako se tehnike napada usavršavaju svakodnevno i kako ne postoji univerzalna zaštita za sve oblike napada. Bitno je kritički promatrati svoju okolinu te se **služiti Internetom odgovorno i savjesno** kako bi umanjili mogućnost napada te pravovremeno i ispravno reagirali.

Svaki korisnik se može do određene mjere zaštiti od ove vrste napada provođenjem preventivnih koraka kao što su:

- prije otvaranja priloga ili poduzimanja nekih drugih radnji zahtijevanih u e-mail poruci provjerite e-mail pošiljatelja te mu, ako je e-mail sumnjiv, pošaljite odvojen e-mail kako biste utvrdili da se radi o legitimnoj poruci,
- nemojte otvarati linkove unutar sumnjivih (pošiljatelja vam je nepoznat, e-mail poruku niste očekivali, unutar poruke se zahtjeva provođenje radnji kao što su otkrivanje Vaših osobnih podatka, uplata financijskih sredstava i sl.) e-mail poruka,

- nemojte otvarati arhivske (ZIP, RAR, 7zip i dr.) datoteke unutar sumnjivih e-mail poruka,
- ne posjećujte nepouzdane Internet stranice (npr. kocka, klađenje, torrent i dr.).

Lijep pozdrav,

Croatia banka d.d.