KRAĐA IDENTITETA POZIVOM

tzv. Vishing (kombinacija riječi Voice i Phising) je telefonska prevara u kojoj prevaranti pokušavaju navesti žrtvu da otkrije svoje lične, finansijske ili sigurnosne podatke, ili da im uplate novčana sredstva.

KAKO SE ZAŠTITITI?

- Budite oprezni kada primate neočekivani telefonski poziv. Uzmite broj pozivatelja i recite da ćete ih nazvati.
- U svrhu potvrđivanja identiteta, potražite telefonski broj organizacije-firme i izravno ih kontaktirajte, nemojte zvati na telefonski broj koji ste dobili.
- Prevaranti mogu naći vaše podatke online npr. na društvenim mrežama, aplikacijama (Viber ili sl.) ili internet pretraživačima. Nemojte misliti da je prevarant ta osoba za koju se predstavlja samo zato što zna takve pojedinosti o vama.
- Nikada nemojte drugima davati vaš broj kartice (broj u dnu na prednjoj strani bankovne kartice) ili CVC/CVV brojeve sa poleđine kartice, neka vam to bude prvi pokazatelj da "nešto ne štima". Nemojte davati PIN kartice ili lozinku za online bankarstvo. Ove podatke vaša banka ili neka druga institucija neće nikada tražiti!!!
- Ne šaljite novac na druge bankovne račune na osnovu telefonskih zahtjeva nepoznatih osoba. Ako primate poziv koji vam je sumnjiv a tema razgovora budu vaši bankovni podaci, odmah obavijestite vašu banku.

PHISING – MREŽNA KRAĐA IDENTITETA

Krađa identiteta odnosi se na lažne poruke e-pošte koje imaju za cilj prevaru primatelja i navođenje na dijeljenje ličnih, sigurnosnih ili bankovnih podataka.

KAKO PREPOZNATI ZNAKOVE?

- Poruke izgledaju identično tipu korespodencije koju banka ima sa klijentima
- Prevaranti repliciraju logotipe, izgled i ton stvarnih e-poruka
- Traže preuzimanje priloženih dokumenata ili da kliknete na poveznicu
- Koriste izraze koji ostavljaju dojam hitnosti

ŠTA MOŽETE UČINITI?

- Redovno ažurirajte softver uključujući preglednike, antivirusni i operativni sistem
- Budite posebno oprezni ako se u poruci e-pošte od strane „banke" traže osjetljivi podaci (npr. lozinka za online bankarstvo, brojevi sa vaše kartice i sl.)
- Detaljno pregledajte e-poštu: uporedite adresu sa prethodnim porukama primljenim od banke. Provjerite tačnost pravopisa i gramatike
- Nemojte odgovarati na sumnjive e-poruke nego je proslijedite svojoj banci na način da sami upišete adresu od banke
- Nemojte kliknuti na poveznice ili dokumente u prilogu.
- Ako vam je nešto sumnjivo, nazovite banku ili provjerite lično na šalteru banke.

MUP TK

UPRAVA POLICIJE

SIGURNI NA MREŽI

- **LAŽNE STRANICE BANAKA**
- **PHISHING – MREŽNA KRAĐA IDENTITETA**
- **KRAĐA IDENTITETA POZIVOM**
- **INTERNETSKA SIGURNOST KOD KUĆE**
- **ROMANTIČNA PREVARA**

122 NE BUDI ŽRTVA 122

WWW.MUPTK.BA

LAŽNE STRANICE BANAKA

Kompromitovana E-pošta koja dolazi kao da je od banke, obično sadrži poveznice koje vode na lažnu stranicu banke, gdje će vam tražiti da otkrijete svoje lične i finansijske podatke.

KAKO PREPOZNATI ZNAKOVE?

Lažne stranice banaka izgledaju gotovo identično njihovim pravim stranicama. Na takvim stranicama često će iskočiti „prozor“ koji traži da unesete bankovne podatke (brojeve i cvc/cvv kodove kartica, PIN, lozinka za online bankarstvo). Stvarne stranice banaka ne koriste takve „prozore“.
Ovakve stranice često prikazuju:

- **Hitnost:** takve poruke nećete pronaći na pravim stranicama banke.
- **Loš dizajn:** budite posebno oprezni sa stranicama koje imaju čudan dizajn ili pogreške u pravopisu i gramatici.
- **Skočni prozori:** obično se koriste za prikupljanje osjetljivih informacija od vas. Nemojte kliknuti i unijeti vaše lične ili bankovne podatke.

ŠTA MOŽETE UČINITI?

- Nikada nemojte kliknuti na poveznice u porukama u kojima se tvrdi da vode do stranice vaše banke. Uvijek upišite vezu ručno ili koristite vezu iz popisa u favoritima
- Koristite preglednike koji omogućuju blokiranje skočnih prozora
- Ako vam treba skrenuti pažnju na nešto važno, banka će to uvijek učiniti nakon što pristupite svom online računu.

INTERNETSKA SIGURNOST KOD KUĆE

- Napravite sigurnosne kopije dokumenata i redovno ažurirajte softver
- Wi-Fi: Uvijek promijenite zadanu lozinku za ruter
- Provjerite dozvole za aplikacije i izbrišite one koje ne koristite
- Osigurajte elektroničke uređaje lozinkama, PIN-om ili biometrijskim podacima. Redovno mijenjajte PIN-ove i lozinke. Koristite dvostepenu autentifikaciju gdje god je to moguće
- Ne koristite iste lozinke za više različitih uređaja ili računa
- Provjerite postavke privatnosti na računima društvenih mreža.

ŠTA MOŽETE UČINITI?

- Ne odgovarajte na sumnjive poruke ili pozice
- Ne otvarajte priloge ili poveznice u sumnjivim e-mailovima ili porukama
- Ne dijelite podatke o svojoj bankovnoj kartici ili finansijama
- Ne kupujte stvari od sumnjivih prodavača ili stvari koje su već negdje drugo rasprodane
- Ne šaljite novac nepoznatim osobama ili organizacijama
- Ne prosljeđujte vijesti iz nepouzdanih izvora
- Ne donirajte novac humanitenim organizacijama bez provjere autentičnosti
- Provjerite postavke sigurnosti i privatnosti pametnih igračaka
- Koristite opciju roditeljskog nadzora internetske aktivnosti djece
- Promjenite tvorničku lozinku i redovno ažurirajte softver
- Razgovarajte sa djecom o internetskoj sigurnosti, saslušajte njihova iskustva te im objasnite važnost sigurnosti na internetu
- Ako postanete žrtva kompjuterskog krivičnog djela, obavezno prijavite policiji.

ROMANTIČNA PREVARA

Prevaranti ciljaju na žrtve na stranicama za upoznavanje ali koriste i društvene mreže ili e-poštu da uspostave kontakt.

KAKO PREPOZNATI ZNAKOVE?

- Neko koga ste nedavno online upoznali, iskazuje snažne osjećaje za vas tražeći privatan razgovor
- Poruke su često loše napisane i nejasne
- Njihovi online profili često nisu u skladu sa onim što govore, te mogu tražiti da pošaljete intimne slike ili videozapise o sebi
- Prvo zadobiju vaše povjerenje a zatim traže novac, darove ili podatke o bankovnom računu /kartici
- Ako ne pošaljete novac često ćete biti meta ucjenjivanja a ako ga pošaljete, tražit će još novca.

ŠTA MOŽETE UČINITI?

- Budite vrlo oprezni koliko privatnih podataka dijelite na društvenim mrežama i stranicama za upoznavanje
- Uvijek budite svjesni rizika, prevaranti su prisutni i na najsigurnijim web stranicama i svim društvenim mrežama
- Provjerite podatke, fotografije i profil te osobe da vidite jesu li upotrebljavani negdje drugo
- Pazite na pravopisne i gramatičke greške, nedosljednosti u pričama i izgovorima da kamera ne radi ili sl.
- Ne dijelite nikakav kompromitirajući materijal sa kojim bi vas neko mogao poslije ucjenjivati
- Ako se dogovorite na susret sa takvom osobom, uvijek recite rodbini i prijateljima gdje idete
- Nikada ne šaljite novac ili podatke o svojoj bankovnoj kartici, lozinkama za internet bankarstvo ili kopije ličnih dokumenata
- Izbjegavajte bilo kakva plaćanja unaprijed i nemojte slati novac za nekoga drugoga.
- Sačuvajte svu komunikaciju poput chat poruka
- Ako ste dali podatke o vašem bankovnom računu, odmah prijavite banci. Prijavite policiji.