PODIZANJE SVIJESTI KLIJENATA O SIGURNOSTI INFORMACIJA I INFORMACIONIH SISTEMA

PRIVREDNA BANKA SARAJEVO

Krađa identiteta i on-line prevare postaju jedan od najbrže rastućih krimanala u svijetu, a i u Bosni i Hercegovini.

U Privrednoj banci Sarajevo d.d. Sarajevo vrlo ozbiljno pristupamo zaštiti vaših podataka. Smatramo da je zaštita vaših ličnih i povjerljivih podataka obaveza svakog našeg zaposlenika, te Banka u skladu sa svojim godišnjim planom vrši obuku i treninge svih svojih zaposlenika i ulaže značajne finansijske, tehničke i ljudske resurse u implementaciju najsavremenijih rješenja kojima postižemo adekvatnu zaštitu podataka naših cijenjenih klijenata. S obzirom da broj prijavljenih prevara i napada raste iz dana u dan, ovim putem podstičemo i naše klijente da poduzmu potrebne korake kako bi zaštitili sebe i svoje podatke.

U nastavku vam dajemo nekoliko kratkih informacija i načina kako da se zaštitite:

1

Koristite antivirusnu zaštitu na vašim računarima i pametnim telefonima. Ovo je 1.(prvi) i najvažniji korak koji trebate poduzeti u cilju zaštite vaših računara i podataka koji se nalaze na njima od zlonamjernih napadača, virusa i drugog malicioznog koda. Na tržištu postoji veliki broj ponuđača antivirusnog softvera, od kojih se neki plaćaju a drugi su besplatni. Ukoliko koristite besplatnu opciju, provjerite da li je softver izdat od provjerenog proizvođača i istražite kompaniju i njihov proizvod prije nego ga istalirate na vaše uređaje.

2

Nijedan zaposlenik Privredne banke Sarajevo vas neće kontaktirati putem telefona ili elektronske pošte kako bi tražili povjerljive ili lične podatke, kao što su brojevi računa, jedinstveni matični broj, broj lične karte ili drugog identifikacionog dokumenta i slično. Ako se odlučite kontaktirati Privrednu banku Sarajevo putem elektronske pošte, molimo vas da ne šaljete povjerljive podatke putem redovne elektronske pošte koja nije enkriptovana i zaštićena. Ukoliko trebate poslati provjerljive ili lične podatke, kontaktirajte Banku kako bi vas uputili koji je siguran način da to uradite.

3

Na vašim računarima koristite isključivo licencirani, provjereni softver za operativne sisteme i ostale aplikacije, te ih redovno ažurirajte u skladu sa preporukama proizvođača.

4

Ne otvarajte elektronske poruke od sumnjivih pošiljaoca i/ili sa sumnjivim prilozima. Potreban je poseban oprez prije otvaranja i/ili preuzimanja priloga ili klikanja linkova koji su stigli s elektronskom poštom, čak i ako su od poznatog pošiljaoca. Ako niste potpuno uvjereni u bezopasnost priloga ili linka, a ne možete kontaktirati pošiljaoca kako bi potvrdio, potrebno je izbrisati poruku. Nikad ne idite na stranice gde koristite poverljive podatke putem linkova koje ste dobili u email-u već isključivo kucanjem adrese u vašem internet pretraživaču.

5

Sve povjerljive podatke u elektronskom ili papirnatom obliku uništite na adekvatan način ukoliko vam više nisu potrebne (prenosive medije za pohranjivanje podataka, papirnate dokumetne i izvode Banke, stare računare i slično).

6

Uspostavite adekvatne sisteme i kontrole poslovanja kako bi smanjili rizike povezane sa elektronskim prevarama, a posebno ukoliko dokumentaciju kao osnov za plaćanje dobijate putem maila. Koristeći raznorazne tehnike napadači vrlo lako mogu izvršiti izmjenu podataka novčane transakcije navedene u mailu, te na taj način vas navesti da uplatu izvršite na bankovne račune napadača, umjesto vašeg poslovnog partnera. Klijentima se preporučuje da obavezno uspostave kontrolu i provjeru validnosti računa na koji se vrši prenos novčanih sredstava.

7

Koristite raznolike i kvalitetne lozinke. Ovo se posebno odnosi na važne stranice koje sadržavaju podatke o računima, brojevima kartica i ostale lične podatke. Često mijenjajte lozinke i ne koristite iste lozinke za različite prijave/račune. Lozinke nemojte pohranjivati ni prikazivati u čitljivom obliku izvan adekvatno osigurane okoline. Nemojte dijeliti svoje lozinke sa drugim zaposlenicima ili članovima porodice. Ne koristite vlastita imena, imena djece ili kućnih ljubimaca u vašim lozinkama i izbjegavajte korištenje običnih i standardiziranih riječi. Prilikom izbora lozinke koristite kombinaciju brojeva, specijalnih znakova i malih i velikih slova. Lozinke treba izmjeniti ukoliko se pojavi i najmanja sumnja da su njihova povjerljivost ili integritet narušeni.

8 Nemojte koristiti javne računare ili otvorene bežične mreže (Wi-Fi) za slanje povjerljivih podataka ili osjetljive transkacije putem elektronskog bankarstva. Ukoliko pristupate Interentu putem javnih, nezaštićenih mreža trebate biti svjesni da zlonamjerni napadači mogu vrlo lako pristupiti vašim uređajima i doći do vaših povjerljivih podataka.

9 Veoma je bitno da u svakom telefonskom razgovoru budete sigurni sa kim razgovarate i da ne iznosite informacije ukoliko niste u stanju da identificirate osobu sa druge strane. Banka nikada neće tražiti da otkrivate povjerljive podatke putem telefona.

10 Redovno pregledajte vaše transakcije i izvode koje vam dostavlja Banka. Svaku uočenu nepravilnost ili sumnju odmah prijavite Banci, kako bi na vrijeme i zajedno mogli spriječiti zlonamjerne napadače u njihovoj namjeri da dođu do vaših povjerljivih podataka i iskoriste ih u kriminalne svrhe. I sam pokušaj krađe je krivično djelo. Za prijavu ili više informacija kontaktirajte nas putem telefona **033 278 520 ili na info@pbs.ba.**

Phishing

Phishing ili mrežna krađa identiteta (phishing od engleske riječi fishing, što znači pecanje) je vrsta prevare u kojoj napadači lažnim predstavljanjem i različitim „mamcima“ pokušavaju „upecati“ žrtvu. Phishing se može iskoristiti tako da se osobi ukrade novac ili nanese neka druga šteta (provala u žrtvin e-mail račun, krađa identiteta i slično). Pošiljatelj navodi žrtvu da otkrije osobne informacije (obično finansijske) upisivanjem istih na internetskoj adresi navedenoj u elektronskoj poruci. Navedena adresa (link) je vrlo sličnog imena kao i stvarna adresa. Tehnike koje neovlašteni korisnici koriste u ovu svrhu vrlo su složene što uzrokuje značajan broj žrtava phishing napada. Broj phishing napada i njihova sofisticiranost raste svakim danom, a količina poruka koja se šalje broji se u milionima.

Kako izgleda phishing poruka?

Poruka može izgledati kao obavijest iz banke, internetske trgovine i sl., no žrtvu se navodi kliknuti na link koji je "udica" na kojoj počinitelj internetskog zločina izvlači tražene podatke od žrtava.

Žrtve potom na njoj upišu lične informacije (u poruci se često navodi da korisnik treba potvrditi ili promijeniti podatke)

Kad korisnik upiše podatke na lažnoj stranici, informacije dolaze do vlasnika lažne stranice

Lažna internetska stranica izgleda (skoro) identična pravoj, ali URL u adresnoj traci joj je drugačiji

Socijalni inžinjering

Socijalni inžinjering je vrsta napada s ciljem nagovaranja korisnika da ispune zahtjeve napadača. Tu se prvenstveno radi o načinu skupljanja podataka do kojih napadač ne bi mogao doći legalnim putem. Pri tome se napad usmjerava na najslabiju kariku cjelokupnog lanca – ljudski faktor.

Najčešće metode prijevare su:

• Lažno predstavljanje – najčešća metoda napada, postupak u kojem se napadač predstavlja kao neka druga osoba;

• Uvjeravanje/nagovaranje – nagovaranje ili uvjeravanje je postupak pri kojem napadač nagovora i uvjerava žrtvu da obavi postupke koje mu nalaže napadač.

• Stvaranje odgovarajuće situacije – napadač stvara “plodno tlo” za izvršenje napada na način da iskoristi žrtvine slabosti, zbližavanje sa žrtvom kako bi došao do informacija, iskorištavanje nespremnosti ili nepažnju žrtve kako bi učinila pogrešan potez i slično.

• Moralna odgovoronost – žrtva pokuša pomoći napadaču jer se osjeća da je to njena moralna obaveza, žrtve nisu ni svjesne da na taj način odaju korisne informacije napadaču.

• Želja za pomaganjem – iskorištavanje želje žrtve da pomogne drugima. Čest je slučaj da napadač uvjeri žrtvu da će on postupiti isto u situaciji kada žrtvi bude potrebna pomoć.

• Iskorištavanje starih veza i korupcija – napadač stvara odnos koji je dovoljan za sticanje povjerenja ili potkupljuje korisnika, koji mu odaje željene informacije.

Način izvršenja napada:

• Telefonski inžinjering – jedan od najčešćih i najlakših načina izvršavanja socijalnog inžinjeringa; napadač naziva jednog od zaposlenika, te svojim komunikacijskim vještinama lako stiče njegovo povjerenje;

• Pretraživanje otpada – jedan od načina sakupljanja informacija je pretraživanje otpada pri čemu se saznaje mnogo korisnih informacija za izvođenje napada;

• Korištenjem interneta – brojni su načini prikupljanja informacija putem internet, a najčešći je slanjem lažnih poruka, kojima napadač potiče korisnika na odavanje vrlo važnih i tajnih informacija.

• Zavirivanje – tip socijalnog inžinjeringa pri kojem napadač pokušava očitati žrtvine pokrete kako bi dobili željene podatke (npr. posmatranje pokreta rukom pri upisivanju lozinke prilikom prijave na sistem).

• Forenzička analiza – do korisnih informacija napadač može doći pregledom nepažljivo odbačenih medija za pohranjivanje podataka.

PRIVREDNA BANKA SARAJEVO

Spoofing

Spoofing u širem smislu znači da ste dobili poruku u elektronskom obliku od osobe koju poznajete i imate povjerenja u nju. U stvari vi ste dobili poruku od osobe koja je na neki način ukrala virtuelni identitet osobe koju poznajete. Tipičnim lažnim predstavljanjem zlonamjerni napadač pokušava da izvuče vaše povjerljive podatke.

Postoje tri tipa spoofinga na internetu:

Email spoofing - Relativno prostim mijenjanjem uzglavlja email poruke dobijate poruku koja liči ili je ista kao email koji stiže iz banke ili druge institucije. Tipičan primjer za to su spam poruke. Više od 80 % elektronske pošte na internetu čini spam. Najčešće poruke koje dobijate u ovakvim email porukama su da vam je istekla lozinka ili zbog sigurnosti morate da promijenite lozinku na vašem računu u banci.

IP spoofing (internet protocol spoofing) - Sve što radite na internetu stiže ili se šalje u paketima, a svaki paket nosi adresu svog pošiljaoca. Ideja internet kriminalaca sastoji se u tome da se stvore paketi sa lažnom adresom izvora. Ovakav vid se koristi prilikom napada na mrežnu infrastrukturu, gdje se pokušava da se zavara operativni sistem računara primaoca i njegovi sistemi za autentifikaciju kako bi napadači preuzeli kontrolu nad računarima i lokalnom mrežom.

URL spoofing - To je pokušaj da se Universal Resource Locator (URL) ili adresa lažne web stranice prikaže kao URL prave stranice. Za ovu metodu se najčešće koriste sigurnosni propusti u internet pretraživačima. Lažne web adrese dobijate najčešće u email porukama a na njih odlazite nesmotrenim klikanjem na linkove u elektronskoj poruci.

Jednostavnost, dostupnost, efikasnost i sigurnost elektronskog poslovanja osnovne su prednosti u odnosu na klasično poslovanje, kako za Banke tako i za naše klijente. Iako su elektronske prevare dio naše svakodnevnice, klijenti ne trebaju zazirati od korištenja tehnologija i inovativnih rješenja koja nam olakšavaju poslovanje. Pridržavajući se gore navedenih smjernica i uz manji oprez, možete jednostavno zaštiti sebe i svoj novac.

PODIZANJE SVIJESTI KLIJENATA O SIGURNOSTI INFORMACIJA I INFORMACIONIH SISTEMA