Uvod

U cilju unapređenja svojih usluga banke su, kao jedan od prioriteta svog poslovanja, uvele mogućnost elektronskog bankarstva. To je rezultiralo velikom ekspanzijom ovakvog oblika bankarskog poslovanja u Republici Srbiji u poslednjih nekoliko godina.
Činjenica je da korisnici bankarskih usluga, korišćenjem '*online*' plaćanja, imaju veliku uštedu vremena što im ostavlja prostor za unapređenje poslovanja, ali i više slobodnog vremena koje mogu provesti u krugu porodice, prijatelja ili na bilo koji drugi način.
Korišćenjem elektronskog bankarstva ušteda vremena je i na strani banaka, kao pružaoca ovih usluga i ovakav vid uštede im pomaže u kreiranju novih proizvoda i veće dostupnosti. Zbog navedenih pogodnosti, sasvim je jasno zašto se broj korisnika ovih usluga svakodnevno uvećava.
Ono što predstavlja eventualnu pretnju prilikom korišćenja elektronskog bankarstva, jeste moguća zloupotreba ovakvog pristupa bankovnim računima od strane napadača, odnosno hakera.
Navešćemo neke od najčešćih vidova moguće zloupotrebe kada je reč o elektronskom bankarstvu.

Fišing ('*Fishing*') napadi

'Fishing' napadi predstavljaju najzastupljeniji vid moguće zloupotrebe od strane napadača. U okviru ovakvog napada, hakeri pokušavaju da dođu do vaših kredencijala (korisničkog imena i lozinke) kojima pristupate aplikaciji za elektronsko bankarstvo, broju vašeg računa, vašem matičnom broju i sl. Tom prilikom oni se predstavljaju kao vaša banka i u tekstu mejla vam traže da izmenite svoje kredencijale, a zatim proslede link ka lažnoj veb stranici banke na kojem je predviđeno da uradite ovu izmenu. Na ovaj način dolaze do vaših podataka, koji im omogućavaju pristup i zloupotrebu vaših računa. Dodatno, hakeri se mogu predstaviti i kao neka druga institucija, dok se u nekim slučajevima mogu predstaviti čak i kao fizičko lice. Ono što treba znati je da banka u kojoj imate otvoren račun, ili bilo koja druga legitimna institucija vam ni u jednom slučaju neće tražiti da im date svoje kredencijale i zbog toga treba dodatno biti na oprezu ako vam se, prilikom logovanja ili korišćenja aplikacije za elektronsko bankarstvo, pojavi bilo kakva poruka u kojoj se od vas traži izmena ovakvih podataka. Kredencijale korisnici menjaju isključivo po sopstvenom nahođenju (npr. prilikom redovne promene lozinke), a nikako po nalogu nekog drugog subjekta.

Malver ('*Malware*') napadi

Maliciozni softver, poznatiji kao malver, je jedan od načina koji je često u upotrebi od strane napadača, kada govorimo o zloupotrebi aplikacije za elektronsko bankarstvo. Korišćenjem ovog softvera, napadači mogu izvršiti krađu podataka koji se tiču vašeg računa, zatim krađu računa, kao i kreiranje lažne Internet stranice banke, koju postavljaju na vaš računar i predstavljaju kao zvaničnu Internet stranicu za '*online*' transakcije.
Krađa podataka se izvršava tako što maliciozni softver prikupi podatke koje vi unosite prilikom kucanja na tastaturi u toku logovanja na aplikaciju elektronskog bankarstva. Tako prikupljene podatke haker može iskoristiti u bilo kom trenutku, jer ima sve što mu je neophodno za pristup vašem nalogu za elektronsko bankarstvo.

Prilikom logovanja na aplikaciju za elektronsko bankarstvo, odnosno na vaš '*e-bank*' nalog, maliciozni softver može pokrenuti skriveni prozor dodatnog Internet pretraživača, koji se postavi ispred legitimnog Internet sajta banke, kojem pokušavate da pristupite i tako izvrši prenos sredstava sa vašeg računa na bilo koji drugi račun koji haker odabere.

Korišćenjem malicioznog softvera, hakeri takođe mogu kreirati celokupnu lažnu Internet stranicu, koju mogu postaviti kao legitimnu. Ukoliko korisnik ne obrati pažnju, lako se može dogoditi da sve informacije učini dostupnim i time omogući neovlašćen pristup svom računu.
Iz tog razloga potrebno je obratiti posebnu pažnju da li u adresnoj liniji, koja se nalazi na vrhu stranice Internet pretraživača (počinje sa HTTP:// ili HTTPS://), stoji ispravna adresa internet stranice banke kojoj želite da pristupite, ili ne.
Neke od mogućih izmena mogu biti u vidu zamene brojeva i slova. Takav primer može biti u reči '*Online*' gde napadač slovo O zameni brojem 0 (nula), ili umesto domena '.rs' napiše npr. '.sr', dok preostali deo teksta bude nepromenjen i klikom na takav link vi izvršite logovanje na 'svoj e-bank' nalog, na lažnoj Internet stranici.

Preporuke

Navedeni primeri su samo neke od mogućih zloupotreba, a hakeri svakodnevno i vredno rade na tome da nađu nove načine kako da stignu do vašeg novca. U cilju sprečavanja moguće zloupotrebe, neophodno je voditi računa prilikom svakog logovanja na aplikaciju za elektronsko bankarstvo. Ovde pre svega mislimo na sledeće: kreiranje jakih lozinki koje u sebi treba da sadrže najmanje devet alfanumeričkih/znakovnih karaktera (koji uključuju velika i mala slova), njihovo čuvanje i nedeljenje sa drugim licima, zatim redovnu izmenu lozinke (preporuka je da najmanje jednom u tri meseca izmenite svoju lozinku), pažljivo otvaranje imejl poruka od pošiljaoca koji vam nisu poznati, izbegavanje klika na linkove iz imejl poruka koje vam se učine nelegitimnim, provera URL adresa za pristup aplikacijama na internet stranici banke i sl. Takođe, neophodno je instalirati antivirusni softver i vršiti redovno preporučeno ažuriranje verzija kad god je to moguće.
Primenom ovih preporuka u značajnoj meri smanjujete mogućnost bilo kog vida zloupotrebe vaših naloga za elektronsko bankarstvo, ali njihova apsolutna zaštita jednostavno nije moguća. Bar ne u ovom trenutku.