Bezbedno korišćenje digitalnih servisa Banke i interneta

Korisni saveti za bezbednije korišćenje interneta

Koristite najnovije verzije operativnog sistema

Redovno ažurirajte aplikacije na uređajima

Instalirajte i koristite najnovije verzije antivirus softvera

Ne prosleđujte svoje lične podatke (JMBG, korisničko ime, lozinku, broj kartice) putem društvenih mreža (facebook-a, twitter-a,..)

Ne odgovarajte na poruke koje su Vam stigle na e-mail od nepoznatog pošiljaoca i ne otvarajte priloge od istih

Korisni saveti za sigurnije i bezbednije korišćenje Mobilnog i Elektronskog Bankarstva

• Mobilnu aplikaciju Eurobank Direktne preuzmite samo sa zvaničnih internet platformi (Apple app-store i Google Play store)

• Na e-Banking aplikaciju logujte se samo putem zvaničnog sajta Eurobank Direktne

• Kreirajte "jaku" lozinku za pristup, koja sadrži kombinaciju slova i brojeva (bar jedno slovo veliko). Nemojte koristiti lako prepoznatljive lozinke, npr. Vaš datum rođenja ili lozinku 1234

• Nikada ne otkrivajte svoju lozinku drugom licu i izbegavajte automatska logovanja koja čuvaju (pamte) Vašu lozinku za pristup

• Redovno proveravajte podatke vezane za poslednju prijavu na m/e-Banking aplikaciju

• Nikada ne čuvajte svoj sertifikat za elektronski potpis na hard disku svog računara

• Ako primetite neku sumnjivu transakciju koju niste Vi kreirali i potpisali, molimo Vas odmah obavestite Banku

• Uvek se pravilno izlogujte iz aplikacije, obavezno upotrebom komandi za napuštanje i zatvaranje aplikacije

Razumevanje Internet pretnji

Pre nego što naučimo kako da se zaštitimo, moramo da naučimo koje su pretnje prisutne na internetu:

• **Phishing** je tehnika krađe podataka korisnika internet servisa putem obmane korisnika koji otvore link distribuiran (uglavnom) putem mejla i direktno pristupaju lažnom sajtu gde ostavljaju svoje podatke

• **Biznis e-mail prevara (Business E-mail Compromise - BEC)** je vrsta phishing prevare, gde sajber kriminalac, pretvarajući se da je poslovni saradnik ili rukovodilac firme, navodi žrtvu da izvrši određenu finansijsku transakciju, a novac ustvari, završi na računu napadača

• **Pharming** je tehnika koju hakeri koriste za preusmeravanje korisnika na lažni veb sajt u svrhu krađe poverljivih informacija, brojeva računa i ličnih podataka korisnika

• **Spam** je neželjeni e-mail koji sadrži informacije ili obaveštenja o proizvodima i uslugama za koje niste nikada izrazili interesovanje, a mogu biti i neprijatnog sadržaja i početna faza distribucije nekih od već spomenutih napada

• **Virus** je zlonamerni program koji je dizajniran da zarazi računar, brzo se šireći i kopirajući se iz jedne datoteke u drugu i pritom izaziva veliku štetu. Prenosi se uglavnom preko interneta, mejlova sa zaraženim prilozima i preko USB-a

• **Worms (Crvi)** su slični, osim što se brzo šire preko mreže da bi se kopirali na druge računare, bez ljudske pomoći

• **Browser hijacking** je zlonamerni softver koji modifikuje podešavanja internet pretraživača bez znanja korisnika, uglavnom u svrhu dodavanja neželjene reklame, a u najgorem slučaju i za prikupljanje korisničkih informacija za pristup e-B@nking i e-mail servisima (kao jedna od fazi većeg napada)

• **Ransomware** je malver koji zaključava računar, odnosno sve fajlove na njemu. Kako bi otključali računar, napadači od korisnika zahtevaju da plati otkupninu. Uglavnom se distribuira mejlom, u čijoj poruci se nalazi maliciozni link ili fajl za preuzimanje. Kada korisnik klikne na link ili preuzme zaraženi fajl, malver ulazi u sistem i lako se širi na ostale računare u mreži

• **Miner** za rudarenje kripto valuta funkcioniše tako što iskorišćava snagu zaraženog računara. Obe pretnje (ransomware i miner) su ove godine na samom vrhu liste sajber pretnji

From: direktor@firma.com

To: pera.finansije@firma.com

Subject: Uplata

Uvek sa posebnom pažnjom pročitajte bezbednosna uputstva i pridržavajte ih se. Uživajte u korišćenju interneta na bezbedan način!