

Uputstvo za prevenciju distribucije neželjene elektronske pošte

Saveti za fizička lica

Praktikujte pojačan oprez prilikom otvaranja mejlova koji u sebi sadrže priloge ili traže da dostavite osetljive podatke.

Nikada nemojte slati osetljive podatke kao što su vaše lozinke, brojevi platnih kartica, kodovi sa poledine platnih kartica, pin kodovi, slike platnih kartica i dr. Banka od Vas nikada neće tražiti ovakve podatke.

Vaše mejl naloge hostujte kod provajdera koji podržavaju bezbedno slanje i prijem poruka upotrebom modernih sistema zaštite i bezbednih protokola. Proverite da li su podešavanja ovih mehanizama podrazumevano uključena ili potražite uputstva kako da ih uključite i konfigurišete kako bi se dodatno zaštitili.

Saveti za pravna lica

Informišite se o mogućnostima koje nudi vaš provajder usluga. Proverite da li su podešavanja ovih mehanizama podrazumevano uključena ili potražite uputstva kako da ih uključite i konfigurišete kako bi se dodatno zaštitili. Ukoliko ste sami vlasnik servera za slanje i prijem elektronskih poruke tražite od tehničkog osoblja zaduženog za konfigurisanje vašeg servera da vam konfigurišu protokole za autentifikaciju i proveru elektronskih poruka. Pravilno korišćenje ovih protokola može značajno da smanji distribuciju lažiranih poruka.

Preporuke za bezbedno konfigurisanje sistema za prijem i slanje pošte

Pretnja: Lažno predstavljanje u ime vaše kompanije i obmanjivanje korisnika širom interneta
Prijem elektronske pošte sa lažnom informacijom o pošiljaocu poruke

Cilj: Prevencija prijema fišing mejlova kroz detekciju lažnih pošiljaoca
Prevencija krađe identiteta i zloupotreba domenskog imena kompanije

Registracijom SPF, DMARC i DKIM mehanizama značajno smanjujete mogućnost zloupotrebe vašeg domenskog imena u elektronskoj komunikaciji, i povećavate procenat detekcije lažiranih mejlova koji dolaze do vašeg mejl servera.

Sender Policy Framework SPF

Sistem za detekciju lažnih mejlova. U cilju iskorišćavanja prednosti ovog sistema potrebno je da registrujete SPF unos u svom DNS serveru (lično ili preko provajdera kod koga hostujete vaš domen).

DomainKeys Identified Mail DKIM

Standard kojim se obezbeđuje integritet poslatih i primljenih poruka uz pravilnu upotrebu javnih i privatnih kriptografskih ključeva

Domain-based Message Authentication, Reporting and Conformance DMARC

Standard koji omogućava vlasnicima domena da definišu polise kojima ukazuju primaocima mejlova kako da postupaju sa primljenom porukom. Na osnovu informacija koje dostavlja primalac moguće je pratiti dešavanja sa elektronskom poštom u njenom životnom ciklusu.

Sva tri servisa zahtevaju registraciju unosa u DNS serverima. Za pravilno korišćenje DMARC servisa podrazumeva se da su SPF i DKIM unosi ispravno registrovani.

Napomena Za pravilno funkcionisanje gore navedenih servisa potrebno je izvršiti konfiguraciju servera u skladu sa uputstvima proizvođača.

Implementacija SPF, DKIM i DMARC servisa

Izvršiti identifikaciju svih servera, servisa ili drugih entiteta koji imaju dozvolu za slanje pošte u vaše ime. Za sve identifikovane servere izvršiti registraciju SPF unosa.

Primer unosa: *v=spf1 a mx a:<domain/host> ip4:<ipaddress> -all*

Standardi iz oblasti bezbednog konfigurisanja i upotrebe elektronske pošte

Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1

<https://tools.ietf.org/html/rfc7208>

Domain-based Message Authentication, Reporting, and Conformance (DMARC)

<https://tools.ietf.org/html/rfc7489>

<https://dmarc.org/>

DomainKeys Identified Mail (DKIM) Signatures

<https://tools.ietf.org/html/rfc6376>

<http://dkim.org/>