

Prilog 4: Pravilnik o zaštiti od spama

Svrha

Internetom putuje sve više neželjenih komercijalnih poruka, tzv. spam. Masovne poruke elektroničke pošte najjeftiniji su način reklamiranja. Cijenu plaćaju korisnici i tvrtke, jer čitanje i brisanje neželjenih poruka troši radno vrijeme i umanjuje produktivnost.

Dio neželjenih poruka nastoji uvući primatelja u kriminalne aktivnosti, na primjer otvaranje računa za pranje novca, ili su prijevera, nastoje pobuditi samilost kako bi se izvukao novac (enlg. hoax). Za prepoznavanje ovakvih poruka korisnici mogu koristiti uslugu CARNet CERT-a Hoax recognizer.

Pravila za administratore

Administratori poslužitelja elektroničke pošte dužni su konfigurirati računala na taj način da se što više neželjenih poruka zaustavi (*spamassasin*).

Prva mogućnost jest da se definira ulazni filter koji će prilikom primanja poruke konzultirati baze podataka koje sadrže popise poslužitelja koji su otvoreni za odašiljanje (open relay), te baza s adresama poznatih spamera. Pošta koja dolazi s tako pronađenih adresa neće se primati.

Druga razina zaštite je automatska provjera sadržaja. Poslužitelj može poruke koje su obilježene kao spam spremati na određeno vrijeme u karantenu.

Pravila za korisnike

Korisnici ne smiju slati masovne poruke, bez obzira na njihov sadržaj (osim obavijesti).

Upozorenja na viruse su često lažna i šire zablude.

Korisnici ne smiju radi stjecanja dobiti odašiljati propagandne poruke koristeći računalnu opremu koja pripada ustanovi.

Nepridržavanje

Protiv korisnika koji se oglašuju o pravila prihvatljivog korištenja i šalju masovne neželjene poruke biti će pokrenut stegovni postupak.