

PHISHING

Phishing (varijanta engleske riječi za pecanje, fishing) je vrsta kriminalne aktivnosti u kojoj koristeći razne načine manipulacije, kriminalci od korisnika pokušavaju prikupiti povjerljive podatke (korisnička imena, lozinke, podaci s kreditnih kartica i sl.) kako bi ostvarili financijsku korist. U pravilu, phishing poruke prenose se putem elektroničke pošte koja navodi korisnika da klikne na određeni link koji ga dalje vodi na stranice zloćudnog web poslužitelja. Takve zloćudne



Web stranice obično se lažno predstavljaju kao Web stranice banaka, servisa za elektroničko plaćanje (PayPal i dr.) i sl. krivotvoreći, odnosno imitirajući njihov izgled. U svrhu phishing-a, osim elektroničke pošte, mogu poslužiti i drugi servisi poput foruma, servisa za izravnu komunikaciju (Windows Messenger, ICQ, Skype, Google Talk i dr.) te društvene mreže (Facebook, MySpace). Društvene mreže posebno su opasne jer podaci prikupljeni sa njih mogu poslužiti za krađu identiteta, ali i zbog činjenice da poruke dobivene od prijatelja, kojima su kompromitirani (oteti) račun, imaju određeni kredibilitet

Kako izbjeći phishing

- nikad ne odgovarajte na elektroničke poruke koje traže osobne podatke
- nikad ne slijedite linkove koji se nalaze unutar sumnjivih i neočekivanih e-mail poruka
- koristite dobre lozinke i često ih mijenjajte - dobre lozinke sastoje se od kombinacije velikih i malih slova, brojeva i simbola što ih čini vrlo teškim za probijanje
- provjerite da li web stranica preko koje unosite povjerljive podatke koristi HTTPS protokol - Web adresa financijskih institucija trebala bi počinjati s https:// umjesto sa http://
- koristite antivirusni softver - ova vrsta programa prepoznaje maliciozni softver koji se također može koristiti za prikupljanje osobnih informacija
- koristite antispymware softver
- redovito ažurirajte softver koji koristite
- budite u toku, pratite informacije o phishingu na internetu – sigurnosna edukacija je najefikasnija obrana od pokušaja phishinga

