

Phishing

E.B., L.J., I.M., M.P.

Objašnjenje



- engleski naziv phishing koji je iskrivljeni oblik riječi fishing (engl. pecanje) obje riječi se izgovaraju isto iako se pišu različito.
- Phishing ili mrežna krađa identiteta je vrsta prijevare putem elektroničke pošte odnosno elektroničke poruke. Pošiljatelj navodi žrtvu otkriti osobne informacije upisivanjem istih na lažiranoj internetskoj stranici čija je poveznica dana u poruci. Adresa i sadržaj te lažirane stranice vrlo su slični adresi i sadržaju neke autentične stranice.
- Oblici phishinga:
 - jednostavan zahtjev
 - Lažni linkovi e-maila
 - Lažna web sjedišta
 - Lažni (popup) prozor na legitimnim web sjedištima banaka
 - Tabnabing



Tko i kako ?

- "Phisher" se često koriste adresama internetskih servisa poput Apple, Microsoft ili Dropbox, a poruke su gotovo identične onima koje primamo u obliku različitih obavijesti ovih organizacija. Tako se nama čini da poruka dolazi od organizacije kojoj vjerujemo i, ako nismo dovoljno oprezni, nasjedamo na mamac.
- Ako smo povjerovali u vjerodostojnost pošte i kliknuli na poveznicu, link u *mailu* ili na lažnoj *web* stranici, prevarant može do željenih podataka doći na nekoliko načina:
 - Instalacija programa na naše računalo koji koristi rupe u sistemu i snimke zaslona za dobivanje osobnih podataka.
 - Instalacija softvera za špijuniranje koji bilježi aktivnost naše tipkovnice te šalje podatke prevarantu, koji potom lako dolazi do šifri i pristupnih podataka za različite internetske usluge koje koristimo - od *oglašavanja apartmana* do *e-bankinga*.
 - Stjecanje povjerenja i navođenje da sami pružimo svoje podatke, bilo putem *maila*, bilo preko *web* stranice prevaranata.

Primjer phishinga

- Stiže vam e-mail u kojem netko, odnosno pošiljalatelj, traži da kliknete na poveznicu (link) u e-mailu ili da preuzmete privitak, usput navedeni pošiljalatelj izgleda potpuno uvjerljivo i vjerodostojno.
- Najčešće korištene prijekave u zadnje vrijeme: e-mail sandučić vam je pretrpan te uskoro više nećete moći primati poruke, poziv na hitno plaćanje, poruke banke o nepodmirenom dugovanju, dospijeeće paketa na vašu adresu i sl.
- Primjer tipičnog phishing maila sadrži se od tri glavne značajke :
 - 1.NASLOV
 - Naslov e-poruke će često sadržavati nešto što će izazvati vašu neprimjerenu i ishitrenu reakciju.
 - 2.POŠILJATELJ
 - Ako vam pošiljalatelj izgleda nepoznato, ili ako se e-mail adresa pošiljalatelja ne podudara s kontekstom sadržaja e-poruke, odmah obratite pozornost i ne klikajte prije provjere.
 - 3.SADRŽAJ S POVEZNICOM (link)
 - Mail sadrži poveznicu (link) koja može izazvati otkrivanje vaših informacija.

Pošiljalatelj: Olt Director <Olt.Director@tgje.ro>

Poslano: 20. veljače 2020. 10:44

Primatelj: no-reply@microsoft.net

Predmet: Vaš račun za e-poštu treba odmah potvrditi

MICROSOFT VAŽNA OBAVIJEST

Vaš račun za e-poštu treba odmah **potvrditi** ili će vaš račun za e-poštu biti obustavljen ako nije potvrđen sada.

<https://ismcadmissions.wixsite.com/mysite>

Hvala na razumijevanju

Microsoftov tim za provjeru



Savjet

- Glavni savjet koji vam možemo dati, ma koliko paranoično izgledao, jest: sumnjajte u sve! Na kojoj god ste platformi! :
- Provjerite Adresu Pošiljatelja
- Pregledajte Naslov E Poruke
- Provjerite Kontekst E Poruke
- Ne Otvarajte Privitke
- Ne Šaljite Osobne Podatke
- Potražite Gramatičke Greške
- Nedajte Se Prestrašiti...



Video “skeč”

[Video skeč phishinga](#)



KRAJ