

ESET

Previdnost v socialnih omrežjih

..OSEBNE STRANI UPORABNIKOV SOCIALNIH OMREŽIJ POSTAJAJO PRAVE BIOGRAFIJE. PREMISLITE, PREDEN OBJAVITE SVOJE OSEBNE INFORMACIJE..

Število uporabnikov socialnih omrežij kot so Facebook, LinkedIn, Twitter in ostala še vedno narašča. Prav tako narašča tudi čas, ki ga uporabniki teh omrežij porabijo za posodabljanje svojih profilov, navezovanje stikov, objavljanje informacij in slik ter vsega ostalega. Ta omrežja zato kiberkriminalcem predstavljajo pravo zlato jamo. Brez večjih težav lahko v nekaj minutah o neprevidnem posamezniku izbrskajo informacije, ki jih kasneje uporabijo za prevare ali krajo identitete.

UPOŠTEVAJTE NASVETE

ZA VARNEJŠE SOCIALNO MREŽENJE

Bodite previdni koga dodate med prijatelje. Večina socialnih omrežij temelji na modelu priljubljenosti - številčenje prijateljev, povezav ipd. Avtorji socialnih omrežij s tem privarčujejo ogromno sredstev pri oglaševanju, saj večino dela opravijo uporabniki sami, s številom prijateljev pa na žalost narašča tudi možnost zlorabe. Premislite tudi, preden kliknete na povezave, bodite nezaupljivi. Tudi povezave, ki vam jih pošiljajo znanci, vas lahko pripeljejo na spletne strani, ki vsebujejo škodljivo kodo. Veliko nevarnost lahko predstavljajo tudi različni dodatki in spletne aplikacije za socialna omrežja. Te so lahko precej ranljive, preko njih se lahko kiberkriminalci zlahka dokopljejo



do vaših uporabniških podatkov. Priporočljivo je, da za obiskovanje spletnih strani socialnih omrežij uporabljate različne spletne brskalnike. Veliko manjša verjetnost je, da bodo kiberkriminalci zlorabljali varnostne luknje v brskalnikih, ki niso ravno standardni. Pogosta napaka je tudi ta, da uporabniki za dostop do različnih socialnih omrežij ter vseh ostalih spletnih storitev uporabljajo enaka uporabniška imena in gesla. Izogibajte se pravilno črkovanim besedam, tako angleškim, slovenskim (izbira gesel s šumniki ni priporočljiva) kot ostalim, v gesla ne vključujte delov svojega imena, priimka ali uporabniškega imena, imen svojih sorodnikov, krajev, kjer živite, ali osebnih in-

formacij kot sta telefonska ali registracijska številka avtomobila, imen operacijskih sistemov ali računalnikov, imen priljubljenih TV zvezdnikov, oddaj, filmov ipd. Prav tako si ne izbirajte gesel, ki uporabljajo izključno majhne ali velike črke. Najboljša gesla vsebujejo kombinacijo velikih in majhnih črk, števil ter znakov kot so podčrtaj, klicaj ipd., dolžina gesla pa naj bo vsaj osem znakov.

Kiberkriminalci socialna omrežja vse bolj pogosto zlorabljajo tudi za širjenje neželenih sporočil in škodljive kode. Ker veliko uporabnikov ta omrežja obiskuje tudi v službah, je nevarnost še toliko večja, saj so poslovna omrežja veliko večja.

Poskrbeti pa moramo tudi, da imamo na svojem računalniku nameščeno zadnjo različico svoje varnostne rešitve, redno moramo posodabljanje svoj operacijski sistem, brskalnike ter vso ostalo programsko opremo. Nič manj pomembno ni, da je naša protivirusna zaščita posodobljena z zadnjimi definicijami. ESETovi programi za zaščito pred škodljivo kodo poleg virusnih definicij uporabljajo tudi najnaprednejšo proaktivno zaščito na trgu, ThreatSense. Ta poskrbi, da ste varni tudi pred najnovejšimi grožnjami, saj škodljivo kodo analizira in prepozna v realnem času, tudi če grožnja med virusne definicije še ni dodana. (P.R.)

Varujemo vašo zasebnost

ESET SMART SECURITY

Antivirus
Antispyware
Firewall
Antispam

ESET NOD32 ANTIVIRUS

Antivirus
Antispyware

www.eset.si

SI SPLET, d.o.o. | Dolenjska c. 138, Ljubljana
01 428 94 05 | info@sisplet.com