



ESET

Varnost v brezžičnih omrežjih

..PRI POVEZOVANJU V INTERNET V JAVNIH BREZŽIČNIH OMREŽJIH OBSTAJA NEKAJ OSNOVNIH PRAVIL ZA VEČJO VARNOST, KI JIH VELJA UPOŠTEVATI V VSEH PRIMERIH..



Ne glede na to, ali ste za povezavo na internet v brezžičnem omrežju plačali ali ne, če ste na letališču, v kavarni ali na plaži – v javnih brezžičnih omrežjih vedno obstaja nevarnost, da nekdo spremlja in beleži ves spletni promet. To pomeni, da si lahko nepridripravi tako zagotovijo dostop do vseh vaših zaupnih informacij, kijih na spletu vpisujete, vključno uporabniškimi imeni in gesli, številkami kreditnih kartic, elektronsko pošto in vsem ostalim, kar lahko uporabijo ali preprodajo.

Z upoštevanjem nekaj osnovnih navodil se lahko takšni izpostavljenosti izognete:

- Uporabljajte dobro protivirusno rešitev s proaktivno zaščito in posodobljeno zbirko virusnih definicij.

- Uporabljajte močna gesla s kombinacijo velikih in majhnih črk, števil ter znakov kot so podčrtaj, klicaj ipd., dolžina gesla pa naj bo vsaj osem znakov.
- Redno posodablajte svoj operacijski sistem in drugo programsko opremo; tako se boste izognili večini vdorov z izrabljanjem varnostnih lukenj.
- Uporabljajte požarni zid, ki preverja tako vhodni kot odhodni promet.

Poleg tega velja v javnih brezžičnih omrežjih upoštevati še nekaj drugih osnovnih navodil:

- Na prenosniku brezžično mrežno kartico takrat, ko niste na spletu preprosto izklopite. Nekateri prenosniki to omogočajo s posebnim gumbom ali kombinacijo tipk, ostali pa lahko to storite tako, da brezžično kartico onemogočite v upravitelju naprav. Gre za preprosto in zanesljivo metodo, ki bo poleg vsega bateriji vašega prenosnika prihranila tudi nekaj energije.
- V javnih brezžičnih omrežjih se izogibajte spletnemu nakupovanju, elektronskemu bančništvu ter vsem ostalim spletnim stranem, ki od vas zahtevajo številke kreditnih kartic, uporabniška imena in gesla ali druge zaupne osebne informacije. Kolikor je to nemogoče, se prepričajte vsaj, da so te spletne strani varne in uporabljajo šifriran prenos podatkov. Takšne spletne strani imajo v naslovu



oznako https, v spodnjem desnem kotu brskalnika pa boste opazili tudi sličico ključavnice.

- Izklopite možnost skupne rabe datotek. V nekaterih operacijskih sistemih Windows je skupna raba nekaterih datotek na vašem trdem disku omogočena že po privzetih nastavitvah. To pomeni, da lahko do njih dostopajo vsi uporabniki v istem omrežju. V domačih omrežjih je ta možnost verjetno dobrodošla, v javnih pa precej nevarna.
- ESET Smart Security in ESET NOD32 Antivirus ter vse ostale ESETove protivirusne rešitve poleg klasičnih, reaktivnih metod preprečevanja širjenja zlonamerne kode z zbirkami protivirusnih definicij uporabljajo tudi tehnologijo ThreatSense, ki so jo razvili ESETovi raziskovalci. Gre za najbolj napredno in izpopolnjeno proaktivno metodo na tržišču, ki škodljivo kodo prepozna v realnem času in ne šele po prenosu zbirke protivirusnih definicij. (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