ESET

Primeri dobre prakse na spletu

..Svetovni dan telekomunikacij in informacijske družbe, ki so ga 17. maja praznovali po celem svetu, je namenjen ozaveščanju o možnostih, ki nam jih nove tehnologije ponujajo za boljše življenje..

Pri uporabi informacijsko-komunikacijskih tehnologij spada naša dežela med srednje razvite države v Evropski uniji. Po podatkih Statističnega urada Republike Slovenije je v prvem četrtletju lanskega leta pri nas imelo dostop do svetovnega spleta že 64 odstotkov gospodinjstev, narašča pa tudi število spletnih nakupov ter vseh ostalih storitev, ki lahko neprevidne uporabnike privedejo tudi v težave. Spodaj je deset primerov dobre prakse, s katerimi se lahko izognemo večini pasti na spletu:

Izogibajte se odpiranju sumljivih povezav, ki jih v e-sporočilih, pogovornih oknih ali na socialnih omrežjih prejmete od neznanih pošiljateljev. Največ uporabnikov na okuženih ali lažnih, ribarskih spletnih straneh pristane ravno zaradi klikanja na takšne povezave.

Izogibajte se spornim spletnim stranem, ki jih kiberkriminalci največkrat oglašujejo s pomočjo oglasov za razne popuste, brezplačno programsko opremo ali multimedijsko vsebino. Gre za obliko premetenega socialnega inženiringa, ki se ga moramo vsi uporabniki dobro zavedati.

Redno posodabljajte svoj operacijski sistem in programsko opremo, saj se boste s tem izognili večini škodljivih programov, ki za svoje širjenje izrabljajo varnostne luknje.

Programsko opremo prenašajte iz uradnih spletnih strani. Spletnih strani, ki ponujajo priljubljeno programsko opremo, je na internetu ogromno, velikokrat pa se zgodi, da v program vključijo tudi svojo nevarno kodo.

Uporabljajte varnostno programsko opremo – dobra protivirusna in protivohunska zaščita, požarni zid in filter pred neželeno pošto predstavljajo pomembnejši del obrambe pred nevarnimi programi, ki se širijo preko interneta, z USB ključki ipd. Uporaba takšnih rešitev močno zmanjša tveganje in izpostavljenost takšnim grožnjam.

Svojih osebnih informacij ne vpisujte v vsak obrazec. Na spletu se pogosto srečamo z raznimi obrazci, ki od nas zahtevajo vpisovanje osebnih informacij ter različnih uporabniških imen in gesel. V takšnih primerih se vedno prepričajte, da gre za zaupanja vredno spletno stran.

Bodite previdni pri rezultatih iskalnikov. Kiberkriminalci se predvsem ob odmevnejših svetovnih dogodkih radi poslužujejo tehnike Black Hat SEO, ki njihove nevarne spletne strani v spletnih iskalnikih pogosto uvrsti med prve zadetke. Novicam je najbolje slediti na spletnih straneh, ki jim zaupate.

Spremljajte le znane kontakte. Pri programih za neposredno sporočanje ali na socialnih omrežjih kot je Facebook spremljajte le tiste, ki jih poznate in jim zaupate. Tako se boste izognili različnim grožnjam kot so ribarska sporočila, izsiljevanje preko spleta ipd.

Ne odpirajte sumljivih datotek. Škodljiva koda se najpogosteje nahaja v zagonskih datotekah. Vse takšne datoteke, ki jih prenesete preko omrežij p2p, eMule, sumljivih spletnih strani ipd., pred zagonom vedno analizirajte s pomočjo protivirusnega in protivohunskega programa.

Uporabljajte dobra 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 informacij kot sta telefonska ali registrska 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, številk ter znakov kot so podčrtaj, klicaj ipd., dolžina gesla pa naj bo vsaj osem znakov. (P.R.)