Novičnik št. 2

Katere so nevarnosti interneta, na katere je treba biti pozoren?

Nevarnosti na internetu, ki se jih je treba zavedati, se jih paziti in jih po potrebi obravnavati, lahko strnemo v 9 splošnih kategorij.

1) Spletne strani z zlonamerno programsko opremo in virusi, ki lahko okužijo vaš računalnik

Med brskanjem po internetu lahko zelo enostavno kliknete na napačno povezavo in odprete spletno mesto, ki v računalnik naloži zlonamerno programsko opremo. Če imate v računalniku nameščen posodobljen protivirusni program, bo ta virus skoraj vedno zaustavljen, še preden bo lahko povzročil kakršno koli škodo. Največja nevarnost, poleg nevarnosti protivirusnega programa, ki spregleda virus, je, da se ne zavedate, da ste tvegali okužbo, ki lahko ogrozi delovanje vašega računalnika ali celovitost vaših podatkov. Prav zaradi nepozornosti številnih ljudi so se v zadnjem letu zelo razširili virusi izsiljevalske programske opreme, kot je Cryptlocker, ki šifrirajo osebne datoteke in zahtevajo odkupnino.

Vemo, katera spletna mesta so nevarna, na splošno tista, ki se ukvarjajo s piratstvom, spletnimi mesti za predvajanje video vsebin, vsebino za odrasle, zmenki in nezakonitim gradivom. Če se obisku teh spletnih mest ne morete izogniti, bodite zelo previdni, kje klikate, saj se virus lahko skriva kjer koli. Dovolj je, da kliknete na napačen gumb "Prenesi", da namestite zlonamerno programsko opremo. Ne pozabite na oglasna obvestila, ki vam sporočajo, da je vaš računalnik okužen, čeprav v resnici ni.

Če ste v dvomih, so na voljo orodja za prepoznavanje in izogibanje nevarnim povezavam in sumljivim spletnim mestom. Ključni dejavnik pri prepoznavanju in izogibanju spletnih mest z virusi je uporaba posodobljenega brskalnika, ki je zaščiten pred vsemi do zdaj odkritimi napakami.
Med najnevarnejšimi spletnimi mesti, ki lahko vsebujejo zlonamerno programsko opremo, so zagotovo spletna mesta za odrasle, piratska spletna mesta vseh vrst, skoraj vsa spletna mesta s torrenti (tudi piratska), spletna mesta za nezakonit prenos (na primer filmov in glasbe) ter spletna mesta z nezakonito odklenjeno programsko opremo.

Če morate obiskati takšno spletno mesto, je najbolje, da brskate v tako imenovanem peskovniku (*sandbox)*. V operacijskih sistemih Windows 10 in Windows 11 lahko uporabite funkcijo navideznega namizja, ki ni le varnostno orodje, temveč tudi odličen način, da v računalniku opravljate stvari, ne da bi jih zabeležili ali si jih zapomnili, podobno kot anonimni način *(incognito)* v spletnih brskalnikih. To orodje se imenuje peskovnik in je namenjeno kot območje v računalniku, v katerem vse, kar počnemo, nima vpliva na sistem in se izbriše takoj po zaprtju. Peskovnik deluje kot virtualni stroj za enkratno uporabo, v katerem lahko varno zaženete vse, kar želite; lahko celo odprete virus ali zlonamerno programsko opremo, ne da bi vas skrbelo, da bo poškodovala računalnik ali ukradla podatke iz računalnika.

2) Spletna zasebnost je vedno v nevarnosti

Povsem očitno je, da se boste morali, če želite internet uporabljati aktivno, tj. z vključevanjem v forume, družbena omrežja in klepete, odreči delu svoje zasebnosti. Na straneh, kot je Facebook, je treba navesti svoje pravo ime, medtem ko je na drugih straneh še vedno treba pustiti elektronski naslov, prek katerega lahko po želji izsledimo lastnika. V bistvu pri običajni uporabi interneta anonimnost ne more obstajati, in če bi koga zanimalo, kdo smo, in bi imel ustrezne hekerske sposobnosti in talent, bi teoretično lahko o nas izvedel vse.

Zaščita zasebnosti v spletu ne pomeni, da hekerju ne moremo preprečiti vohunjenja za našim življenjem, saj razen če nas zasleduje zalezovalec ali počnemo stvari, ki so nezakonite in jih je treba skriti, nihče verjetno ne bo zapravljal časa z vdiranjem v naše življenje. Po drugi strani pa spletna zasebnost pomeni, da nekatere občutljive informacije, kot so številke naših kreditnih kartic, gesla, kje se nahajamo, kaj iščemo na internetu in podobno, ostanejo zasebne.

3) Nezaščitena spletna mesta

To je nevaren dejavnik, ki ga večina ljudi še vedno zanemarja. Spletna mesta niso vsa enaka in se delijo na varna spletna mesta, kjer so podatki, ki jih posredujete, šifrirani in jih ni mogoče prestreči od zunaj, in običajna spletna mesta, ki posredujejo podatke v prosti obliki. *Navigaweb.net* je trenutno nešifrirano spletno mesto, kar ne pomeni, da ni varno, vendar ker za prijavo ne zahteva gesla, informacij ni treba zaščititi. Vsa spletna mesta, na katerih morate vnesti geslo, morajo biti šifrirana, ta zaščita pa je prepoznavna po ključavnici na spletnem naslovu in predponi *https* namesto *http*. Kadar je spletno mesto v protokolu HTTPS in nima napak v certifikatu, potem vsi podatki, ki jih pošljemo, vključno z gesli za dostop, številkami kreditnih kartic ali bančnih računov, na internetu niso vidni nikomur, niti upravljavcu spletnega mesta, ki mu te podatke pošljemo. Samoumevno je, da na vseh spletnih mestih s protokolom *http* in brez protokola *https* ne smete posredovati osebnih podatkov. Če še vedno uporabljate e-poštno storitev brez protokola *https* ali tako površno spletno banko, jo nemudoma zamenjajte.

4) Kraja spletnih gesel in osebnih podatkov (phishing)

Med nevarnimi spletnimi mesti na splošno je posebna kategorija goljufivih spletnih mest, kot so neznana in odsvetovana nakupovalna spletna mesta ali, še huje, lažna spletna mesta, ki so videti enaka znanim spletnim mestom in so ustvarjena za krajo gesel za račune.

Izdelovanje lažnih kopij spletnih mest za bančništvo ali nakupovanje je ena najpogostejših tehnik, ki jo hekerji uporabljajo za krajo gesel za spletne račune in se imenuje *phishing*. Phishing vedno deluje tako, da pošljete sporočilo prek e-pošte, Facebooka, sporočil SMS, Whatsappa itd. Najboljši način, da ne nasedete tej tehniki, je, da jo uporabite kot izgovor za krajo gesel. Najboljši način, da se ne ujamete v tovrstno past, je, da nikoli ne zapisujete gesel in pomembnih podatkov (niti po elektronski pošti), razen na uradnih spletnih mestih računov, ki jih prepoznate po naslovu, zapisanem na vrhu brskalnika, in HTTPS z zeleno ključavnico. Najbolje bi bilo, če bi uporabljali e-poštni odjemalec, kot je Microsoft Outlook, in ta sporočila blokirali s filtrom za nezaželeno pošto.

5) Neželena pošta *(spam)*

Nevarnost neželene pošte je danes veliko manjša kot pred nekaj leti. Spam je celotna kategorija neželenih sporočil, oglaševanja, phishinga in virusov ali neuporabnih sporočil. Na srečo imajo današnje vrhunske e-poštne storitve, kot sta Gmail in Outlook.com, učinkovit filter za nezaželeno pošto, ki ureja sprejemanje e-poštnih sporočil.

6) Napačne informacije

Kljub temu, da gre za del kategorije neželene pošte, so napačne informacije na internetu v zadnjem letu postale resnična nevarnost zaradi širjenja lažnih novic z lažnih spletnih strani, ki se jih moramo naučiti prepoznati, da ne bi bili videti kot bedaki, ki verjamejo vsemu, kar preberejo na internetu ali Facebooku.

7) Spletni zmenki

To je ena najresnejših nevarnosti, ki jih mladim prinaša internet. Sliši se slabo, vendar bi morali odgovorni starši ne glede na okoliščine preveriti, ali njihovi otroci klepetajo z neznanci prek interneta. Z neznancem se lahko pogovarjate v spletni igri, na spletnem mestu za priložnostne zmenke, v družabnem omrežju, na forumu in v kateri koli drugi klepetalnici. Ne glede na to, ali gre za spolne razloge, zmenke ali zgolj za rekreacijo, je pomembno, da ne izdate preveč osebnih podatkov: ne povejte svoje prave starosti, ne povejte, kje živite, ne povejte, katero šolo obiskujete, ne povejte pravih imen družine ali prijateljev in ne povejte svoje telefonske številke. Spletni plenilci se znajo zelo dobro izdajati za običajne otroke in znajo izkoristiti slabosti najstnikov, ki jih ne znajo izkoristiti niti najboljši psihologi, v najhujših primerih pa jih vodi bolezen (pedofilija).

8) Spletno ustrahovanje *(cyberbullying)*

Klepetanje z neznanci je lahko nevarno, saj nikoli ne veste, kdo stoji za tipkovnico, nevarno pa je lahko tudi klepetanje z znanimi ljudmi. Spletno ustrahovanje deluje približno takole: če vas v šoli ali med prijatelji zasmehujejo, lahko eden od njih na Facebooku ali drugih družabnih omrežjih objavi videoposnetek ali fotografijo, ki lahko žrtev spravi v zadrego.

Drug primer spletnega ustrahovanja so lahko anonimna sporočila, ki žrtev močno žalijo in ji celo grozijo. V primerjavi s pravim nasilnežem ima spletni nasilnež to prednost, da ni nadzora in da lahko govori, kar hoče, ne da bi žrtvi pogledal v obraz ali celo anonimno, skrit za tipkovnico. V obeh primerih to ne bi bilo tako težko, vsaj na tehnični ravni. Veliko bolj zapletena pa je obramba na psihološki ravni, pri kateri je morda potrebna pomoč staršev ali strokovnjaka. Za začetek bi bilo dobro izbrisati račun na Ask.fm, enem od spletnih mest, ki so najbolj primerna za spletno ustrahovanje.

9) Popolno nepoznavanje računalniške varnosti

To je očitna nevarnost, ki je tako razširjena, da je človek presenečen. Ali je mogoče, da je še danes najpogostejše geslo na svetu 123456? Ali ljudje mislijo, da jim noben heker ne bo ukradel računa, ker nimajo česa skrivati? Kako lahko ljudje še vedno uporabljajo isto geslo za vsako spletno mesto?

In še vedno obstajajo tisti, ki svoja gesla, ki so morda vsa različna in si jih je težko zapomniti, napišejo na list papirja, ki ga lahko prebere vsakdo?

Ta projekt je financirala Evropska komisija. Ta dokument odraža le stališča projektnih partnerjev, Komisija pa ni odgovorna za kakršno koli uporabo informacij, ki jih ta dokument vsebuje.