8 stvari na koje trebate paziti kako bi zaštitili svoju privatnost na internetu

Iz priručnika za roditelje”Delete Cyberbullying”, koji je izradila Udruga roditelja “Korak po korak”, prenosimo vam savjete za zaštitu privatnosti na internetu:

1) Oni pitaju, vi ne kažete

Samo zato što vas pitaju, ne znači da vi morate odgovoriti. Ako samo izrađujete profil za elektroničku poštu, nema potrebe za sveobuhvatnim profilom, a ako se pridružujete nekoj društvenoj mreži, možete ograničiti količinu osobnih podataka koje dajete na minimum. Kada vam nije potreban odgovor, uvijek možete jednostavno izmisliti neku adresu e-pošte.

Mnoge web stranice traže od korisnika da se registriraju svojom adresom e-pošte kako bi mogli pregledavati sadržaj. Prilikom registracije može dogoditi se i da se pretplatite na newsletter i reklamne poruke. Ovo se može izbjeći uklanjanjem kvačice ispred rečenice koja nudi opciju pretplate u formularu za registraciju, a moguće je i otkazati newsletter ili reklame klikom na opciju unsubscribe u dnu poruke e-pošte ili je blokirati pomoću alata za filtriranje i blokiranje neželjene pošte u postavkama vašeg računa e-pošte.

2) Lozinke

Ne koristite svugdje istu lozinku i ne upotrebljavajte korisničko ime s jedne stranice kao lozinku na drugoj jer hakeri mogu uspoređivati podatke. Upotrebljavajte brojke i slova, neka tiskana, u kombinacijama koje nemaju značenje, odnosno nisu stvarne riječi.

Važno je sačuvati svoju adresu e-pošte i profile na društvenim mrežama od provale. Ukoliko netko provali u nečiju e-poštu, može svim njezinim kontaktima poslati poruku u kojoj traži novčanu pomoć. Osoba u čiji je mail provaljeno neće znati što se događa, što može poprilično našteti njezinom ugledu.

3) Spam

Svrha spama (neželjena pošta) je oglašavanje, a od “običnog” oglašavanja se razlikuje po tome što se šalje velikom broju primatelja koji nisu zatražili poruku. Osobe i organizacije koju šalju spam, do adresa e-pošte dolaze na različite načine. Pretražuju web u potrazi za znakom: @, i dolaze do javno objavljenih adresa e-pošte; koriste alate pomoću kojih mogu pogoditi adresu e-pošte (kao i lozinku – zato lozinka treba biti što kompliciranija); provaljuju u e-poštu različitih osoba i organizacija i tako dolaze do svih njihovih kontakata; provaljuju u baze podataka organizacija i servisa koje skupljaju podatke svojih korisnika; kupuju adrese e-pošte od servisa koji skupljanju podatke svojih korisnika – zato pročitajte sitna slova prilikom registracije na različite portale i web stranice.

4) Scam

Scam je pokušaj prevare korisnika i navođenje na trošenje novaca ili kompromitiranje korisnikovih podataka (društvene mreže, računi e-pošte). Ovaj se fenomen često naziva i socijalnim inžinjeringom. Puno je lakše nekoga prevariti i nagovoriti da dobrovoljno oda svoje podatke ili instalira malver nego zaobići tehničku zaštitu (npr. antivirusne programe). Cyber kriminalci računaju na lakovjernost i neiskustvo korisnika, zbog čega su djeca osobito ranjiva skupina.

Pokušaj krađe lozinke za ulazak u e-poštu ili račun na društvenoj mreži (phishing) postaje sve teže uočljiv: e-pošta koju prima korisnik izgleda kao "prava" e-pošta koja stiže od primjerice pružatelja usluga neke društvene mreže. Često korištena metoda je i navođenje korisnika na klikanje koje ih vodi na oglas/spam/scam umjesto na sadržaj kojem su htjeli pristupiti putem neprimjetnog spajanja oglasa/spamova/scamova sa sadržajem (na primjer stvaranjem velikog gumba za "download" /preuzimanje/ koji vas preusmjeravaju na drugi sadržaj i manje uočljiv za stvarno preuzimanje datoteke koju ste tražili). Zloćudni softver se često spaja sa datotekom koju ste htjeli preuzeti pa uz video ili glazbu, preuzimate i malver.

Primjeri prevara uključuju: online obrazac koji vas upozorava na to da će vam korisnički račun na društvenoj mreži biti obrisan ukoliko hitno ne utipkate osobne podatke (lozinke) u online obrazac; lažna modna agencija koja traži od korisnika da im pošalju fotografije na kojima su oskudno odjeveni ili bez odjeće; e-pošta koja izgleda kao da je stigla od nekoga od vaših prijatelja ili poznanika, a traže da na određeni broj računa pošaljete novac jer se vaš prijatelj koji je u inozemstvu našao u nevolji (opljačkan je i sl); pop-up prozor koji vas obavještava da vam je računalo zaraženo virusom i nudi vam program koji trebate instalirati kako biste računalo očistili od virusa – a zapravo je riječ o štetnom softveru koji se bez vaše pomoći ne bi mogao instalirati na računalo.

5) Ništa nije besplatno

Većina online usluga/servisa/platformi/igara koje su besplatne za korisnike financiraju se ili kroz oglašavanje ili prodajom podataka svojih korisnika oglašivačima. Na primjer, mnogo usluga uključujući i društvene mreže oslanjaju se na razne elemente kako bi ostvarivale prihod od oglašavanja. Među njima je i maksimiziranje korisničkog sudjelovanja (dijeljenje, komentiranje, postanje, interakcije, linkanje, itd.) jer će im to omogućiti prodaju detaljnijih informacija o njihovim korisnicima oglašivačima i stoga povećati učinak njihovih reklamnih kampanja, koje će ciljati na vrlo specifične korisnike temeljem velike količine podataka i informacija koje generiraju. Vjerojatno ste primijetili da kada jednom kliknete na neki proizvod, slični se proizvodi počinju sve češće pojavljivati na vašem profilu.

To također znači da te usluge imaju interes u tome da ljudi svoje profile drže otvorenima (umjesto da svoj sadržaj u potpunosti zaključate, što bi značilo da će vaši postovi/aktivnosti biti vidljivi ograničenoj publici) i da čuvaju što je više moguće podataka o korisnicima (odvraćajući ih od toga da "očiste" svoje račune redovno ili izbrišu ogromnu količinu prošlih uključivanja i postova). Pogledajte profile drugih ljudi – što možete pročitati o njima, oni mogu pročitati o vama.

Jednom kada ste svoje podatke ili osobne fotografije objavili na internetu imat ćete jako malo kontrole nad njihovom upotrebom. Isto tako, što je vaš profil, ili profil vašeg djeteta, vidljiv većem broju ljudi, veća je vjerojatnost od zlouporabe pa i elektroničkog nasilja.

6) Svoje osobne podatke držite pod ključem

Društvene mreže su zlatni rudnik za skupljače podataka, zato im otežajte život najrigoroznijim postavkama zaštite privatnosti. U žustroj raspravi može vam se dogoditi da otkrijete više nego ste željeli, stoga pazite što objavljujete kako bi bili sigurni da vam nikakvi osobni podaci neće 'pobjeći'.

7) Osobni podaci vaše djece

Pazite s objavljivanjem fotografija vaše djece na društvenim mrežama. Razmislite o tome koliko informacija na takav način činite javno dostupnim i može li se iz objava na vašem profilu, uz fotografiju djeteta doznati i ime i prezime djeteta, mjesto rođenja, kućna adresa ili vrtić ili škola koju pohađa? Znate li tko sve može vidjeti objave s vašeg profila i, ukoliko su vaši prijatelji "lajkali" vašu objavu ili bili "tagani", tko sve može doći do fotografija i informacija o vašoj djeci?

Jednom objavljeni, komentari i fotografije ostaju online zauvijek. Razmislite o tome hoće li vaše dijete jednog dana biti zadovoljno s online identitetom koji ste za njega stvorili. Prije objavljivanja fotografija drugih ljudi online, uvijek treba zatražiti njihovo dopuštenje, inače kršimo njihovo pravo na privatnost. Jeste li sigurni da bi vaše dijete dalo dopuštenje za objavu fotografije koju planirate podijeliti s vašim kontaktima?

8) Zatvorite prva vrata prije nego otvorite sljedeća

Ostati prijavljen na svoj račun na društvenoj mreži ili bankovnom računu isto je što i ostaviti otključan auto: potpuno ste otvoreni upadu hakera. Izbjegnite zato rizik i odjavite se iz svojih računa prije nego nastavite pregledavati internet.