4.4. Opasnost gdje god klikneš

Koliko ste se puta kao roditelj zatekli kako razmišljate o opasnostima u kojima se moglo i može naći vaše dijete? Do sada su te opasnosti bile povezane uz fizički svijet, a sada se prenose u digitalne oblike. Već ste se susreli s različitim oblicima nasilja na internetu i ovdje neće biti riječ o još jednome takvu obliku nasilja, već o opasnostima s kojima se vaše dijete može susresti pretražujući internet.

Kad kontaktiraju s prijateljima, djeca se, osim društvenim mrežama, koriste i elektroničkom poštom. To je, uostalom, i najučestaliji oblik komunikacije na internetu, ne samo među djecom nego i među ostalim korisnicima interneta. Primjer za to su trgovački lanci koji imaju svoje klubove u koje se možete učlaniti ako im ostavite svoje podatke kako bi vam na kućnu adresu slali obavijesti o akcijama koje u određenome razdoblju možete iskoristiti u njihovim prodavaonicama. Nerijetko vas na tim prijavnicama traže i adresu elektroničke pošte kako bi obavijesti stizale i tim putem. Na takve poruke trebate biti spremni kad potpisujete bilo kakvu prijavnicu i pritom ostavljate svoju adresu: svojim potpisom dajete pristanak na njih. Međutim, postoje *spam* poruke koje su također promidžbenoga sadržaja, ali vi na njih niste (barem ne svjesno) dali svoj pristanak. Takve poruke mogu sadržavati poveznice na stranice s neprimjerenim sadržajima ili neke druge poveznice koje skrivaju potencijalne opasnosti, napose za vaše računalo. Neke su od njih virusi, crvi i *trojanci*.

Virus je mali program koji se širi s jednoga računala na drugo i ometa rad računala. Računalni virus može oštetiti ili izbrisati podatke na računalu, proširiti se na druga računala s pomoću programa za e-poštu ili čak izbrisati sav sadržaj tvrdoga diska.

Crv je računalni kod koji se širi čak i bez korisnikova djelovanja. Većina crva u početku su također privitci poruka e-pošte koji po otvaranju zaraze računalo. Crv pregledava zaraženo računalo tražeći datoteke, npr. adresare ili privremene mrežne-stranice koje sadržavaju adrese e-pošte. S pomoću tih adresa crv šalje zaražene poruke e-pošte te često oponaša (ili krivotvori) adresu pošiljatelja u daljnjim porukama e-pošte da bi primatelj pomislio kako poznaje pošiljatelja poruke. Crvi se zatim automatski šire e-poštom, mrežom ili iskorištavanjem slabih točaka sustava te ih često svladaju prije nego što se utvrdi uzrok. Crvi ne djeluju uvijek štetno na računala, no obično uzrokuju probleme sa svojstvima i stabilnošću računala i mreža.

Trojanski konj zlonamjeran je program skriven unutar drugih programa. Trojanski konj obično se ne širi sam, širi se virusima, crvima ili preuzetim programom. Sam termin *trojanski konj*, zbog sličnosti djelovanja, preuzet je iz grčke mitologije. Napadač, koji se koristi trojanskim konjem, predstavlja se kao netko drugi kako bi mogao ući u sustav računala. Kad se to dogodi, napadač preuzima potpunu kontrolu nad računalom. Trojanski konj najčešće se koristi namjerno, s točno određenim ciljem.

Usporeno radi.

Nema slobodnoga prostora.

Podatci mogu biti izbrisani.

Prikazuje uvredljivu poruku.

4.4. Opasnost gdje god klikneš

Iako postoje neprimjereni sadržaji i poveznice na internetu koje skrivaju potencijalne opasnosti, djecu nije teško zaštititi ako se pridržavate nekih mjera predostrožnosti. Ono što može pomoći u sprječavanju zaraze jest:

- upotreba antivirusnoga programa s ažuriranom (izrađenom) bazom podataka mogućih napada
- redovito nadograđivanje (*update*) operacijskoga sustava i najkorištenijih programa kao što su Microsoft Office, Adobe Reader, Mozilla Firefox i dr.
- redovita izrada rezervnih kopija podataka ili operativnoga sustava
- oprez i neaktiviranje bilo kakve datoteke ponuđene elektroničkom poštom ili nekim drugim internetskim servisom
- imati uključen vatrozid (*firewall*) – to je zaštita računala koja obavlja filtriranje, analizu i provjeru paketa podataka koji nose informacije s interneta i na internet.

Unatoč svemu što poduzmete kako biste zaštitili svoje računalo, ipak se može dogoditi da se vaše računalo zarazi. Tada je najbolje:

- očistiti računalo odmah nakon zaraze i nikako ne ignorirati upozorenja antivirusnoga programa
- zloćudni program ukloniti nekim antivirusnim programom
- ako se zloćudni program unatoč tomu ne da očistiti, potrebno je deinstalirati operacijski sustav.

SIGURNOST

Obiteljske aktivnosti

Kako biste naučili dijete da se pridržava tih mjera prevencije i kako bi znalo što treba učiniti ako do zaraze dođe, trebate i sami prakticirati isto.

Vlastitim primjerom pokažite mu kako odabrati i postaviti dobar antivirusni program, kako uključiti vatrozid i kako ne zanemarivati upozorenja koja nam takvi programi šalju.
I zapamtite – opasnost može biti na svakoj stranici ili u svakoj elektroničkoj pošti, ali vi ne morate biti njezina žrtva.

Za više informacija možete pročitati ove članke: *Sprečavanje i uklanjanje virusa, Više o virusima, Sigurno na internetu*, petzanet.HR/Modul3/poveznice.