



ENJOY SAFER TECHNOLOGY™

safer**kids**online

**Starševski vodnik
za družbena
omrežja**

Uvod

Se spomnite časov, ko so se otroci igrali zunaj in so se domov vračali šele, ko so bili lačni? Internet je vse spremenil. Dandanes lahko mladi vsak dan ure in ure preživijo na družbenih omrežjih.

Mnogi od nas pri ESET smo starši in razumemo skrbi, ki se pojavljajo, ko je vaš otrok ujet v spletnem svetu, zato smo pripravili ta vodnik. V njem boste našli informacije o možnih grožnjah, ki se skrivajo na družbenih omrežjih in rešitve s katerimi boste zaščitili svojo družino.



1. Na kaj je potrebno biti pozoren

Zlonamerna programska oprema

Zlonamerna programska oprema z drugimi besedami pomeni škodljiva koda, to so na primer virusi, črvi in trojanci. Prevaranti uporabljajo omrežja z namenom, da privabijo uporabnike k prenosu zlonamerne programske opreme, pogosto z obljubo pridobitve piratske programske opreme ali iger.

Phishing

Izraz je vpeljan iz angleške besede fishing (ribolov), kot vaba za lovljenje žrtev. Veliko napadalcev uporablja to metodo za krajo občutljivih podatkov- na primer podatkov za prijavo na profil otrokovega družbenega omrežja. Običajno se pojavi v obliki elektronskega sporočila, ki je povezano s kopijo spletnega mesta družbenega omrežja. Precej težko je prepoznati ponarejeno stran, saj so razlike resnično majhne, otroci pa lahko zlahka vstavijo svoje podatke, brez da bi se zavedali da je nekaj narobe.

Kraja identitete

Poskrbite, da vaši otroci ne bodo objavljali občutljivih podatkov, kot so domači naslov, naslov šole, telefonska številka ali datum rojstva, ki bi jih lahko uporabili za njihovo identifikacijo. Kraja identitete je razširjena oblika spletnega kriminala, kjer napadalci pridobijo osebne informacije uporabnikov in jih uporabljajo za lažno predstavljanje.

Napadalec lahko pride do teh podatkov na dva načina:

Pogosto se na družbenih omrežjih pretvarja, da je otrokov prijatelj.

Uporablja informacije, ki so javno dostopne na profilu družbenega omrežja - izbira ustreznih nastavitev zasebnosti so ključne.

Spletno nadlegovanje in zloraba

Ni nujno, da vse grožnje vašim otrokom na družbenih omrežjih vključujejo spletne kriminalce. Težava so lahko tudi njihovi vrstniki. Ustrahovanje se ne dogaja samo v šolah, dandanes se v veliki meri pojavlja tudi na internetu in je lahko škodljivo enako kot v resničnem življenju.

Še eno resno tveganje predstavlja grooming, zlasti kadar gre za mlajše otroke. Gre za odraslega človeka, ki skuša pridobiti otrokovo zaupanje in zgraditi odnos z njim, da bi ga prepričal k spolnim aktivnostim. To pogosto vključuje sexting (sporočila z neprimerno vsebino, ki so lahko poslana vašemu otroku ali jih pošlje vaš otrok).

2. Katere ukrepe lahko sprejmete, da zaščitite svoje otroke?

Z zavedanjem pojava možnih groženj, se družbena omrežja zdijo nevarna aktivnost. Da bi svojemu otroku prepovedali uporabo, ne zveni kot rešitev, saj bodo našli pot, da dosežejo svoje. Spodaj najdete nasvete, ki bodo uporabo družbenih omrežij naredili varnejšo in z njimi zagotovite ustrezno zaščito za svoje otroke in družino.

Pogovor

Dialog je eden glavnih dejavnikov, da zaščitite svoje otroke na spletu, zlasti kadar govorimo o družbenih omrežjih. Odprta in poštena komunikacija z vašimi otroki je ključnega pomena, če želite da zaupajo vaši presoji in upoštevajo vaše nasvete.

Dober primer je spletno ustrahovanje in njegovo preprečevanje. Otroku dajte vedeti, da mora kadarkoli naleti na takšno vedenje (četudi ne zadeva neposredno njega) o tem nemudoma obvesti nekoga - vas, učitelja ali drugo odgovorno osebo.

Uporaba programske opreme za starševski nadzor

ESET Smart Security vam omogoča, da ustvarite seznam blokiranih spletnih mest in omejite otrokov čas, ki ga lahko preživi na spletu

Tudi otroci naj imajo nekaj besede pri tem, zato jim ESET Parental Control za Android omogoča, da vas prosijo za dovoljenje za obisk določenih spletnih strani ali dovoljenje do podaljšanega časa preživetega na spletu, če so končali hišna opravila ali domačo nalogo opravili prej kot pričakovano.

Uporaba zanesljive varnostne rešitve

Ker je zlonamerna programska oprema ena najbolj razširjenih groženj v spletnem okolju, je namestitev varnostne rešitve z možnostmi zaznavanja v otrokovih napravah bistvenega pomena za preprečevanje okužb pri uporabi družbenih omrežij.

Orodja za zaščito pred neželeno pošto in požarni zid omogočajo optimizacijo varnosti brez tveganj. Prav tako naj vaš otrok ne uporablja skrbniškega računa pri brskanju po družbenih omrežjih. Nastavite poseben uporabniški profil za svoje otroke in s tem zmanjšajte vpliv varnostnih incidentov.

Uporaba močnih gesel in dvo faktorskih preverjanj

Ali vaši otroci vedo kako izgleda varno geslo? Prepričajte se, da ne uporabljajo gesel, ki jih je zlahka ugotoviti, na primer "geslo" ali "12345". Mora biti dolg vsaj deset znakov, vsebovati velike in male črke, številko in poseben znak kot je # ali @. Prilagoditev besedne zveze ali besedila pesmi je lahko v pomoč:

Izidor ovčice pasel postane Izidorovcicep@se1

Prav tako jih opomnite naj ne delijo svojega gesla z nikomer, niti najboljšimi prijatelji.

Ko se povezujejo na Facebook, Twitter ali drugo popularno družbeno omrežje, se prepričajte, da uporabljajo dvo faktorsko preverjanje ponujeno v varnostnih nastavitvah. Prejem gesla za enkratno uporabo na njihov pametni telefon doda še en varnostni sloj za napadalce.

Sprememba nastavitvev profila v "zasebno"

Privzete nastavitve zasebnosti ne zagotavljajo varnosti za vašega otroka. Priporočljivo je, da si vzamete čas in jih nastavite ter preverite katere informacije bi lahko uhajale. Poglejmo si Facebook za primer:

Facebook

Uporabite nastavitve profila za zagotavljanje, da vse informacije niso deljene z drugimi uporabniki. Če je možno naredite informacije dostopne samo njihovim prijateljem in družini, če je mogoče samo malim skupinam (ožja družina ali najboljši prijatelji).

Omejite občinstvo, ki lahko vidi slike, statuse in drugo vsebino v kateri je bil vaš otrok označen. Preprečite aplikacijam dostop do osebnih podatkov ali objavljanje na njihovem zidu.

Naučite jih naj sprejmejo prošnje za prijateljstvo le od ljudi, ki jih osebno poznajo. Razložite jim, da je pogovor z neznanci ali stik z njimi na internetu enako nevaren kot v resničnem svetu.

Za podrobne informacije o uporabi nastavitvev na Facebook, si preberite naš blog: <http://blog.eset.com/2011/05/25/facebook-privacy>

Twitter

Twitter ima svoje posebno obravnavo, na primer omejitev na 280 znakov ali pogosta uporaba skrajšanih naslovov URL. Tudi te razlike bi morali izpostaviti, ko otroku razlagate kako ostati varen.

Poleg tega, da sledijo samo osebam, ki jih poznajo in se izognejo sumljivim povezavam, naj preverijo legitimnost sporočil, ki jih prejmejo. Zlonamerna sporočila pogosto prepoznajo drugi uporabniki in deljene informacije, kot je hitro iskanje po delu sporočila lahko pomaga.

Na njihov računalnik prav tako namestite ugleden vtičnik brskalnika, ki omogoča da vaši otroci vidijo izvirno povezavo s kratkega naslova URL, brez da bi nanjo kliknili.

Druga družbena omrežja

Obstaja veliko družbenih omrežij, ki skrbijo za različne interese in starostne skupine. Pomembno je preveriti, da vaši otroci uporabljajo tiste, ki so primerne za njih. Imamo video vodiče, ki pokrivajo Snapchat, Instagram in YouTube, sestavili pa smo tudi seznam ustreznih družbenih omrežij za otroke.



3. Za konec

Družbena omrežja so lahko dragocen vir za internetne uporabnike. Še vedno pa ta vodnik dokazuje, da obstaja mnogo groženj za vaše otroke, katerim so lahko izpostavljeni ko uporabljajo družbena omrežja. Ne podcenjujte spletnih kriminalcev ali drugih zlonamernih akterjev. Bistveno je, da uporabite zanesljiva varnostna orodja in zaščitite pomembne ljudi v vašem življenju.

Pomagati jim pri pravilni nastavitvi njihovih družbenih omrežij in nuditi preproste, a koristne nasvete je ključna stvar za zagotavljanje njihove varnosti.



10 top nasvetov

1. Naučite svoje otroke, da se ustavijo in premislijo preden kliknejo na povezave ali gumbе za prenos
2. Naučite jih pristopiti k spletni komunikaciji z občutkom previdnosti
3. Račune svojih otrok nastavite na zasebni način
4. Naučite jih odkloniti prošnje za prijateljstvo, ki jih pošljejo neznanci
5. Ohranite njihov operacijski sistem in varnostno programsko opremo posodobljeno
6. Bodite dober vzor in imejte svojo digitalno uporabo pod nadzorom
7. Glejte za signali, ki bi lahko nakazovali, da je otrok žrtev spletnih ustrahovalcev
8. Uporabite ugledno aplikacijo za starševski nadzor kot je ESET Parental Control
9. Spodbudite jih k uporabi močnih gesel
10. Prosite jih, naj premislijo preden delijo osebne informacije, videe ali fotografije.