Socialinių tinklų vadovas tėvams

ENJOY SAFER TECHNOLOGY™

Įžanga

Dar ne taip seniai vaikai daugiausia žaisdavo lauke ir grįždavo namo tik labai išalkę. Visgi, interneto bumas šiuos įpročius pakeitė. Šiandien, vietoj išėjimo į lauką, jauni žmonės dažnai renkasi naršymą internete ar bendravimą socialiniuose tinkluose.

Mes, kompanija ESET, taip pat esame tėvai ir suprantame Jūsų nerimą stebint, kaip Jūsų vaikai pasineria į kibernetinį pasaulį. Šiame vadove Jūs rasite informaciją apie grėsmes, tykančias socialiniuose tinkluose, taip pat sprendimus, kurie padės Jums apsaugoti šeimą ir vaikus.

1. Į ką reikėtų atkreipti dėmesį?

Kenkėjiškos programos

Kitais žodžiais, tai yra kenksmingas kodas. Tokio tipo kenkėjiškos programos, tarp kurių virusai, kirminai ir trojanai, yra gerai žinomos tiek teoriškai, tiek stebint realius pavyzdžius. Šios programos atakuoja vartotojus, nepaisant jų amžiaus.

Vienas iš pavyzdžių, kirminas *Koobface*, kuris paplito *Facebook* socialiniame tinkle 2009-aisiais metais. Naudodamas įvairias patrauklias žinutes, jis paversdavo kompiuterius *Botnet* atakos aukomis. Apkrėsti kompiuteriai tapdavo *zombių armija*, kurią užpuolikai galėdavo valdyti nuotoliniu būdu. Jo nauja versija, pasirodžiusi po dviejų metų, buvo dar tobulesnė – socialinių tinklų vartotojai, naudojantys Windows, Mac ar Linux operacines sistemas, likdavo visiškai bejėgiai.

Sukčiavimas

Daugelis sukčių naudoja šį metodą išgauti jautriai informacijai – pavyzdžiui, Jūsų vaiko socialinių tinklų profilio prisijungimo duomenys. Tai dažniausiai daroma per el. paštą, kurio prisijungimo duomenys sutampa su socialinių tinklų prieigos duomenimis. Suklastotus puslapius kartais sunku atpažinti, nes skirtumai tarp jų dažniausiai yra neryškūs, tad apgauti asmenys gali toliau naudotis paskyra ir talpinti informaciją net nepastebėję, kad paskyra pateko į sukčių rankas.

Tapatybės vagys

Įsitikinkite, kad vaikai neviešina savo asmeninės informacijos, kuri gali juos identifikuoti, pavyzdžiui, namų adreso, telefono numerio, lankomos mokyklos ar klasės, gimtadienio ir kitų duomenų. To priežastis – tapatybės vagystė, viena iš labiausiai paplitusių kibernetinių nusikaltimų formų, kuomet interneto nusikaltėliai, pasinaudoję internete gauta informacija, apsimeta Jumis ar Jūsų vaiku.

Yra du pagrindiniai būdai, kaip sukčiai gali gauti tokią informaciją:

Naudojimasis socialine inžinerija – bendravimas siekiant išgauti konfidencialią informaciją, neretai apsimetant draugu ar bendraamžiu.

Netaisyklingi tinklo nustatymai vaiko socialiniame profilyje gali atskleisti per daug informacijos. Svarbu paminėti, kad tai nėra tik jaunų žmonių problema, lygiai taip pat daugelis saugusiųjų gali su tuo susidurti.

Persekiojimas ir užgauliojimas internete

Ne visi pavojai Jūsų dukters ar sūnaus socialiniame profilyje gali būti susiję su kibernetiniais nusikaltėliais. Jos ar jo bendraamžiai taip pat gali būti rimta problema. Norime pasakyti, kad patyčios nebėra vien tik mokyklos ar klasės iššūkis. Dabar visa tai persikėlė į interneto erdvę, su lygiai ta pačia žala kaip ir anksčiau.

Kita rizika yra *viliojimas*, labiausiai nukreiptas į mažus vaikus. Taip apibūdinamas suaugusio žmogaus apsimetinėjimas esant vaiku, siekiant lengviau užsitarnauti vaikų pasitikėjimą ir įtikinti juos elgtis nepadoriai. Tai glaudžiai siejasi su erotinių žinučių rašymu, kurios gali būti išsiųstos tiek Jūsų vaikui, tiek ir paties vaiko.

2. Kokių priemonių reikėtų imtis?

Atsižvelgiant į aptartas grėsmes, naudojimasis socialiniais tinklais atrodo itin pavojinga veikla. Visgi, gąsdindami vaiką jais nesinaudoti, veikiausiai problemos neišspręsite – atvirkščiai, vaikai greičiausiai tik stengsis apeiti taisykles. Žemiau rasite patarimus, kurie padės saugiau jaustis socialiniuose tinkluose.

Kalbėkitės

Pokalbis yra vienas svarbiausių dalykų, kai kalbame apie vaikų saugumą internete – ypač socialiniuose tinkluose. Palaikyti atvirą pokalbį ir vystyti supratingą požiūrį yra būtina, jei norite, kad vaikas vėliau kreiptų dėmesį į Jūsų perspėjimus ir patarimus.

Pavyzdžiu temai galėtų būti patyčios internete ir jų prevencija. Paaiškinkite savo dukrai ar sūnui, kad jei šie kada susidurs su patyčiomis, iškart informuotų Jus, mokytoją ar kitą atsakingą asmenį (priklausomai nuo to, kur tai vyksta), net ir tuo atveju, jei tai nėra asmeniškai nukreipta į juos pačius. Svarbu pabrėžti – niekuomet neištrinkite užgaulių žinučių, tai yra vienintelis Jūsų įrodymas.

Naudokite tėvų kontrolės programą

Priklausomai nuo Jūsų vaikų amžiaus, naudokitės tėvų kontrolės programa ir jos privalumais. ESET Smart Security 9 leidžia Jums sudaryti draudžiamų svetainių sąrašą ir riboti vaiko praleidžiamą laiką internete. Kita vetus, vaikams taip pat turėtų būti leista išsakyti savo nuomonę. Todėl programėlė ESET Parental Control for Android suteikia galimybę jiems prašyti Jūsų leidimo apsilankyti tam tikrame puslapyje ar naršyti ilgiau internete, jei šie pabaigė visus namų darbus anksčiau nei tikėtasi.

Naudokite patikimą apsaugos sprendimą

Kadangi kenkėjiškos programos yra labiausiai paplitusi grėsmė kibernetiniame pasaulyje, įdiekite patikimą antivirusinę programą, kuri užtikrins visapusį saugumą net ir tuomet, kai naudojamasi socialiniais tinklais.

Ugniasienė ir apsauga nuo brukalo yra vieni iš įrankių, kurie apsaugo sistemą nuo įvairių rizikų. Taip pat Jūsų vaikas niekuomet neturėtų naudotis administratoriaus paskyra, kol naršo socialiniame tinkle. Tam sukurkites specialų vartotojo profilį vaikui – sumažinkite grėsmės tikimybę.

Naudokite https protokolą

Įsitikinkite, kad Jūsų vaikas naršo https protokolu apsaugotaose svetainėse (matysite tai adreso laukelyje, kur Jūs suvedate svetainės pavadinimą). Tai padės išvengti šnipinėjimo atakų, bandančių nužiūrėti vedamus duomenis. Kol naudojatės https protolu, visi duomenys – ne tik Jūsų atžalos slaptažodis ar prisijungimas – bus užkoduotas ir neįskaitomas jokiam nusikaltėliui.

Patarkite savo jaunuoliams protokolu naudotis prisijungiant ir prie viešo Wi-Fi tinklo.

Naudokite sudėtingą slaptažodį ir dvigubą patvirtinimą

Ar Jūsų vaikai žino, kaip atrodo patikimas slaptažodis? Įsitikinkite, kad jie tikrai nenaudos lengviausiai atspėjamo varianto, kaip kad *slaptazodis* ar *12345*. Apskritai, slaptažodį turėtų sudaryti daugiau nei 10 simbolių, įskaitant skaičius ar ženklus, pavyzdžiui, # ar @. Taip pat priminkite jiems niekam neperduoti savo slaptažodžio, netgi savo geriausiems draugams.

Jei jungiamasi prie *Facebook*, *Twitter* ar kito plačiai paplitusio socialinio tinklo, įsitikinkite, kad Jūsų vaikas naudoja dvigubą patvirtinimą, siūlomą saugumo nustatymuose. Gaudami specialų vienkartinį slaptažodį į savo telefoną, užsitikrinama dviejų sluoksnių apsauga, kurią sunku apeiti net ir gudriausiems sukčiams.

Peržiūrėkite socialinių tinklų privatumo nustatymus

Numatytieji socialinių tinklų privatumo nustatymai neužtikrins saugumo Jūsų vaikams. Todėl patartina skirti šiek tiek papildomo laiko tam, kad nustatytumėte juos teisingai ir nuspręstumėte, kuria informacija norite dalintis, o kurios niekam neatskleisti. Tam, kad suprastumėte, ką turime mintyje, naudojame *Facebook* pavyzdį:

Facebook

Įsitikinkite, kad be išimčių jokia Jūsų vaiko profilio informacija nėra viešai pasiekiama. Geriausiu atveju, informaciją matoma padarykite tik jo / jos draugams ar nedidelei jų grupelei, pavyzdžiui, šeimai ar artimiems draugams.

Ribokite auditoriją, kuri gali matyti nuotraukas, statusą ar kitą turinį, kuriame buvo pažymėtas Jūsų vaikas. Ribokite programėlių prašomą prieigą prie vaikų asmeninės informacijos bei jų skelbiamus įrašus jų paskyroje.

Perspėkite juos, kad kvietimus *draugauti* priimtų tik iš tų žmonių, kuriuos jie pažįsta. Paaiškinkite, kad bendravimas su nepažįstamaisiais internete yra lygiai taip pat pavojingas, kaip ir realiame gyvenime.

Parodykite savo vaikams, kaip valdyti savo profilį naudojantis *veiklos istorija* – savo *Facebook paskyroje* peržiūrint savo ar kitų veiksmus, kurie yra tiesiogiai su jais susiję. Daugiau informacijos rasite ESET tinklaraštyje anglų kalba:: http://blog.eset.com/2011/05/25/facebook-privacy

Twitter

Twitter turi savo specifiką, pavyzdžiui, 140 simbolių pranešimo limitas ar dažnas trumpų nuorodų naudojimas. Tai yra skirtumai, apie kuriuos taip pat reikėtų papasakoti vaikui, siekiant, kad jis liktų saugus.

Be to, *Twitter* paskyroje patartina sekti tik tą žmogų, kurį vaikai pažįsta ar vengti įtartinų nuorodų, jie taip pat turėtų patikrinti neaiškių žinučių teisėtumą. Jei jos yra kenkėjiškos, vaikai atlikę paiešką su jų dalimis, gali atrasti, kad kažkas internete jau paskelbė apie socialiniame tinkle plintančią apgaulę.

Taip pat rekomenduojame į kompiuterį ar kitą įrenginį įdiegti įskiepį, kuris įgalins jų kompiuterį ar kitą įrenginį rodyti pilnus nuorodų adresus, nebūtinai jas paspaudžiant.

Kiti socialiniai tinklai

Ar Jūsų vaikas leidžia laiką kituose socialiniuose tikluose kaip *Snapchat*, *Instagram* ar *YouTube*? Peržiūrėkite kitus mūsų siūlomus šaltinius, pasakojančius apie šiuos socialinius tinklus. Taip pat iš mūsų sudaryto sąrašo Jūs galite išrinkti tinkamiausius socialinius tinklus savo vaikams.

3. Išvados

Be abejonės, socialiniai tinklai yra labai svarbūs interneto vartotojams. Visgi, kaip ir buvo minėta šiame dokumente, socialiniai tinklai slepia daugelį grėsmių, su kuriomis gali susidurti Jūsų vaikas. Nenuvertinkite kibernetinių nusikaltėlių, apsimetėlių, kenkėjiškų programų ar veiksmų, ir naudokite IT įrankius tam, kad apsaugotumėte brangiausius žmones gyvenime.

Padėdami savo vaikams tinkamai susikurti socialinio tinklo profilį ir pasiūlydami naudingą patarimą prisidedate prie jų saugumo.

P.S.

Jei norite prisiminti svarbiausius šiame dokumente pateiktus patarimus, įsiminkite šiuos 10 punktų, kuriuos pavadinome Kibernetinio saugumo *dekalogu*:

1. VENKITE ĮTARTINŲ NUORODŲ

2. NIEKUOMET NESILANKYKITE ABEJOTINOS REPUTACIJOS SVETAINĖSE

3. NUOLATOS ATNAUJINKITE OPERACINĘ SISTEMĄ IR NAUDOJAMAS PROGRAMAS

4. PROGRAMĖLES SIŲSKITĖS TIK IŠ OFICIALIŲ SVETAINIŲ

5. NAUDOKITĖS SAUGUMO SPRENDIMAIS

6. VENKITE PATEIKTI SAVO ASMENINIUS DUOMENIS ABEJOTINOSE FORMOSE

7. BŪKITE ATSARGŪS NAUDODAMIESI INTERNETO NARŠYKLĖSE PATEIKTAIS PAIEŠKOS REZULTATAIS

8. PRIIMKITE Į DRAUGUS TIK PAŽĮSTAMUS KONTAKTUS

9. VENKITE ATIDARYTI ĮTARTINUS FAILUS

10. NAUDOKITE SUDĖTINGUS SLAPTAŽODŽIUS