ENJOY SAFER TECHNOLOGY™

saferkidsonline

Rețele sociale
Ghid pentru părinți

Introducere

Nu cu mult timp în urmă, copiii se jucau în principal afară și intrau în casă doar atunci când le era foame. Însă dezvoltarea internetului a schimbat tot. Acum, tinerii în loc să meargă afară, petrec câteva ore pe zi în realitatea virtuală a rețelelor sociale.

Aici la ESET suntem părinți, de asemenea și înțelegem grijile pe care le aveți văzându-vă copiii absorbiți de lumea cibernetică. Acesta este motivul pentru care vă oferim acest ghid. Veți găsi informații despre amenințările care pândesc pe rețelele sociale precum și soluțiile ce vă vor ajuta în menținerea familiei și copiilor dumneavoastră în siguranță.

1. La ce ar trebui să fiți atenți?

Malware

Este o abreviere din limba engleză a termenilor “malicious” și “software” – sau cu alte cuvinte un cod dăunător. Virușii, viermii și troienii sunt unele dintre exemplele cunoscute. Folosind mesaje atractive, infractorii cibernetici încearcă să determine utilizatorii să downloadeze malware, prin promisiunea unor versiuni gratuite de software sau jocuri.

Phishing

Termenul de phishing preste derivat din "fishing" deoarece atacatorii folosesc o momeală pentru a atrage victimele. Mulți atacatori folosesc această metodă pentru a fura informații sensibile – cum ar fi datele de autentificare ale profilului rețelei sociale ale copilului dumneavoastră. Se realizează de obicei prin e-mailurile ce fac legătura către un site de social media. Poate fi dificil de idetificat pagina falsă, deoarece diferențele sunt de obicei minore, iar copiii păcăliți pot insera datele fără a observa că ceva este în neregulă.

Furtul de identitate

Asigurați-vă că nu sunt postate informațiile sensibile de către copiii dumneavoastră precum adresa de acasă, numărul de telefon, școala sau clasa pe care o urmează, ziua de naștere sau alte date ce ar putea fi folosite pentru a-i identifica. Motivul este furtul identității, unul dintre cele mai răspândite forme de infracțiuni cibernetice, prin care infractorii obțin informații dvs. personale și le folosesc pentru a vă păcăli pe dvs. sau pe copiii dvs. în scopuri malițioase.

Există două moduri principale prin care atacatorul poate obține aceste date sensibile:

Folosind ingineria socială, pretinde a fi un prieten al copilului dvs. de vârsta lui, și încearcă să extragă datle personale prin această modalitate.

Folosind setările de rețea necorespunzătoare, prea multe informații pot fi accesibile de pe profilul rețelei sociale al copilui dumneavoastră.

Hărțuirea Online și Abuzul

Nu toate amenințările la care este expus copilul dvs. pe rețelele sociale implică infractorii cibernetici. Bullying-ul nu mai ține doar de școală și de sala de clasă. Astăzi, s-a mutat în spațiul cibernetic, hărțuirea fiind la fel de dăunătoare.

Un alt risc este manipularea psihologică, care vizează în principal copiii.
În spatele manipulării este un adult care pretinde a fi copil, fiind mai ușor să le câștige încrederea și să-i convingă să facă activități sexuale. Această activitate este conectată, de asemenea, cu mesajele sexuale care includ conținut sexual care pot fi trimise către sau de copilul dumneavoastră.

2. Ce măsuri de protecție există pentru a vă ajuta copiii?

În aceste scenarii de amenințări, utilizarea rețelelor sociale pare o activitate periculoasă. Totuși, interzicerea copilului dvs. să le folosească, nu va ajuta la soluționarea acestei probleme, ducând numai la neascultarea regulilor. Mai jos, veți găsi sfaturi care vor face utilizarea rețelelor sociale mai sigură și care vă vor oferi o protecție adecvată pentru copii și familie.

Discutați

Dialogul este una dintre cele mai importante părți din menținerea copilului dvs.în siguranță în mediul online - mai ales când discutăm despre rețelele sociale. Menținându-vă mintea deschisă în fața întrebărilor și discuțiilor este crucial dacă doriți să aibă încredere copiii în sfaturile dumneavoastră.

Un bun exemplu este hărțuirea cibernetică și prevenția. Clarificați fiicei sau fiului dvs. că dacă vor întâlni un astfel de comportament, chiar dacă nu îi implică pe ei în mod direct, trebuie să înștiințeze imediat profesorul sau educatorul sau pe dvs.

Folosiți un software de control parental

În funcție de vârsta copiilor dvs., folosiți un software de control parental și funcționalitățile lui. ESET Parental Control , vă permite să setați o listă de site-uri blocate și restricționează, de asemenea, timpul și numărul de ore pe care copilul dumneavoastră le poate petrece online.

Pe de altă parte, copiii ar trebui să aibă un punct de vedere. Astfel că, aplicația ESET Parental Control pentru Android le permite să solicite permisiuni pentru a putea vizita un anumit site sau să ceară ore în plus pentru rețelele sociale, dacă își termină toate sarcinile și temele mai devreme decât era setat.

Folosiți soluții de securitate de încredere

În vreme ce malware-ul este cea mai răspândită amenințare în spațiul cibernetic, instalând un software de securitate ce oferă capabilități de detecție proactivă și o bază de semnături actualizată pe dispozitivul copilului dvs., este esențial pentru a evita infectarea când folosește rețelele sociale.

Funcționalitățile de antispam și firewall optimizează sistemul de securitate pentru a face față acestor riscuri. De asemenea, copilul dvs., nu ar trebui să aibă contul de administrator când folosește rețelele sociale. Setați un profil special de utilizator pentru copilul dvs., pentru a minimiza impactul în fața incidentelor.

Folosiți parole puternice și verificarea în doi pași

Copiii dvs. știu cum arată o parolă puternică? Asigurați-vă că aceștia nu vor folosi parole ușor de ghicit cum ar fi "password" sau "12345". În plus, ar trebui să conțină cel puțin 10 caractere, să includă majuscule și minuscule, numere și simboluri speciale precum # sau @.

De asemenea, amintiți-le să nu spună nimănui parola, nici măcar celor mai buni prieteni.

Dacă se conectează la Facebook, Twitter sau alte rețele sociale populare, asigurați-vă că micuții dvs. folosesc autentificarea în doi-pași, oferită de setările de securitate. Primind un singur cod de siguranță pe smartphone-ul lor adaugă un nou strat de securitate care este foarte greu de spart de atacatori.

Schimbați setările profilelelor sociale în "privat"

Setările de confidențialitate ale rețelelor sociale implicite nu garantează securitatea copilului. Totuși, este recomandat să alocați suficient timp când le setați și verificați, de asemenea, ce informații pot fi sustrase. Pentru a vă arăta la ce ne referim, am folosit rețeaua Facebook drept exemplu:

Facebook

Asigurați-vă că nicio setare a profilului copilului dvs. nu este disponibilă în mod public, fără excepții. De preferat este ca aceste informații să fie disponibile numai pentru prietenii săi și dacă este posibil, numai unui grup mic (cum ar fi familia sau prietenii apropiați) dacă aceștia sunt prea mulți.

Limitați audiența care poate vedea pozele, statusurile și alte informații unde copilul dumneavoastră a fost etichetat . Interziceți aplicațiilor să acceseze informațiile lui personale sau să posteze pe profilul acestuia.

Învățați-i să accepte numai cererile de prietenie doar de la cei pe care îi cunosc personal. Spuneți-le clar că dacă vorbesc cu străinii sau dacă îi contactează în spațiul cibernetic, este la fel de periculos cum este în mediul offline.

Pentru informații detaliate despre modul de administrare al profilul de Facebook: http://blog.eset.com/2011/05/25/facebook-privacy

Twitter

Twitter are propriile setări, cum ar fi tweet-uri de maximum 280 de caractere sau folosirea URL-urilor scurte . Aceste diferențe ar trebui adresate copilului dvs. când îi explicați cum să fie în siguranță.

Pe lângă lucruri precum following-ul persoanelor cunoscute sau evitarea link-urilor suspecte, ei ar trebui să verifice legitimitatea oricărui mesaj ciudat. Dacă un mesaj pare malițios și caută părți din acesta, este probabil ca cineva să fi descoperit deja înșelătoria și a expus-o deja în rețeaua socială.

De asemenea, instalați un plug-in la browser pe calculatorul dvs. sau pe dispozitiv care poate scurta adresele URL și care permite copiilor să vadă link-ul original fără a avea nevoie să le acceseze.

Alte rețele sociale

Există multe site-uri de socializare pentru alt tip de interese și grupe de vârstă. Este important să verificați dacă cei micile folosesc pe cele potrivite lor. Vă punem la dispoziție ghiduri video care dezbat Snapchat, Instagram și YouTube și am întocmit inclusiv o listă de rețele sociale adecvate pentru copii.

3. Concluzie

Fără îndoială, rețelele sociale sunt o resursă valoroasă pentru utilizatorii de internet. Totuși, după cum a arătat și acest ghid, sunt multe amenințări la care poate fi expus copilul dvs. când le utilizează. Totuși, nu subestimați infractorii cibernetici sau alți actori malițioși și utilizați instrumente IT pentru a vă proteja cei mai importanți oameni pe care îi aveți în viața voastră.

Ajutându-i să-și configureze corect profilele rețelelor sociale și oferindu-le sfaturi simple, dar utile poate fi un pas decisiv de făcut când discutăm despre menținerea lor în siguranță.

10 sfaturi de reținut

1. Învățați-i pe copii să se oprească și să se gândească înainte de a da clic pe linkuri și butoane de descărcare
2. Învățați-i să abordeze comunicarea online cu un sentiment de prudență
3. Setați conturile copiilor dvs. în modulul privat
4. Învățați-i să refuze solicitările prietenilor din online pe care nu îi cunosc
5. Mențineți-le sistemul de operare și software-ul de securitate actualizat
6. Fiți un model bun și țineți-vă sub control timpul petrecut în online
7. Căutați semnale care ar putea indica faptul că cel mic este o victimă cyberbullying-ului
8. Utilizați o aplicație de control parental de renume precum SET Parental Control
9. Încurajați-i să folosească parole puternice
10. Cereți-le să se gândească înainte de a împărtăși informații personale, videoclipuri sau fotografii.