LUNA EUROPEANĂ A SECURITĂȚII INFORMATICE

CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ
CERT-RO

GHID

Securitatea în rețele sociale și controlul parental în mediul online

Ghid realizat de către:

Bitdefender

în cadrul campaniei de conștientizare a riscurilor de securitate cibernetică derulată în România sub egida ECSM de către CERT-RO.

BE AWARE, BE SECURE.
www.enisa.europa.eu/cybersecmonth

www.cert.ro/tag/ecsm

Pagină alba

CUPRINS

INTRO **4**

AMENINŢĂRI ÎN REŢELE SOCIALE **4**

METODE DE ÎMBUNĂTĂȚIRE A SECURITĂȚII ÎN REȚELE SOCIALE **9**

CONTROLUL PARENTAL ÎN MEDIUL ONLINE **11**

SFATURI DE SECURITATE PENTRU PĂRINȚI **14**

CONCLUZIE **15**

Securitatea în rețele sociale și controlul parental în mediul online

INTRO

Securitatea în rețelele sociale preocupă tot mai mulţi utilizatori din întreaga lume. Este şi firesc, din moment ce oamenii împărtăşesc o multitudine de informaţii personale, la care au acces nu doar prietenii şi familia, ci şi escrocii, care creează ameninţări tot mai variate. Anul acesta, cei aproximativ 900 de milioane de utilizatori Facebook au fost expuşi la scam-uri "clasice" de tipul "*ghici cine ți-a vizualizat profilul*", dar şi la campanii frauduloase care promiteau premii substanţiale.

Bitdefender prezintă câteva aspecte mai puţin ştiute despre reţelele sociale şi metodele care vă ajută să staţi departe de escroci, viruşi, fraude şi alte ameninţări distribuite pe Facebook, Twitter, Pinterest sau LinkedIn. Producătorul de soluţii de securitate va defini apoi cele mai importante probleme cu care se confruntă copiii în mediul online şi va arăta cum pot părinţii să îi protejeze pe cei mici folosind software de control parental.

AMENINŢĂRI ÎN REŢELE SOCIALE

Toate reţelele sociale sunt ameninţate de vulnerabilităţi, fie că este vorba de probleme de conectare, erori de tip "cross-site scripting" sau vulnerabilităţi Java pe care hackerii le pot exploata. Un simplu Troian de tip „dropper” pe care un atacator îl ascunde întrun banner sau link de pe o reţea socială poate ajunge uşor, de la un utilizator la altul, direct pe sistemele vulnerabile. Când utilizatorul intră apoi pe site-ul unui magazin online sau îşi plăteşte facturile pe Internet, Troianul îi poate fura parolele, datele de identificare ale cardului bancar, precum şi alte informaţii personale pe care le trimite la un server de comandă şi control (C&C).

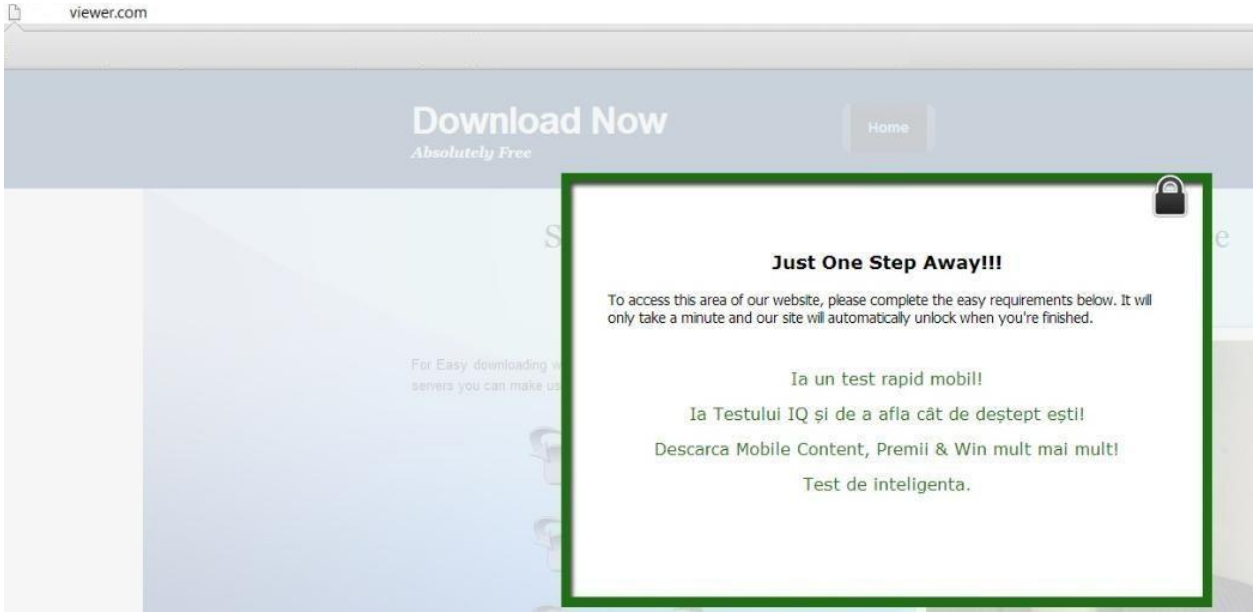
Deşi reţelele sociale precum Facebook au propriul sistem „cloud” în care stochează datele utilizatorilor, multe aplicaţii externe neverificate accesează o multitudine de informaţii personale pentru că oamenii le acordă prea multe permisiuni. Odată ce acestea sunt introduse în sistemul de stocare al aplicaţiilor, nimeni nu mai poate controla ce se întâmplă cu ele.

În ultimii doi ani, numărul de viruşi propagaţi prin reţele sociale, cel mai adesea prin scam-uri de pe Facebook, a crescut. În 2013, cel mai popular virus care a circulat şi pe timeline-uri din România a fost Dorkbot. Acesta s-a răspândit prin chat-ul de pe Facebook sub forma unor linkuri trimise accidental de prieteni. Virusul îşi putea face singur actualizările pentru a-şi instala cea mai nouă versiune şi fusese deja detectat de Bitdefender într-o versiune iniţială, în urmă cu doi ani. Pentru că avea capacităţi rootkit, virusul putea să împiedice soluţiile obişnuite de securitate să se actualizeze şi, totodată, spiona activitatea utilizatorilor în browser. Dorkbot nu se răspândea doar prin mesageria instant, ci şi prin dispozitive USB.

În aprilie 2013, un studiu realizat de Bitdefender a arătat că, în România, cele mai populare escrocherii de pe Facebook sunt de tipul *"vezi cine ţi-a vizualizat profilul".* Acestea le promit utilizatorilor că pot primi o listă a persoanelor care le urmăresc activitatea, mesajele şi pozele de pe reţeaua socială.



În topul site-urilor periculoase răspândite pe Facebook se află şi linkurile frauduloase, care încearcă să îi convingă pe utilizatori să participe la sondaje pentru a câştiga premii, de obicei telefoane mobile sau tablete.



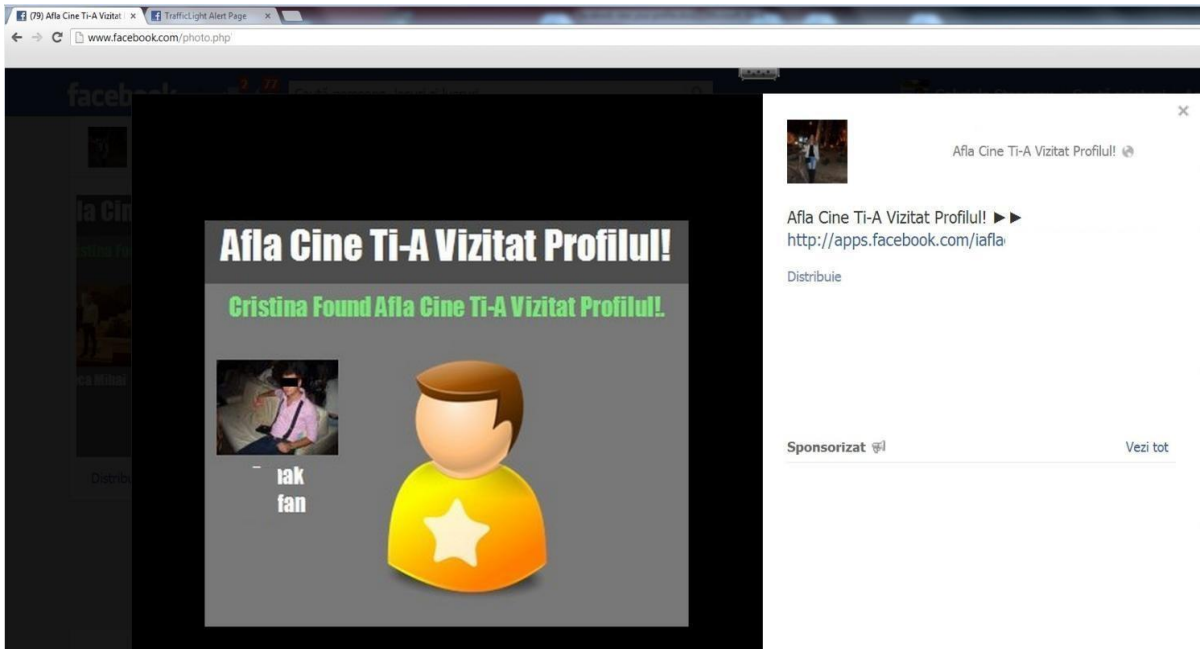
Pentru că utilizatorii au învăţat să recunoască mesajele de tip phishing, prin care le sunt furate datele personale, această ameninţare nu mai este atât de populară ca acum câţiva ani.



După mesajele false de tipul *"cine ţi-a văzut profilul"*, pe locul doi în topul escrocheriilor de pe Facebook se află un filmuleţ care ar înfăţişa-o pe cântăreaţa Rihanna în ipostaze indecente. Un click pe un astfel de link instalează viruşi pe calculatoarele victimelor şi îi păcăleşte să dezvăluie date personale.

Astfel de escrocherii sunt recurente, apărând periodic pe reţeaua socială. Iniţiatorii campaniilor variază doar numele vedetelor şi mesajul folosit, fără a schimba alte coordonate ale scam-ului. Studiul Bitdefender a arătat că, anul acesta, Rihanna şi Taylor Swift au fost numele de vedete cele mai folosite pentru a păcăli utilizatorii. Acestora leau urmat Kim Kardashian, Megan Fox, Justin Bieber, Selena Gomez şi Chris Brown.

O campanie spam populară pe Facebook la nivel internaţional a fost adresată utilizatorilor care îşi doreau să schimbe tematica standard a profilului într-una diferită (de culoare verde sau roşie). Scam-ul le cerea utilizatorilor să descarce şi să execute un fişier de pe un link din afara reţelei sociale. Acesta era, în unele cazuri, o extensie de browser pentru Firefox sau Chrome care îi redirecţiona către pagini cu sondaje şi servicii cu supra-taxă pentru horoscop sau tonuri de apel.



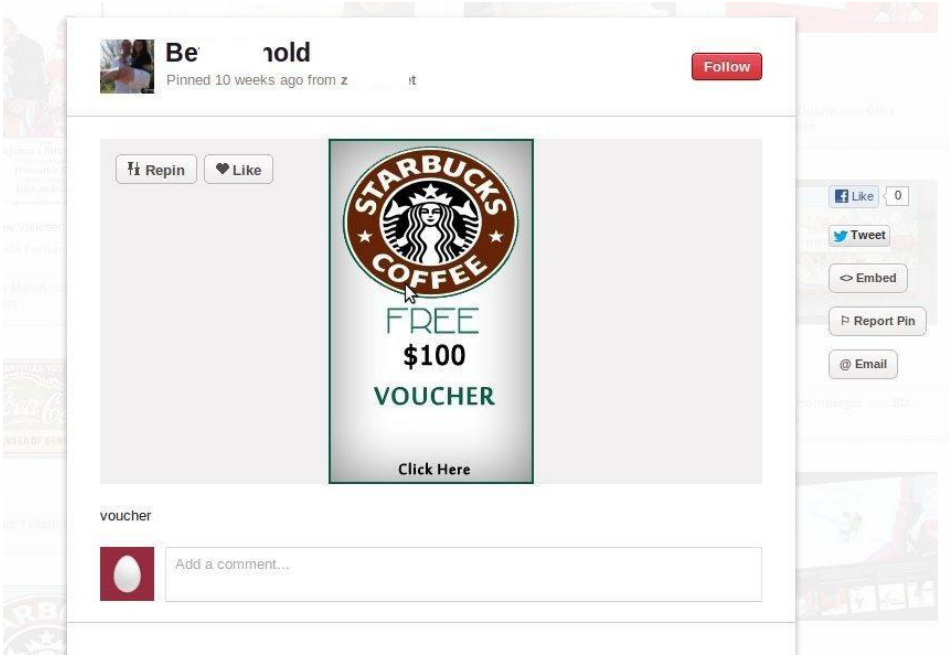
Pentru că frecvenţa anumitor teme în escrocheriile de pe reţelele sociale le poate indica utilizatorilor care sunt mesajele de care să se ferească, Bitdefender a realizat şi un top 10 al escrocheriilor de pe Facebook:

1. Numărul total de vizitatori - 23,86% (limba engleză)
2. Video porno cu Rihanna şi iubitul ei - 17,09% (limba engleză)
3. Am aflat cum să îi văd pe cei care se uită la profilul meu - 5,31% (limba spaniolă)
4. Verifică dacă te-a şters un prieten - 5,18% (limba engleză)
5. Spune adio paginii de Facebook albastre- 4,16% (limba franceză)
6. Clip video porno cu Taylor Swift - 3,76% (limba engleză)
7. Bilete “gratis” la Disneyland - 2,55% (limba engleză)
8. Activează-ţi butonul “nu îmi place”- 2,15% (limba engleză)
9. Îi pot vedea pe cei care mă spionează - 1,67% (limba engleză)
10. Schimbă-ţi culoarea de Facebook- 1,64% (limba spaniolă)

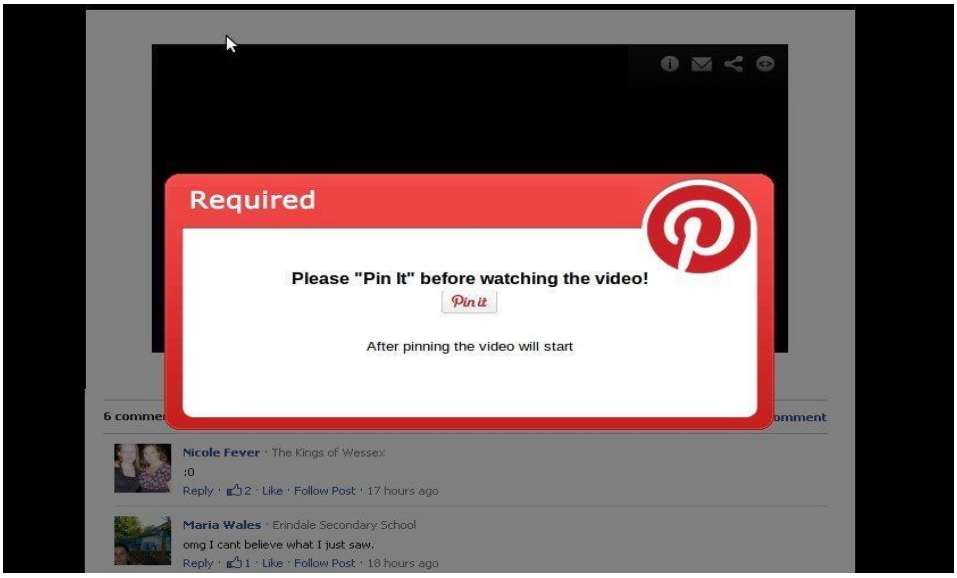
Altele - 32,53%

Dacă în România utilizatorii sunt mai atraşi de escrocheria *"vezi cine ţi-a vizualizat profilul”*, în Franţa oamenii se lasă adesea păcăliţi să îşi "schimbe" culoarea paginii de Facebook. În schimb, englezii şi spaniolii cad repede în capcana promisiunii că pot afla care dintre foştii iubiţi le verifică profilul.

Deşi este destinaţia socială cea mai populară pentru escroci, Facebook nu este singura platformă care le-a acaparat atenţia. Anul acesta, Pinterest a început să devină, de asemenea, o platformă de proliferare a unor scam-uri similare.



Multe companii mari au început să folosească Pinterest pentru a îşi promova produsele, iar unii retaileri spun că utilizatorii de Pinterest ar avea o putere de cumpărare mai mare decât cei de pe Facebook. Cu aproape un milion de utilizatori activi zilnic pe platformă şi un impact vizual puternic, Pinterest le oferă şi spamerilor, şi escrocilor ocazia de a răspândi linkuri frauduloase. Cele mai populare sunt falsele premii şi promoţii, de obicei la gadget-uri, dar şi la companii de zbor sau lanţuri fast-food.



În 2013, securitatea pe Twitter a fost zdruncinată în mod repetat după o serie de atacuri cibernetice asupra unor companii media precum Associated Press, Wall Street Journal, New York Times şi CNN, prin care hackerii le-au preluat controlul conturilor. Spre deosebire de Facebook şi Pinterest, astfel de preluări ilegale ale profilurilor Twitter sunt adesea folosite ca farse la cel mai înalt nivel.

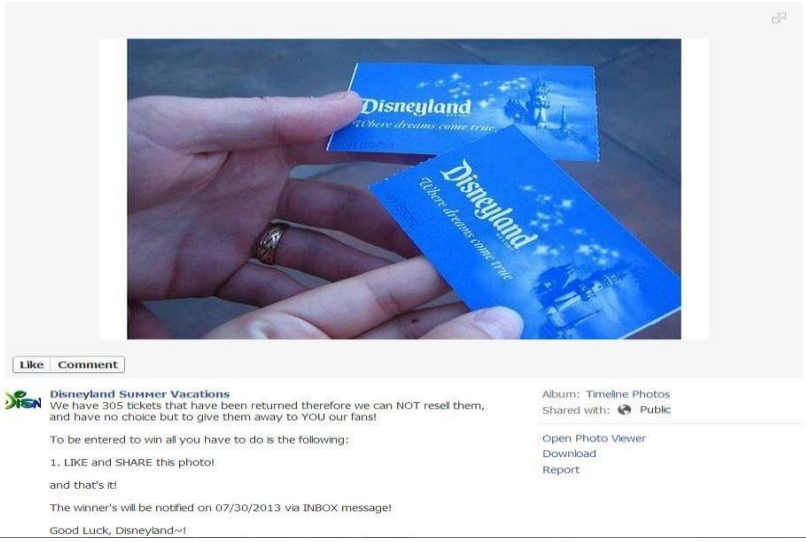
Anul acesta, hackerii au spart contul de Twitter al lanţului fast-food Burger King şi au anunţat că ar fi făcut un parteneriat cu firma rivală McDonald's. Anul a început cu stângul şi pentru utilizatorii obişnuiţi ai reţelei sociale, după ce hackeri pe care compania i-a numit "profesionişti" au furat parolele a aproximativ 250.000 de utilizatori.

METODE DE ÎMBUNĂTĂȚIRE A SECURITĂȚII ÎN REȚELE SOCIALE

Securitatea reţelelor sociale începe cu parola. De obicei neglijată de utilizatori, această înşiruire de caractere este unul dintre lucrurile cele mai dorite de hackeri. Uneori, treaba lor nu este atât de dificilă precum s-ar crede, după cum arată şi topul celor mai "înspăimântătoare" parole din 2012. Acesta include parole mai vechi precum "password", "123456", dar şi cuvinte ca "jesus" şi "ninja", nou intrate în clasament.

O parolă puternică ar trebui să conţină litere mici, litere mari, cifre şi caractere speciale (!@#$%A&*() +-!~=\'{}[]:";~<>?../), să aibă cel puţin 8 caractere, sa fie schimbate cu regularitate (la cel puţin 6 luni) şi să nu fie divulgată în niciun fel altor persoane. Evitaţi folosirea unor informaţii personale precum zilele de naştere, numele animalelor de companie sau numele de dinainte de căsătorie al mamei. Acestea sunt uşor de găsit prin tehnici de inginerie socială sau din simple căutări pe reţelele sociale. Nu folosiţi aceeaşi parolă de la un cont la altul şi asiguraţi-vă că aveţi o parolă puternică la toate serviciile online utilizate.

Escrocii îi tentează pe utilizatori cu opţiuni pe care reţelele sociale nu le au, de exemplu posibilitatea de a vedea cine le-a urmărit profilul, care pe Facebook nu există din motive ce ţin de protejarea vieţii private. Staţi la curent cu noile opţiuni introduse de reţelele sociale şi nu vă încredeţi în nicio aplicaţie promovată înaintea unei lansări oficiale. Menţineţi o atitudine sceptică şi faţă de falsele promoţii cu gadget-uri, bilete de avion sau bilete Disney care nu sunt publicate pe paginile oficiale ale companiilor.



Sfătuim utilizatorii să îşi actualizeze atât soluţia antivirus, cât şi sistemul de operare şi aplicaţiile folosite. Viruşii devin inutili atunci când întâlnesc o soluţie de securitate cu actualizările la zi. În caz că ajung în sistem, ei caută vulnerabilităţi pe care să le exploateze şi care sunt uşor de găsit în software-ul piratat şi neactualizat.

Pe Facebook, utilizatorii se pot proteja de ameninţările apărute cu aplicaţia gratuită Bitdefender Safego, care le scanează timeline-ul şi îi protejează de cele mai noi ameninţări informatice, spam, phishing şi malware, dar şi de supra-expunerea datelor personale.

Utilizatorii nu trebuie să dea click pe mesaje care, deşi par fotografii, sunt fişiere executabile. Chiar dacă par că sunt transmise de prieteni, astfel de mesaje pot instala la descărcare un software periculos ce oferă atacatorilor control asupra calculatorului infectat. Executarea unui astfel de fişier (cu extensia '.exe') este periculoasă în general, indiferent că este primit de la prieteni sau de la persoane necunoscute, prin intermediul programelor de mesagerie instantă (Facebook, Yahoo Messenger etc.)

Toate reţelele sociale au o serie de opţiuni de securitate ce pot fi ajustate. Pe Facebook, de exemplu, informaţiile sunt publice de la sine, la fel ca întregul profil. De curând, compania a lansat un nou serviciu care ajută la căutări mai bine agregate şi care poate returna rezultate precum *"prieteni care urmăresc emisiunea X",* dar şi *"vegetarieni din oraşul meu care iubesc brânza"*. Utilizatorii pot preveni apariţia lor în rezultatele noului Graph Search dacă îşi ajustează setările de securitate şi modifică statutul *"like-urilor"* din public, în privat
.
Totodată, este importantă securitatea navigării în browser, ca metodă de prevenţie a atacurilor de tip phishing. Tastaţi direct adresa site-ului reţelei sociale şi verificaţi că aveţi o conexiune sigură (*https*), acolo unde este posibil. Conectarea de pe reţele Wi-Fi publice şi nesigure trebuie, de asemenea, evitată.

Luaţi în calcul riscurile care există atunci când împărtăşiţi pe FourSquare, Twitter sau Facebook locul unde vă aflaţi. Un check-in nu le spune doar prietenilor unde sunteţi, ci şi hoţilor, care află cu această ocazie şi locul unde nu vă aflaţi: acasă. Natura publică a platformei Twitter face ca securitatea informaţiilor să fie mai greu de controlat. Autentificarea în doi paşi ajută, totuşi, utilizatorii să fie siguri că ei sunt cei care îşi accesează contul, şi nu hackerii. Prin această metodă, se trimite un cod de verificare către telefon, aşa că doar cineva care are acces şi la telefon, şi la parolă se poate conecta la contul de Twitter.

Pe Pinterest, toate informaţiile pe care le împărtăşiţi devin imediat publice. Din fericire, există setări care pot ascunde detaliile şi fotografiile în secţiunea de vizibilitate. Selectaţi opţiunea "Ascunde profilul Pinterest de motoarele de căutare" pentru a va ţine board-ul Pinterest departe de căutările publice.

Pe Google+, oricine poate urmări un alt utilizator fără a îi cere acordul. De aceea, este bine să vă faceţi mesajele private şi să schimbaţi setările pentru diferitele "*cercuri*" de cunoştinţe.

Ca reţea socială professională, LinkedIn poate părea un loc mai sigur în care să vă stocaţi informaţiile personale. Totuşi, platforma are şi ea vulnerabilităţi, iar anul acesta a suferit un atac cibernetic de proporţii, prin care s-au furat peste 6,5 milioane de parole. Utilizatorii LinkedIn sunt cel mai adesea supuşi valurilor de spam, dar şi ingineriilor sociale. Ei trebuie să fie foarte atenţi la persoanele pe care le adaugă în cercul de conexiuni, pentru că unele profiluri pot fi false.

CONTROLUL PARENTAL ÎN MEDIUL ONLINE

Până relativ recent, cele mai multe familii aveau câte un computer în casă, cu care îi puteau introduce în siguranţă pe copii în mediul online, fiind cu ochii pe ceea ce făceau, putând de asemenea să-i şi monitorizeze gradual cu ajutorul unui software cu funcţii de control parental. Odată ce copiii au început să obţină propriile calculatoare, a devenit mult mai dificil de a fi monitorizaţi, de a fi siguri că aceştia au vizitat site-uri adecvate şi nu vorbesc online cu persoane necunoscute.

Acum, desigur, în era telefoanelor inteligente (smartphones) şi a tabletelor, când aceste mini-computere pot fi utilizate oriunde, cei mai mulţi părinţi se confruntă cu o adevărată provocare pentru a educa şi monitoriza copiii în ceea ce priveşte comportamentul lor în mediul online.

Potrivit celor mai recente date EU Kids Online, copiii sunt o prezenţă tot mai activă pe Internet, unde desfăşoară o varietate de activităţi educaţionale şi recreaţionale: cei cu vârste între 9 şi 16 ani utilizează Internetul pentru pregătirea temelor (85%), pentru jocuri (83%), pentru a viziona clipuri video (76%) şi pentru mesagerie instant (62%). Peste jumătate dintre cei cu vârsta între 9 şi 16 ani au un profil pe o reţea socială – incluzând 26% dintre copiii de 9-10 ani şi 49% dintre copiii de 1112 ani. Reţelele sociale sunt cele mai populare în Olanda (80%), Lituania (76%) şi Danemarca (75%), şi cel mai puţin populare în România (46%), Turcia (49%) şi Germania (51%). Utilizarea Internetului este acum complet integrată în viaţa de zi cu zi a copiilor. Ei accesează Internetul la vârste din ce în ce mai fragede. 93% dintre tinerii cu vârste cuprinse între 12 şi 16 ani sunt deja prezenţi în mediul online, în timp ce 63% intră pe Internet zilnic sau aproape zilnic, conform unui studiu realizat de Top Ten Reviews.



Securitatea copiilor pe Internet a devenit la fel de importantă ca siguranţa pe care părinţii le-o dau în viaţa de zi cu zi, iar multe dintre pericolele sociale s-au mutat în mediul online.

Un studiu Bitdefender realizat în 2013 a arătat că cei mici accesează conţinut inadecvat chiar de la 6 ani, iar un sfert dintre copiii de 12 ani şi 17% dintre cei de 10 ani au cel puţin un cont pe o reţea de socializare. Adesea, aceştia mint în privinţa vârstei lor pe Facebook, unde, pentru a avea un cont, trebuie să aibă cel puţin 13 ani.

Cele mai frecvente tipuri de pagini pe care copiii din România încearcă să le acceseze sunt cele cu conţinut pornografic, magazinele online, site-urile de unde pot descărca conţinut piratat şi reţelele de socializare. Cele patru categorii au o pondere de aproape

jumătate din totalul categoriilor de pagini web blocate de părinţi prin programe de control parental.

Cercetarea la care au participat peste 19.000 de părinţi la nivel global mai arată că vârsta de la care copiii accesează programe de mesagerie instantă şi jocuri descreşte, astfel că 2% dintre "pasionaţii" de jocuri pe calculator au cinci ani.

Iată principalele capcane în care pot cădea copiii atunci când folosesc un calculator şi navighează nesupravegheaţi pe Internet:

• *Site-urile cu conţinut nepotrivit*
Conţinutul pornografic sau violent este cel mai blocat de părinţi cu ajutorul programelor de control parental. Pentru a asigura o protecţie ridicată a copiilor în mediul online, o mai bună filtrare include şi alte categorii precum: crimă, droguri, sinucidere, hacking, site-uri care încurajează ura şi altele. Bitdefender Parental Control blochează 31 de astfel de categorii de website-uri nepotrivite.

• *Dependenţa faţă de calculator*
Petrecerea unui număr prea mare de ore pe Internet le poate afecta copiilor performanţa şcolară şi poate genera probleme de integrare socială. Prin programele de control parental, părinţii au şi posibilitatea de a seta intervalul orar în timpul căruia copiilor li se permite să acceseze Internetul, anumite aplicaţii sau jocuri.

• *Acţiunile ilegale*
Copilul lăsat singur la calculator poate săvârşi acţiuni ilegale fără să realizeze implicaţiile lor, de exemplu să descarce fişiere protejate de legea drepturilor de autor precum filme sau muzică. Pentru a fi siguri că acest lucru nu se întâmplă, părinţii pot folosi modulul de control al aplicaţiilor din Bitdefender Parental Control, care le va permite să blocheze software-ul utilizat pentru a descărca fişiere piratate.

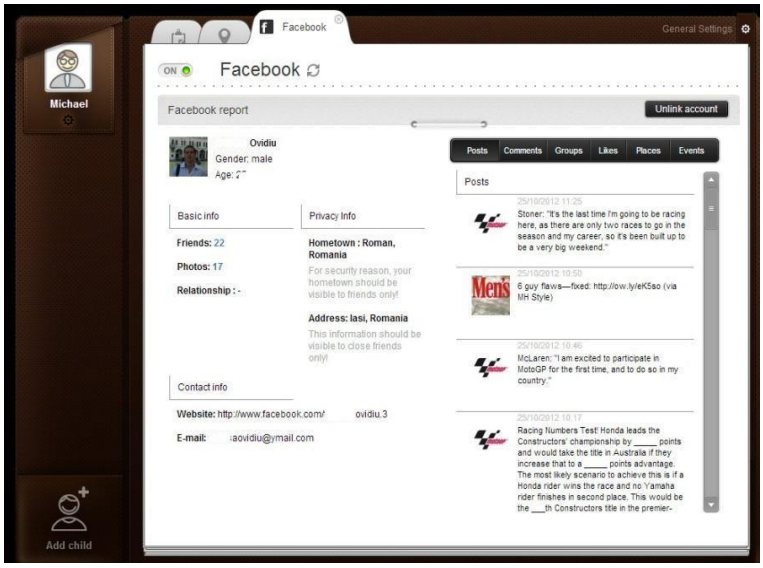
• *Agresiunea sau hărţuirea online (cyber-bullying)*
Copilul poate hărţui alte persoane sau poate deveni victima acestor acţiuni, mai ales prin intermediul serviciilor de mesagerie instant. Potrivit unui studiu EU Kids Online, 6% dintre copiii cu vârsta între 9 şi 16 ani au primit pe Internet mesaje răutăcioase sau care i-au supărat, iar 3% au trimis la rândul lor astfel de mesaje. Peste jumătate dintre cei care au primit mesaje de hărţuire au fost destul de afectaţi.
Părinţii au posibilitatea de a monitoriza activitatea copiilor pe Internet şi pot bloca anumite persoane sau pre-defini o listă de cuvinte-cheie care să declanşeze blocarea unei persoane folosind modulul de monitorizare al mesageriei instant integrat în Bitdefender Parental Control.

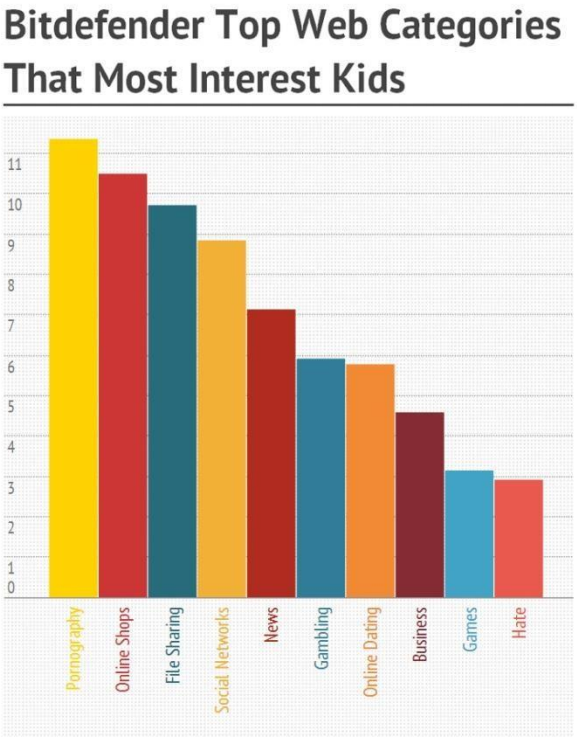
• *Informaţiile personale dezvăluite online*
Acestea îi pun în pericol atât pe copii, cât şi pe alţi membri ai familiei. Cei mici pot dezvălui involuntar date personale despre ei sau despre părinţi care pot merge de la adrese, numere de telefon sau numere personale, până la combinaţia numerică a alarmei de la casă. Modulele de control parental pot fi setate să identifice informaţiile cu caracter personal care sunt dezvăluite prin intermediul reţelelor sociale.

• *Reţelele sociale*

Reţelele sociale sunt un pericol pentru copii dacă aceştia nu cunosc câteva reguli de utilizare. Curioşi fiind, copiii pot fi uşor tentaţi să accepte prietenia unor necunoscuţi. Potrivit unui raport EU Kids Online, cea mai frecventă activitate online riscantă pentru copii este comunicarea cu persoane pe care nu le-au întâlnit faţă în faţă. 30% dintre copiii europeni cu vârsta între 9 şi 16 ani care folosesc Internetul au comunicat online cu o persoană pe care nu o întâlniseră faţă în faţă. Această activitate poate fi riscantă nu doar în viaţa online: 9% dintre copii şi-au dat şi întâlnire cu persoane cunoscute pe Internet. În România, mulţi părinţi subestimează gravitatea întâlnirilor copiilor lor cu persoane necunoscute şi comunică ineficient cu cei mici, care preferă să le ascundă adevărul. Doar 6% dintre părinţi aveau cunoştinţă de acest comportament, potrivit EU Kids Online.

Reţelele sociale sunt periculoase pentru copii şi din perspectiva scam-urilor propagate în acest mediu. Cei mici sunt utilizatori vulnerabili şi pot să dea click cu uşurinţă pe linkuri periculoase şi escrocherii. În spatele unor jocuri şi aplicaţii aparent inofensive se pot ascunde extensii de browser periculoase, linkuri frauduloase sau scheme cu SMS-uri cu supra-taxă. Părinţii îi pot educa pe cei mici să fie foarte prudenţi în acceptarea prieteniei unor necunoscuţi. Ei pot folosi o aplicaţie de control parental pentru a monitoriza activitatea copiilor pe Facebook şi pentru a-i proteja de eventuale pericole.





Potrivit Bitdefender, principalele zece categorii de site -uri pe care părinţii le blochează prin programe de control parental, în funcţie de procentul copiilor care accesează aceste site-uri, sunt:

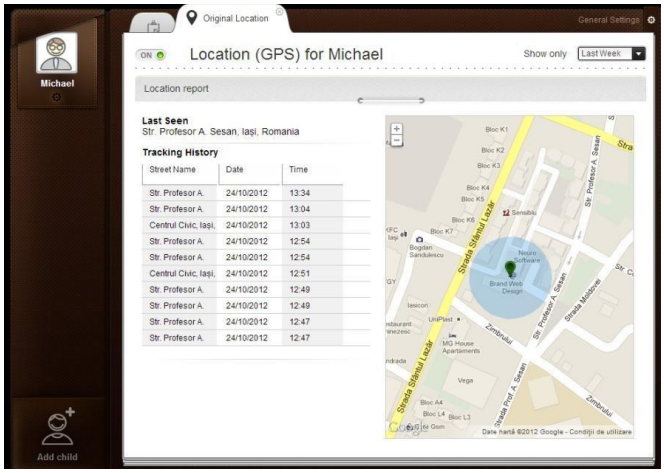
1. Pornografie – 17,5%
2. Magazine online – 11,7%

3. Partajare de fişiere – 11,5%
4. Rețele sociale – 9,4%
5. Știri – 7,4%
6. Business – 7,2%
7. Jocuri de noroc – 5,1%
8. Motoare de căutare – 3,8%
9. Site-uri care încurajează ura - 3%
10. Mesagerie instant - 3%

SFATURI DE SECURITATE PENTRU PĂRINȚI

- Amplasaţi calculatorul familiei într-un loc de unde puteţi supraveghea monitorul.
- Stabiliţi reguli clare când vine vorba de folosirea calculatorului, tabletei şi a telefonului de către copii. Vorbiţi cu cei mici despre pericolele care pot exista pe Internet şi care îi pot afecta atât în viaţa online, cât şi în cea offline.
- Sfătuiţi-vă copiii să nu răspundă la mesaje spam, la hărţuiri de tip cyber-bullying sau mesaje cu conţinut obscen sau agresiv.
- Când consideraţi că cei mici au vârsta potrivită pentru crearea unor profiluri pe reţele sociale, ajutaţi-i să îşi seteze opţiunile de securitate. Încurajaţi-vă copiii să restricţioneze numărul de informaţii publicate online şi să nu accepte prietenia virtuală a unor oameni pe care nu îi cunosc şi în viaţa de zi cu zi.
- Sfătuiţi-i pe copii să fie atenţi când se joacă pe telefon sau tabletă și să aibă grijă la aplicaţiile instalate. Unele jocuri aparent inofensive conţin reclame agresive *(adware)* şi viruşi capabili să trimită mesaje la numere cu supra-taxă şi să acceseze informaţii confidenţiale stocate în telefon.
- Ajutaţi-vă copiii să stea departe de pedofili şi escroci care abuzează de noua opţiune Facebook Graph Search. Reţeaua socială permite şi apariţia minorilor în rezultate, iar datele personale publicate de cei mici pot fi vizate şi de criminalii informatici.

- Folosiţi o aplicaţie de control parental pentru a vă uşura munca de parinte. Bitdefender Parental Control pentru Windows şi Android este inclus în Bitdefender Total Security şi Bitdefender Internet Security, dar poate fi folosit şi ca aplicaţie de sine stătătoare, inclusiv într-o variantă gratuită. Controlul parental include facilităţi de recunoaştere a site-urilor de tip adult, care conţin violenţă, rasism etc., cu ajutorul unui proces rafinat de blacklistare. În funcţie de vârsta copiilor, parinţii pot bloca paginile web folosind filtrul euristic. Site-urile sunt scanate şi clasificate în 31 de categorii, iar cele periculoase sunt blocate în mod automat. Aplicaţia de control parental de la Bitdefender permite şi localizarea copiilor prin GPS, o trăsătură indispensabilă la vârste mici, care ulterior poate fi folosită ca măsură de securitate discretă.



CONCLUZIE

Securitatea reţelelor sociale şi controlul parental în mediul online sunt lucruri care sunt la îndemâna utilizatorilor obişnuiţi, iar utilizatorii trebuie să fie informaţi asupra riscurilor la care se supun în momentul aderării la astfel de platforme de socializare.

Pentru că tehnologia evoluează odată cu noi, avem la dispoziţie şi aplicaţii gratuite sau contra-cost care ne pot ajuta să ne îmbunătăţim experienţa navigării pe Internet întrun mediu mai sigur atât online, cât şi offline.

Securizarea sistemelor de pe care accesăm Internetul, fie ele telefoane mobile sau calculatoare, cu o soluţie antivirus este cea mai sigură metodă care îi ţine departe de viruşi, fraude, phishing şi alte ameninţari atât pe adulţi, cât şi pe copii.