



CROWDSTRIKE

6 PERICOLE LA CARE SE EXPUN COPIII IN MEDIUL ONLINE

LIVIU ARSENE
DIRECTOR CERCETARE AMENINTARI INFORMATICE
CROWDSTRIKE

- Cele 6 pericole online la care se expun copiii

- Malware & Adware
- Phishing
- Cyberbullying
- Furtul de identitate
- Ademenirea / Santaj
- “Hackareala”

- Sfaturi pentru parinti, profesori si copii

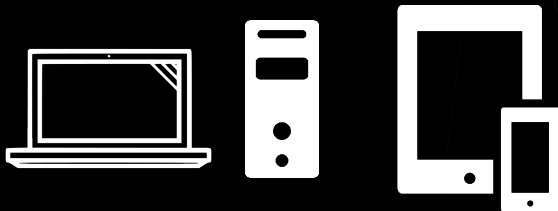
1. MALWARE & ADWARE ASEMANARI SI DIFERENTE

Este este un malware (virus)?

Virusul informatic este un program malware de dimensiuni mici care în general se instalează singur, fără voia utilizatorului, atașându-se altor programe și poate provoca pagube atât în sistemul de operare cât și în elementele fizice ale dispozitivului.

Este este adware (reclame agresive)?

Adware-ul este un program care afișează reclame de conținut promoțional la rularea acestuia, reclame care pot fi afișate ca bannere în fereastra programului, sau de tip pop-up. Unele programe adware pot să colecteze ilegal informații sensibile fără știrea utilizatorului: autentificări, adresa de e-mail, adresa IP, a calculatorului, locația acestuia etc. De obicei, adware-ul nu conține cod nociv ca un virus.



1. MALWARE & ADWARE ASEMANARI SI DIFERENTE

Malware (Virusi)

- Corupe sau cripteaza fisiere
- Colecteaza date personale stocate (e.g. poze, documente, parole, etc.)
- Spioneaza (e.g. inregistreaza conversatii, inregistreaza audio/video, etc.)
- Instaleaza alte tipuri de malware
- Foloseste sistemul compromis in alte atacuri informatice
- Infecteaza si alte dispozitive din retea

Adware

- Afișează reclame pop-up, banere, și link-uri
- Redirectionează către website-uri de pe browserul web
- Instalează componente adiționale fără autorizarea utilizatorului: bare de unelte, alte adware-uri și software-uri terțe nedorite.
- Urmărește activitatea utilizatorului de pe internet și adună informații despre interesele lor, cele mai vizitate website-uri, datele introduse, etc.
- Degradarea generală a performanței sistemului.
- Nu oferă funcție de dezinstalare pentru a preveni eliminarea din sistem.

1. MALWARE & ADWARE CUM ITI PROTEJEZI COPILUL?

Telefon / Tableta

- Nu instalati aplicatii din magazine neoficiale
- Verificati cu atentie permisiunile aplicatiilor instalate si dezactivati permisiunile care nu sunt necesare
- Cititi review-urile si comentariile la aplicatii deoarece va pot spune despre experienta altora cu aplicatia
- Dezinstalati aplicatii pe care nu le folositi deoarece exista riscul ca in urma unor actualizari ele sa introduca noi comportamente nedorite (adware)
- Folositi o solutie de Securitate pentru terminale mobile

Laptop / PC

- Nu instalati aplicatii decat din surse de incredere
- Nu deschideti fisiere sau documente de la persoane necunoscute
- Instalati actualizarile de securitate pentru sistemul de operare si aplicatii
- Nu vizitati website-uri suspecte sau de care nu ati auzi
- Nu instalati programe precum crack-uri, keygen, etc.
- Folositi o solutie de Securitate pentru laptop / PC

2. PHISHING

Ce este phishing?

Phishingul este o metoda prin care, folosind ingineria sociala, se incearca obtinerea unor date personale sau confidentiale, ce pot fi folosite ulterior in mod ilegal de catre atacatori.

Prin telefon:

- este o modalitate prin care o persoana pretinde ca suna din partea unei surse de incredere (banca, membru al familiei, autoritate) si, apeland la tehnici de inginerie sociala, solicita informatii confidentiale cum sunt adresa, nume complet, datele parintilor, etc.

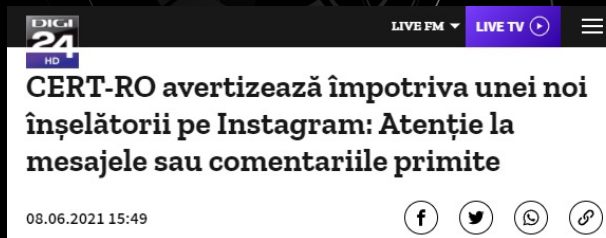
Prin email:

- este un mesaj electronic trimis catre sute sau mii de destinatari (adresele lor fiind colectate prin diverse metode, prin intermediul Internetului), pretinzand a fi din partea unei surse legitime (prieten, institutie, magazine virtual, etc.)



2. PHISHING CUM TE AFECTEAZA?

- Pierzi date personale si sensibile
- Pierzi accesul la conturi (e.g. email, retele de socializare, etc.)
- Pierzi date financiare
- Instalezi malware (virusi) si alte amenintari informatice
- Poti infecta si alte dispozitive din retea
- Devii sursa atacurilor care vizeaza prieteni, institutii, organizatii, etc.



2. PHISHING

CUM RECUNOASTEM?



- Subiectele atrag atentia si indemne la o actiune urgenta (e.g. schimbare de parola in urma depistari acesului neautorizat la contul victimei)
- Se solicita introducerea de date confidentiale folosind un link catre un site indicat in textul mesajului sau deschiderea unui fisier atasat infectat
- Mesajele contin erori gramaticale
- Ofertele sunt prea bune pentru a fi adevarate

2. PHISHING

CUM ITI PROTEJEZI COPILUL?



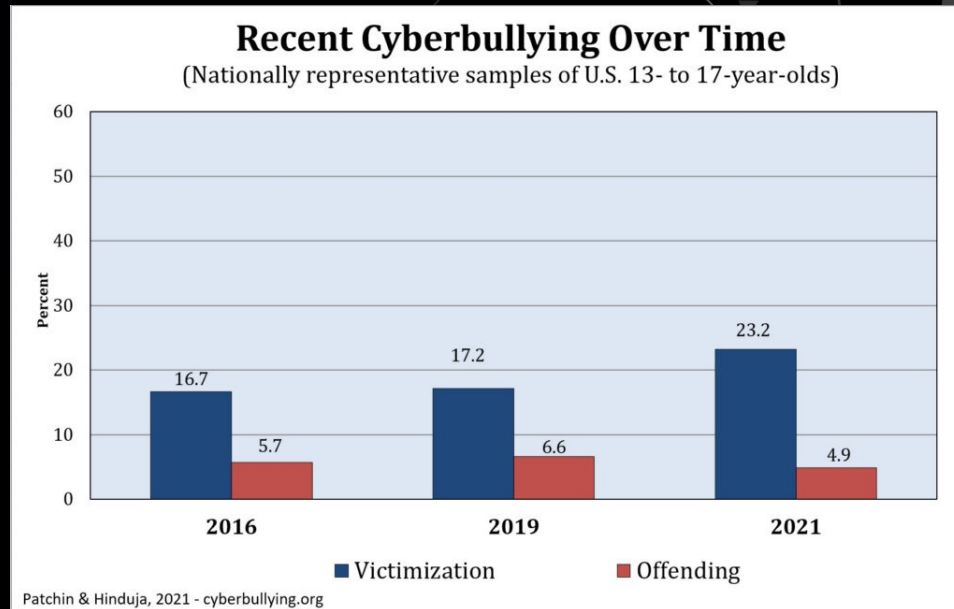
- Nu deschidem email-uri nesolicitate, care provin de la persoane necunoscute
- Nu deschide fisiere atasate sau link-uri din mesaje nesolicitate
- Raportam si stergem email-urile nesolicitate
- Folosim o solutie de securitate

3. CYBERBULLYING

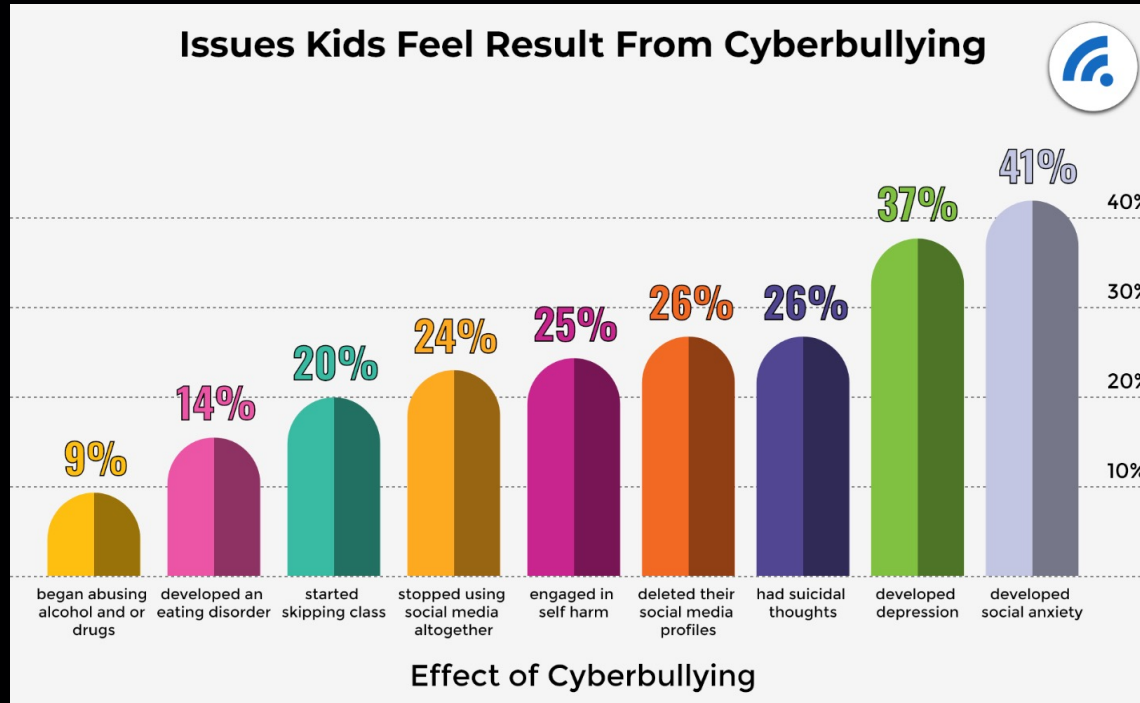
Ce este cyberbullying?

Cyberbullying-ul este o practica prin care cu ajutorul tehnologiei sau mijloacelor de comunicare informatica au ca scop umilirea, abuzul sau amenintarea.

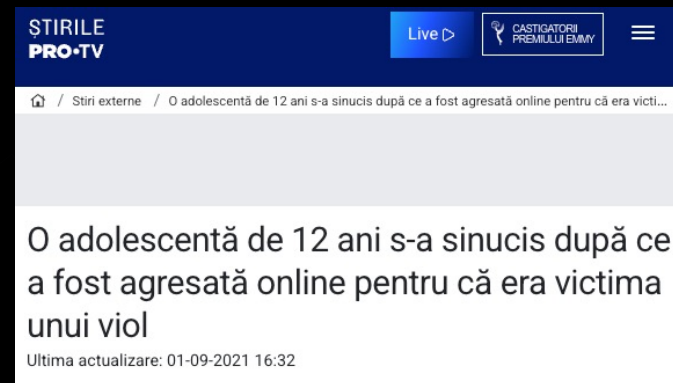
- 60% dintre adolescent au confirmat ca au fost victime ale cyberbullying-ului
- 70% au confirmat ca au fost imprastiate zvonuri false despre ei



3. CYBERBULLYING CUM TE AFECTEAZA?



3. CYBERBULLYING EXEMPLE



3. CYBERBULLYING CUM ÎTI PROTEJEZI COPILUL?

Pentru copii si adolescenti

- Nu este vina ta
- Nu raspunde sau riposte
- Salveaza dovezi
- Instiinteaza persoana sa inceteze
- Cere ajutorul unui adult (e.g. profesor, parinte)
- Blocheaza persoana respective
- Proteseaza conturile cu parole si autentificare in 2-pasi
- Nu dezvalui parolele

Pentru parinti

- Esti norocos daca copilul tau cere ajutor
- Ințelege pe deplin situatia care a general evenimentul
- Raspundeti cu empatie, nu impulsive
- Analizati incidentul din perspective multiple
- Ascultati fara sa judecati
- Ajutati sa-si redobandeasca respectul de sine
- Asigurati suportul moral necesar pentru ai ajuta sa depaseasca

Pentru profesori

- Sprijiniți victima agresiunii în așa fel, încât să-l permită redobândirea controlului asupra emoțiilor sale
- Abordați agresorul explicând de ce este inacceptabil acest tip de comportament
- Responsabilizați spectatorii/observatorii prin apreciere sau informații referitoare la felul în care să acționeze în viitor
- Impuneți consecințe logice, non-violente
- Dacă este posibil, discutați ulterior cu victima agresiunii pentru a vă asigura că bullying-ul s-a oprit.

Comunică-le copiilor tăi că este în regulă să-și blocheze „prietenii” sau să se deconecteze de la website-ul respectiv dacă cineva sau ceva îi face să se simtă incomozi în mediul online. Ei dețin controlul, ei sunt cei care decid dacă blochează sau se deconectează, însă este bine ca ei să discute aceste probleme cu un adult pe care îl cunosc și în care au încredere. Astfel, copiii și tinerii vor avea convingerea că au acționat într-un mod sigur și pozitiv.

3. CYBERBULLYING - IMPORTANT -

LEGE nr. 106 din 3 iulie 2020

1. Articolul 3:

În sensul prezentei legi, violența domestică înseamnă orice inacțiune sau acțiune intenționată de violență fizică, sexuală, psihologică, economică, socială, spirituală sau **cibernetică**, care se produce în mediul familial sau domestic ori între soți sau foști soți, precum și între actuali sau foști parteneri, indiferent dacă agresorul locuiește sau a locuit împreună cu victima.

La articolul 4 alineatul (1), după litera g) se introduce o nouă literă, litera h), cu următorul cuprins:

h) **violența cibernetică** - hărțuire online, mesaje online instigatoare la ură pe bază de gen, urmărire online, amenințări online, publicarea nonconsensuală de informații și conținut grafic intim, accesul ilegal de interceptare a comunicațiilor și datelor private și orice altă formă de utilizare abuzivă a tehnologiei informației și a comunicațiilor prin intermediul calculatoarelor, telefoanelor mobile inteligente sau altor dispozitive similare care folosesc telecomunicațiile sau se pot conecta la internet și pot transmite și utiliza platformele sociale sau de e-mail, cu scopul de a face de rușine, umili, speria, amenința, reduce la tăcere victima.

4. FURTUL DE IDENTITATE

Ce este furtul de identitate?

Furtul de identitate este furtul de date personale în scopul asumării identității unei alte persoane, de obicei pentru avantaje financiare.

Problema nu este nouă, însă ea a fost accentuată de internet, deoarece infractorii au la dispoziție căi noi de a colecta date personale, la o scară mult mai largă. Infractorii folosesc o gamă variată de metode pentru a colecta date personale, de la colectarea datelor deja publicate online (pe profilurile online și rețelele de socializare), până la folosirea unei diversități de tehnici de spam, phishing și pharming.

4. FURTUL DE IDENTITATE

CUM DETECTEZI?

Monitorizezi in mod regulat prezenta ta online.

Prin simpla cautare pe Google sau pe retele de socializare a numelui tau poti identifica tentative de furt de identitate atunci cand cineva creaza conturi sau profile folosiind datele tale personale.

Atentie la mesajele care iti cer sa confirmi accesul la servicii la care nu te-ai abonat.

Cand cineva iti fura identitatea este posibil sa se aboneze la diverse servicii online pentru a obtine beneficii in numele tau (e.g. retele de socializare, vouchere, etc.). Astfel de mesaje nesolicitate care confirma abonarea pot indica tentative de furt de identitate.

4. FURTUL DE IDENTITATE CUM NE PROTEJAM?

Limitați informațiile pe care le împărtășiți online

Cea mai bună modalitate de prevenire a furtului de identitate este, să îl sfătuiești pe copil să nu publice pe internet date personale precum numărul contului bancar, adresa, numărul de telefon, datele din documentul de identitate, etc.

Autentificarea in doi pasi

Utilizați o parolă puternică și unică pentru toate conturile online și activați autentificarea în doi pasi ca protecție suplimentară pentru cele mai importante conturi.

5. ADEMENIREA / SANTAJ

Ce este ademenirea / santajul online?

Ademenirea copiilor se referă la toate activitățile realizate de o persoană cu scopul de a se împrieteni și stabili o legătură emoțională cu un minor (sextortion). Scopul acestei „relații speciale” este acela de a îndepărta inhibițiile copilului, în vederea unui abuz sexual sau a unei exploatări.

Ademenirea copiilor se poate folosi pentru a atrage minorii în activități ilicite, precum prostituția infantilă sau pornografia infantilă.

5. ADEMENIREA / SANTAJ CUM TE AFECTEAZA?

Copii racolați pe internet, apoi șantajați cu materiale pornografice

11 februarie 2021, 14:22 de

Sinziana Ionescu

♥ Devino fan



Salvează în arhivă

**Patru noi cazuri de adolescenți șantajați cu
poze indecente**

🕒 2019-03-23 06:42:02

DIGI 24 HD LIVE FM LIVE TV

HOME > Știri > Actualitate > Justiție > Un bărbat acuzat că racola fetețe ...

Un bărbat acuzat că racola fetețe pe internet mințind că e de vârsta lor, arestat

07.10.2020 16:37

f t w s

5. ADEMENIREA / SANTAJ CUM NE PROTEJAM?

- Nu dam curs solicitarilor de prietenie in mediul online persoanelor pe pe care nu le cunoastem sau nu avem prieteni in comun
- Blocam mesajele nesolicitate de la persoane necunoscute
- Nu divulgam date personale in chatroom-uri publice (e.g. jocuri, game rooms, etc.)
- Nu distribuim poze compromitatoare (chiar si in chat-uri private) in mediul online
- Anuntam parintii sau profesorii cu privire la orice tentativa de amenintare / santaj

6. “HACKAREALA”

Ce este hacking?

Atunci cand copii vor sa faca farse, vor sa-si spioneze “iubitul/iubita”, sau vor recunoastere prin demonstrarea abilitatilor, nu realiza **consecintele accesului neautorizat la sisteme informatice**.

Art 360 Accesul ilegal la un sistem informatic | Codul Penal

- (1) Accesul, fără drept, la un sistem informatic se pedepsește cu închisoare de la 3 luni la 3 ani sau cu amendă.
- (2) Fapta prevăzută în alin. (1) săvârșită în scopul obținerii de date informatice, se pedepsește cu închisoarea de la 6 luni la 5 ani.
- (3) Dacă fapta prevăzută în alin. (1) a fost săvârșită cu privire la un sistem informatic la care, prin intermediul unor proceduri, dispozitive sau programe specializate, accesul este restricționat sau interzis pentru anumite categorii de utilizatori, pedeapsa este închisoarea de la 2 la 7 ani.

6. “HACKAREALA” CUM NE AFECTEAZA?

Pentru victima (copii si adolescenti)

- Invadarea vietii private
- Furtul de date personale si acces la conturile personale
- Pasibil de santaj si abuz

Pentru agresor (copii si adolescenti)

- Risc de savarsire a unei fapte penale
- Pedeapsa cu privarea de libertate

6. “HACKAREALA” CUM NE PROTEJAM?

- Folosim parole (telefon si conturi) complexe, unice, si greu de ghicit
- Nu impartasim parolele cu alte persoane
- Activam serviciul de autentificare in 2-pasi (2FA)
- Activam Lock Screen pentru telefon si alte dispozitive
- Instalam solutii de securitate informatica pe toate dispozitivele personale
- Activam serviciul de Find my Device
- Folosim solutii de control parental pentru a instiinta parinti de orice tentativa de hacking sau cyberbullying
- Citim permisiunile aplicatiilor si dezinstalam aplicatiile pe care nu le folosim
- Nu publicam date personale pe social media si nu acceptam invitatii de conectare de la persoane pe care nu le cunoastem sau cu care nu avem prieteni in comun

CONCLUZII

- Sunt peste 1.3 miliarde de amenintari informatice pe internet la momentul actual
- Un nou malware la fiecare 0.2 secunde*
- 95% din malware vizeaza Windows*
- Android detecteaza doar 82% din malware, mult mai putin decat o solutie de Securitate***
- Adware reprezinta peste 57% din infectiile ce vizeaza terminalele mobile ****
- 81% din email-uri sunt deschise de pe terminale mobile.
- 75% din infectiile din prima jumatate a lui 2021 s-au realizat prin intermediul email-ului**
- 60% dintre adolescent au confirmat ca au fost victime ale cyberbullying-ului
- 70% au confirmat ca au fost imprastiate zvonuri false despre ei

RECOMANDARI GENERALE

- Cea mai bună apărare împotriva riscurilor în mediul online constă în **deschidere, conștientizare și educație**.
- Discută cu copiii tăi despre mediul online, fii la curent cu experiențele lor și învață din ele.
- Ajută-i să utilizeze tehnologia în mod pozitiv și responsabil, stabilește limite și oferă-le sfaturi și asistență.

Q&A

