



FEBRUARIE - MAI 2017

EDUCATIA SMARTFON

GHID EDUCATIONAL PENTRU PROFESORI SI EDUCATORI

W

WORKSHOP EDUCATIONAL 3- SIGURANTA DIGITALA



Erasmus+

INDEX

WORKSHOP EDUCATIONAL 1 – SIGURANTA DIGITALA	3
<i>Demers metodologic</i>	3
<i>Activitatea CITITOR : “ Responsabilitatea postarii ”</i>	4
<i>Activitatea UTILIZATOR : “ Crearea unui profil”</i>	4
<i>Activitatea CRITIC “ Legislatia web ”</i>	4
<i>Activitatea EVALUATOR “ Monitorizeaza-te online”</i>	7

Demers Metodologic

Introducere

Retelele sociale si smartfon-ul permit distribuirea, oricand si in orice loc, a unor momente din viata noastra sau fotografii cu noi. Acestea este unul din motivele pentru care sunt atat de folosite:aceste doua instrumente ofera posibilitatea de comunicare cu un mare numar de persoane, distribuind informatii si perspective, si dovedindu-ne abilitatea de a fi permanent in legatura cu prietenii.Pretul de a fi o parte a unei comunitati, coincide, deseori, cu transferal de date personale,de exemplu: multe dintre cele mai populare media sociale sunt bazate pe geolocalitate si interactioneaza cu alte media sociale care cer utilizatorului acces la datele sale personale, garantand securitatea lor (fara a sti exact pentru ce). Aceasta reprezinta un risc: a expune public datele personale ale cuiva sau miscarile/deplasari acestuia, poate fi considerat un lucru necugetat.De asemenea, o mai mare atentie asupra riscurilor si instrumentele pe care diferite aplicatii le fac accesibile pentru protejarea vietii noastre private, ii pot determina pe tineri sa se simta in siguranta.

Participantii la discutii pot face alegeri prudente, fara a-si pierde simtul umorului.

Obiective

- Sporirea cunostintelor legate de politica de confidentialitate a unei aplicatii
- Sa recunoasca informatiile care pot fi riscante
- Sa identifice oportunitatile oferite de media sociala
- Sa recunoasca instrumentele si cele mai bune practici pentru protejarea datelor personale.

Fisa de lucru

DESCRIERE	Identificarea unor elemente potential riscante sau utile, pornind de la doua profile false. Examinarea politicii de confidentialitate pe Whatsapp. Definirea unui Decalog de instrumente si bune practici..
CUVINTE CHEIE	Drepturi, obligatii, dependent,riscuri,oportunitati.
GRUP TINTA	12-17 ani
DURATA	1 ora
MODALITATE	brainstorming, navigare, lucrul in echipa
ECHIPAMENT TEHNIC	Sala cu proiector si speaker,smartfone

Scop

Acest workshop are ca scop sa-l determine pe participant sa gandeasca ce fel de informatii pot fi distribuite in media sociala; daca acestea reprezinta oportunitati sau aduc beneficii, si care ne expun la riscuri (in mod indirect) prin comunicarea datelor personale. Prin cercetarea politicii de protejare a datelor personale pe Whatsapp,workshop-ul duce la identificarea unor instrumente si actiuni protective care sa ne permita sa alegem, in mod constient, nivelul de distribuire.

Activitatea CITITOR : “ Responsibilitatea postarii ”

Pentru inceput, profesorul/educatorul propune clasei/grupului sa urmareasca spotul video Belgian “Un uimitor cititor de ganduri isi dezvaluie “darurile” (<https://www.youtube.com/watch?v=F7pYHN9iC9I>)

Filmul video permite profesorului/educatorului sa inceapa problematizarea pornind de la ideea securitatii online. Discutia se poate baza pe urmatoarele intrebari:

- Credeti ca aceasta ar putea fi o situatie reala?
- Ati regretat vreodata ca ati postat anumite informatii pe net?
- Exista vre-un comportament pe care il considerati riscant in media sociala?

Activitate UTILIZATOR : “ Crearea unui Profil”

Inainte de a incepe activitatea, profesorul/educatorul imparte participantii in grupe.

Apoi distribuie fiecarei grupe cate o fisa de lucru numita “Profiluri” care reproduce continuturile paginilor sociale a doi participanti ipotetici/imaginari

Profesorul/educatorul cere participantilor sa scrie raspunsurile la urmatoarele intrebari:

- Care dintre informatiile oferite in profil pot reprezenta un risc.De ce?
- Care dintre informatiile oferite in profil pot reprezenta o oportunitate?.De ce?

Apoi, grupele isi impartasesc observatiile.Profesorul/educatorul poate sa le compare cu sugestiile cuprinse in fisa “Profile”

Profesorul cere participantilor care au un profil media sa se uite pe propria lor pagina si sa se intrebe (pe ei insusi) aceleasi intrebari, luand in considerare factorii potentiali de risc si oportunitate din postarile lor.

La sfarsitul activitatii, participantii isi impartasesc parerile legate de:

- Care are cei mai multi factori de risc?
- Care are mai multe elemente ce creaza oportunitati?

Activitatea CRITIC : “ Legislatia Web”

Folosind grupele din activitatea precedenta, profesorul/educatorul cere participantilor sa utilizeze smartfon-ul ca sa caute Politica de confidentialitate la Whatapp sau Instagram.Grupele trebuie sa gaseasca raspunsuri la intrebarile de mai jos(sau macar la cateva dintre ele):

Nivel 1:

- Care este varsta minima la care poti avea un cont?
- Care este scopul si/sau obiectivele unei media sociala?
- Poti alege cine sa-ti vada continuturile postate?
- Ce setari de confidentialitate sunt permise

Nivel 2:

- *Ce informatii personale oferim in momentul cand ne inscriem?*
- *Cum sunt folosite informatiile noastre?*
- *Cine este proprietarul mediei sociale?*

La sfarsitul activitatii,profesorul/educatorul invita grupele sa impartaseasca raspunsurile gasite si sa le compare, daca este nevoie, cu continutul “Legislatia Web-Instagram” si “Legislatia Web-Whatsapp”unde avem niste raspunsuri de dat

Fisa

“Legislatia pe net – Instagram”

Aceasta fisa este un suport pentru a identifica paragrafele cu regulile Instagram pentru a raspunde la intrebarile adresate. Nu uitati ca aceste reguli sunt schimbate destul de frecvent. Acest text se refera la “Conditii de utilizare” si “Politica de confidentialitate” a Instagram in vigoare in Ianuarie 2017.

Raspunsurile la unele intrebari pot fi gasite vizitand Centrul de Ajutor Instagram (<https://help.instagram.com>)

INTREBARE	INDICATII INSTAGRAM
Care este varsta minima la care poti avea un cont?	Trebuie sa ai cel putin 13 ani ca sa utilizezi acest site (“Conditii de utilizare”)
Care este scopul si/sau obiectivul aplicatiei?	Instagram este o aplicatie pe mobil pe care o poti descarca pe IOS ,telefoane Android,tablete ca si pe telefoane Windows 8 sau mai recente.Retineti ca puteti posta doar fotografii si video de pe aplicatia mobilului. (Centrul de Ajutor Instagram)
Pot decide cine sa-mi vada postarile?	Prin utilizarea serviciilor noastre, trebuie sa retii si sa accepti ca noi oferim o platforma pe care sa postezi diferite continuturi, inclusiv fotografii, comentarii si alte materiale. (Continutul utilizatorului) .Asta inseamna ca alti utilizatori pot cauta,vedea,folosi sau distribui orice din Continutul contului tau, pe care l-ai facu t disponibil public prin Service, in concordanta cu Termenii si Conditiiile Politicii de Confidentialitate. (le gasesti la: http://instagram.com/legal/term).
Ce informatii personale trebuie sa oferim cand ne abonam? Cum sunt folosite aceste informatii?	Raspunsul la aceasta intrebare se gaseste in Politica de Confidentialitate,mai exact in sectiunea “Informatii pe care sa ni le oferi direct noua” Sau mergi la Centrul de Ajutor Instagram (https://help.instagram.com)
Ce postari confidentiale sunt permise?	In mod implicit, oricine iti poate vedea profilul si postarile pe Instagram. Poti sa-ti faci postarile private asa incat pot fi vazute doar de catre cei din lista ta de prieteni.Daca postarile tale sunt setate ca private, doar prietenii acceptati pot sa le vada in rubrica Fotografii din Search si Explorer sau pe hashtag sau paginile locatiei.Postarile nu pot fi setate ca secrete de pe un calculator. Pentru mai multe informatii adresati-va Centrului de Ajutor Instagram
Ce continuturi sunt permise?	Consulta “Ghidul de Comunitatii” de pe Centrul de Ajutor Instagram

Fisa

“Legislatia pe net – Whatsapp”

Aceasta fisa este un suport pentru a identifica paragrafele cu regulile Whatsapp pentru a raspunde la intrebarile adresate.

Nu uitati ca aceste reguli sunt schimbate destul de frecvent. Acest text se refera la “Conditii de utilizare” si “Politica de confidentialitate” a Whatsapp in vigoare in Ianuarie 2017.

Raspunsurile la unele intrebari pot fi gasite vizitand www.whatsapp.com.

Whatsapp nu este o retea sociala in sine, ci o aplicatie de transmitere a textelor in timp real. De exemplu, nu exista caracteristici prin care sa se faca public continutul-catre prieteni sau prietenii prietenilor. Din acest motiv, nu este interesant pentru noi, si de aceea nu este retinut pe server (cu unele exceptii cum ar fi cerintele arhivei noastre).

Ar trebui sa reflectam la faptul ca putem furniza toata memoria telefonului acestei aplicatii, si apoi ca dam informatii care nu sunt ale noastre si pe care n-ar trebui sa le folosim.

INTREBARE	INDICATII WHATSAPP
La ce varsta poti sa-ti faci un cont ?	Trebuie sa ai cel putin 13 ani ca sa folosesti Service-ul nostrum (sau varsta prevazuta in legislatia tarii tale ca sa folosesti serviciul nostrum fara acordul parintilor). In plus, daca nu ai varsta minima prevazuta pentru a folosi serverul nostrum ,dar nu mai mult de varsta maxima admisa de legislatia din tara ta, parintii sau tutorele tau trebuie sa-si dea acordul inlocul tau. (“Conditii ale Serverului”)
Care este scopul si/sau obiectivul acestei aplicatii?	WhatsApp Inc. ofera mesagerie, apeluri pe internet si alte servicii utilizatorilor din intreaga lume (“Conditii ale Serverului”) Ca alternativa,, mergi la “Caracteristici” pe www.whatsapp.com
Pot sa decid cine sa vada continutul pe care il postez?	Pentru aplicatia Whatsapp acesta intrebare nu-si are rostul : fiind vorba de un serviciu de mesagerie privata, continutul este vazut doar de destinatar. Mesajele trimise nu sunt stocate si Whatsapp iti ofera controlul deplin asupra comunicarii pe serverul nostrum. (“Politica de Confidentialitate”).
Ce informatii personale trebuie sa oferim cand ne abonam? Cum sunt folosite aceste informatii?	Raspunsul la aceste intrebari se gasesc pe “Politica de Confidentialitate” la urmatoarele rubric: 1. Informatii pe care le furnizezi 2. Informatii colectate automat ; 3. Informatii terțe Sau mergi la “Securitate” pe www.whatsapp.com
Ce setari de confidentialitate sunt premise?	Gestioneaza-ti -ti informatiile. Daca vrei sa gestionezi, schimba, reduce sau strege informatiile tale, noi vom fi de accord s-o faci cu urmatoarele instrumente: -Servicii de setare.Poti sa-ti schimbi setarile pentru a gestiona anumite informatii accesibile si altor utilizatori (ora si data ultimei accesari). Poti sa-ti gestionezi contactele, grupurile si lista de difuzare, sau folosesti caracteristicile noastre de blocare , ca sa gestionezi utilizatorii cu care comunic -Schimbarea numarului de telefon, numele de profil si fotografia si situatia mesajelor.Trebuie sa-ti schimbi numarul de telefon folosind aplicatia noastra si sa-ti transferi contul pe noul numar de mobil. Iti poti schimba si numele de profil, fotografia de profil sau situatia mesajelor,oricand. . (“Politica de confidentialitate”)
Cum pot sa-mi sterg contul? Ce artrade dupa sine?	Poti sa-ti stergi contul Whatsapp oricand (inclusiv daca doresti sa renunti la acceptul dat ca noi sa folosim informatiile tale) folosind serviciul nostru in-app sterge caracteristicile contului meu.Cand iti stergi contul Whatsapp , mesajele tale netrimise vor fi sterse din serverul nostrum la fel ca si orice alta informatie de care noi nu mai avem nevoie . Tine minte ca daca doar stergi serverul nostrum din telefonul tau , fara a folosi caracteristica noastra in-app stergere caracteristicile mele,informatiile tale pot fi stocate pe o perioada mai lunga.Retine ca atunci cand iti stergi contul, acest lucru nu afecteaza informatiile pe care alt utilizator ti le-a trimis, cum ar fi copii ale mesajelor pe care ti le-a trimis cineva. (“Politica de confidentialitate”)

Activitate EVALUATOR : “ Monitorizeaza-te online”

Se mentin grupele anterioare si profesorul/educatorul le propune se creeze un Decalog de bune practici care sa fie aplicate pentru protejarea datelor si persoanelor, si identificarea acelor instrumente care sa exploateze oportunitatile oferite de media sociala fara riscuri.

La sfarsitul activitatii/ profesorul/educatorul invita grupele sa-si impartaseasca raspunsurile gasite, sa le compare, daca este necesar, cu continutul fisei de lucru “Decalogul Securitatii Digitale”, pentru a crea o singura lista continand contributiile tuturor participantilor

Fisa de lucru

“Decalogul Securitatii Digitale”

Istructiuni pentru un nivel mai ridicat de securitate

- ✓ Alege o **parola** sigura. Foloseste o combinatie de cel puțin șase numere, litere și semne de punctuație (cum ar fi “!” sau “&”). Parola trebuie să fie diferită de alte parole pe care le-ai folosit pe Internet.
- ✓ Schimba parola periodic, mai ales dacă vezi un mesaj care îți cere să faci asta. În timpul controlului automat de securitate, uneori Instagram retrage accesul la informațiile care au fost furate de pe alte site-uri. Dacă Instagram descoperă că parola ta ar fi putut fi furată, schimbarea parolei pe Instagram sau alte site-uri, ajută la protejarea contului tău și previne atacul hackerilor pe viitor.
- ✓ Nu spune niciodată parola unei persoane necunoscute sau uneia în care nu ai încredere.
- ✓ Asigura-te că ai un cont e-mail protejat. Persoanele care îți pot citi e-mailurile, pot, de asemenea, să-ți acceseze contul.
- ✓ Deconectează-te de la media socială când folosești un computer sau smartphone cu care lucrează și alte persoane. Nu bifa casuta “Tine-mă minte” când te conectezi la un computer public, deoarece accesul tău va fi pastrat chiar dacă închizi fereastra de căutare (browser window)
- ✓ Personalizează-ți setările de confidențialitate a mediei sociale pe care o folosești.
- ✓ În unele cazuri este mai util să selectezi din modul de căutare anonim sau confidential, pentru protejarea informațiilor bancare pentru plăți sau informații personale – cum ar fi detalii de logare în media socială, ori de câte ori computerul este utilizat de mai multe persoane sau când este supus la risc de furt.
- ✓ Informează-te dacă contul tău este public sau privat și cum vor fi diseminate/răspandite conținuturile.
- ✓ Include funcția locație geografică a smartphone-ului tău dacă nu vrei ca alții să știe unde te afli.

Comportamente adecvate

- ✓ Dacă cineva a distribuit fotografii/video care te deranjează, poți să ștergi sau să blochezi persoana. Poți, de asemenea, raporta conținuturi neadecvate direct din aplicație, dacă ești convins că acestea violență principiile aplicației.
- ✓ Asigura-te că nu ai probleme dacă fotografiile/video pe care le postezi și le distribuie arată cine ești, unui public mult mai mare decât dorești (cum ar fi părinți, profesori, sau viitori angajați).
- ✓ Reflectează mult înainte de a autoriza aplicații de la terți (intermediary)
- ✓ Nu accepta niciodată să faci sau să distribuie ceva ce te face să te simți jenat.
- ✓ Dacă ești agresat, cere ajutorul familiei sau al unui profesor de încredere. Poți, de asemenea, să ștergi comentariile la o fotografie pe care ai distribuit-o și să raportezi acte de violență și intimidare la Centrul de ajutor pentru media socială
- ✓ Cere permisiunea înainte de a posta fotografii cu alte persoane.

In collaboration with

