Erasmus+

Erasmus + project

European media coach in action 2018-2020

E-safety concept handbook

Spanish version

Co-funded by the
Erasmus+ Programme
of the European Union

Proyecto Erasmus+ KA229-544BC79A-EN

Media Coaches in Action

IES FRANCISCO FIGUERAS PACHECO
C/ Fernando Madroñal, nº35 - 03007 Alicante
Teléfono 965 93 64 95 - Fax 965 93 64 96
03001908@gva.es

Erasmus+

GENERALITAT VALENCIANA
CONSELLERIA D'EDUCACIÓ, INVESTIGACIÓ, CULTURA I ESPORT

Unión Europea
Fondo Social Europeo
El FSE invierte en tu futuro

UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

"Proyecto cofinanciado por los Fondos FEDER, dentro del Programa Operativo FEDER de la Comunitat Valenciana 2014 - 2020"

Coordinadores:

- Gloria Gómez Monllor
- José Manuel Doménech
- Carlos Sampedro Sigalat

Manual basado en:

lmz Landesmedienzentrum Baden-Württemberg

PROGRAMA DE CIBERTUTORES (*MEDIA COACHES IN ACTION*) PARA ESTUDIANTES

(Schüler-Medienmentoren-Programm, SMEP)

PREFACIO

Benvolgut estudiant:

Els mitjans de comunicació són una part natural de la teua vida. Passes molt de temps amb els mitjans de comunicació a través de telèfons intel·ligents i Internet. Per a ser honests, els adults no sempre entenem el que fas a Internet ni amb quin entusiasme ho fas. Quan navegues, sovint no ets conscient dels drets d'autor, drets personals, protecció de dades, negocis en línia o fins i tot ciberassetjament. I encara que no veges moltes coses com nosaltres, és precisament en aquestes preguntes on podem ajudar-te. Són suggeriments, idees i fets en els quals hem de pensar junts – perquè una cosa està clara: les oportunitats i possibilitats que ofereixen els mitjans digitals són grans, però cal prendre consciència de com i per a què es poden utilitzar amb seny i atenció. La competència en els mitjans de comunicació és indispensable per a això, tant en la teua futura vida professional com en la vida privada.

El Programa de Cibertutors per a Estudiants s'ha dissenyat per contribuir de forma important a això. L'objectiu és formar tutors dels mitjans de comunicació en els centres escolars que puguen tractar, analitzar i dissenyar diferents mitjans i ofertes mediàtiques, per a que després pugen transmetre els seus coneixements, experiència i consells essencials a altres estudiants. Els estudiants que tenen aquesta competència mediàtica poden informar sobre les seues relacions amb els mitjans de comunicació des de la seua pròpia experiència. Vosaltres sereu els experts que serviran com a socis de contacte per als vostres companys de classe en el futur i que informaran sobre l'ús dels mitjans de comunicació, la producció de mitjans de comunicació i la protecció dels mitjans de comunicació dels joves a les escoles.

Paraules com xarxes socials, protecció de dades i drets d'autor, ús de telèfons intel·ligents o empreses en línia són molt importants avui en dia i ho seran cada vegada més en el futur. Volem que estigues assabentat d'aquests temes per a que sigues capaç de resoldre possibles problemes. Solem dir que la " xarxa no oblida res" perquè qualsevol cosa que fas en línia, deixa rastres de dades. El que es publica en les xarxes socials, però també en missatgers com WhatsApp, pot ser llegit per tot el món. Així que la protecció hauria de ser part de la teua vida digital tant com en la vida real. Per a tu, com a estudiant tutor dels mitjans de comunicació, la Protecció Pedagògica dels Joves en els Mitjans de Comunicació consisteix en:

1. *Resoldre els dubtes d'altres estudiants sobre temes importants.*
2. *Oferir oportunitats per a un compromís apropiat amb els mitjans de comunicació i els temes relacionats amb els mitjans de comunicació. Animar els companys de classe a tractar conscientment els potencials perills i actuar en conseqüència.*
3. *Formar professors per a que treballen temes relacionats amb els mitjans de comunicació a les escoles.*
4. *Convertir-te en un model per als companys en termes d'ús dels mitjans de comunicació i comunicació en línia.*

ÍNDICE

Marco Teórico

PROTECCIÓN DE LOS MEDIOS DE COMUNICACIÓN DE LOS JÓVENES

En una ojeada: PROTECCIÓN DE LOS MEDIOS DE COMUNICACIÓN DE LOS JÓVENES

Aquest mòdul tracta temes importants del teu ús dels mitjans de comunicació i com pots protegir-te de possibles problemes o com pots gestionar els mitjans de comunicació tan conscient i críticament que no sorgisquen problemes en absolut.

Coneixeràs les mesures legals adoptades per l'Estat i les autoritats públiques "per protegir els joves", especialment pel que fa als mitjans de comunicació. A més, es refereix als camps temàtics més importants dins l'àmbit de la protecció dels mitjans de comunicació educatius dels joves. Aquests són:

Comunicació

- **Xarxes socials:**
  - El públic, però prou privat, significava l'ús d'imatges a la xarxa (+ full de treball)
  - Missatges - qui voldrà saber això? I qui pot saber-ho? (+full de treball)
  - Configuració de privacitat
  - Emmagatzematge central de dades (+ full de treball)
  - Economia i finançament de xarxes socials
- **Telèfon mòbil i telèfon intel·ligent**
  - Avantatges i desavantatges
  - Consells importants per a l'ús de telèfons mòbils i telèfons intel·ligents
- **Mobbing i l'assetjament cibernètic**
  - Definició
  - Aspectes Legals
  - Ofertes d'assistència
  - Contracte de classe (materials) - plantilles d'impressió

Privacitat de dades

- **Protecció de dades i autodeterminació informativa**
- **Tipus especials de dades personals i dades personals**

El dret d'autor a Internet

- **Descàrregues il·legals**
  - Pujades il·legals a YouTube, *Facebook*, ebay, etc.
  - Advertiments
  - Streaming (informació general)
- **Descàrregues legals**
  - *Creative Commons* (patrimoni comú creatiu)

Comunicació

Escriure cartes és una cosa del passat, avui xarrem en línia. Els xiquets i els joves utilitzen Internet principalment per a comunicar-se i entretenir-se i un poc menys per a obtenir informació.

Els adolescents es comuniquen en i amb els mitjans de comunicació!

Escriu quins mitjans de comunicació digital utilitzes i quantes hores (entre parèntesis) passes cada setmana aproximadament. El mitjà / dispositiu més important a la part superior:

1) _____

2) _____

3) _____

4) _____

La comunicació dels joves a Internet es realitza principalment a través de les xarxes socials, la lectura i l'escriptura de correus electrònics i diverses sales de xat. En aquest cas, perills com la publicitat, que prometen coses gratis i causen costos considerables en retrospectiva, són un problema.

Per tant, presta atenció al que fas clic i tanques en Internet, ja que això pot tenir conseqüències costoses si s'actua desconsideradament. Pott evitar fàcilment aquests problemes amb la teua pròpia atenció i, sobretot, per una actitud crítica cap a les ofertes a Internet, per exemple, en els correus electrònics publicitaris.

Quins problemes poden ocórrer quan et comuniques amb amics i coneguts o fins i tot amb persones desconegudes al xat? Dóna alguns exemples a l'entrada de la pàgina següent. A continuació, pots unir-te al grup *CIBERTUTORS* i definir les regles més importants per evitar possibles problemes.

Quines són les **teues 5 regles més importants** per a la comunicació a Internet?

1) _____

2) _____

3) _____

4) _____

5) _____

Xarxes socials

Conèixer als teus amics a *Facebook* és probablement tan important com veure vídeos a *YouTube*, jugar a jocs d'ordinador o simplement escoltar música. Internet t'ofereix moltes possibilitats d'ocupació i comunicació. Per això les xarxes socials són tan populars entre els joves. Aquestes xarxes socials tenen funcions importants, diuen els experts.

Els mitjans de comunicació són importants companys de creixement

Probablement t'agrade utilitzar Internet de forma intensiva com a plataforma de comunicació, ja que pots posar-te en contacte amb altres persones de forma fàcil i ràpida. (p. ex., a través de missatgeria instantània com WhatsApp). Pots trobar companys o persones amb idees afins a Internet si tens problemes personals o preguntes que preferiries que es responguereen de forma anònima (p. ex. en blogs i fòrums).

La Xarxa Social també ofereix noves formes de tractar amb tu mateix i amb el teu entorn i, per tant, també de trobar la teua identitat. Hi ha moltes més oportunitats allà que en el món real. A les xarxes socials, les proves d'identitat són fàcils i amb uns pocs clics en el teu perfil, pots provar nous rols. La xarxa ofereix moltes possibilitats d'autoretrat, que no són tan múltiples en el món real. En el món virtual pots canviar la teua identitat tantes vegades com vulgues. Com es veu en el món real? Per què és tan important orientar la teua identitat cap al món real?

Les relacions que fas en línia poden variar des d'amics de xat no vinculant a grups de xarxes socials i amistats reals. Joguinejar a la xarxa pot ser divertit per un curt temps, però quan es tracta de la pròpia identitat, les veritables amistats que sempre estan connectades amb el que un realment és són molt importants.

La comunicació en línia no substitueix les relacions personals, sinó que les complementa i aprofundeix. Totes les xarxes socials viuen de l'alegria de la comunicació i presentació dels seus usuaris. En els perfils, més de dos terços dels joves dipositen fotos i vídeos en línia.

Quin és el problema? Internet és una xarxa i no oblida res!

Internet no oblida res. Això sempre s'ha de tenir en compte. Quin és el problema? Proveu un motor de cerca de persones com *www.yasni.de* o *www.Google.com* (especialment recerca d'imatges). Allà pots trobar el que pots trobar a la xarxa. No tot està bé, com les fotos de benjamí en el futbol o el grup de ball de l'escola primària, que ja no vols veure. La informació individual que publiques sobre tu mateix pot ser reunida per a formar una imatge molt completa d'una persona. I això també pot tindre un impacte en la vida professional: Cada vegada més ocupadors, per exemple, utilitzen les xarxes socials per informar-se sobre els candidats o perquè els seus futurs empleats treballen en xarxes socials.

Les xarxes socials i la teua tasca com a cibertutor.

L'elecció de les respectives xarxes socials a Internet està oberta a tots. Cadascú pot decidir per si mateix quina informació personal introdueix ahí. No obstant això, com un tutor dels mitjans de comunicació pots ser un company útil per a l'ús correcte de les xarxes socials per a altres estudiants amb la informació obtinguda ací.

També ha de quedar clar que ningú ha d'unir-se a una xarxa durant els cursos de mitjans de comunicació per a utilitzar una plataforma de comunicació central i sense complicacions com a grup. Informa't sobre els distribuïdors de correu electrònic adequats o les xarxes descentralitzades (per exemple, Diàspora), que no emmagatzemen dades.

Grups de correu o llistes de distribució de correu electrònic

Els grups de correu també es denominen llistes de distribució de correu electrònic que pots configurar amb el proveïdor de correu electrònic. Si hi ha un servidor de l'escola, és encara millor arreplegar l'adreça de correu electrònic de tots els participants i crear un llistat de distribució amb els participants en el projecte *CIBERTUTORS*.

Xarxa descentralitzada com a alternativa a les xarxes comercials

La xarxa descentralitzada Diàspora és una bona alternativa si no desitges comunicar-te amb altres a través d'una plataforma comercial a Internet. Descentralitzat vol dir que les dades no poden emmagatzemar-se i utilitzar-se en un servidor (per exemple, *Facebook*), sinó que totes les dades romanen sempre en el seu propi ordinador.

Quina informació pots trobar sobre tu mateix a la web?

Buscant la teua empremta virtual!

Introdueix el teu nom a www.*Google*.es i documenta la teua taxa d'encerts en la taula amb l'ajuda d'un llistat de resultats.

	Compte	Observacions
Imatges normals		
Imatges qüestionables		

No has pogut trobar cap informació sobre tu a la web? Intenta-ho amb figures públiques, per exemple, el director de l'escola o l'alcalde!

	Compte	Observacions
Imatges normals		
Imatges qüestionables		

Què és el que no et va agradar en absolut, què s'escriu sobre tu o altres a la xarxa?

Com vols gestionar els teus missatges i dades en el futur? Estableix algunes regles per a tu i intenta evitar el contingut qüestionable sobre tu a la xarxa.

L'exercici de la teua empremta virtual hauria de mostrar-te la informació ja ajustada sobre tu a la xarxa. En la següent secció de *CIBERTUTORS* pots aprendre com gestionar la informació sobre tu. Això no vol dir que has de detindre totes les activitats d'Internet immediatament. Molts altres estudiants de la teua escola poden beneficiar-se dels coneixements que adquireixes ací.

Has de ser conscient que qualsevol informació que poses en l'Internet romandrà allí i pot ser fàcilment trobada.

Configuració de privacitat a *Facebook* i creació de llistes d'amics!

El major problema de la gent en les xarxes socials en aquest moment és el correcte ús de la configuració de privacitat, per exemple, en *Facebook*. Moltes persones publiquen fotos i informació sobre si mateixes a Internet sense pensar.

No obstant això, la configuració de la teua privacitat i, sobretot, la creació de llistes d'amics a *Facebook* ja no hauria de ser un problema per a tu després de la teua formació en *CIBERTUTORS*.

Atès que *Facebook* canvia la configuració de privacitat amb força freqüència, hauries (si fas servir *Facebook*) estar sempre al dia, per exemple pel que fa a les teues llistes d'amics o cròniques. En el següent full de treball pots trobar la informació més important per a establir la teua privacitat.

Sovint pot passar que tu mateix utilitzes les teues dades amb molta cura i no publiques fotos a la xarxa. Però si altres, per exemple els teus companys de classe, publiquen fotos teues a la xarxa, comences de nou des del principi. Has de reaccionar absolutament a això i assenyalar a la gent que tu no has donat el teu consentiment per a posar aquestes fotos a Internet.

Un dels millors portals d'Internet per a l'ús mediàtic dels joves és www.klicksafe.de. Busca les instruccions adequades per a la configuració de privacitat en *Facebook*! Escriu els enllaços corresponents:

Xarxes socials - milers de milions d'usuaris signifiquen milers de milions en ingressos!

"Què bé, aquestes cadenes! No he de pagar res i, tanmateix, em permet tindre i utilitzar una xarxa mundial. Tots els dies!" Aquesta declaració es pot escoltar una i altra vegada. Probablement ja saps la resposta i també saps per què les xarxes socials com *Facebook* poden ser gratuïtes. Descobreix en aquesta pel·lícula per què *Facebook*, per exemple, guanya tants diners. És realment només publicitat o és també la forma en què es pot col·locar la publicitat?

"*Facebook* en el Present i Futur - Vendes de Dades i Models de Negoci"

http://www.youtube.com/watch?v=YfkFuh8aW8I

Les xarxes socials amb els números d'usuari més importants

Xarxa	breu descripció	edat / grup destinatari	xifres d'usuaris
Facebook (FBK)	la major xarxa social del món	a partir dels 13	més de 1100 milions a tot el món
Skype	servei de comunicació (càmera web)	a partir dels 13	665 milions d'usuaris o més a tot el món
Twitter	servei de comunicació “Tweets”	sense límit d'edat, principalment per a adults	517 milions d'usuaris a tot el món

Google +	semblant a *FBK*	a partir dels 13	més de 500 milions usuaris a tot el món
Instagram	intercanvi de fotos i vídeos	cap límit d'edat	més de 100 milions usuaris a tot el món

Font: www.socialmediastatistik.de

Telèfon mòbil i Telèfon intel·ligent *(Smartphone)*

Els telèfons mòbils i cada vegada més els telèfons intel·ligents amb accés a Internet estan en mans de tots els joves. La Internet mòbil, és a dir, l'accés a la *World Wide Web* a través de telèfons intel·ligents, ofereix innombrables possibilitats de comunicació. No obstant això, l'ús de les opcions de comunicació a través de telèfons intel·ligents no només pot resultar en alts costos, sinó que també es poden transmetre dades sensibles, com informació sobre la pròpia vida i la persona.

Les diverses possibilitats multimèdia dels telèfons intel·ligents moderns, com les càmeres fotogràfiques, les gravadores d'àudio i les càmeres de vídeo, s'utilitzen sovint de forma descuidada i els resultats, com els vídeos d'amics borratxos o les fotos vergonyoses dels companys de classe, es publiquen ràpida i fàcilment a Internet.

Els vídeos violents i la pornografia en el propi mòbil o telèfon intel·ligent es consideren il·legals. Es comet un delicte, en particular quan els continguts pornogràfics es transmeten a menors de 18 anys.

Aplicacions - Robatori de dades en el propi telèfon intel·ligent

Els telèfons intel·ligents moderns ofereixen possibilitats gairebé infinites a través de les aplicacions. Aquestes aplicacions es poden utilitzar per a la navegació, els mitjans socials, els missatgers o la creativitat multimèdia.

Les aplicacions en particular poden llegir dades personals emmagatzemades al telèfon intel·ligent, com noms, adreces i números de telèfon. Fins i tot pot ser possible llegir la teua pròpia llibreta d'adreces, l'historial de cerca a Internet i el tràfic de correu electrònic. Es tracta de dades importants que poden ajudar els fabricants d'aplicacions a guanyar diners, ja que aquestes dades també poden ser utilitzats per tercers amb finalitats publicitàries.

Per evitar això, és essencial llegir la política de privacitat del proveïdor. Especialment si hi ha un indici que **"es transmetran dades personals"**, aquesta aplicació no s'hauria d'instal·lar.

Consells importants per a l'ús de telèfons mòbils i telèfons intel·ligents

La **comunicació a través del telèfon mòbil i del telèfon intel·ligent** ha de ser tan agradable i amigable com quan es coneix a la gent a la realitat. Per tant:

- Insultar altres persones a través del telèfon mòbil no és possible, això és intimidació!
- No pots simplement fer una foto / vídeo i després posar-lo a Internet! Pregunta amb cada foto / vídeo:

  A qui es pot veure a la foto i el vídeo?

  Tens el consentiment de la persona?

  Per què cal pujar la imatge / vídeo a Internet?

Localització *GPS* - La localització *GPS* pot ser molt útil per a la navegació i mostrar-te el camí millor, però tota la resta té poc sentit. Les dades sobre tu es recullen ací! Es tracta d'on ets i quan. Es diu perfil de moviment.

- Revisa totes les aplicacions per veure si el rastreig *GPS* és realment necessari.
- Activa els serveis de rastreig *GPS* per la seua funcionalitat només quan realment ho necessites.

Bluetooth - La funció *Bluetooth* pot causar problemes perquè permet als teus amics accedir al teu telèfon.

- Activa la funció Bluetooth només si ho necessites.
- Comprova el contingut que arriba al teu telèfon mòbil a través de Bluetooth!
- Si tens un telèfon intel·ligent, comprova també la (pre) configuració de Bluetooth!

WLAN - Si configures la teua pròpia *WLAN* a través del teu telèfon intel·ligent, moltes persones poden accedir:

- Si configures una WLAN, encripta el tràfic de radi amb una contrasenya.
- Apaga la WLAN quan no la necessites.
- Atenció als *hotspots*! Sempre esbrina què tan segur és el *hotspot*.
- Seguretat i privacitat de contrasenyes - Hi ha molta informació personal en el teu telèfon que ha de ser protegida:
- Protegeix el teu telèfon mòbil de l'accés no autoritzat amb un PIN segur.
- No emmagatzemes contrasenyes en el teu telèfon mòbil ni en el teu telèfon intel·ligent (notes, etc.).

Porno i vídeos violents - Posseir i transmetre continguts prohibits al telèfon mòbil és punible:

- No participes en la distribució de vídeos pornogràfics i violents!
- Si has vist un contingut pertorbador, parla d'això amb els pares o mestres.

Protecció antivirus i trampes de costos - la publicitat que arriba per correu electrònic o *SMS*, sovint oculta virus o trampes de costos:

- Obri els correus electrònics en el teu telèfon intel·ligent només si coneixes al remitent de forma segura.
- No et subscrigues per telèfon mòbil.
- Para atenció al teu dret de desistiment i fes ús d'ell en cas de dubte!

Com, quan i per què faig servir el mòbil / telèfon intel·ligent?

Probablement sempre tens el teu mòbil / telèfon intel·ligent amb tu i ho fas servir molt. Sovint, inconscientment, busques el teu telèfon mòbil o telèfon intel·ligent i l'encens. Per a tu, com a estudiant de *CIBERTUTORS*, és interessant saber quant de temps passes en el teu mòbil / telèfon intel·ligent, per quines activitats i a quina hora del dia.

Intimidació e intimidació cibernètica

(Mobbing & Cybermobbing)

"Amb ciberassetjament *(Cyberbullying)* o ciberintimidació *(Cybermobbing)* entenem insultar, amenaçar, exposar o assetjar a les persones a través dels nous mitjans de comunicació - per exemple, telèfons mòbils, correus electrònics, llocs web, fòrums, xats i comunitats."

Definició del Ministeri Federal de la Família, la Tercera Edat, la Dona i la Joventut

Font: http://www.bmfsfj.de/BMFSFJ/cybermobbing,did=168.578.html

Quan la gent és intimidada, això generalment es fa per mitjà de l'escriptura i el llenguatge. Exposar, amenaçar, denigrar i insultar són possibles procediments dels assetjadors. Les falsetats i l'assetjament s'utilitzen per a humiliar les víctimes durant un període de temps més llarg.

El ciberassetjament és una nova forma d'assetjament, però en general representa només l'anomenat "cim de l'iceberg de l'assetjament". En l'assetjament cibernètic, els assetjadors utilitzen els mitjans digitals moderns i els mitjans electrònics de comunicació per a caçar a les seues víctimes. Les víctimes es veuen afectades per aquests atacs electrònics en tots els àmbits de la vida, ja que es pot arribar a moltes persones i les mentides es propaguen en qüestió de segons a través dels mitjans de comunicació moderns.

Com totes les formes d'intimidació, la intimidació cibernètica pot causar estrès psicològic i físic greu. Les crisis d'identitat i d'autoestima són sovint les conseqüències que poden portar a una actitud d'ansietat davant la vida. En qualsevol cas, els autors són castigats principalment pel ciberassetjament a la xarxa.

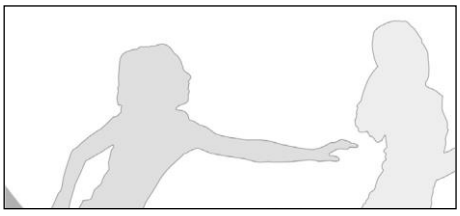
L'assetjament cibernètic i la llei

Tot i que el ciberassetjament no és un delicte en si mateix, les manifestacions individuals com els insults, la calúmnia o la difamació són delictius i poden ser castigades en conseqüència.

Com a prova, l'instructor de tutors pot projectar una pel·lícula en el grup *CIBERTUTORS*, o també teniu la possibilitat de veure la pel·lícula a Internet:

"Let's fight it together" - Childnet.com Spot

Assetjament cibernètic - Què pots fer?



Com ja saps, l'assetjament cibernètic és una forma d'assetjament en què algú és assetjat durant un període de temps més llarg a través de l'ús dels mitjans moderns de comunicació, com Internet i els telèfons mòbils. Es diferencia de la intimidació en els següents factors addicionals:

- Les publicacions ofensives i dolentes no es poden eliminar de la web o només es poden eliminar amb dificultat.

- La naturalesa dinàmica d'Internet vol dir que el contingut pot ser distribuït ràpidament a un nombre infinit de persones.
- No hi ha lloc de retir per a la víctima, ja que la tecnologia moderna el fa accessible en tot moment.
- La publicació ràpida de vídeos / fotos a través d'un telèfon intel·ligent sovint condueix a intimidacions no desitjades. Aquestes entrades i comentaris poc meditats poden convertir-se ràpidament en un cas de ciberassetjament. Per tant: penseu sempre quines conseqüències pot tindre abans que les fotos, els vídeos i els missatges es publiquen a la xarxa.

Per a previndre l'assetjament cibernètic per avançat, com a tutor de *CIBERTUTORS* en l'àrea de protecció dels mitjans de comunicació juvenils, pots fer una contribució important i explicar els companys de classe sobre les causes i conseqüències de l'assetjament cibernètic. Si cal, també pots transmetre la informació als pares i professors.

Quina és la millor manera de tractar amb un cas d'assetjament cibernètic?

- Si hi ha un cas de ciberassetjament en el teu ambient, t'ho has de prendre seriosament. Discuteix amb un tutor (o un altre adult amb qui tingues confiança) el procediment a seguir i no actues arbitràriament!
- L'assetjament cibernètic és un procés complex en el qual poden participar moltes persones diferents. Per això és important mantindre la calma, no per provocar (més) confrontació, sinó desenvolupar una estratègia amb els altres.
- Si algú que és o ha sigut víctima d'assetjament cibernètic es posa en contacte amb tu, pots donar els primers consells:

  Res d'accions precipitades i desconsiderades! Res d'intimidació en sentit contrari!

  Fes captures de pantalla dels atacs d'assetjament cibernètic i recopila proves.

  Si hi ha formes d'informar a la plataforma de comandament, fes-ho primer.

  Apaga tots els mitjans de comunicació i informa del cas.

  Involucra un adult de confiança.

Privacitat de dades

La protecció de dades significa que cada un té el dret de decidir per si mateix sobre la divulgació i l'ús de les seues dades. En altres paraules, la protecció de dades hauria de protegir els ciutadans de la curiositat de l'Estat i de la fam de dades en l'economia. Qualsevol persona que vulga utilitzar les dades d'altres ha de primer demanar el consentiment de la persona i indicar el propòsit de la recopilació de dades.

No està permesa la recopilació o l'ús de dades per a fins indeterminats (prohibició de retenció de dades). El "dret a la lliure determinació informacional" requereix que els proveïdors de telecomunicacions s'abstinguen de la retenció de dades.

No importa el que fem, on treballem o on ens mudem, deixem rastres de dades a tot arreu. Quan comprem a la xarxa, revelem el nostre gust per la música o els llibres, quan

parlem per telèfon revelem on som i en les xarxes socials proporcionem una visió profunda del nostre comportament, els nostres desitjos i el nostre entorn social. El món digital en xarxa és còmode i ràpid, els usuaris paguen el preu amb les seues dades. Cada consulta de cerca proporciona a *Google* una indicació de com es pot adaptar millor el resultat de la recerca a l'usuari la propera vegada. En resum, la informació que deixem sobre nosaltres mateixos a Internet és la matèria primera, la moneda que les empreses utilitzen per assegurar la seua quota de mercat.

Protecció de dades i autodeterminació informativa

La privacitat és un tema d'actualitat, impulsat principalment per les discussions sobre gegants de tecnologia i informació com *Google* i *Facebook*. Per exemple, atès que *Facebook* està registrat en els EE.UU. i que les normes de protecció de dades són completament diferents a les d'Europa, *Facebook* simplement no compleix la Llei de Protecció de Dades a dels països europeus.

Això restringeix l'ús de les plataformes *Google* i *Facebook*, ja que no es garanteix la protecció de les dades. Les empreses intenten recopilar la major quantitat de dades personals possible, ja que venen aquestes dades a altres empreses (per exemple, empreses de publicitat) o permeten a tercers fer publicitat específicament adaptada a l'usuari. Guanyaràs molts diners amb això. La captació de dades personals a les xarxes socials contrasta amb el "dret fonamental a l'autodeterminació informativa".

Llig les directrius d'ús de dades de *Facebook*. Aquí es t'informarà sobre les dades que has transmès i com *Facebook* utilitzarà les teves dades:

Pautes d'ús de dades de *Facebook*

https://www.*Facebook*.com/about/privacy/

En realitat, depèn de tu la quantitat de dades personals que proporciones. L'usuari ha d'estar d'acord amb el subministrament de dades personals i l'ús posterior de les dades personals per part de les empreses (venda, enviament, etc.).

Dades Personals

Si aprens a concebir les teues dades com un bé que val la pena protegir i tens cura a Internet per a no revelar massa dades personals, rebràs menys molestos correus publicitaris, trucades o anuncis. Un altre problema és que les dades personals poden conduir al robatori d'identitat. En cas de robatori d'identitat, les dades personals furtades d'una persona física i identificable s'utilitzen, per exemple, per obtenir crèdit. No obstant això, aquest crèdit no es paga al propietari de les dades personals, sinó al lladre d'identitat. No obstant això, el deutor del préstec serà la persona les dades del qual van ser furtades.

Exemples de dades personals:

- Nom, cognom, adreça, data de naixement
- Adreça de correu electrònic / Adreça d'Internet
- Número de targeta d'identificació
- Adreça IP (del PC, telèfon intel·ligent...)
- Detalls com sexe, títol, talla, color de cabell, etc.

Exemples de dades personals d'un tipus especial:

- Origen ètnic
- Opinió política
- Religió
- Afiliació sindical
- Sexualitat
- Informació de salut

Totes aquestes són dades que proporcionen informació important sobre una persona i poden dibuixar una imatge molt precisa i detallada de la persona.

Els drets d'autor a Internet

En els mòduls 1 a 3 de *CIBERTUTORS* ja has pres consciència dels drets d'autor i, sobretot, estàs motivat per a donar el teu propi espai de creativitat i crear els teus propis mitjans de comunicació. Per exemple, pots crear la teua pròpia música per configurar el teu propi vídeo amb música. Si encara necessites arxius d'àudio o imatge, sempre pots fer servir mitjans que vénen amb llicències *Creative Commons*.

Descàrregues il·legals

No tot el que és tècnicament possible també està legalment permès. L'accés a les descàrregues a Internet és realment molt fàcil i els llocs d'intercanvi d'arxius *p2p* (*peer-to-peer*, company a company) són molt comuns. Aquests llocs d'intercanvi d'arxius, en particular, sovint són monitoritzats per oficines d'advocats, raó per la qual les descàrregues i càrregues il·legals poden resultar en altes multes.

Sovint falta la consciència que una obra (pel·lícula de cinema, CD de música, imatges, etc.) d'un autor també costa diners. Què passaria si ja ningú produïra eixes obres, ja que els artistes ja no guanyen diners amb elles?

Has d'adonar-te d'això en descarregar!

- Quan t'ofereixen gratuïtament descàrregues d'artistes coneguts o de pel·lícules actuals, pots assumir que violes els drets d'autor en descarregar.
- Els llocs d'intercanvi d'arxius i els portals de descàrregues a Internet estan sotmesos a un control molt estricte i s'inclouen en la majoria dels casos són il·legals o pagats.
- Els serveis de *streaming* tampoc s'haurien d'utilitzar, ja que encara no està legalment clar si l'*streaming* dels llargmetratges actuals constitueix un delicte.
- Descarregar vídeos de *YouTube* com arxius *mp3* i reproduir-los només per a tu en el teu reproductor *mp3* està bé. Però si puges els arxius descarregats a Internet o els envies a altres persones, és il·legal i per tant no està bé.

Pujades il·legals

No només les descàrregues il·legals d'Internet, sinó també les càrregues, és a dir, els continguts d'altres autors, que vostè retorna a Internet (per exemple, fotos de productes en

una oferta d'eBay, obres d'altres autors com fotos, música o vídeos) poden donar lloc a costoses advertències. Un no pot, per exemple, posar els èxits musicals actuals per baix dels vídeos de creació pròpia i pujar-los a *YouTube*.

Aquests són els punts mínims que has de tindre en compte abans de carregar!

- Has de ser el propietari, és a dir, lautor, de totes les obres (fotos, música i vídeo) que puges.
- No pots publicar imatges de persones que no hagen acceptat publicar la seua foto. Això també s'aplica a la teua parella o al teu millor amic! Tots els particulars tenen dret a la seua pròpia imatge. Per tant, has d'estar d'acord amb l'ús de la imatge en què es mostra.

Més informació, especialment sobre els costos que poden causar càrregues i descàrregues il·legals, es mostra en el vídeo:

https://www.youtube.com/watch? feature=player_embedded&v=cz3a_dhml9o#t=28

Descàrregues Legals

Cada vegada són més les persones creatives que publiquen les seues obres per a baixar legalment a Internet. A través de la possibilitat de llicències *Creative Commons*, també anomenades "llicències de tot el món", les persones creatives poden determinar per si mateixes les llicències de les seues obres, és a dir, regular els drets d'ús i explotació.

També pots triar entre una sèrie de llicències, que o bé alliberen completament l'ús de les teues pròpies obres o bé vinculen algunes condicions a l'ús de les obres.

Directrius per a l'ús de mitjans sota llicència *Creative Commons*

Si una ment creativa ja està posant els seus mitjans a disposició, és particularment important esmentar el nom de l'autor i fer referència ací també al tipus de llicència que té l'arxiu de mitjans. Això també és important per a altres persones que també vulguen utilitzar aquest arxiu. A continuació s'enumeren les diferents "llicències *CC*" i es mostren les icones corresponents. A la següent pàgina trobaràs un exemple de com ha de ser el títol quan fas servir imatges amb llicències *Creative Commons*.

Icona	Condicions d'ús	Número de llicència
	Menció del nom	CC-BY
	Reconeixement i no processament	CC-BY-ND
	Reconeixement i no comercial	CC-BY-NC
	Reconeixement i no comercial i sense processament	CC-BY-NC-ND
	Reconeixement i trasllat en les mateixes condicions	CC-BY-SA
	Reconeixement i no comercial i divulgació en les mateixes condicions	CC-BY-SA

Ací veiem com s'indica correctament el nom de l'autor i es fa referència a la llicència.

Foto: TilarX CC-BY

Cerca de mitjans amb llicència *Creative Commons*

Igual que en els mòduls 1 a 3 de *CIBERTUTORS*, la recerca de mitjans sota llicències *CC* s'ha d'esmentar ací de nou. La pàgina més important per a buscar mitjans sota llicències *CC* és la pàgina principal de *CC* a **http://search.creativecommons.org**. Es poden seleccionar les diferents pàgines, com flickr.com o *Google*.com, que s'inclouen en la recerca.

SESIONES PRÁCTICAS

CIBERVIOLENCIA

CIBERSEGURIDAD

FAKE NEWS

INTERNET Y SALUD

SESSIÓ 1 - CIBERVIOLÈNCIA

1.1. Presentació de diapositives.

1.2. Exemples de ciberviolència

1.3. Sexting

1.4. Grooming

1.5. Radicalització

1.6. Videojocs

1.1 PRESENTACIÓ DE DIAPOSITIVES

CIBERVIOLÈNCIA

Un malson digital

https://youtu.be/i4GKXsAOYZE

SEXTING

SEXTING

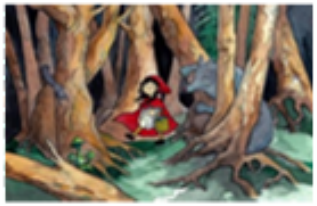
Un l'enll de greu màxim !!!

En què consisteix?

Compartir fotografies personals de l'àmbit privat, compromeses o de contingut sexual a través del mòbil, xarxes socials o cels privats.

Qué pot passar a qui ho fa?

- Que les fotografies es comparteixen a terceres sense permís i es faça pública la intimitat de la persona
- Que s'utilitzen per a extorsionar-la/lo i obtenir un benefici econòmic o de qualsevol altre tipus
- Que es produisca com a conseqüència algun tipus d'abús sexual



GROOMING

SAPS QUI S'AMAGA DARRERE DE LA PANTALLA??????

ULL!!!!!

Si sóm desconeguts tal vegada no sóm qui diuen ser

Els depredadors sexuals s'amaguen darrere d'identitats falses

- Solen ser homes
- Majors d'edat
- Adopten identitats de xiquets joves
- Es fan passar per amiguets per guanyar-nos confiança
- Les víctimes són joves entre 12 i 16 anys

QUÈ VOL UN GROOMER

1. Tolerels amistat, bones paraules, comprensió...

per a aconseguir la seua confiança

1. Conèixer la seua rutina i identificar: qué fas, amb qui vas, quins horaris, qué t'agrada, qué et preocupa, els seus estats d'ànim...

Quan més sap més control té sobre la seua vída

1. Que li envies fotos íntimes seues!

Ara ja té un motiu per a amenaçar-te, obligar-te a fer el que ell vulga...

sotmetent-te a la seua voluntat

FORMES DE XANTATGE

- Abusar sexualment de tu a través de la càmera del teu ordinador. O en la vida real
- Extorsionar-te econòmicament o moralment...
- Evitar que el denuncies
- I què més?

Discurs extremista neonazi

RADICALITZACIÓ

Discurs extremista yihadista

BUSCA ELS SÍMBOLS IDENTIFICADORS

RADICALISME

- Difamació política d'extrema dreta
- Xenofòbia i racisme
- Discurs Supremacista contra les minories
- Conductes antidemocràtiques/ violències
- Actituds masclistes
- Negacionisme de l'existència de violència de gènere
- Atacs contra les dones i el moviment feminista

- Defensa de la lluita armada contra els Infidels (especialment Occident)
- Captació de musulmans per a la Guerra Santa
- Difusió de missatges contra Occident
- Violència extrema i actes terroristes
- Ideologia antidemocràtica
- Aplicació de la Sharia

INOFENSIUS?

EDUCATIUS? ADICTIUS?

Videojocs

- INCREMENT DEL TEMPS QUE ELS NENS I NENES PASSEN CONNECTATS A VIDEOJOCS

CAUSES

PROS I CONTRES

- Violència extrema
- Igualança de realitat el grau de verisemblança
- Temàtiques i contingut no educatius
- Continguts i temàtiques que promouen comportaments sense valors ni ètica: combats, destrucció, enfrontaments, assassinats, morts...
- Estratègies dels creadors altament addictives
- Presentació d'estereotips de dones no reals, amb cossos inversemblants i altament eròtics.

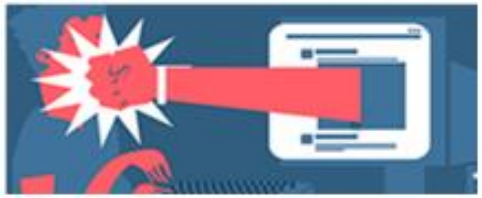
- Joca amb caràcter educatiu
- Ens d'aprenentatge i d'estimulació de les habilitats mentals i habilitats físiques
- Ens per millorar l'atenció visual i la concentració/destresa
- Ens terapèutics per a tractar problemes de salut
- Ens que potencien estratègies de treball en grup i/o desenvolupament d'habilitats com l'empatia, l'assertivitat, la solidaritat.

VIDEOJOCS

Poden provocar

- Alteració de conductes en jugadors
- Conductes antisocials
- Alteració de la salut
- Dependència greu

CIBERVIOLÈNCIA DE GÈNERE



CIBERVIOLÈNCIA DE GÈNERE

Violència de gènere tradicional a l'entorn digital

Com es produeix?

- Control dels dispositius d'accés a Internet i xarxes socials de la dona víctima
- Control dels continguts que la víctima comparteix en Internet
- Limitació del dret de la víctima per a usar lliurement els seus dispositius electrònics
- Assetjament de la víctima en l'entorn digital: insults, vexacions, amenaces....
- Reproducció de patrons de conducta patriarcals: l'home exerceix el seu poder sobre les dones.

1.2. EXEMPLES DE CIBERVIOLÈNCIA

1. LLIG ELS EXEMPLES de ciberviolència que tens més avall.
2. Comenta els casos exposats:
    - coneixes víctimes d'aquests exemples ?
    - Podries explicar quin tipus de persones eren?
3. Quin és el perfil o personalitat tipus que podria ser víctima de Ciberviolència ? Edat? Gènere?
4. Li podria passar a qualsevol persona ? O algun grup en especial?
5. Qui participa com assetjador d'aquest tipus de comportaments? Quin és el perfil de l'assetjador? Edat? Gènere?
6. Podria ser qualsevol persona un assetjador/a? Els teus amics/ amigues podrien ser-ho?
7. Tu podries tenir comportaments d'assetjador/a? Per què?
8. Alguna vegada has participat d'algun comportament com els descrits?

- Colgar en Internet una imagen comprometida (real o efectuada mediante fotomontajes) datos delicados, cosas que pueden perjudicar o avergonzar a la víctima y darlo a conocer en su entorno de relaciones.

- Dar de alta, con foto incluida, a la víctima en un web donde se trata de votar a la persona más fea, a la menos inteligente… y cargarle de puntos o votos para que aparezca en los primeros lugares.

- Crear un perfil o espacio falso en nombre de la víctima, en redes sociales o foros, donde se escriban a modo de confesiones en primera persona determinados acontecimientos personales, demandas explícitas de contactos sexuales…

- Dejar comentarios ofensivos en foros o participar agresivamente en chats haciéndose pasar por la víctima de manera que las reacciones vayan posteriormente dirigidas a quien ha sufrido la usurpación de personalidad.
  Dando de alta la dirección de correo electrónico en determinados sitios para que luego sea víctima de spam, de contactos con desconocidos…

- Usurpar su clave de correo electrónico para, además de cambiarla de forma que su legítimo propietario no lo pueda consultar, leer los mensajes que a su buzón le llegan violando su intimidad.

- Provocar a la víctima en servicios web que cuentan con una persona responsable de vigilar o moderar lo que allí pasa (chats, juegos online, comunidades virtuales…) para conseguir una reacción violenta que, una vez denunciada o evidenciada, le suponga

la exclusión de quien realmente venía siendo la víctima.

- Hacer circular rumores en los cuales a la víctima se le suponga un comportamiento reprochable, ofensivo o desleal, de forma que sean otros quienes, sin poner en duda lo que leen, ejerzan sus propias formas de represalia o acoso.

- Enviar menajes amenazantes por e-mail o SMS, perseguir y acechar a la víctima en los lugares de Internet en los se relaciona de manera habitual provocándole una sensación de completo agobio.

1.3. SEXTING

1. Saps què significa la paraula anglesa SEXT: to Sext , de la que que deriva el substantiu "sexting (sex+text)"? Busca en el diccionari "on line" Word reference el significat

2. Per què fan sexting els menors? contesta i compara les teues respostes amb la informació que trobaràs en aquest enllaç

https://www.is4k.es/necesitas-saber/sexting

3. Es pot fer Sexting de manera segura?

1.4. GROOMING

Què significa la paraula anglesa GROOM?
(Nuvi, to GROOM: llepar-se, preparar-se)

1. Llig el de cas de GROOMING següent:

La siguiente conversación de Messenger es real. La presentó un padre a la policía española y dio lugar a la detención de uno de los pedófilos más activos de la Red. Éste había desarrollado un sistema muy elaborado: primero entraba en contacto con las menores en algún chat fingiendo ser una chica de 14 años. Les pedía su cuenta de Messenger, las agregaba como contacto y les enviaba una postal simpática de un corazón, de amor, o un gusanito. "Haz clic aquí si quieres ver el gusanito", decía el mensaje. Si la niña picaba, automáticamente se descargaba un virus en su ordenador y la próxima vez que teclease su clave de acceso a su correo electrónico se la estaría enviando también al acosador. En esto, básicamente, consiste el grooming. Sólo se ha modificado el nombre de la víctima, una niña catalana de 14 años, por el de Bea:
LucySoto. Ola perdona si te he agregado.
Bea. Ola.
LucySoto. Es q tengo algo importante q decirte.
Bea. A mi? k?
LucySoto. Te he cambiado tu contraseña y pregunta secreta [necesarias para activar la cuenta de Messenger] si cierras tu msn no podras abrirlo.

LucySoto. Te he robado tu msn te lo devolvere.
LucySoto. Solo quiero q me hagas un favor.
LucySoto. Contesta o me meto en tu msn.
Bea. Oyeee komo sabes mi clave?
LucySoto. Tu pregunta secreta era muy facil.
LucySoto. Me podrias hacer el favor que te pedi?
Bea. K favor era?
LucySoto. Conoces a una Rosita?
Bea. Si k la conozco
LucySoto. A ella tambien le hice lo mismo hace 2 semanas y le devolvi su msn porque ella me hiso un favor.
Bea. K favor era?
LucySoto. Primero quiero conocer con quien hablo.
LucySoto. Me llamo lucy y tengo 14 años tu?
LucySoto. Date prisa q me meto en tu msn y no hables con nadie.
Bea. Bea.
LucySoto. Soy de argentina tu?
Bea. España.
Bea. X favor me puedes devolver el msn.
LucySoto. Primero ponte la cam pa conocerte ok?
Bea. Ok.
LucySoto. No te veo bien.
LucySoto. Acomodala.
Bea. Aora?
LucySoto. Ok te pedire lo mismo q a tu amiga.
LucySoto. Primero quiero q sepas q soy les [lesbiana] no te molesta?
Bea. Yo soy bi.
LucySoto. Preguntale a tu amiga lo q le pedi y luego me dices si puedes hacerlo ok.
LucySoto. Pero date prisa.[]
Bea. Me vas a devolver el msn?
LucySoto. Si.
Bea. Seguro.
LucySoto. A tu amiga se lo devolvi.
LucySoto. Tengo un minuto date prisa.
Bea. Tengo k ensenyarte las tetas no?
LucySoto. Si.
LucySoto. Las dos.
Bea. Ya ta no?
LucySoto. Ok.
Bea. Me devuelves el msn xfavor?
Bea. Puedo kitar ya la cam?
LucySoto. Aun no.
LucySoto. Antes de devolverte la clave quiero q veas este video.
[LucySoto le envía el vídeo de la propia Bea mostrando sus pechos]
LucySoto. Viste el video?
Bea. Si xfavor lo puedes borrar?
LucySoto. Es un recuerdo para mi te molesta?
Bea. Mucho xfavor lo puedes borrar?
LucySoto. Sabes q he copiado a todos tus contactos? q harias si se lo mando a todos?
Bea. Me moriria de verguenza.

Bea. Xfavor no lo hagas.
LucySoto. No lo hare no te preocupes.
Bea. K me voy a poner a llorar.
Bea. Estoy temblando.
LucySoto. Puedes hacer algo? Cierra la puerta pa q nadie nos moleste.
LucySoto. No quiero q te vean llorando.
Bea. Sta cerrada.
LucySoto. Y no hables con nadie.
Bea. Xfavor.
LucySoto. Soy les [lesbiana] ya te lo dije y quiero hacerme un dedo viendote.
LucySoto. Si haces lo q te pido no pasara nada ok.
Bea. No me pidas nada mas xfavor.
LucySoto. Quiero hacerme un dedo viendote.
LucySoto. Si no te juro q mando el video.
Bea. Noooooo.
Bea. Xfavoooor.
LucySoto. Tu dime lo haraas o no?
Bea. K es?
LucySoto. Cierra las ventanas y todo pa q no nos molesten ok?
LucySoto. Date prisa.
Bea. Ya ta.
LucySoto. Sera algo rapido.
LucySoto. Mientras mejor lo hagas sera mejor.
Bea. K es!!!!!!!!!
LucySoto. Primero quítate eso negro q llevas arriba.
LucySoto. Date prisa.
Bea. Spera.
LucySoto. Con quien hablas.
Bea. Kon nadie.
LucySoto. Entonses?
Bea. Tengo miedo.
Bea. Xfavor no me lo agas acer.
LucySoto. De q tienes miedo?
Bea. De ti.
LucySoto. No tengas miedo.
Bea. Aora vengo esk me stoy mareando.
LucySoto. Solo has lo q te pido y me piro.
Bea. Es k no puedo.
LucySoto. Entonses lo siento.
LucySoto. Te dije q solo seria un mo¬¬mento.
LucySoto. Me voy.
Bea. Donde vas?
LucySoto. A tu msnnnnnnnnnn.
[LucySoto abandona la conversación]

En mayo, la persona tras el nick LucySoto fue detenida gracias a la denuncia de Bea y otras de sus víctimas. Resultó ser M. A. S. Q., un limeño (Perú) de 32 años al que se acusa de robo de contraseñas, coacciones y abusos sexuales.

2. Consulta l'enllaç següent i busca les Xifres de denúncies de GROOMING en Espanya:

https://www.eldiario.es/nidos/delitos-sexual-menores-Internet-cuadruplican_0_758024914.html

3. Consulta l'enllaç següent i explica com està tipificat el grooming en el Codi Penal Espanyol i quines penes es podrien aplicar als delinqüents

https://www.tuabogadodefensor.com/child-grooming/

4. Recordes el conte de Caputxeta vermella? Busca semblances entre els personatges i les situacions d'aquest conte tradicional i els casos de grooming:

- víctimes i delinqüents:
- delinqüents que oculten la seua identitat:
- edat de la víctima:
- procés d' anagnòrisi:
- entorn perillós:
- conducta perillosa de la víctima:
- càstig:
- herois:
- component sexual:

5. Segons el psicòleg Premi Nobel, Bruno Betelheim, els contes tradicionals ajuden els xiquets a madurar. En l'enllaç següent pots trobar informació sobre l'anàlisi del conte de Caputxeta roja i el llop del seul llibre *Psicoanàlisi dels contes de fades*

https://www.reeditor.com/columna/18513/24/psicologia/la/caperucita/roja/el/complejo/edipo/sigmund/freud/bruno/bettelheim

1.5. RADICALITZACIÓ

1. Llig els articles següents sobre com funciona la propaganda yihadista en internet:

http://www.expansion.com/economia-digital/companias/2016/10/19/58067a5ee5fdea1f3a8b4691.html

https://www.elespanol.com/espana/20181211/canales-yihadistas-llaman-atentar-barcelona-imagenes-decapitaciones/359715187_0.html

https://www.minutouno.com/notas/1509345-por-que-telegram-es-la-app-mensajeria-preferida-los-yihadistas

a) En quines xarxes socials hi ha major difusió de propaganda yihadista?
b) Per què reben crítiques companyies tecnològiques com facebook, google, youtube..?
c) Com s'està contrarestant en internet la propaganda yihadista?
d) Creus que és suficient el que fan les grans empreses d'internet per desactivar la propaganda?
e) Estàs d'acord amb l'afirmació que no Isis no existiria si no existira internet?
f) A quin mitjà en internet ha migrat majoritàriament la propaganda yihadista? per què?

2. Creus que este tipus de pàgines no són un perill per als nostres adolescents?

3. Creus que hi ha un perfil d'adolescent que podria ser-ne víctima? Quin perfil en concret Descriu-lo.

https://www.naciodigital.cat/noticia/159698/whatsapp/restringeix/reenviament/massiu/missatges/lluitar/contra/fake/news

https://elpais.com/politica/2018/12/15/actualidad/1544865020_776679.html

https://motherboard.vice.com/en_us/article/xw5bxk/youtube-neo-nazi-propaganda-atomwaffen

4. Com identificaries una pàgina de difusió d'ideologia neonazi?
5. Quina estètica i indumentària caracteritza als seguidors de grups neonazis?
6. Quina classe de continguts creus que hi ha en estes pàgines?
7. Coneixes el grup *València 2000?* Coneixes Noms de partits polítics, associacions, grups...d'ideologia neonazi? A Europa, Espanya o a altres països del món?
8. Analitza els temes i el vocabulari d'una pàgina de difusió d'ideologia neonazi i fes-ne un llistat.

1.6. VIDEOJOCS

TREBALL EN GRUP

A) Preparen els grups les preguntes per al formulari
B) Simultàniament dues persones traslladen les preguntes al formulari "on Line"

1. PREPAREU UN QÜESTIONARI DE GOOGLE FORMS per a conéixer els hàbits dels vostres companys pel que fa als usos dels videojocs en la seua vida diària. El contingut de les preguntes hauran de ser sobre almenys els temes següents:

- Temps que dediquen diàriament a jugar "on Line" o a videjocs
- tipus de jocs a que solen jugar
- noms dels jocs
- característiques dels jocs
- aspectes positius del temps que dediquen a jugar
- aspectes negatius del temps que dediquen a jugar
- problemes amb els pares derivats del temps que dediquen a jugar
- problemes amb altres jugadors
- problemes de salut derivats del temps que dediquen a jugar
- problemes amb companys de l'institut o coneguts
- coneixença de gent que tinga problemes d'addicció
- Altres...

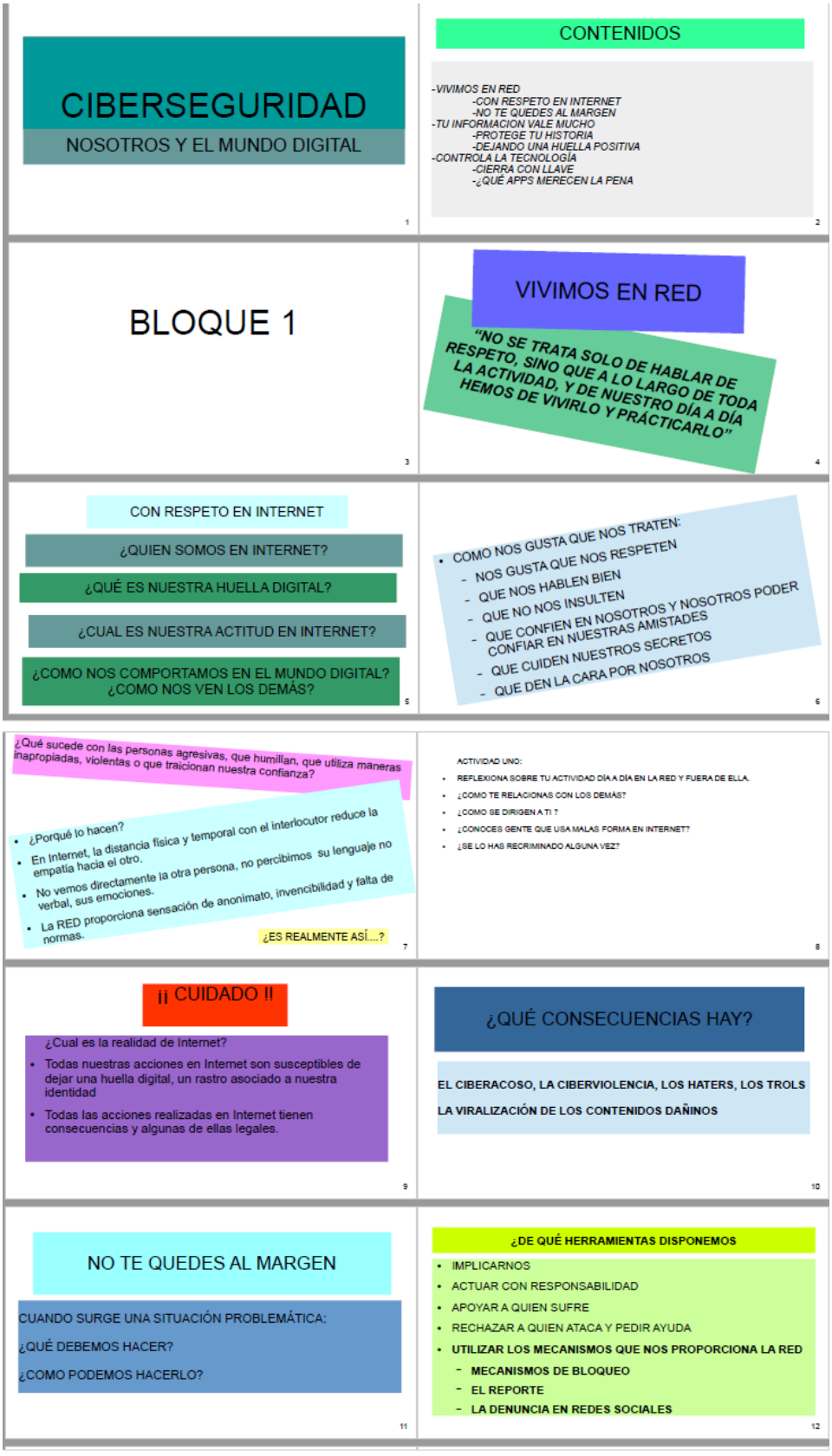
2. Envieu -vos el formulari i contesteu-lo.
3. Analitzeu els resultats
4. Prepareu el formulari per poder passar-lo als companys de les classes a qui formareu.

SESIÓN 2 - CIBERSEGURIDAD

1.1. Presentación de diapositivas.

1.2. Actividades

2.1 PRESENTACIÓN DE DIAPOSITIVAS



ACTIVIDAD 2:

COMO BLOQUEAMOS Y REPORTAMOS EN LAS PRINCIPALES REDES:

- REFLEXIONA, INVESTIGA Y COMPARTE. CONSULTA LAS PAGINAS DE AYUDA DE LAS APLICACIONES Y ELABORA UNAS FICHAS DE CONSEJOS :
  - WHATSAPP
  - INSTAGRAM
  - SNAPCHAT
  - TWITTER
  - FACEBOOK
- EXPLICA Y REPASA LAS OPCIONES DE BLOQUEO Y REPORTE EN ESTAS APLICACIONES

13

Enlaces a páginas de aplicaciones y vídeos de seguridad

https://www.is4k.es/preguntas-frecuentes#bloquear_reportar

Centro de seguridad de Facebook / Videotutorial de privacidad en Facebook

Centro de seguridad de Twitter / Videotutorial de privacidad en Twitter

Centro de seguridad de Instagram / Videotutorial de privacidad en Instagram

Centro de seguridad de YouTube / Videotutorial de privacidad en YouTube

Centro de seguridad de Snapchat / Videotutorial de privacidad en Snapchat

Página de ayuda de WhatsApp / Videotutorial de privacidad en WhatsApp

14

BLOQUE 2

15

TU INFORMACIÓN VALE MUCHO

"CUANDO SE COMPARTE ALGO EN INTERNET, YA NO HAY VUELTA ATRÁS... ESCAPA A NUESTRO CONTROL"

PRIVACIDAD

PROTECCIÓN DE LA PROPIA INFORMACIÓN

IDENTIDAD DIGITAL POSITIVA

MI REPUTACIÓN EN LINEA

16

PROTEGE TU HISTORIA

¿QUÉ INTERES TIENE NUESTRA VIDA PRIVADA PARA LOS DEMÁS?

¿QUIEN PUEDE VER MI INFORMACIÓN EN INTERNET?

¿COMO PUEDO PROTEGER MI INFORMACIÓN?

17

¿COMO SE PROPAGA LA INFORMACIÓN E INTERNET?

¿QUE SIGNIFICA "VIRAL"?

¿CONOCES LA TEORIA DE LOS SEIS GRADOS?

¿ES BUENO QUE DESCONOCIDOS TENGAN INFORMACIÓN SOBRE TI?

18

3,57 GRADOS DE SEPARACIÓN

¿QUÉ SIGNIFICA ESTA FRASE?

https://es.noticias.yahoo.com/video/facebook-demuestra-que-ya-no-140811072.html?guccounter=1

19

- ACTIVIDAD 3:
- REFLEXIONA SOBRE EL VIDEO MOSTRADO
- ¿DE VERDAD PODEMOS ESTAR CONECTADOS CON CUALQUIER PERSONA DEL MUNDO?
- ¿CON LAS REDES SOCIALES ES MAS SENCILLO?
- ¿PODER CONECTARSE CON CUALQUIERA ES POSITIVO TIENE ALGUN RIESGO?
- COMPRUEBA EN TU ENTORNO INMEDIATO CON CUANTOS PAISES TIENES CONEXIÓN

20

ACTIVIDAD 4: DINAMICA INTERACTIVA

COMPARTIR O NO?
¿QUÉ INFORMACIÓN COMPARTIMOS?

FORMAR 10 GRUPOS DE ALUMNOS (DE TRES A SEIS PERSONAS)
LOS MIEMBROS DE CADA FíGRUPO COMPARTEN TARJETAS DE PERSONAJES (SOY DE)
CADA TARJETA TIENE DOS CIRCULOS DE AMISTADES
UNA PERSONA AL AZAR ELIJE UNA TARJETA DE CONTENIDO.
LA PERSONA DEBE DECIDIR SI COMPARTE EL CONTENIDO Y ON CUAL DE SUS DOS CIRCULOS DE AMISTADES
LA CADENA SIGUE.....

21

- ACTIVIDAD 5:

DISEÑA UN CARTEL O UNA TARJETA CON CONSEJOS SOBRE COMO LIMITAR LA DIFUSIÓN DE LOS CONTENIDOS EN INTERNET:

- LIMITAR LITAS DE CONTACTO
  - UN AMIGO DE UN AMIGO ES UN DESCONOCIDO
  - UN AMIGO VIRTUAL CONOCIDO SOLO A TRAVES DE ALGUNA APLICACION O JUEGO ES UN DESCONOCIDO
- USAR CUNTS PROVADAS
- CONFIGURAR LAS OPCIONES DE SEGURIDAD
- PENSAR ANTES DE COMPARTIR
- REPORTAR Y BLOQUEAR LOS CONTENIDOS NO DESEADOS
- PROTEGER LOS DISPOSITIVOS
- ESTAR AL DÍA

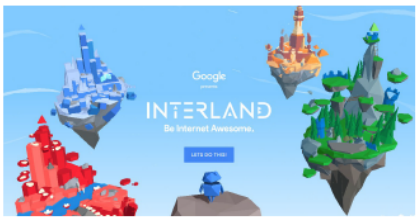
22

Aprende a compartir con precaución

Página de google con juegos interactivos sobre el buen uso de internet:

https://beinternetawesome.withgoogle.com/en_us/interland

23



24

- ACTIVIDAD 6: JUEGO ONLINE:
- "MONTAÑA DE LA CONSCIENCIA"
  - JUEGO BASADO EN LA SELECCION DE CON QUIEN COMPARTIMOS LA INFORMACIÓN

https://beinternetawesome.withgoogle.com/en_us/interland/

25

RECUERDA

- CUIDA TU PRIVACIDAD EN INTERNET
- CONTROLA LAS LISTAS DE AMISTADES
- REVISA LOS AJUSTES DE PRIVACIDAD
- COMPARTE DE MANERA RESPONSABLE
- MANTÉN TUS EQUIPOS ACTUALIZADOS

26

DEJANDO UNA HUELLA POSITIVA

TODO LO QUE HACEMOS EN LINEA, SE QUEDA EN LINEA... Y CUALQUIERA PUEDE VERLO.
¿COMO TE GUSTARÍA QUE LOS DEMÁS TE VIERAN EN INTERNET?

¿QUE CONSECUENCIA TIENE LA INFORMACION QUE COMPARTO EN INTERNET?
¿COMO PUEDO MEJORAR MI IMAGEN EN INTERNET?
¿QUÉ ACTITUDES REFUERZAN MI IMAGEN?

27

"Antes de publicar un mensaje o una foto, valorar sus posibles lecturas e implicaciones para uno mismo y para los demás, ver si puede dar pie a malentendidos, conflictos y asegurarse de que nos ayuda a tener una mejor imagen y mejores relaciones en la Red."

28

HABLEMOS DE EGOSURFING

BUSQUEMOS INFORMACIÓN SOBRE NOSOTROS MISMO EN INTERNET.
¿QUE IMAGEN TENGO?
https://youtu.be/JOli4tNRelY

EL REINO DE LA AMABILIDAD

https://beinternetawesome.withgoogle.com/en_us/interland/

29

BLOQUE 3

30

CONTROLA LA TECNOLOGÍA

CUIDA LA PROTECCIÓN DE TUS DISPOSITIVOS Y SERVICIOS ONLINE
GESTIONA BIEN TUS CONTRASEÑAS
CONFIGURA TUS OPCIONES DE SEGURIDAD Y PROTECCIÓN
RECHAZA LAS APLICACIONES POTENCIALMENTE PELIGROSAS

31

CIERRA CON LLAVE

"LA MEJOR HERAMIENTADE SEGURIDAD ES TU SENTIDO COMÚN. LA MEJOR PREVENCIÓN, TUS BUENOS HÁBITOS EN EL USO DE LA TECNOLOGÍA

CREA CONTRASEÑAS ROBUSTAS.
TEN HÁBITOS DE SEGURIDAD
NO COMPARTAS TUS CONTRASEÑAS
UTILIZA PATRONES DE DESBLOQUEO
COMPRUEBA TUS AJUSTES DE SEGURIDAD

32

COMPARA LA SEGURIDAD DE TU VIDA FÍSICA CON LA DE TU VIDA DIGITAL:

CUANDO SALES DE CASA, ¿CIERRAS LA PUERTA CON LLAVE?
CUANDO DEJAS TU COCHE EN LA CALLE, ¿DEJAS LAS LLAVES PUESTAS?
¿TE PREOCUPAS POR TU SEGURIDAD EN INTERNET ? O TIENES UNA ACTITUD DESPREOCUPADA

33

ACTIVIDAD 7: PRUEBA DE EMPAREJAMIENTO

BUSCA TU PAREJA ENTRE TUS COMPAÑEROS:

-SI TIENES UN PROBLEMA BUSCA UNA SOLUCIÓN

-SI POR EL CONTRARIO TIENES UNA SOLUCIÓN, BUSCA A QUIEN PUEDES AYUDAR.

-SI YA TIENES FORMADA LA PAREJA ORIENTA A LOS DEMÁS

34

ACTIVIDAD 8: JUEGO DEL TESORO

JUEGO ONLINE : APRENDE A PROTEGER TU INFORMACIÓN Y CREAR CONTRASEÑAS ROBUSTAS Y SEGURAS

https://beinternetawesome.withgoogle.com/en_us/interland/

https://password.kaspersky.com/es/

35

ACTIVIDAD 9:

CON LA AYUDA DE TUS COMPAÑEROS, DISEÑA UNA CONTRASEÑA.

SI NO TIENES LOS ELEMENTOS NECESARIOS, NEGOCIA CON LOS DEMÁS GRUPOS.

AL FINALIZAR, COMPRUEBA TU CONTRASEÑA EN EL SIGUIENTE ENLACE.

https://password.kaspersky.com/es/

36

¿QUÉ APPS MERECEN LA PENA?

"CUANDO INSTALAS UNA APP LE DAS ACCESO A MUCHA INFORMACIÓN PRIVADA"

¿COMO SELECCIONAMOS LAS APPS QUE INSTALAMOS EN NUESTROS DISPOSITIVOS.

¿NECESITAMOS REALMENTE ESA APLICACIÓN?

¿CONOZCO LOS PERMISOS QUE DOY A LA APLICACIÓN?

37

¿ES SEGURA LA APLICACIÓN?

¿QUE DEBO PREGUNTARME?

¿De dónde la saco?
Descargar las apps siempre de las tiendas oficiales.
Desconfiar de archivos descargados de Internet o de tiendas no oficiales **¿Seguro que es ésta?**
Si buscamos una app conocida, sospechar de posibles variantes en el nombre de la app, su logotipo o su desarrollador.
¿Quién está detrás?
Desconfiar si no hay dirección del desarrollador o la política de privacidad.
¿Qué hace con mis datos?
Los usos se han de indicar en su política de privacidad, aunque los permisos que solicita la app pueden darnos algunas pistas.
¿Qué permisos pide la apicación?
Deben ser coherentes con su finalidad
¿Popularidad igual a seguridad?
No necesariamente

38

ACTIVIDAD 10 JUEGO DE LAS APPS

Formar pequeños grupos:

-Elegir una ficha
-Analizar la aplicación propuesta
-Identificar posibles riesgos y decidir si es mas o menos seguro instalarlas.

Repetir el debate con varias fichas y poner en común.

39

¿SON REALMENTE GRATIS LAS APPS GRATIS?

Las aplicaciones "GRATUITAS" TE PUEDEN COBRAR DE MUCHAS MANERAS:

Pueden llevar compras integradas para aumentar susprestaciones, servicios o proporcionar objetos virtuales para juegos.

Pueden disponer de nuestros datos de registro y ofrecerlos a empresas de estudio de mercado o a otras entidades interesadas en información de usuarios.

Nos muestran publicidad . Las empresas publicitadas pagan a las aplicaciones para bombardear el usuario con sus ofertas

¡¡¡**CUIDADO!!!**
CUANDO NO NECESITES UNA APLICACION, DESINSTALALA
LAS APLICACIONES DE PAGO TAMBIEN PUEDEN UTILIZAR ESTOS MÉTODOS PARA CAPTAR TUS DATOS.

40

PERMISOS DE LAS APSS

APPS DE PAGO Y COMPRAS INTEGRADAS

https://www.youtube.com/watch?v=8q3EJnZKsx4

VIDEO SOBRE PERMISOS DE LAS APPS

https://www.youtube.com/watch?v=UXeR3iLG_ro

41

ENLACES DE INTERES PARA TU SEGURIDAD

- OFICINA DE SEGURIDAD DEL INTERNAUTA: https://www.osi.es/es
- INSTITUTO NACIONAL DE CIBERSEGURIDAD: https://www.incibe.es/
- INTERNET SEGURA FOR KIDS:https://www.is4k.es/
- INTERLAND (JUEGA CON GOOGLE): https://beinternetawesome.withgoogle.com/en_us/interland/
- COMPRUEBA TUS CONTRASEÑAS: https://password.kaspersky.com/es/
- HERRAMIENTAS DE SEGURIDAD EN INTERNET: https://www.osi.es/es/herramientas

42

2.2. Actividades

Programa de Jornadas Escolares para el uso seguro y responsable de Internet por los menores

Unidad Didáctica 3

CONTROLA LA TECNOLOGÍA

La protección de dispositivos y servicios online, la gestión de contraseñas, opciones de seguridad y protección frente a aplicaciones potencialmente peligrosas.

SESIONES Y OBJETIVOS

3.1. Cierra con llave
- Valorar las consecuencias de no proteger sus dispositivos y servicios online.
- Asumir buenas prácticas para la gestión de contraseñas.
- Configurar opciones de seguridad en dispositivos móviles y redes sociales.

3.2. ¿Qué apps merecen la pena?
- Reforzar el espíritu crítico al descargar y utilizar aplicaciones móviles.
- Conocer las motivaciones que hay detrás de las aplicaciones gratuitas.
- Aprender a seleccionar aplicaciones de calidad con seguridad.

Cofinanciado por la Unión Europea
Mecanismo «Conectar Europa»

SESIÓN 3.1. Cierra con llave

RESUMEN

Más allá de mostrar cómo crear una contraseña robusta, nos centraremos en enseñar hábitos de seguridad para proteger los dispositivos y la información, como es por ejemplo no compartir las contraseñas, establecer patrones de desbloqueo y ajustes de seguridad para las cuentas online.

METODOLOGÍA

Centrada en promover la reflexión sobre problemas de seguridad y posibles soluciones a través de dinámicas cooperativas. Complementariamente se plantea la práctica de ciertas técnicas para obtener contraseñas robustas.

MATERIALES

Tarjetas de juego (anexo 3.1.a) para cada alumno, listado de papeles emparejados (anexo 3.1.b) para el docente, equipo audiovisual con internet para el grupo, equipos conectados a Internet (o en su lugar juego de caracteres [anexo 3.1.c]) para cada pequeño grupo.

DESCRIPCIÓN DE LAS ACTIVIDADES

1. **Reflexión inicial** (10')
   Reflexión grupal sobre la protección de nuestros dispositivos y servicios online haciendo una analogía entre la seguridad física de nuestra vida cotidiana (¿dejamos la puerta de casa abierta?, ¿las llaves del coche puestas?) y la ciberseguridad en nuestro día a día digital (¿y qué pasa con nuestro móvil?, ¿seguro que nadie puede acceder a nuestras redes sociales?, ¿nunca nos hemos dejado el móvil desbloqueado en un lugar con más personas?).
2. **Dinámica interactiva** (25')
   Cada participante dispone de una tarjeta de juego (anexo 3.1.a) que puede ser una herramienta de seguridad o una conducta de riesgo. Sin desvelar cuál tiene, cada uno debe buscar su pareja, es decir, quien tenga una herramienta de seguridad debe encontrar una conducta de riesgo a la que pueda hacer frente, y quien tenga una conducta de riesgo debe encontrar una herramienta de seguridad que le pueda proteger. Cada tarjeta está directamente ligada a otra (aunque puede haber varias parcialmente relacionadas), por lo que al final de la actividad todos los participantes deben estar emparejados (ver anexo 3.1.b). Terminado el tiempo, se presentarán por parejas ante el gran grupo debatiendo si efectivamente su asociación es la más adecuada, si la herramienta de seguridad protegería efectivamente frente al riesgo y si habría otras herramientas de seguridad que podrían complementarla.
3. **Juego online** (15')
   A modo de conclusión, se recuerda la necesidad de tener contraseñas seguras, con el juego online de Google "Torre del tesoro" (que nos ofrece sencillos trucos para crear contraseñas robustas y seguras) y una herramienta online para comprobar la fortaleza de una contraseña, o bien una dinámica de construcción de contraseñas utilizando distintos caracteres (anexo 3.1.c).

NOTAS PARA DOCENTES

"La mejor herramienta de seguridad es tu sentido común. La mejor prevención, tus buenos hábitos en el uso de la tecnología"

La reflexión inicial pretende hacer una analogía entre las medidas de seguridad de nuestro día a día (cerrar la puerta de casa, quitar las llaves del coche, etc.) y las de los medios digitales.

En la seguridad de nuestro móvil, ¿tenemos una actitud responsable o despreocupada?, si cerramos la puerta de casa, ¿por qué dejamos el móvil sin un bloqueo de pantalla seguro? (lo mínimo es un patrón de desbloqueo. Mejor una contraseña o una huella digital).

Si creemos que nadie puede acceder a nuestras redes sociales planteémonos si nunca nos hemos olvidado el móvil (aunque fuera un momento), o si nunca nos hemos dejado abierta una web en un PC del centro, o incluso si nuestra contraseña (o la pregunta de seguridad para recuperarla) es tan sencilla que siguien que nos conozca la puede adivinar.

La dinámica interactiva busca el diálogo y la reflexión del alumnado sobre los riesgos y problemas que se pueden encontrar online y la manera de protegerse frente a ellos.

A cada alumno se le entrega una tarjeta (anexo 3.1.a), con una "solución", herramienta o conducta de seguridad (cabecera verde claro), o bien un "problema" de seguridad o una conducta de riesgo (cabecera gris oscuro). Cada "problema" está ligado a una "solución" (anexo 3.1.b), de modo que los participantes tienen una y solo una pareja. Su objetivo es tanto encontrar a su pareja, como ayudar a sus compañeros/as a encontrar las suyas.

Hay herramientas de seguridad que podrían hacer frente a varios riesgos, así como riesgos para los que se podrían aplicar varias herramientas de seguridad. Pero cada situación presenta ciertos matices, de modo que solo hay una combinación "ideal" para cada uno.

A la indicación de la persona dinamizadora, se moverán por el aula en busca de pareja. Deben emplear sus propias palabras para explicar su papel y su comportamiento, evitando utilizar los títulos de sus tarjetas. Han de hacer preguntas a los demás para ver si podrían ser sus parejas. Quien tenga una herramienta de seguridad debe encontrar una conducta de riesgo a la que pueda hacer frente, y quien tenga una conducta de riesgo debe encontrar una herramienta de seguridad que le pueda proteger.

Al juntarse una pareja deben continuar con el juego, yendo juntos a ayudar a sus compañeros (pueden cambiar de pareja si encuentran otra más ajustada a su papel).

Cuando se hayan formado todas las parejas se comprobarán los resultados. Cada pareja se presentará ante el grupo leyendo sus papeles y explicando por qué la herramienta de seguridad protegería frente al riesgo. De este modo se da pie a un pequeño debate sobre si es la combinación más adecuada (por ejemplo ¿algún otro compañero/a cree que su solución/problema se ajustaría mejor?). Cuando estemos de acuerdo en que se trata de la combinación correcta (anexo 3.1.b), podemos analizar si habría otras herramientas de seguridad complementarias en ese caso, por ejemplo:

- **Frente a virus/malware:** antivirus, actualizaciones de sistema y aplicaciones, copias de seguridad, desconfiar y sospechar de mensajes, publicaciones y archivos, etc.
- **En dispositivos móviles:** además de lo anterior, descargar apps solo de tiendas oficiales, comprobando la información disponible sobre ellas, sus permisos, etc.

- **Para evitar que accedan a nuestra información:** proteger la pantalla de desbloqueo, acordarse de cerrar sesión, configurar la verificación en dos pasos, utilizar contraseñas robustas, no compartirlas con nadie, dar los mínimos datos personales, etc.
- **Para evitar fraudes:** desconfiar y sospechar de mensajes, apps, no dar datos, etc.

Finalmente se plantea utilizar el juego online de Google "Torre del tesoro", para aprender algunos trucos que nos permitirán crear contraseñas robustas y seguras:

Nos movemos hacia adelante, pudiendo solo girar y saltar (con las flechas del teclado) para esquivar los obstáculos y recoger los caracteres (dados ❑). En el 1º nivel solo hay dados ❑ *verdes* con letras minúsculas. Al terminarlo, formaremos palabras (en inglés) con las letras recogidas, a modo de base (sencilla de recordar) para una contraseña segura.

En los siguientes niveles encontraremos también dados ❑ *azules* con letras mayúsculas y dados ❑ *rojos* con números y símbolos. Al completarlos nos aparecerá la palabra creada anteriormente, lista para combinar con las mayúsculas, números y símbolos recogidos, de modo que obtenemos una contraseña mucho más robusta sobre la misma base sencilla.

Finalmente, se puede apuntar la contraseña obtenida como ejemplo para crear nuestras futuras contraseñas de manera segura, e incluso se puede acceder a una web para comprobar su fortaleza.

Como alternativa se plantea una dinámica de construcción de contraseñas en pequeños grupos (3-4 personas), utilizando caracteres de papel (anexo 3.1.c).

En primer lugar a cada grupo se le facilitan las letras minúsculas. Deben repartírselas en un tiempo breve para formar cada uno una palabra sencilla. Si les faltan letras, han de llegar a acuerdos con sus compañeros (se puede utilizar letras "similares", o dejar palabras incompletas a la espera de las mayúsculas, los números y los símbolos).

Seguidamente se les darán las mayúsculas para completar sus palabras o cambiar algunas minúsculas por mayúsculas. En una tercera fase se les facilitarán los números y los símbolos, de modo que puedan añadirlos o sustituir algunas letras. De este modo habrán obtenido una contraseña suficientemente robusta sobre una base sencilla de recordar.

A continuación podrán debatir en pequeño grupo si las contraseñas que han obtenido les parecen más o menos seguras y por qué motivos. Deberán ponerse de acuerdo a la hora de elegir la que consideran más robusta.

Finalmente se realizará una puesta en común en gran grupo de las contraseñas seleccionadas y los motivos por los que consideran que son más seguras ¿estamos todos/as de acuerdo en que son buenas contraseñas?, ¿nos ha parecido muy difícil construirlas?

RECUERDA

Si no proteges tus dispositivos y cuentas de redes sociales, te expones a multitud de problemas online. Ponte al día y revisa sus opciones de seguridad, es más sencillo de lo que parece.

SESIÓN 3.2. ¿Qué apps merecen la pena?

RESUMEN

Antes de instalar una app, valorarla críticamente en términos de necesidad, funcionalidad, desarrollador, permisos que requiere, comentarios, etc. a fin de determinar si parece útil y positiva o puede ser potencialmente peligrosa.

METODOLOGÍA

Se centra en la reflexión y el debate sobre casos ficticios (aunque realistas) de aplicaciones móviles disponibles para instalar. Complementariamente se incluyen recursos multimedia.

MATERIALES

Un equipo multimedia conectado a Internet para el grupo, fichas de apps (anexo 3.2.a) y material de escritura.

DESCRIPCIÓN DE LAS ACTIVIDADES

1. **Reflexión inicial** (10')
   Se plantean varias preguntas sobre nuestro uso de las aplicaciones móviles: ¿cuántas apps tenemos en el móvil/tablet?, ¿son todas gratuitas?, ¿nos hemos planteado alguna vez por qué pueden ser gratuitas?, ¿solemos mirar la información de una app y sus permisos antes de instalarla?
2. **Dinámica debate** (20')
   Cada grupo analizará las fichas de las apps (anexo 3.2.a) y debatirá sobre la seguridad o no de instalar cada una de ellas. Se debe plantear la relación entre la necesidad que motiva su instalación, sus funcionalidades, los permisos que solicita y el resto de información disponible sobre la misma: ¿qué apps instalaríais?, ¿cuál os parece más útil?, ¿os habéis fijado en los permisos que pide, o en la información de la ficha?, ¿son adecuados o excesivos? Asimismo, se plantean los riesgos que se pueden desprender de su uso ¿qué datos manejan sobre nosotros?, ¿Cómo podrían obtener un beneficio? Finalmente se pondrán en común las conclusiones a las que ha llegado cada grupo.
3. **Demostración sobre permisos y apps** (10')
   Algunas personas voluntarias enseñarán desde el PC del aula la forma en que se muestra la información de las apps y sus permisos en Google Play. Asimismo presentarán la manera de revisar los permisos de las apps instaladas en un móvil o tablet (invitando al alumnado a comprobar en casa en sus dispositivos familiares los permisos de las apps instaladas).
   Como alternativa se plantea la creación en pequeños grupos de un listado de buenas prácticas sobre la instalación y uso de apps, poniéndolo en común en gran grupo.
4. **Conclusiones** (10')
   Proyección de un vídeo a elegir: Privacidad y permisos en apps y Videojuegos "gratuitos" (PantallasAmigas), Permisos de apps (PrivacyNow). Se planteará la reflexión sobre lo que más nos haya llamado la atención del vídeo y su relación con esta sesión.
   Para terminar, se pedirá a algunas personas voluntarias que recapitulen lo aprendido en la sesión resumiéndolo en una frase o consejo.

NOTAS PARA DOCENTES

"Cuando instalas una app le das acceso a mucha información privada"

La reflexión inicial pretende hacernos más conscientes del uso que hacemos de las aplicaciones móviles (apps)

En cuanto al número de apps en nuestro móvil/tablet, seguramente tenemos muchas más de las que imaginamos y de las que utilizamos a diario. Sobre la gratuidad de las apps, ¿nos planteamos cómo es posible?, ¿de dónde obtienen ingresos? Se suele pensar en la publicidad, pero también puede haber publicidad personalizada, venta de datos de perfiles personales, compras integradas en la app, etc. En este sentido, ¿solemos mirar la información de una app y sus permisos antes de instalarla o bien aceptamos los términos y condiciones sin más?

La dinámica plantea el debate en pequeños grupos sobre las fichas de apps (anexos 3.2.a y b) identificando posibles riesgos y llegando a un acuerdo sobre si es más o menos seguro instalarlas. Recordar que se trata de fichas totalmente ficticias, y con una información limitada.

En primer lugar se distribuirán los participantes en grupos de 3-4 personas, repartiendo una ficha de app (anexo 3.2.a) a cada grupo. Deben leer cada ficha, analizar la información disponible, plantearse la necesidad que puede motivar a buscar una app así, comparar sus funcionalidades con los permisos que solicita, valorar el resto de información disponible (categoría, opiniones, fecha de última actualización, número de descargas, información del desarrollador, política de privacidad). Su objetivo es identificar los posibles riesgos de instalar esa app y debatir entre ellos si les parece o no de confianza y por qué.

El tiempo para el análisis ha de ser suficiente para que haya debate en cada grupo. En cuanto se termine el análisis de una app, se intercambiará la ficha con otro grupo para analizar una nueva. En el momento en que la persona dinamizadora considere oportuno (por ejemplo tras analizar 3 ó 4 apps), se dará paso a una puesta en común donde se presentará cada app y las conclusiones de los grupos que la habían analizado.

A nivel general conviene hacerse algunas preguntas sobre la seguridad de una app:

- **¿De dónde la saco?** Descargar las apps siempre de las tiendas oficiales (Google Play en Android y App Store en iOS). Desconfiar de archivos descargados de Internet o de tiendas no oficiales, especialmente ante versiones gratuitas de apps de pago.
- **¿Seguro que es ésta?** Si buscamos una app conocida, sospechar de posibles variantes en el nombre de la app, su logotipo o su desarrollador. Si no estamos seguros, mejor contrastar la información (por ejemplo visitando la web oficial del desarrollador).
- **¿Quién está detrás?** La información del desarrollador puede ser muy escueta (basta con un nombre y un email). Desconfiar si no da su dirección o la política de privacidad.
- **¿Qué hace con mis datos?** No es posible tener la certeza absoluta de qué pueden llegar a hacer con ellos. Los usos se han de indicar en su política de privacidad, aunque los permisos que solicita la app pueden darnos algunas pistas.
  Es bastante habitual que los utilicen para proporcionarnos publicidad personalizada o para venderlos a otras empresas. Incluso cuando se ceden "anonimizados" (sin la información de identificación personal), sigue siendo posible unir esos datos con los de otras empresas o con datos públicos creando perfiles detallados de gustos, contactos, etc., lo que es muy valioso para marketing y publicidad.

- **¿En qué tenemos que fijarnos con los permisos?** En que sean coherentes con las funcionalidades de la app. Desconfiar si nos pide acceso a cuestiones que no están relacionadas (por ejemplo una app de linterna que pide acceso a los contactos). Siempre es útil que el desarrollador explique por qué los necesita.
- **¿Popularidad igual a seguridad?** No necesariamente. Si bien hay que desconfiar de apps que no se hayan actualizado desde hace mucho tiempo, de apps con pocas descargas, pocos comentarios y una valoración media baja, también es habitual encontrar apps poco recomendables con buenas valoraciones.

En los casos concretos de las fichas trabajadas (anexo 3.2.a), podemos ver un sencillo análisis en la tabla anexa (3.2.c). De ahí podemos extraer que con cualquier app pueden existir riesgos. No es lo mismo una app legítima, bien valorada, con detallada información del desarrollador y una política de privacidad que explique el uso de nuestros datos (normalmente con fines publicitarios y para su venta/cesión), que una app poco conocida de un desarrollador particular, sin más información sobre su funcionamiento (que también podría ser malicioso).

Obviamente para realizar un mejor análisis de riesgos habría que estudiar en detalle sus políticas de privacidad (donde indican qué datos nuestros recogen y qué hacen con ellos), y los permisos concretos que piden (por ejemplo, en la categoría "Teléfono" no es lo mismo "consultar el registro de llamadas" que "editar el registro de llamadas" o "redirigir llamadas salientes"). Asimismo, para minimizar los riesgos de posibles apps maliciosas (malware), conviene disponer siempre de un antivirus.

Respecto al beneficio económico de las apps conviene dejar claro que **nada es gratis:**

- Desarrollar una app conlleva un tiempo, un esfuerzo y unos gastos, de modo que es lógico que los desarrolladores busquen una contraprestación económica.
- Las apps "gratuitas" también nos cobran, solo que de otra manera: con compras integradas (de funciones avanzadas, objetos virtuales para un juego, etc.), con nuestros datos personales (aun tratados anónimamente, generan perfiles y tendencias de consumo para su explotación comercial) o mostrándonos publicidad (incluso personalizada según nuestro perfil e intereses).
- Las apps "de pago" no siempre son más respetuosas con nuestra privacidad. En algunos casos emplean esas mismas técnicas para obtener más ingresos.

En resumen, la app perfecta no existe. A la hora de elegir una app se ha de valorar tanto lo que nos aporta, como los riesgos que presenta, para en su caso poder asumirlos conscientemente. Además, a partir de Android 6.0 y de iOS 8 podemos permitir/rechazar cada permiso independientemente (y cambiarlo en cualquier momento). Finalmente, cuando nos deje de hacer falta una app, lo mejor es desinstalarla.

La demostración trata de enseñar la forma de ver los permisos y la información de las apps en Google Play y en App Store (por ejemplo con la ficha de una app) y en un dispositivo Android (ajustes – aplicaciones – permisos).

Para más información sobre los permisos se puede consultar la ayuda de Google: permisos en Android 6.0 y posteriores y permisos en 5.1 y anteriores y de Apple privacidad y localización en iOS 8 y posteriores.

Como alternativa se plantea crear un listado de buenas prácticas sobre instalación y uso de apps móviles. Para validarlas podemos fijarnos en las notas de la dinámica debate. En todo

caso se invitará al alumnado a comprobar en su casa los permisos de las apps instaladas en sus propios móviles o en los dispositivos de su familia.

En conclusión se refuerza la idea de la importancia de los móviles y sus apps en relación con nuestra seguridad y privacidad. Sobre los vídeos indicados destacar:

- Privacidad y permisos en apps: la app pide permiso para acceder a contactos y redes sociales y lo usa para vender información personal y publicitarse automáticamente.
- Videojuegos "gratuitos": se desbloquea una función a cambio de un pequeño pago...
- Permisos de apps: la sorpresa al "leer" los permisos de las apps que tienen instaladas.

Así pues, se animará a los participantes a relacionar los vídeos con el trabajo realizado en esta sesión. Se puede aprovechar para guiar una recapitulación de lo aprendido, concluyendo con una frase o un consejo con el que se haya quedado cada uno/a.

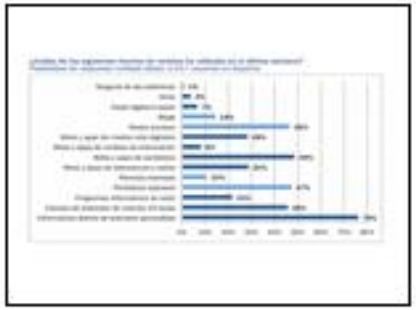
RECUERDA

Cuando necesitamos instalar una app, hemos de ser conscientes que puede poner en riesgo nuestra privacidad y seguridad. Siempre se debe elegir la app más adecuada, valorando sus beneficios y sus riesgos, según la información disponible.

SESIÓN 3 – *Fake News*

3.1. Presentación de diapositivas.


BÚSQUEDA DE INFORMACIÓN EN INTERNET




¿Cómo es la información disponible en internet?


FAKE NEWS

FAKE NEWS

¿Cómo las definirías?

FAKE NEWS

- Son noticias falsas o sin comprobar.
- Persuaden a los receptores para que realicen una acción o adquieran una determinada creencia.

Observá detenidamente estas dos imágenes...

... ¿qué similitudes y diferencias podés encontrar entre las imágenes?

INFORMAR: aquella acción a través de la cual se da a conocer algún hecho, evento, acontecimiento.

PERSUADIR: incluso, mover a alguien a adquirir una creencia y/o realizar una acción.

PERSUADIR: incluso, mover a alguien a adquirir una creencia y/o realizar una acción.

La PUBLICIDAD más persuasiva para incitar a incrementar el consumo de un producto o un servicio.

FAKE NEWS

- Son noticias falsas o sin comprobar.
- Persuaden a los receptores para que realicen una acción o adquieran una determinada creencia.

FAKE NEWS

- Son noticias falsas o sin comprobar.
- Persuaden a los receptores para que realicen una acción o adquieran una determinada creencia.
- Toman como objetivo la manipulación de nuestras opiniones y el beneficio económico.
- Su difusión en internet ha multiplicado las consecuencias negativas y dificulta su control.

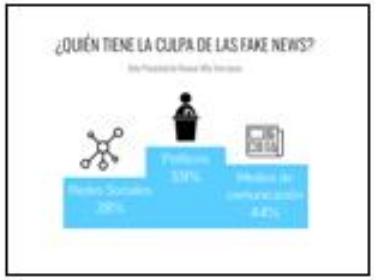
FAKE NEWS

¿Desde cuándo existen?


DINOSAURS!


"YOU ARE FAKE NEWS"


FAKE NEWS
¿Quién las genera?


¿QUIÉN TIENE LA CULPA DE LAS FAKE NEWS?


FAKE NEWS
¿Qué repercusión tienen?

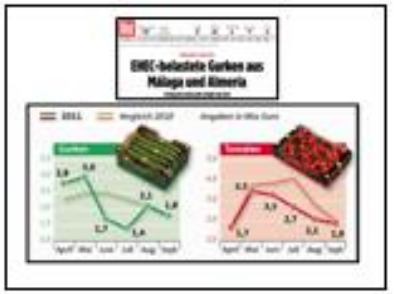

PORCENTAJE DE POBLACIÓN QUE ADMITE HABER CREÍDO UNA NOTICIA FALSA


twitter


MEGA DOSIS DE VITAMINA C


Lavoisa del pepino (2011)


EHEC-belastete Gurken aus Málaga und Almería


EHEC-belastete Gurken aus Málaga und Almería

SESIÓN 4 – *Internet y Salud*

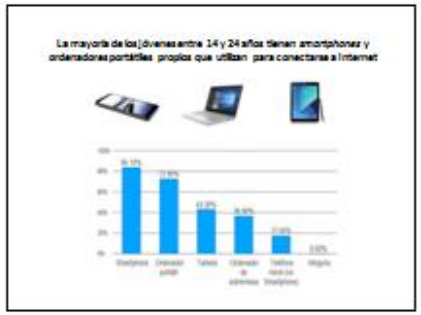
4.1. Presentación de diapositivas.

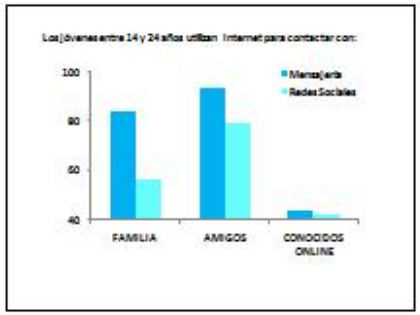

INTERNET
y
SALUD


Jóvenes en el mundo virtual:
usos, prácticas y riesgos
Megías & Rodríguez, sept. 2018
Estudio sobre el uso habitual y los riesgos asociados al uso de las TIC en la población joven. Participaron 1400 jóvenes entre 14 y 24 años.
fad

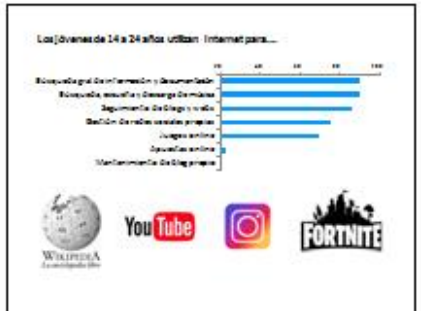

La inmensa mayoría se conecta diariamente, utiliza servicios de mensajería online y gestiona redes sociales propias


Para aprender cómo el uso de internet y los dispositivos móviles afectan a la salud de los jóvenes...
?
+SALUD
... primero debemos saber qué uso realizan los jóvenes de internet y los dispositivos móviles.


La mayoría de los jóvenes entre 14 y 24 años tienen smartphones y ordenadores portátiles propios que utilizan para conectarse a Internet

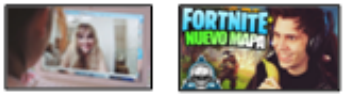

Los jóvenes entre 14 y 24 años utilizan Internet para contactar con:
100
80
60
40
Mensajería
Redes Sociales
FAMILIA
AMIGOS
CONOCIDOS ONLINE

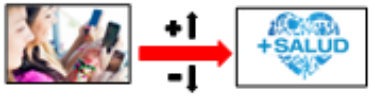

¿Cómo los jóvenes utilizan Internet y los dispositivos móviles?


Los jóvenes de 14 a 24 años utilizan Internet para...
YouTube
FORTNITE


¿Cómo afectan internet y los dispositivos móviles a la salud de los jóvenes?
+?
-?
+SALUD

Efectos positivos sobre la salud





Debemos aumentar los efectos positivos y reducir los efectos negativos de Internet y los dispositivos móviles en la salud

- por el esfuerzo de enfocar objetos próximos
- por la alta intensidad de la luz azul

Efectos negativos sobre la salud

La sobreexposición a las pantallas daña la vista

La luz de las pantallas altera el sueño

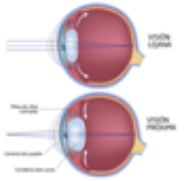
El calor que desprenden los móviles daña el oído

La mala postura causa dolores musculares y articulares

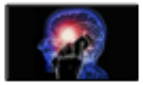
Debemos aumentar los efectos positivos y reducir los efectos negativos de Internet y los dispositivos móviles en la salud

- por el esfuerzo de enfocar objetos próximos

El uso de móviles en la cama para enfocar objetos próximos



Efectos negativos sobre la salud

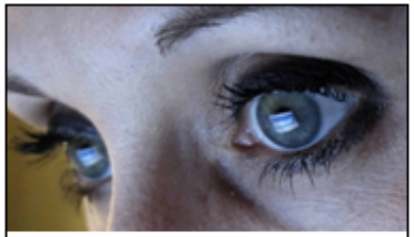


Las radiaciones emiten radiaciones electromagnéticas

Los dispositivos móviles favorecen el sedentarismo

Insomnio y los dispositivos móviles son adictivos

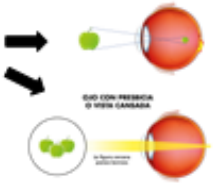
Un uso abusivo puede provocar ansiedad, estrés, depresión

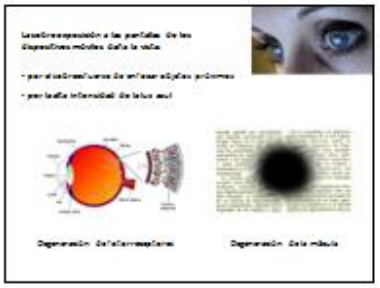


La sobreexposición a las pantallas de los dispositivos móviles daña la vista

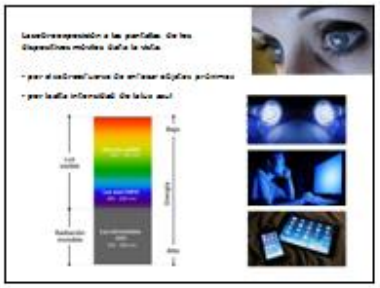
- por el esfuerzo de enfocar objetos próximos

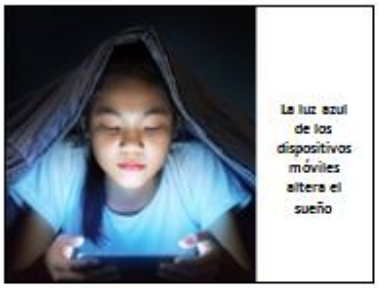
Demasiada cerca de los ojos
Sin iluminación ambiental
Letra y objetos muy pequeños





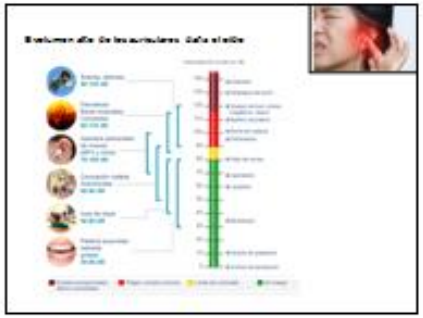

La evidencia no es concluyente

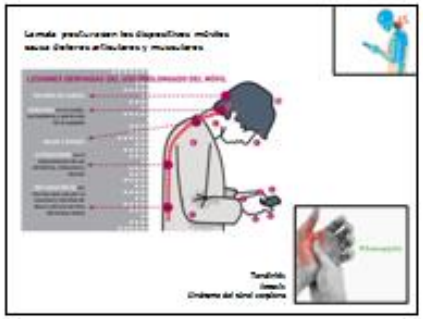



La luz azul de los dispositivos móviles altera el sueño


VAMPING
4 - 5 h
sueño nocturno

El volumen alto de los auriculares daña el oído





PROYECTO

Diseño y exposición de una presentación de diapositivas

PROYECTO
Diseño y exposición de una presentación de diapositivas.

Una vez realizada la formación teórica y las sesiones prácticas del curso, los aspirantes a cibertutores (*media coaches in action*) deben de elaborar una presentación de diapositivas y mostrarla a sus compañeros/as de 1r y 2º ESO del centro. Esta presentación debe promover el uso correcto de Internet y las redes sociales, prevenir el ciberacoso, el sexting y el grooming, y concienciar sobre los hábitos saludables en el uso de los dispositivos móviles.

Consejos para una correcta elaboración de un presentación de diapositivas y su exposición.

1. Identifica el mensaje que deseas transmitir

Tu presentación no son sólo tus diapositivas. Se trata del mensaje que quieres comunicar.

2. Escríbela tu presentación

Comienza en un documento de texto, y realiza el desarrollo secuencial o guión de toda la presentación para darte una idea de cómo la información presentada "fluirá", y cómo el público la verá en secuencia.

3. Resalta lo más importante

Una presentación cubre las piezas más cruciales únicamente. Por tanto, elige puntos clave.

4. Conoce a tu audiencia

Como hablas en una sala llena de profesionales de la medicina debería ser diferente a la manera en que hablas en una sala llena de jóvenes empresarios. La selección de tu tema, el lenguaje que usas, los ejemplos que das para ilustrar puntos. Tu presentación será mostrada a alumnos y alumnas de 12 – 14 años de 1r y 2º ESO. Ten esto en cuenta a la hora de decidir qué lenguaje vas a utilizar y qué materiales mostrarás.

5. Ensaya mentalmente y en voz alta la presentación mientras la construyes.

Nunca es demasiado temprano para acostumbrarte al ritmo de tu presentación, y tomar nota de conceptos que quieres enfatizar. Mientras lo dices en voz alta, comenzarás a desarrollar un "sentimiento" para el material y notarás que algunas cosas funcionan bien, mientras que otras no y podrías necesitar trabajar en ello.

Es importante la presentación no sea aburrida y genere distracción. A continuación tienes unos consejos para el diseño de la presentación para asegurarte de que ésto no te ocurra.

6. Elabora diapositivas sencillas

Ten en cuenta que menos es más (efectivo). Una diapositiva muy llena de información causa distracción. Genera confusión a una audiencia: ¿En qué parte de la diapositiva debería enfocarme? ¿Debería leer la diapositiva o prestar atención al presentador? Por otro lado, una

diapositiva sencilla y visualmente atractiva cautivará a tu audiencia, manteniéndolos atentos con tus principales conceptos.

7. Limita las palabras en tus diapositivas

Menos es más efectivo también en lo que se refiere a las palabras. Si es posible, evita las viñetas por completo. La audiencia debería escuchar, no leer.

8. Utiliza fotografías y gráficos de alta calidad

Las personas probablemente te tomarán más en serio si tu presentación es visualmente atractiva. Los usuarios ven el diseño atractivo como más utilizable, por lo que una presentación más atractiva será también más efectiva. Así que asegúrate de usar fotografías y gráficos de alta calidad en tu presentación.

9. Usa esquemas y gráficas precisas y relevantes

Esquemas y gráficas también puedes causar distracción si no se utilizan adecuadamente. Asegúrate que el diseño de tu información sea simple y limpio para que la audiencia no pase todo el tiempo tratando de descifrar lo que dice tus gráficos.

10. Usa plantillas frescas de alta calidad

¿Has visto la antigua plantilla que parece papel desgastado y utiliza salpicaduras de tinta? Si, también tu audiencia. Las plantillas pueden causar distracción si son demasiado básicas o si el diseño se siente anticuado. Afortunadamente hay un número de plantillas para presentación de diapositivas efectivas para ayudarte si no eres un diseñador.

11. Elige las fuentes apropiadas

Las fuentes son una parte importante para cautivar a tu audiencia. Elecciones de fuentes y tipografía tienen un efecto subconsciente en el público, causando que caractericen la presentación y marca de tu compañía positiva o negativamente.

12. Elige bien el color

Similar a la elección de la fuente, los colores causan específicas reacciones subconscientes en el público. Elegir una combinación de color anticuada para tu presentación la volverá inefectiva.

13. Asegúrate que todos los objetos estén alineados

Una simple manera de crear una presentación bien diseñada es asegurarte de que todos los objetos en una diapositiva estén intencionalmente alineados. Para hacer esto: mantén presionada la tecla mayúsculas + selecciona todos los objetos que quieres incluir, luego elige Organizar en la barra de opciones, y aplica Tipo de Alineación.

14. Limita la puntuación

Enfatiza tus puntos (mientras hablas). No incorpores (!!) para que lo hagan por ti.

15. Evita exagerar el formato en tus puntos

No hay necesidad de que cada palabra de cada viñeta esté en mayúsculas, o que las letras en todas tus viñetas tengan el tamaño de un título.

16. ¡Ensaya, ensaya, ensaya!

La exposición es probablemente más importante que el contenido. Experimenta con pausas, gestos y lenguaje corporal. Aquí está cómo llegar a estar más consciente de tus propias gesticulaciones, y cómo realizar la presentación como un profesional.

17. Práctica con un cronómetro

La consistencia es la clave para una presentación de diapositivas eficaz. Los intervalos deberían ser similares (idealmente los mismos) cada vez que ensayas.

18. Ten un ritmo pausado y haz pausas con más frecuencia.

Muchos de los mejores oradores hoy en día hablan despacio intencionalmente. Tendrás oportunidad de enfatizar, parecer más pensativo, y hacer que tu información sea más fácil de digerir. Hacer pausas más frecuentes, permite que los principales conceptos sean enfatizados y que la información se capte perfectamente. Necesitas permitir que los conceptos clave respiren un poco antes de pasar a la siguiente sección.

19. Grábate tu Mismo

Usa la grabadora de tu teléfono. Evalúate y critícate tu mismo. Considera:

¿Son tus pausas demasiado cortas o demasiado largas? ¿Estás hablando lo suficientemente lento? ¿Demasiado lento?

Siempre es extraño escuchar tu propia voz grabada, no te preocupes.

20. Elige tres puntos focales en la sala

Si miras fijamente el mismo punto (o incluso más siniestro, a la misma persona) todo el tiempo, tu presentación será inefectiva (y mala). Las personas se distraerán por ti, preguntando qué miras fijamente. Intenta ésto: elige tres puntos en la sala (típicamente: izquierda, centro, derecha) y tómate el tiempo para dirigir tu exposición hacia cada punto focal físico en la sala. También, enfócate en el centro cuándo abordes tus conceptos principales.

21. Varía la extensión de tu oración y modúlate.

Esto te hace sonar más interesante y es más fácil de seguir para tu audiencia. Piensa breve y sustancioso. O ve largo y complejo para un efecto dramático. Modúlate: no hables en el mismo tono toda tu presentación. Sé consciente de subir y bajar el tono de tu voz.

22. Practica frente a un espejo

La manera en cómo te ves es tan importante a cómo suenas. Finge como si sólo tuvieras una conversación normal, y permite que tus manos se muevan con tu discurso-enfatizando tus conceptos.

23. Usa el "modo presente" cuando ensayes

Si utilizas Powerpoint, asegúrate de que utilices la opción Usar Vista del Moderador cuando pulses Mostrar Presentación. Esto te permitira (y solamente a ti) ver notas adicionales sobre cada diapositiva en caso de que olvides algo.

¡Momento de la Presentación! Ten en cuenta estos consejos para el día de la presentación:

24. Respira Profundo y tómalo con calma.

Respirar profundo está probado que alivia el estrés. Es sencillo y te ayudará a mantener la calma y en el momento también. Incluso hasta el último minuto antes de comenzar. Cuando estamos tensos o nerviosos, tendemos a hablar más rápido. Conscientemente, ¡respira profundo de nuevo y recuérdate tomarlo con calma!

25. ¡Fínge Hasta que lo Logres!

Avanza con confianza. Si actúas con confianza, comenzarás a sentirte más confiado. Muévete lentamente con gracia, habla claramente, sonríe, viste algo bonito, y parecerás confiado ante todos los asistentes (no importa cómo te sientes internamente).

26. No utilices transiciones de diapositiva muy llamativas

Estas transiciones generan distracción y son anticuadas.

27. Evitar leer directamente de tu papel o las diapositivas

Leer durante la presentación te hace ver que no estás preparado. Muchas personas lo hacen, pero no deberían. Como regla general, deberías únicamente estar presentando algo que sabes bien y al menos haz memorizado en su mayor parte los principales conceptos importantes.

¡Buena Suerte!

Aprender a escribir, diseñar y presenetar una presentación de diapositivas altamente efectiva es una habilidad invaluable para ofrecer en una compañía, a un empleador y/o a tu comunidad. Si eres un buen comunicador de mensajes importantes, nunca pasarás hambre.

Desarrollo del proyecto

SCHEDULE, DEVELOPMENT AND MAIN RESULTS OF THE PROJECT

Project Development

1 Sep 2018 - Start

The project starts and it will last 24 months (two years)

Sep 2018 - Preparing the Meeting C1 in Heidelberg

In September, the coordinators planned and organized the logistics for the Meeting C1 in Heidelberg (Germany). We translated the Student Media Coaches Program (SMEP) Handbook from the State Communication Center in Baden-Wüttemberg from German into Catalan and prepared a slide show on the topic "Cyberviolence".

8 – 12th Oct 2018 - Meeting C1: Teacher Training Meeting (Heidelberg, Germany)

The second week of October, the project coordinators from the six schools met in Heildelberg (Germany). There they were trained about the risks of Internet and mobile devices (cyberbullying, cibersecurity, fake news...). The training is based on the Handbook from the State Communication Center (Heidelberg) and the information collected by the coordinators from the six countries. Two project coordinators from Spain travelled to Germany and the costs of travel, accommodation and meals of them in this meeting sum 1314 euros.

15 – 16th Oct 2018 - Initial Training Conference for School Exchange Association Projects (KA229; Toledo)

The week after the C1 Meeting in Germany we attended a training conference on Erasmus+ Project organized by SEPIE (Spanish Service for the Internationalization of

Education). In these days they explained us how to carry out the organization and management of the project, budgetary items, communication and impact of the project. . .

25 th Oct 2018 – Erasmus+ Conference KA2 Scholars and Adults (Valencia)

The week after the C1 Meeting in Germany, we attended a training session on Erasmus projects organised by the Valencian division of the Erasmus+ National Agency. In these days they explained us how to carry out the organization and management of the project, budgetary items, communication and impact of the project considering the regional laws of la Comunidad Valenciana.

14 th Nov 2018 – Introduction of the project to the teacher staff

At an ordinary staff meeting in November, we communicated them the aims of the project and invite them to participate in future activities and events.

15 th Nov 2018 - Meeting with the 3rd and 4th grade tutors

We requested the collaboration of the 3rd and 4th grade tutors to help us to recruit students for our project. In their tutoring time, the tutors talked about the project to their students and invited them to participate.

22 th Nov 2018 – Introduction of the project to the 3rd and 4th grade students

More than 30 students interested in the project and attended the first official meeting. In this meeting we discuss the aims of the project, the participants, their functions, the meetings . . .

29 th Nov 2018 - Second meeting of the Erasmus+ Project

One week later, we gave the students an autorization to be signed by the parents which entitled them to participate in the project. We explained again the aims of the project, the participants and their function.

22 th Nov – 20th Dec 2018 - Registration of students in the Erasmus+ Project

More than thirty students registered in the Erasmus+ Project, although they have no clear ideas about the project.Their parents have signed the authorization. We explained them the advantages and disadvantages of the project. Twenty-four of them decide to join. They are registered in E-twinning and Signal, so they can communicate with other European students.

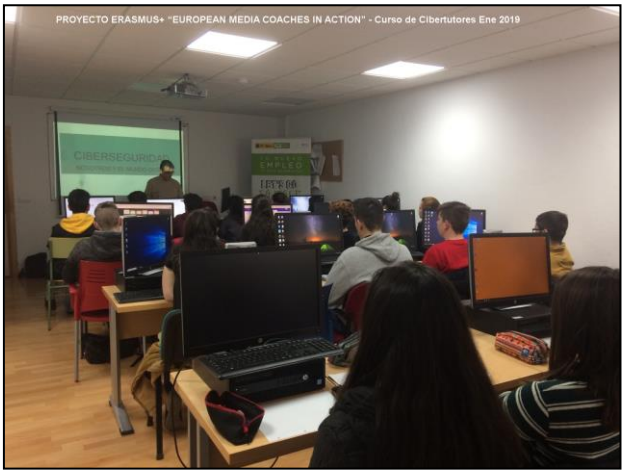
Dec 2018 – Jan 2019 - Organization and management of the Training Course "European Media Coaches in Action"

During these months we meet several times, individually or in group, with the students and we clarify some doubts about the project. We focus on creating motivating and useful materials to raise awareness of the risks of the internet and mobile devices. We decided that the three coordinators will teach the contents. The contents will be divided in four issues: cyberviolence, cybersecurity, fake news and Internet and Health. The teaching will be outside the center.

28th, 29th, 30th Jan 2019 - Training course "European Media Coaches in Action" (20 h)

Over 3 consecutive days, twenty-four 3rd and 4th grade students (14 - 16 years old) selected for the project had three 5-hour training sessions on the following four blocks: cyberviolence (cyberbullying, grooming, sexting, radicalization), cybersecurity, fake news and Internet and health. This training was held at the training centre of the Local Development Agency of Alicante. This Agency, which usually gives training courses for adults, provided us with a computer room for our students. The media coaches spent the remaining 5 hours of

the course to create a first draft from the material received in the course. They will use this material in the training sessions of the 1st and 2nd grade students (12 – 14 years old; peer-to-peer training).



5th Feb 2019 - *E-Safety Day*

Our school celebrated *E-Safety Day* with activities to make students aware of the risks of the inappropriate use of the Internet. We created a large mural with the title "dot and opinion" and invited the students to participate by giving their opinion on cyberviolence, cybersecurity, fake news and the effects of mobile device use on health. More than 200 students read the mural and discussed the importance of preventing risks on the Internet. Sixty of them wrote their opinion on the mural. After the e-safety day, we decided to extend the exhibition one more week, so that the message would reach many more students.

20th Feb 2019 - <u>Certificate delivery</u>

On 20th February we gave the 24 media coaches the certificates of attendance and participation in the course “European Media Coaches in Action" held at the training centre of the local development agency of Alicante on 28 th, 29 th and 30th January 2019.

Mar 2019 -<u>Development of their own material for the peer to peer training</u>

Media coaches spent the month of March developing their own materials for peer-to-peer training. These materials consisted of a slide show, card games, role-playing games, and video visualization. Of the 24 media coaches who were trained, 17 (8 pairs) developed sufficient and appropriate material to introduce their younger peers.

10th Mar 2019 – <u>News about the Training Course and the Erasmus+ Project in the press and TV</u>


ALICANTE

Los institutos combaten por primera vez el ciberacoso formando «Hermanos Mayores»

►Alumnos de 15 y 16 años aprenden a actuar frente al acoso en las redes sociales y se convierten en cibertutores de los más pequeños de 12 y 13 años ►El proyecto lo comparten seis países europeos

Apr 2019 - Supervision and rehearsal of the peer-to-peer training sessions

In April, the project coordinators check the work and the media coaches did the first rehearsals of their training sessions. Each pair of media coaches would train one or two groups of 1st and 2nd grade on the appropriate use of the Internet.

May 2019 -Peer-to-peer training sessions

During three weeks in May, the media coaches will carry out the training sessions for the 1st and 2nd ESO students. Eight groups will receive the training, which add in whole more than 230 students. The coordinators will accompany the media coaches and record the sessions. After the sessions we will gather the media coaches and make a balance.

May – Oct – 2019 - Organizating Meeting C2 in Alicante

From May to October 2019, we will organize the logistics of the Meeting C2 in Alicante. In this meeting, circa seventy media coaches and coordinators from the six participating countries of the project will work together to create new materials to make the educational community aware of the risks of Internet.

25 – 29 Nov 2019 - Meeting "Media Coaches in Action" in Alicante


THE INTERNET DOESN'T
FORGET ANYTHING!


@
MCA


MEDIA COACHES IN ACTION

EL MUNDO España Opinión Economía Internacional Deportes Cultura Tv LOC Más

‹ España | Comunidad Valenciana | Alicante Castellón Arts

EDUCACIÓN · Proyecto en Alicante

Alumnos que guían a otros en el uso seguro de internet

DANIEL MOLTÓ
@danielmolto
Alicante

Actualizado Martes, 26 noviembre 2019 - 07:02

Comentar

Un proyecto del IES Figueras Pacheco de Alicante instruye sobre los riesgos de las redes sociales. En esta segunda fase han participado alumnos de cinco centros europeos.

Una de las actividades entre alumnos de los distintos centros. E.M.

11th Feb 2020 - *E-Safety Day 2020*

Our school celebrated *E-Safety Day* with activities to make students aware of the risks of the inappropriate use of the Internet. We created a large exhibition and invited the students to participate by giving their opinion on cyberviolence, cybersecurity, fake news and the effects of mobile device use on health.

16th Mar 2020 *The project is stopped by the coronavirus crisis*

Project Dissemination

The project was disseminated in the school through:

The introduction of the project to the faculty of teachers

banners and posters in the E-Safety Days 2019 and 2020

the organization of the meeting in Alicante

The project was disseminated beyond the school through:

- the school's website https://figueraspacheco.com/

- uploaded videos in You Tube and Twinspace

- publication in local newspaper Información of Alicante 10th Mar 2019 and 17th Feb 2020

https://www.diarioinformacion.com/alicante/2019/03/10/institutos-combaten-primera-vez-ciberacoso/2126488.html

https://www.diarioinformacion.com/alicante/2020/02/17/institutos-secundaria-estrenan-curso-viene/2235720.html

- interview in regional television À punt in the program À Punt Directe 14th Mar 2019

https://www.youtube.com/channel/UCOGgfN6Ya6OrCOG4TrFkfuQ

- publication in digital press El Mundo 26th Nov 2020

https://www.elmundo.es/comunidad-valenciana/alicante/2019/11/26/5ddc119dfc6c83f63c8b4679.html