SEGURETAT A LES XARXES

PROJECTE ESTADÍSTIC

Marc García, Moncef Boumadian i Àlex Corbalán
Matemàtiques CT - 1r de Batxillerat
Institut Damià Campeny

2023

ÍNDEX

0. INTRODUCCIÓ

Avui dia estem més interconnectats que mai. Vivim en un món on constantment s'envien dades des d'una punta de l'escorça terrestre a l'altre i no sabem ben bé com. Tota aquesta quantitat ingent d'informació viatja per l'aire i fa que tot el nostre entorn funcioni i que puguem gaudir de molts serveis que fins fa poc temps eren impensables.

Anys enrere, totes les comunicacions eren per cable i només una petita quantitat de la població en podia fer ús d'ella. Amb l'invent de les xarxes i la comunicació per senyals, aquest concepte de la informació ha passat de ser una cosa tangible a abstracta, i això ens ha fet pensar que, com "ningú" pot accedir a ella directament, està totalment protegida de ser interceptada i robada per tercers.
Si més no, les empreses que processen les dades que tu els proporciones, moltes vegades indirectament, per tal de fer ús del seu servei, et garanteixen un nivell de seguretat per a aquestes, però la gran part del treball per a protegir-les de veritat resideix en mans de nosaltres.

La principal eina que posseïm com a consumidors i que ens ajuda a protegir-nos són les contrasenyes, un mecanisme de xifratge que restringeix l'accés a la nostra informació a tots aquells que no coneguin la clau d'encriptació. Tot i això, no és pas infranquejable. Depèn de la dificultat de la mateixa que qualsevol intrús la pugui desxifrar, i amb els programes actuals de hackeig, aquesta tasca es fa relativament senzilla per a qualsevol persona amb mínims coneixements en ciberseguretat. A més a més, el fet que ens requereixin contínuament diferents contrasenyes, resulta en que acabem utilitzant, en molts casos, la mateixa, a fi de no oblidar-nos d'ella. L'exemple clar d'aquesta problemàtica és que, només entre els anys 2021 i 2022, la contrasenya més usada a escala mundial va ser "123456", la qual utilitzaven 103 milions d'usuaris i només exigia d'1 segon per ser desxifrada.

A mesura que el món es digitalitza per complet, es posa també en perill la seguretat dels nostres béns i de la nostra persona. El *phishing* o la suplantació d'identitat són models clars d'aquests perills, i tots tenen com a resultat el xantatge o l'estafa, per tal d'obtenir un benefici econòmic.

D'aquí la importància de prevenir i saber protegir-se de la millor manera, sent previngut i perspicaç a l'hora de navegar i compartir per les xarxes. Aquesta és només la punta d'un iceberg que cada cop es fa més gran i amenaça la nostra privacitat, vulnerant els drets fonamentals de les persones. Hem d'estar preparats per al futur, un futur digital i, esperem, segur. Realment ho estem?

Amb aquest estudi tractarem de determinar els coneixements i pràctiques de la població en relació a la seguretat a les xarxes i la prevenció durant la navegació per Internet, focalitzant-nos en el nostre entorn més proper, els alumnes de 1r de Batxillerat de l'IES Damià Campeny.

1. MARC TEÒRIC DE TREBALL

La seguretat a les xarxes, des del punt de vista de l'usuari, consisteix en adoptar les millors estratègies per protegir-se a Internet, a partir de les eines que les plataformes ens proporcionen i dels consells que els experts en la matèria recomanen seguir.
Per determinar els hàbits i el nivell de coneixement que la població té sobre el tema, tractarem, a grans trets, els següents àmbits: contrasenyes, xarxes socials, navegació i problemàtiques.

1.1. CONTRASENYES

a. CONTRASENYES SEGURES

Tal i com ens indica l'empresa Kaspersky, especialitzada en ciberseguretat, una contrasenya ha de:

- Tenir com a mínim 12 caràcters (tot i que quan més llarga sigui millor).
- Estar composta per números, símbols, lletres majúscules i lletres minúscules.
- Tractar de crear contrasenyes basades en sèries de paraules sense connexió.
- Evitar contenir rutes de teclat simples de recordar.

a.1. "Temps que triga un hacker en desxifrar la teva contrasenya (any 2022)":

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Font: Hive Systems

b. CREACIÓ DE CONTRASENYES

A més a més, la revista de tecnologia Xataka cita els següents consells per tal de crear una contrasenya segura i fàcil de recordar:

- Mai utilitzar paraules genèriques com "contrasenya" o "123456".
- Mai no utilitzar informació personal com dates d'aniversari, plaques del cotxe, nom de mascotes, adreces o qualsevol dada que pugui ser investigada.
- Substituir lletres amb números ja no serveix de gaire en paraules òbvies. Per exemple, utilitzar "P455w0rd" en lloc de "Password", ja que als programes per desxifrar contrasenyes els portarà el mateix temps endevinar-la.
- No utilitzar paraules òbvies del diccionari o una combinació de paraules també extretes del diccionari.
- No utilitzar mai com a contrasenya el vostre nom d'usuari.
- Mai utilitzar la mateixa contrasenya per a dos o més llocs.
- No compartir les contrasenyes. Intentar no escriure-les, ja sigui en paper o de forma digital.
- Evitar l'ús de l'opció "recordar contrasenya" dels navegadors.

b.1. "Les 50 contrasenyes més utilitzades (any 2022)":

1. 123456	11. 123123	21. mustang	31. 7777777	41. harley
2. password	12. baseball	22. 666666	32. f*cky*u	42. zxcvbnm
3. 12345678	13. abc123	23. qwertyuiop	33. qazwsx	43. asdfgh
4. qwerty	14. football	24. 123321	34. jordan	44. buster
5. 123456789	15. monkey	25. 1234...890	35. jennifer	45. andrew
6. 12345	16. letmein	26. p*s*y	36. 123qwe	46. batman
7. 1234	17. shadow	27. superman	37. 121212	47. soccer
8. 111111	18. master	28. 270	38. killer	48. tigger
9. 1234567	19. 696969	29. 654321	39. trustno1	49. charlie
10. dragon	20. michael	30. 1qaz2wsx	40. hunter	50. robert

Font: WP Engine

1.2. XARXES SOCIALS

a. COM ACTUAR A LES XXSS

Des del Centre de Transformació Digital (CTD) de Córdoba es recomana el següent, relatiu a l'ús de les xarxes socials:

- **No acceptar sol·licituds d'amistat a desconeguts.**
Moltes vegades fingeixen ser una altra persona per guanyar-se la confiança de la víctima abans de demanar informació o diners.

- **No revelar informació personal.**
Com adreces, número de telèfon, nombre de comptes bancaris, entre d'altres.

- **No fer clic a qualsevol lloc web o enllaç.**
Moltes vegades apareix publicitat falsa, cosa que podria ser un virus i posar en perill les dades personals.

- **Configurar les preferències de privadesa en cada aplicació.**
Evita que aquestes puguin acudir a la secció de privadesa i dades personals.

- **Deshabilitar comptes vells en desús.**
Evita correr risc de deixar dades i informació personal.

- **Ser conscient a l'hora de publicar.**
Quan es publica informació en un lloc, es queda allà per sempre. Encara que hi hagi la possibilitat d'eliminar el compte o el contingut, no és segur saber si algú ja ha fet una captura de pantalla o si ha compartit la informació amb un tercer.

b. POLÍTIQUES DE PRIVADESA

És un document legal que planteja com una organització reté, processa i gestiona les dades de l'usuari o client. Aquesta és utilitzada majoritàriament en un lloc d'internet. La Política de Privadesa és un contracte en què l'organització promet mantenir la informació personal de l'usuari.

L'usuari té com a responsabilitat llegir-la per assegurar-se que no hi ha condicions per les quals es dugui a terme un intercanvi d'informació de l'usuari, la qual es pot veure com una violació de privadesa.

1.3. HÀBITS DURANT LA NAVEGACIÓ

a. COM NAVEGAR PER INTERNET

Segons l'empresa Leader Network, especialitzada en xarxes i comunicacions, aquests són alguns consells que tothom hauria de seguir per navegar de manera segura:

- Anar en compte amb les WiFi i carregadors públics.
Encara que tinguin una contrasenya per a la connexió, les WiFi públiques són vulnerables a atacs externs que podrien afectar tots els que estiguin connectats a aquesta xarxa. Per això, si no és necessari utilitzar-les, millor no accedir a cap servei que necessiti contrasenya, realitzar operacions bancàries o descarregar documents confidencials. Pel que fa als carregadors públics, millor evitar connectar el dispositiu per USB a qualsevol ordinador públic ja que es poden manipular per extreure informació de qualsevol dipòsit USB al qual es connectin.

- Desactivar les xarxes sense cable (WiFi, bluetooth…) si no es faran servir a curt termini.
Els atacants poden utilitzar punts d'accés falsos i enganyar el dispositiu perquè es connecti automàticament a una xarxa de suposada confiança des d'on es monitoritza l'activitat de l'usuari sense que sigui conscient.

- Realitzar actualitzacions de programari.
Els OS mòbils inclouen un sistema d'actualització d'aplicacions amb què informen els usuaris sobre les noves versions disponibles de les aplicacions instal·lades. És fonamental fer aquestes actualitzacions, ja que a més d'incloure noves funcionalitats corregeixen errors de seguretat. Mantenint el sistema actualitzat s'eviten infeccions mitjançant apps vulnerables. Però compte perquè algunes aplicacions gratuïtes que instal·lem; la primera vegada semblen «innocents», però després les actualitzacions venen carregades de modificacions per tenir permisos que no tenen res a veure amb la finalitat de l'aplicació instal·lada.

- Només instal·lar apps des dels repositoris oficials (App Store, Google Play…).
Evitar la principal font d'infecció que és la instal·lació d'aplicacions mòbils des de fonts desconegudes.

- Tapar la càmera dels portàtils i dispositius mòbils.
Accedir a la webcam o micròfon és relativament senzill, i en molts casos no cal que el punter vermell s'encengui per indicar que s'està utilitzant.

1.4. PROBLEMÀTIQUES

a. RISCOS EXISTENTS

Passem gran part de les nostres vides en línia i algunes de les amenaces de seguretat i privacitat a Internet que podem trobar són:

Hackeig	Phishing	Ransomware
Virus o malware	Robatori d'identitat	Botnets
Grooming	Sexting	Ciberassetjament

b. UN EXEMPLE: EL *PHISHING*

El *phishing* és un mètode que s'utilitza per obtenir informació confidencial de forma fraudulenta (contrasenyes, dades bancàries, números de targetes de crèdit…) i amb això cometre una estafa.

El ciberdelinqüent es fa passar per una persona o empresa de confiança, comunicant-se a través d'un correu electrònic, SMS o, fins i tot, mitjançant trucades telefòniques.
Els qui confien en el missatge i fan clic en algun dels enllaços que inclou, accedeixen a un lloc web fals i introdueixen les dades personals. En obtenir aquestes dades, el ciberdelinqüent les utilitza per estafar. Algunes possibles estafes són:

- Robatori en comptes bancaris
- Suplantació d'identitat
- Venda de dades personals
- Enviament de publicitat

c. DELICTES INFORMÀTICS

Segons el Sistema Estadístic de Criminalitat (SEC), a Espanya es van enregistrar més de 305.000 delictes informàtics l'any 2021, atribuïts en part a l'augment de dispositius electrònics i connexió a Internet de les llars. En concret, des de l'any 2017, aquests casos han augmentat un 6%, dels quals un 87,4% estan relacionats amb fraus informàtics.

No obstant això, a l'informe es fa una distinció entre els fets coneguts i els aclarits; per això, malgrat que es van registrar 305.477 estafes per aquests mitjans, només se'n van aclarir 46.141, dels quals 13.801 van tenir com a conseqüència la detenció d'alguns dels agents maliciosos.

2. METODOLOGIA

2.1. ESTUDI DELS ELEMENTS

La població sobre la qual es realitza la investigació són els 80 alumnes que actualment cursen 1r de Batxillerat a l'IES Damià Campeny, amb una edat d'entre 16 i 17 anys, és a dir, nascuts l'any 2006.

La mostra representativa estudiada està composta per 67 alumnes, els quals suposen un 83,75% de la població total. La mida de la mostra ha estat obtinguda; tenint en compte que la població és finita (<100.000 individus) i es realitza amb un **interval de confiança del 95,5%** (per tal de que sigui el més acurat possible) i un error del 5%, mitjançant la següent fórmula:

Nomenclatura:

$n = mida\ de\ la\ mostra$
$N = mida\ de\ la\ població$
$p = dispersió\ poblacional$
$q = 1 - p$
$e = error\ de\ mostreig$

$$n = \frac{4 \cdot p \cdot q \cdot N}{e^2 \cdot (N-1) + 4 \cdot p \cdot q} \Rightarrow$$

$$n = \frac{4 \cdot 0{,}5 \cdot 0{,}5 \cdot 80}{(0{,}05)^2 \cdot (80-1) + 4 \cdot 0{,}5 \cdot 0{,}5} \simeq \mathbf{67}$$

Aclariments:

$p \rightarrow$ La **dispersió** és un concepte que determina la variabilitat dels valors per tal de captar totes les possibles diferències. En el nostre cas, com es desconeix, es suposa la dispersió més desfavorable (*0.5*).

$e \rightarrow$ L'**error de mostreig** és la diferència entre els valors obtinguts de la mostra i els que s'haurien obtingut en treballar amb la població total. El nostre és de *0.05*, un nivell baix degut a que el grau de confiança de l'estudi és alt (*95,5%*).

2.2. VARIABLES

Per determinar els coneixements i pràctiques de la població en relació a la seguretat a les xarxes i la prevenció durant la navegació per Internet, s'analitzen diferents àmbits: contrasenyes, xarxes socials, hàbits durant la navegació, problemàtiques i valoració personal.

a. ENQUESTA

Per abastar-los tots, s'han extret els punts més importants de cada àmbit i s'ha plantejat una pregunta en relació al mateix, per tal de definir i associar la variable. Així doncs, s'ha enviat als enquestats un formulari que consta de 13 preguntes, cadascuna amb una intenció exposada a continuació:

I. Contrasenyes

1. **Utilitzes sempre la mateixa contrasenya?**

[**QUALITATIVA DICOTÒMICA**] - Saber el nivell de seguretat que la mostra té en els seus comptes.

2. **Quants digits/caràcters té la teva contrasenya?**

[**QUANTITATIVA DISCRETA**] - Saber el rang de dígits que la mostra utilitza en les seves contrasenyes.

3. **Creus que la teva contrasenya compleix els requisits mínims, i per tant, és segura?**

[**QUALITATIVA DICOTÒMICA**] - Saber si la mostra coneix els requisits que una contrasenya ha de tenir per ser segura i si ho aplica en les seves.

II. Xarxes Socials (XXSS)

4. **Les teves xarxes socials són públiques o privades?**

[**QUALITATIVA DICOTÒMICA**] - Saber el tipus de privacitat establerts a les xarxes socials de la mostra.

5. **Coneixes personalment a tota la gent que et segueix a les xarxes?**

[**QUALITATIVA DICOTÒMICA**] - Saber si són conscients de qui pot saber tota la informació que publiquen o si s'estan exhibint davant de desconeguts.

6. **Acostumes a llegir les Polítiques de Privadesa de les apps i XXSS?**

[**QUALITATIVA ORDINAL**] **-** Saber si són conscients de tot el que poden fer les pàgines amb la informació que els otorguem.

7. **Creus que és important llegir-les? *Valora-ho de l'1 al 10.***

[**QUANTITATIVA DISCRETA**] **-** Comprovar si la mostra és conscient del que comporta aceptar Polítiques de Privadesa sense saber la informació que proporciona.

III. Hàbits durant la navegació

8. **Tapes la càmera dels teus dispositius?**

[**QUALITATIVA ORDINAL**] **-** Conèixer si la mostra pren mesures per protegir-se de les amenaces a Internet i xarxes.

9. **Quan ingresses en un lloc web, acostumes a acceptar TOTES les *cookies*?**

[**QUALITATIVA NOMINAL**] **-** Saber si la mostra, després de llegir les cookies, les accepta o no. Saber quanta gent llegeix totes les cookies.

IV. Problemàtiques

10. **Saps què és el *phishing*?**

[**QUALITATIVA ORDINAL**] **-** Saber quins coneixements té la mostra sobre les problemàtiques que hi ha a Internet relacionades amb la seguretat.

11. **Has patit, o coneixes a algú que hagi patit algun (intent de) hackeig/suplantació/estafa aquest darrer any?**

[**QUALITATIVA DICOTÒMICA**] **-** Conèixer que tan conscient és la mostra sobre els casos d'estafes relacionades amb internet i XXSS. Saber que tant propers són aquests casos de la nostra mostra.

V. Valoració personal

12. De l'1 al 10, quant consideres d'important la seguretat a les xarxes?

[**QUANTITATIVA DISCRETA**] - Saber si la mostra és conscient de la importància de protegir-se a les xarxes i el que comporta.

13. Valora de l'1 al 10 el teu nivell de prevenció a les xarxes.

[**QUANTITATIVA DISCRETA**] - Saber quina opinió tenen sobre la seva pròpia prevenció per així comparar els seus resultats amb les recomanacions dels experts.

---

b. MÈTODE D'ANÀLISI

Un cop recopilades les respostes i definides les variables, es creuaran entre elles per tal de determinar el següent:

1. [VARIABLES 2-3]

Coneixement i percepció sobre com ha de ser una contrasenya segura respecte al rang de dígits que utilitzen en les seves.

2. [VARIABLES 4-5]

Nivell de privacitat que tenen a les xarxes socials i si, tot i així, accepten com a seguidors a persones desconegudes.

3. [VARIABLES 6-7]

Importància que li donen a les Polítiques de Privadesa, tot i si respecten el compliment de la seva responsabilitat en llegir-se'les.

4. [VARIABLES 10-11]

Coneixement de les problemàtiques que existeixen a Internet respecte als casos que poden haver viscut de prop.

5. [VARIABLES 12-13]

Nivell d'importància que li donen a la seguretat a les xarxes comparat amb la pròpia percepció del seu nivell de prevenció.

6. [VARIABLES 1-5-8-9-13]

Sentiment de pròpia seguretat en comparació a la prevenció real extreta de les diferents respostes de l'enquesta.

3. RECOLLIDA i ANÀLISI DE DADES

3.1. RECOPILACIÓ I TRACTAMENT DE RESPOSTES

Després de rebre les 67 respostes necessàries, els resultats són els següents:

1.	Utilitzes sempre la mateixa contrasenya?
Sí	29
No	38

2.	Quants digits/caràcters té la teva contrasenya?
Entre 1 i 5	9
Entre 6 i 11	37
Entre 12 i 15	21
Més de 15	3

3.	Creus que la teva contrasenya compleix els requisits mínims, i per tant, és segura?
Sí	49
No	18

4.	Les teves xarxes socials són públiques o privades?
Públiques	17
Privades	50

5.	Coneixes personalment a tota la gent que et segueix a les xarxes?
Sí	21
No	46

6.	Acostumes a llegir les Polítiques de Privadesa de les apps i XXSS?
Sempre	3
De vegades	19
Mai les he llegit	45

7.	Creus que és important llegir-les? Valora-ho de l'1 al 10.
1	4
2	4
3	7
4	10
5	14
6	8
7	6
8	7
9	2
10	5

8.	Tapes la càmera dels teus dispositius?
Sí	5
No	36
En alguns casos, però no tots	26

9.	Quan ingresses en un lloc web, acostumes a acceptar TOTES les cookies?
Sí, però no me les llegeixo	39
Sí, i me les llegeixo	5
No, només les necessàries	23

10.	Saps què és el *phishing*?
Sí, sé el que és	19
Em sona el nom, però no sé ben bé el que és	18
No, no he escoltat mai aquesta paraula	30

11.	Has patit, o coneixes a algú que hagi patit algun (intent de) hackeig/suplantació/estafa aquest darrer any?
Sí	41
No	26

12.	De l'1 al 10, quant consideres d'important la seguretat a les xarxes?
1	1
2	-
3	2
4	1
5	3
6	8
7	7
8	6
9	15
10	24

13.	Valora de l'1 al 10 el teu nivell de prevenció a les xarxes.
1	3
2	4
3	3
4	6
5	9
6	15
7	14
8	6
9	3
10	4

3.2. ANÀLISI DE LES DADES

a. ANÀLISI Nº1 (variables 2 i 3)

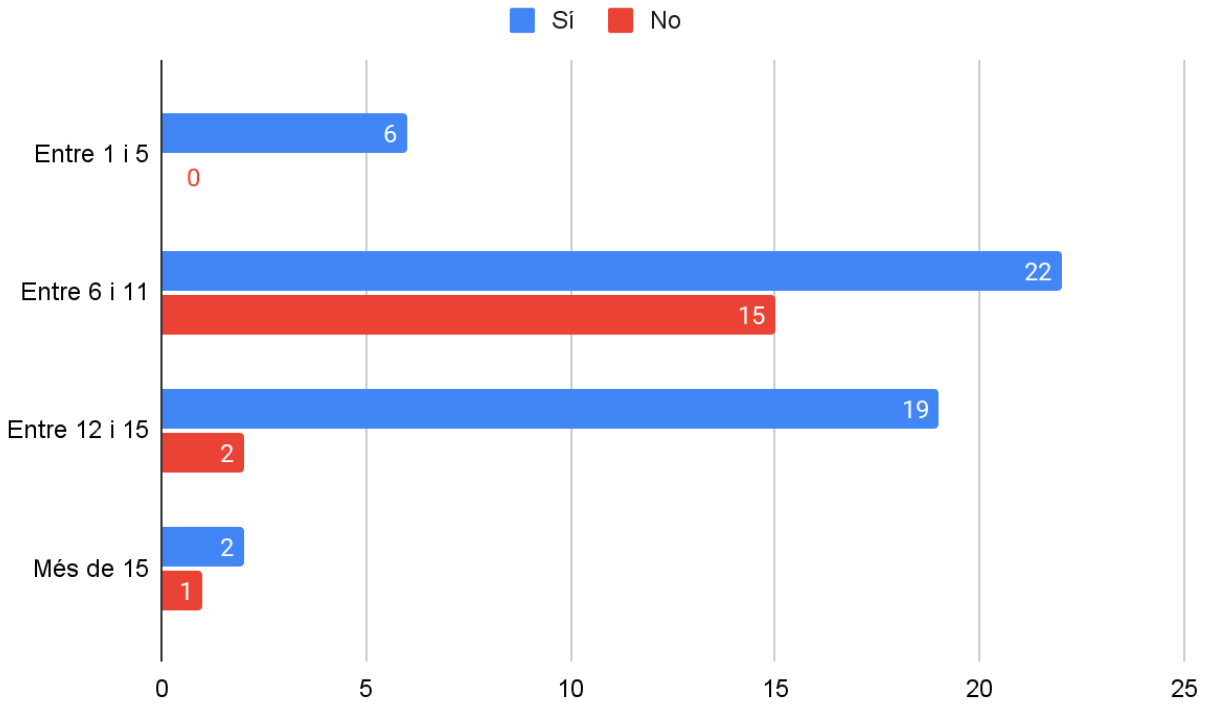
Es pretén determinar el coneixement i percepció sobre com ha de ser una contrasenya segura respecte al rang de dígits que utilitzen els alumnes en les seves.

- Variables en ús:

2/ Rang de dígits de la contrasenya.
3/ Percepció de si és segura o no.

Taula de contingència nº1

2\3	Sí	No	TOTAL
Entre 1 i 5	6	-	6
Entre 6 i 11	22	15	37
Entre 12 i 15	19	2	21
Més de 15	2	1	3
TOTAL	49	18	67



Gràfic nº1 *- Representació de la percepció d'una contrasenya segura en cada rang de dígits*

Els resultats de l'enquesta mostren que un 73% de la mostra creu que la seva contrasenya és segura. Mentre que només un 36% tenen una contrasenya segura segons les recomanacions dels experts, o sigui, que estiguin formades per, com a mínim, 12 caràcters, el que demostra que, en aquest cas, la realitat està força lluny del que les persones creuen.

D'altra banda, més de la meitat de les contrasenyes dels enquestats, un 55%, tenen només entre 6 i 11 dígits i, per tant, estan catalogades com a contrasenyes no segures, tot i que un 60% d'aquests es pensen que la contrasenya que utilitzen sí que és segura.

En definitiva, el 87% de persones que fan servir contrasenyes segures és conscient de la seguretat de la seva contrasenya, el que representa un 22% més que la gent sense contrasenya segura, dels quals el 65% creu que si que utilitza una contrasenya amb certa seguretat.

---

b. ANÀLISI Nº2 (variables 4 i 5)

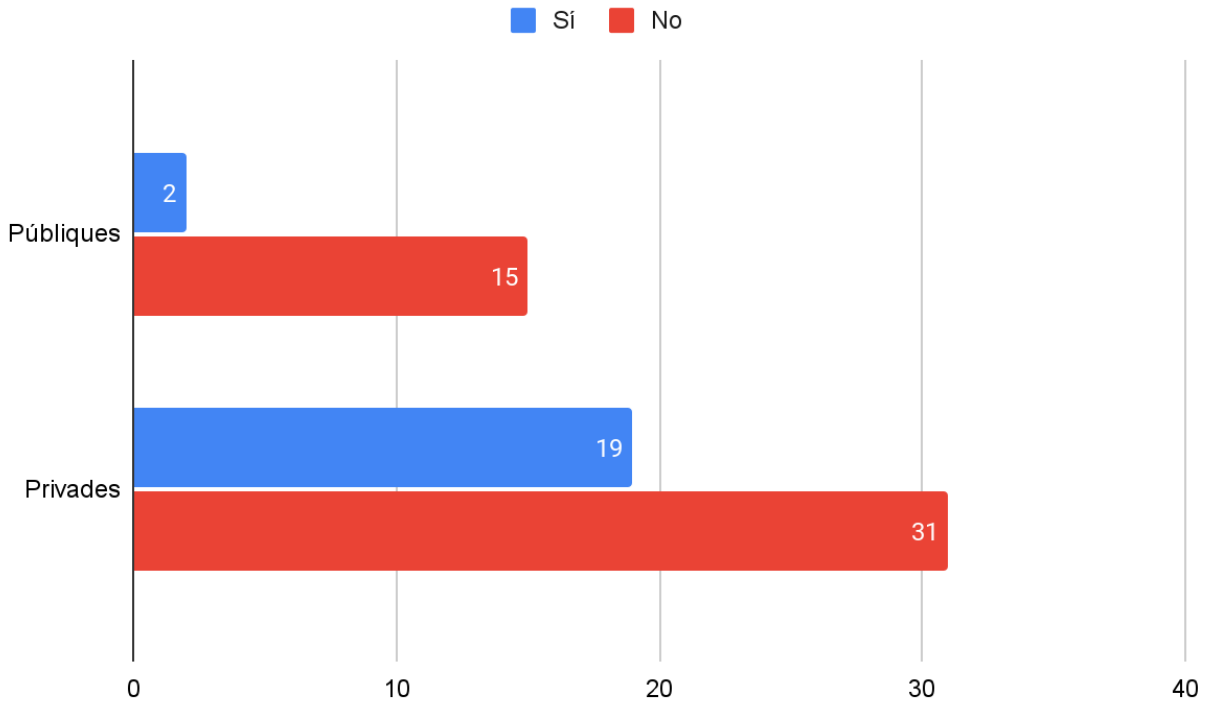
Es pretén determinar el nivell de privacitat que tenen a les xarxes socials i si, tot i així, accepten com a seguidors a persones desconegudes.

- Variables en ús:

4/ Tipus de privacitat a les xarxes.
5/ Si coneixen o no a tots els seus seguidors.

Taula de contingència nº2

4\5	Sí	No	**TOTAL**
Públiques	2	15	17
Privades	19	31	50
TOTAL	21	46	67



Gràfic nº2 - *Representació del coneixement dels seguidors segons la privacitat dels comptes*

Tot i que el gràfic de barres mostra clarament que els alumnes de 1r de Batxillerat del Campeny tenen, en un 75% dels casos, les xarxes socials configurades com a privades, realment només un 38% de les persones amb aquesta configuració afirma conèixer personalment a tots els seus seguidors, el que indica que l'altre 62% té un nivell de privadesa baix tot i tenir el compte privat.
En resum, el 69% de la mostra no coneix a la totalitat dels seus seguidors de xarxes socials.

De les persones amb xarxes socials públiques, només un 12% coneix a tota la gent que segueix el seu compte, tot i que, si un compte és públic, qualsevol persona té accés al contingut que publiques, sigui seguidor o no. Per tant la informació de les xarxes socials d'aquestes persones està exposada també a gent que no coneixen.

---

c. ANÀLISI Nº3 (variables 6 i 7)

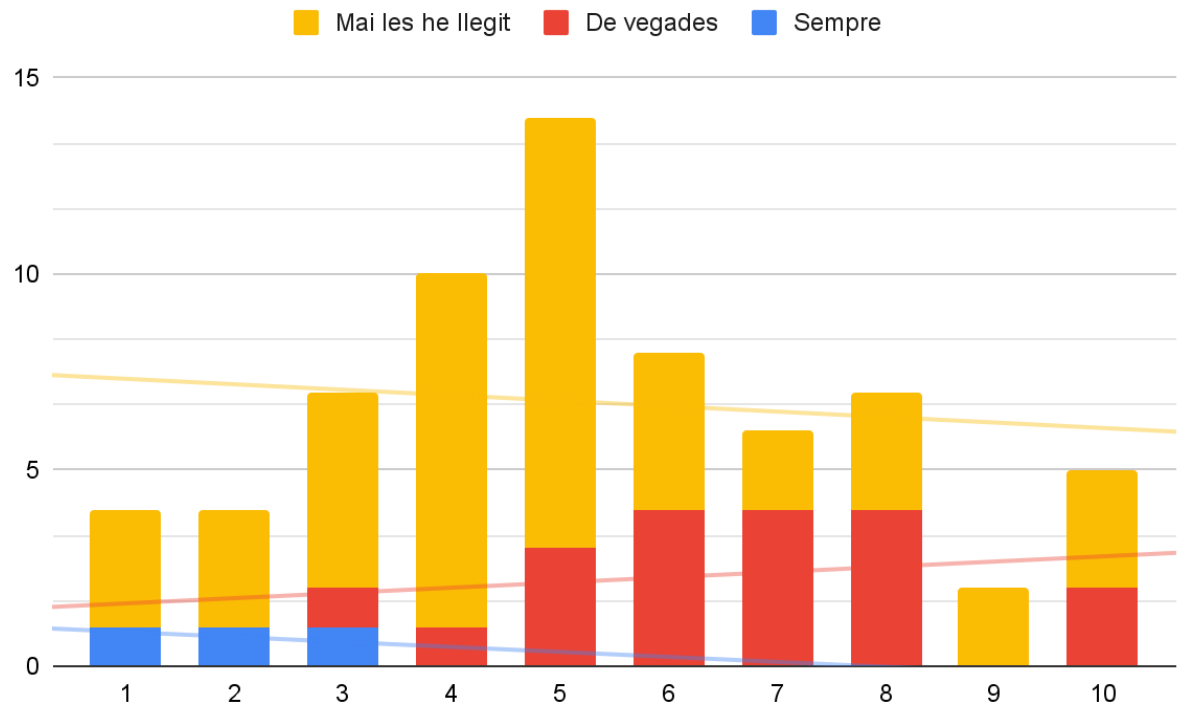
Es pretén determinar la importància que li donen a les Polítiques de Privadesa, tot i si respecten el compliment de la seva responsabilitat en llegir-se'les.

- Variables en ús:

6/ Si llegeixen o no les Polítiques de Privadesa.
7/ Importància de llegir-les (*de l'1 al 10).*

Taula de contingència nº3

7\6	Sempre	De vegades	Mai les he llegit	TOTAL
1	1	-	3	4
2	1	-	3	4
3	1	1	5	7
4	-	1	9	10
5	-	3	11	15
6	-	4	4	8
7	-	4	2	6
8	-	4	3	7
9	-	-	2	2
10	-	2	3	5
TOTAL	3	19	45	67



Gràfic nº3 *- Representació del costum de llegir les polítiques de privadesa respecte la importància*

El gràfic de columnes ens mostra que la importància que creuen que tenen les polítiques de privadesa no concorda amb la importància que els hi donen (si les llegeixen o no). Per tant, es dedueix que moltes persones, tot i que creuen que realment és important llegir-les, no ho fan.

Un 67% de la mostra mai llegeix les polítiques de privadesa de les xarxes socials que utilitza. Convé ressaltar que, tot i així, un 44% d'aquests valora la importància de llegir-les en un 4-5 sobre 10. A més a més, la quantitat d'individus que valoren amb un 10 la importància de llegir-les representa només un 7% del total, resultat major a la quantitat de gent que afirma llegir-les sempre, que encara és més petit, amb un 4,5%.

La valoració de la importància recau, en la seva majoria, sobre el 5, tant per la moda com per la mitjana aritmètica. A més a més, la tendència de les persones que mai se les han llegit es redueix quan més gran és el número de la valoració, mentre que la de les persones que se les llegeixen de vegades augmenta.

---

d. ANÀLISI Nº4 (variables 10 i 11)

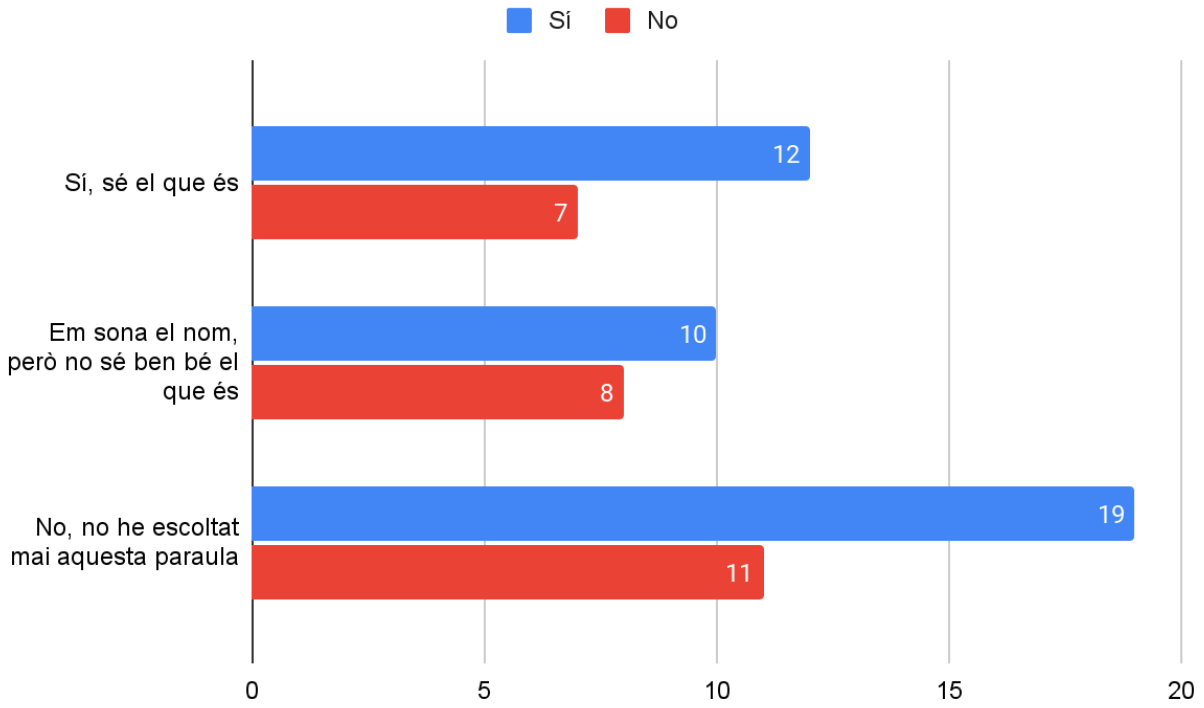
Es pretén determinar el coneixement de les problemàtiques que existeixen a Internet respecte als casos que poden haver viscut de prop.

- Variables en ús:

10/ Si saben què és el *phishing.*
11/ Si han patit o coneixen a algú que hagi patit algun (intent de) hackeig/suplantació/estafa el darrer any.

Taula de contingència nº4

10\11	Sí	No	**TOTAL**
Sí, sé el que és	12	7	19
Em sona el nom, però no sé ben bé el que és	10	8	18
No, no he escoltat mai aquesta paraula	19	11	30
TOTAL	41	26	67



Gràfic nº4 - *Representació del coneixement sobre el phishing respecte a casos propers*

Del total la mostra, un 45% no ha escoltat mai la paraula *phishing*, acompanyat d'un 27%, que no saben ben bé què és, el que demostra que, en conjunt, un 72% no sap què és exactament. D'altra banda, un 53% d'alumnes ha patit o coneixen a algú que ha patit un intent de hackeig/suplantació/estafa a través d'internet els darrers anys.

Si més no, el gràfic mostra una possible relació entre la manca d'informació sobre aquests fets i la gran quantitat de casos que succeeixen cada any, tenint en compte que només un 28% afirma saber què és el *phishing*, dada sorprenent tenint en compte la gran quantitat de casos d'intents de estafes online propers a la nostre mostra.

---

e. <u>ANÀLISI Nº5 (variables 12 i 13)</u>

Es pretén determinar el nivell d'importància que li donen a la seguretat a les xarxes comparat amb la pròpia percepció del seu nivell de prevenció.

- Variables en ús:

12/ Importància que li donen a la seguretat a les xarxes *(de l'1 al 10)*.
13/ Valoració del nivell de prevenció a les xarxes *(de l'1 al 10).*

Taula de contingència nº5

12\13	1	2	3	4	5	6	7	8	9	10	T
1	1	-	-	-	-	-	-	-	-	-	1
2	-	-	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	1	-	-	1	2
4	-	-	-	-	-	1	-	-	-	-	1
5	1	-	-	-	-	1	1	-	-	-	3
6	-	-	1	1	-	5	-	1	-	-	8
7	-	-	1	3	1	1	1	-	-	-	7
8	-	-	-	-	1	2	2	-	1	-	6
9	-	4	-	-	6	1	2	2	-	-	15
10	1	-	1	2	1	4	7	3	2	3	24
T	3	4	3	6	9	15	14	6	3	4	67

Tenint en compte que un 36% dels alumnes del Campeny que cursen 1r de batxillerat valora en un 10/10 la importància de la seguretat en les xarxes socials, i un 22% en un 9/10, això representa que un 58% de la mostra valora la seguretat a les xarxes en un 9-10 sobre 10.

A més a més, només un 6% de la mostra valora el seu nivell de prevenció en un 10 i, no més d'un 4% valora el seu nivell de prevenció en un 9. En altres paraules, tot i que els alumnes són conscients dels perills que comporta i la importància que suposa la seguretat a les xarxes, no prenen mesures corresponents.

Realment són molt poques les persones que pensen que la seguretat a les xarxes no té cap o té poca importància. Malgrat aquest fet, el seu nivell de prevenció, en gairebé tots els casos, és menor a la importància que creuen que té.

f. ANÀLISI Nº6 (variables 1, 5, 8, 9 i 13)

Es pretén determinar el sentiment de pròpia seguretat en comparació a la prevenció real extreta de les diferents respostes de l'enquesta.

- Variables en ús:

1/ Si utilitzen sempre la mateixa contrasenya.
5/ Coneixement personal dels seus seguidors.
8/ Si tapen o no la càmera dels seus dispositius.
9/ Quan ingresses en un lloc web, acostumes a acceptar TOTES les *cookies*?
13/ Valora de l'1 al 10 el teu nivell de prevenció a les xarxes.

f.1. CÀLCUL DE LA PREVENCIÓ REAL DELS ENQUESTATS:

En aquest cas, com del que es tracta és de determinar un nivell de prevenció resultat de les seves respostes per tal de comparar-lo amb la seva percepció, s'ha realitzat el recompte de persones (N) segons el nivell de prevenció que creuen que tenen (variable 13) i s'ha afegit a la taula la freqüència d'individus (f_{nm}) que compleixen les recomanacions dels experts (variables 1, 5, 8 i 9).

Les respostes vàlides que s'han recomptat són les següents:

[variable 1] - "*No.*" [variable 8] - *"Sí."* o *"En alguns casos."*

[variable 5] - *"Sí."* [variable 9] - *"No, només les necessàries."*

Un cop enregistrades les freqüències, s'han sumat i multiplicat per 2,5 $(10 \div 4$ variables diferents) i, finalment, s'ha dividit entre el nombre total de persones (N), donant com a resultat una nota aproximada. Aquesta ha estat la fórmula utilitzada:

$$\text{NOTA}_{\text{aproximada}} = \left(\sum_{i=1}^{n} f_{im} \cdot \ (10 \div nº\ variables) \right) \div N$$

Taula de contingència nº6

N	13\1-5-8-9	Contrasenya	Seguidors	Càmera	Cookies	NOTA
3	1	-	2	-	-	2
4	2	4	-	-	-	3
3	3	-	1	1	-	2
6	4	5	1	2	2	3
9	5	2	2	6	2	3
15	6	5	3	6	5	3
14	7	12	4	8	7	6
6	8	4	3	4	4	6
3	9	2	2	3	2	8
4	10	4	3	1	1	7
TOTAL		38	21	31	23	

La taula de contingència mostra amb claredat la diferència entre el nivell de prevenció a les xarxes que creuen que tenen amb la seva prevenció aproximada extreta de les respostes. Exceptuant la gent que creu que la seva prevenció en quan a seguretat a les xarxes és entre un 1-2 sobre 10, la resta de la mostra valora la seva seguretat a les xarxes considerablement per sobre de la seva prevenció real.

El coneixement personal dels seguidors i les cookies de les pàgines web són els àmbits amb menys prevenció de l'enquesta, i tot i que la contrasenya és l'àmbit amb la que els alumnes tenen més prevenció, segueix sense ser suficient envers la importància que implica (com es mostra al 1r anàlisi de les variables 2 i 3).

Els resultats d'aquesta taula de contingència fan encara més impactant el preocupant resultat del 5è anàlisi, ja que la taula mostra com els alumnes de 1r de batxillerat creuen que la seva prevenció a les xarxes socials és major del que realment és.

4. CONCLUSIONS

Després d'analitzar totes les dades, aquestes són les conclusions que s'han extret:

Primer de tot, i en relació a les contrasenyes, és força preocupant que més de dues terceres parts dels alumnes pensi que té una contrasenya segura mentre que realment només un terç compleix els requisits mínims recomanats pels experts. Això fa pensar que, ja sigui per por a oblidar-la o per mandra d'haver d'escriure una contrasenya llarga, els alumnes acostumen a escriure de més curtes, tot i pensant que són suficientment segures.

Relacionat amb les xarxes socials, àmbit més freqüent d'entre els joves, s'ha pogut comprovar la creació d'una certa bombolla de seguretat en més de la meitat dels alumnes que els fa pensar que estan segurs amb comptes privats mentre que, per contra, estan acceptant com a seguidors del contingut personal que pengen a persones completament desconegudes personalment, i que això pot suposar que algunes d'aquestes siguin assetjadors o ciberdelincuents.
D'altra banda, causa preocupació pensar que pràcticament la totalitat dels alumnes no es llegeixen sempre les Polítiques de Privadesa de les apps i xarxes socials que utilitzen, el que implica que estan acceptant un contracte de com es tractaran les seves dades personals sense saber que faran amb elles o amb qui o a qui les compartiran o vendran. Si bé és cert que les empreses acostumen a crear documents llargs i difícils de llegir per tal de que els obviem, cal fer un esforç per complir amb la nostra responsabilitat i adonar-nos de que estem acceptant.

El desconeixement sobre quines problemàtiques existeixen a Internet, un entorn que utilitzem tant sovint, ens fa susceptibles a poder sofrir més delictes. En aquest cas, unes dues terceres parts dels alumnes no tenen el coneixement de què és un problema tan conegut com el *phishing*, el qual més de la meitat d'ells han viscut de prop però que no en són conscients.
També cal esmentar les incoherències dels alumnes, que mentre la gran majoria creu que saber protegir-se a Internet és important, es valoren amb una prevenció molt baixa, a més a més de que, tal i com s'ha comprovat a l'estudi, està molt allunyada per sota de la realitat.

Si més no, amb això podem determinar que la desinformació és el factor causant de tots els riscos als que els alumnes estan sotmesos, i part de la responsabilitat ha d'estar en mans del sistema educatiu, sobretot quan es parla d'un tema tant important com aquest.

És evident que la digitalització ja és una realitat. Cada cop està més present en àmbits com l'educació, el que implica que els alumnes de les noves generacions fonamentin part del seu aprenentatge en nous mètodes i eines que els preparin per al futur que els espera. Tot i així, i després de concloure aquest estudi, es pot afirmar que malgrat s'imposa aquest nou model digital, no s'està ensenyant a conviure de manera segura i responsable.

5. WEBGRAFIA

Altres fonts consultades:

- https://www.uv.mx/infosegura/general/consejo_contrasenas/
- https://www.xataka.com/seguridad/trucos-para-crear-recordar-buena-contrasena
- https://www.cordoba.gob.ar/10-recomendaciones-para-garantizar-tu-seguridad-en-redes-sociales/
- https://www.aquasocialmedia.com/blog-dynamic/91-que-es-y-para-que-sirve-la-politica-de-privacidad
- https://leader-network.com/actualidad/10-consejos-de-seguridad-para-dispositivos-moviles/
- https://www.xataka.com/privacidad/tapar-o-no-tapar-la-webcam-esa-es-la-cuestion
- https://cso.computerworld.es/tendencias/los-delitos-informaticos-crecieron-un-61-en-espana-en-2021
- https://latam.kaspersky.com/resource-center/definitions/what-is-internet-security