Finestra del Cau

Fitxa d'activitats

Finestra del Cau	Seguretat digital al cau: una responsabilitat i una oportunitat educativa
Nom de l'activitat	L'empremta dolenta
Durada	1 hora
Etapa educativa	Raiers, Pioners i Clan
Nombre de participants	Variable; amb tota la unitat

Objectius

1. Aprendre sobre l'empremta digital i les dades que hem fet públiques.
2. Reduir l'empremta digital amb l'ajuda de les companyes

Material necessari

- Dispositius amb accés a internet
- Fulls
- Bolígrafs
- Targetes amb els títols dels ciberconsells

Desenvolupament

La identitat és un dret fonamental, així ho diu la Declaració dels Drets Humans (Article 6). Aquesta identitat ens permet ser reconegudes oficialment com a membres de ple dret de la societat i ens dona accés a serveis i proteccions essencials. Aquesta identitat és determinada per una sèrie de dades personals que fan una combinació única. Entre aquestes tenim el nostre nom complet, el DNI, i altres dades identitàries físiques, genètiques, psíquiques, econòmiques, etc.

A part, hi ha algunes dades personals que poden ser delicades, ja que el seu tractament té un especial impacte en els drets i llibertats fonamentals del seu titular. Aquestes poden ser dades genètiques, biomètriques, relatives a la salut, relatives a la vida sexual o orientació sexual, a l'origen ètnic o racial i altres dades que revelin opinions polítiques, conviccions religioses o afiliacions sindicals.

És molt probable que, fent ús de dispositius amb accés a internet, hàgiu compartit de forma pública alguna d'aquestes dades o que, tot i guardar-les en un espai digital privat, s'hagin filtrat per culpa de l'empresa o programari que les gestionava.
És per això que començarem fent una anàlisi de quantes dades personals de les quals no teníeu consciència trobeu a Internet (tant el vostre nom complet, com una fotografia on es vegi la vostra cara, o que el vostre correu electrònic s'hagi filtrat sense el vostre coneixement).

Individualment, seguirem les següents passes i apuntarem què ens sorprèn veure:

1. Busca el teu nom complet a Google (o el buscador que facis servir) i apunta quantes vegades has vist informació personal que hauria de ser privada.
2. Busca les teves adreces de correu electrònic a haveibeenpwned.com i apunta quantes filtracions de dades has patit.
3. Ves al teu Gmail (si en tens) i, a l'esquerra sota la paperera, mira la part de "Gestionar subscripcions" i apunta quants correus t'han enviat 10 o més correus recentment.

Un cop acabat, ens reunim en gran grup i cadascú comparteix (si vol i se sent còmode fent-ho) el número de vegades que ha vist infraccions de seguretat en les seves dades i el que més els hagi sorprès de tot el que han vist.

Pot ser que el nombre de filtracions vistes sigui alt, però no està tot perdut. Sempre hi ha maneres de reduir l'empremta digital que tenim.

Us proposem una llista de "ciberconsells" bons i una altra de dolents (encara que alguns ens puguin semblar bons). Anirem donant-los al grup i els hauran de classificar entre bons i dolents.

Bons consells

- **Activa el Doble Factor d'Autenticació (2FA):** És el més important. Encara que et robin la contrasenya, necessitaran un codi al teu mòbil per entrar.

- **Fes servir un gestor de contrasenyes:** No intentis recordar-les totes. Utilitza eines com Bitwarden o 1Password per tenir contrasenyes llargues i úniques per a cada lloc.

- **Actualitza sempre el programari:** Les actualitzacions del mòbil i l'ordinador no són només per estètica; tapen forats de seguretat que els hackers aprofiten.

- **Desconfia per defecte (Phishing o pesca de dades):** Si reps un SMS o correu del teu banc, de Correus o d'una xarxa social amb un enllaç "urgent", no cliquis. Entra tu directament des de l'app o la web oficial.

- **Tanca sessions en dispositius aliens:** Si t'has connectat a l'ordinador d'un hotel o d'un amic, recorda tancar la sessió i, si pots, utilitza el mode incògnit.

- **Talla el rastre de la ubicació:** Revisa quines aplicacions tenen permís per saber on ets en tot moment. Moltes apps (com la llanterna o jocs simples) no ho necessiten per funcionar i venen aquesta dada a tercers.

- **Fes servir "Inicia la sessió amb Apple/Google":** Si no vols crear un compte nou a cada web, aquests sistemes són més segurs perquè no comparteixen la teva contrasenya real amb la web externa. A més, Apple permet "ocultar el meu correu" creant-ne un d'aleatori.

- **Vigila amb el Wi-Fi públic:** Si t'has de connectar al Wi-Fi de l'aeroport o d'una cafeteria, evita entrar al banc o fer compres. Si ho has de fer costi el que costi, fes servir una VPN (Xarxa Privada Virtual) per xifrar les dades.

- **Neteja d'aplicacions "zombis":** Un cop al mes, esborra les apps que no facis servir. Cada app instal·lada és una possible porta d'entrada per a vulnerabilitats si l'empresa deixa d'actualitzar-la.

- **Protegeix físicament els teus dispositius:** Sembla obvi, però posa un codi de bloqueig o empremta al mòbil. Si te'l roben i no té bloqueig, tota la teva empremta digital (fotos, mails, comptes) estarà oberta de bat a bat.

Consells “dolents” o mites

CANVIA LA CONTRASENYA CADA MES

- Creure que així ets més segur.
- Obligar-te a canviar-la sovint fa que acabis posant variants fàcils (com Contrasenya2024 i Contrasenya2025). És millor una contrasenya molt robusta i no canviar-la mai si no hi ha una sospita real de robatori.

ACTIVA EL MODE INCÒGNIT PERQUÈ NO SÀPIGUEN QUÈ VISITES

- Confiar cegament en qualsevol web amb el cadenat.
- El cadenat només diu que la connexió està xifrada, però una web estafa també pot tenir cadenat. Pots estar enviant les teves dades de forma "segura"... directament a un lladre.

NO NECESSITO SEGURETAT PERQUÈ NO SOC NINGÚ IMPORTANT

- Pensar que els hackers només busquen famosos o rics.
- Els atacs són massius i automatitzats. El teu compte de correu o d'Instagram té valor per enviar correu brossa (spam), cometre estafes als teus contactes o segrestar els teus arxius (Ransomware).

L'ANTIVIRUS ÉS UNA EINA QUE PROTEGEIX DE TOTS ELS VIRUS I PROGRAMARI MALICIÓS

- Relaxar-se perquè tens un programa instal·lat.
- El millor antivirus és el teu sentit comú. Cap programa et protegirà si tu mateix dones les claus a un estafador per telèfon.

POSA'T EL PERFIL D'INSTAGRAM EN PRIVAT PER AMAGAR-TE COMPLETAMENT

- Creure que posar el cadenat al perfil et fa invisible i que el que publiques ja és 100% privat.
- Encara que els desconeguts no vegin les teves fotos, Meta (l'empresa de Facebook) continua recollint tota la teva activitat. A més, si un seguidor teu fa una captura de pantalla, la teva "privacitat" desapareix a l'instant.

HE D'ACCEPTAR TOTES LES GALETES (COOKIES) PER PODER LLEGIR LA WEB

- Pensar que si no ho fas no carregarà o et perdràs contingut.
- Des de fa poc, la llei obliga que el botó de "Rebutjar totes" sigui tan visible com el d'acceptar. No triguis ni dos segons més a clicar "Rebutjar"; la web funcionarà igual de bé i no et rastrejaran tant per posar-te publicitat.

PER ESBORRAR UN FITXER COMPLETAMENT, L'HAS D'ESBORRAR DE L'ORDINADOR I DESPRÉS BUIDAR LA PAPERERA DE RECICLATGE

Creure que quan la paperera és buida, la informació ha desaparegut físicament del disc dur.

En informàtica, "esborrar" sovint només vol dir "deixar aquest espai lliure per a una altra cosa". Amb programari especialitzat es poden recuperar fitxers esborrats fa mesos si l'espai no s'ha sobreescrit. Si vols vendre un ordinador vell, has de fer un "esborrat segur" o una formatació del dispositiu.

ELS MAC I ELS IPHONES NO TENEN VIRUS

Pensar que pel sol fet de tenir aquests dispositius ets immune a qualsevol atac.

Aquest és un mite perillosíssim dels anys 2000. És cert que n'hi ha menys que a Windows o Android, però actualment existeix programari maliciós (malware) dissenyat específicament per a productes d'Apple. Ningú és immune.

TAPAR LA WEBCAM AMB UN ADHESIU ET PROTEGEIX DE TOT

Creure que si no et veuen, el hacker no pot fer res més.

Et protegeix que et vegin la cara, sí, però si un hacker entra al teu ordinador, pot continuar escoltant pel micròfon, veure el que escrius al teclat o robar els teus fitxers. Tapar la càmera és una mesura física bona, però no substitueix la seguretat digital.

Un cop acabin la classificació, parlarem de cadascun dels consells i perquè és bo o dolent. Si volem aprofundir una mica més, l'Agència Catalana de Ciberseguretat té un joc web interactiu amb més preguntes.
Per últim, dividirem el grup en parelles o petits grups i aquests s'ajudaran mútuament a reduir l'empremta digital individual que tenen amb l'ajuda dels "ciberconsells".