ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

AGÈNCIA NACIONAL DE CIBERSEGURETAT D'ANDORRA

CONSCIENCIACIÓ EN CIBERSEGURETAT

ELS PERILLS DE LES XXSS PER A MENORS I ADOLESCENTS

Agost 2024
Document d'ús públic

1. INTRODUCCIÓ I CONTEXT

Les xarxes socials formen part de la vida moderna. A través de les xarxes socials parlem amb els nostres amics, parlem de feina, presumim de noves adquisicions, publiquem fotos, guanyem diners, invertim, comprem tecnologia, enviem arxius, mirem pel·lícules, etc. Dit d'una altra manera, tot ho podem fer a través de les xarxes socials.

Facebook, Instagram, TikTok i **Twitter** estan plens de vida, malgrat que la vida que reflecteixen no és del tot real, ja que aquestes plataformes creen un **ecosistema separat de la nostra vida real** i tenen les seves pròpies normes de conducta, lleis, negocis i principis de la comunicació. I a més a més, com a resultat de tot això, tenen els seus propis **delictes**.

Els ciberdelinqüents utilitzen les xarxes socials per enganyar, robar, fer xantatge i obtenir informació, igual que es fa en la vida real. S'aprofiten de la nostra manca d'atenció a l'hora d'interactuar amb les xarxes socials.

Els perills a les xarxes socials són reals i afecten especialment els infants i els adolescents. Aquestes aplicacions van ser dissenyades per a adults, per la qual cosa cal prendre certes mesures per tal que els menors i els adolescents no posin en risc la seva privacitat, reputació i/o seguretat.

Per descomptat que els perills que expliquem a les següents diapositives no només afecten els infants i adolescents, sinó que també afecten els adults, però menys.

2. TIPUS DE PERILLS A LES XARXES SOCIALS

1. Fraus, pesca i programari maliciós

Aquests són els tres tipus de contingut maliciós i enganyós que pots trobar a les xarxes socials. Per exemple, **fer clic en un enllaç vinculat a un lloc web poc fiable**. En aquest aspecte, és clau saber com es pot prevenir el robatori de la teva identitat, ja que en això consisteixen els atacs de pesca: els ciberdelinqüents envien **missatges massius amb enllaços maliciosos** dissenyats amb l'objectiu de recollir la teva informació personal/confidencial, sense que en siguis conscient.

Per tant, l'objectiu dels ciberdelinqüents sol ser instal·lar **programari maliciós** als dispositius de tercers i bloquejar el seu accés a perfils, i robar informació privada. Per exemple, reps un missatge a la safata d'entrada de l'Instagram que anuncia un gran descompte en productes d'una marca coneguda. No obris mai aquesta publicació.

2. Danys en la reputació del menor: abusos i ciberassetjament escolar

Les xarxes socials són l'escenari idoni per als abusadors i els pedòfils. Les plataformes els donen l'**anonimat** que necessiten per contactar amb possibles víctimes, guanyar-se la seva confiança i manipular-les perquè comparteixin informació personal o vídeos de caràcter íntim.

Pel que fa al **ciberassetjament escolar**, pot ser que una persona anònima assetgi el menor mentre juga en línia, però en molts casos l'assetjament prové d'algú que coneix a la vida real. **El ciberassetjament és un tema que es tracta a les escoles i en els darrers anys s'han publicat protocols d'actuació per erradicar-lo.**

3. Contingut inapropiat per als menors

Molts menors consumeixen contingut que no és apropiat per a la seva edat. A vegades segueixen influenciadors que parlen de temes relacionats amb la **sexualitat** o la **violència** i que són continguts no adequats per a la seva edat.

Per això, et recomanem que facis servir **eines de control parental** per supervisar els comptes o els llocs web als quals accedeixen els menors. Els centres educatius també apliquen **protocols** que inclouen **programari de supervisió.**

4. Nivells de seguretat escassos

Si molts adults desconeixen la importància de la ciberseguretat i els trucs bàsics per protegir la seva identitat en línia, els menors encara en són menys conscients. Per aquest motiu, **el paper dels pares i dels educadors és essencial en aquests aspectes.**

També és imprescindible parlar dels perills i de les conseqüències negatives dels videojocs. No ens referim només a l'abús d'hores davant de la pantalla, sinó també als **atacs informàtics** que poden patir els menors.

5. Videojocs violents i xats perillosos

Els videojocs molt violents no són adequats per als infants. Per tant, cal que els pares comprovin que la temàtica sigui adequada per a l'edat dels fills.

Els youtubers i els influenciadors que s'han fet famosos gràcies a les seves habilitats com a *gamers* no sempre comparteixen contingut adequat per als més petits.

Hi ha casos en què aquests *gamers* han fet comentaris sexistes davant d'una audiència de milers o de milions de persones, entre les quals hi havia molts menors d'edat. Per aquest motiu, **és important supervisar quins són els perfils preferits dels menors i quins temes s'hi tracten.**

6. L'impacte negatiu de les xarxes socials en l'autoestima

L'adolescència és una època de canvis i de redefinició de la personalitat de la persona. A Instagram o a Facebook, per exemple, **les fotografies són perfectes i tots els usuaris joves saben fer servir a la perfecció els filtres.**

Aquest estat continu de buscar la perfecció i que tot sembli idíl·lic i perfecte afecta directament l'autoestima dels infants i dels adolescents.

7. L'incompliment de l'edat mínima

L'**edat mínima legal** establerta per poder usar les xarxes socials és: Twitter i Snapchat, 13 anys; Facebook, 14 anys; Instagram, 16 anys; LinkedIn i WhatsApp, 18 anys.

És obvi que aquestes normes no es compleixen actualment.

8. Recollida de dades i anuncis invasius

El desconeixement sobre la recopilació de dades dels usuaris a les xarxes socials és enorme. **Desconeixem què es fa amb la informació personal que els facilitem i que posteriorment serveix per crear-nos un perfil de consumidor digital.**

La publicitat digital basa gran part de les seves campanyes en aquest tipus de mètodes.

9. La poca importància que es dona al contingut publicat a les xarxes socials

L'**empremta digital** pot fer que perdis la feina. Cal anar amb compte amb les opinions polítiques o els comentaris que fem a les xarxes socials, en el futur poden repercutir-nos negativament. De fet, **es recomana que els menors comparteixin el mínim d'informació personal a les xarxes socials.**

Ara, a més, amb la **intel·ligència artificial** fins i tot es podria manipular un vídeo íntim d'una persona i fer-lo passar per teu. Aquest tipus d'accions poden arruïnar la reputació d'una persona de per vida.

10. Notícies falses: com s'informen els més joves

En especial després del confinament, les notícies falses (*fake news*) van passar a formar part de la nostra opinió pública.

És clau que verifiquem sempre les fonts d'informació, la metodologia emprada i qui firma la notícia en qüestió.

3. COM ES PODEN PREVENIR ELS PERILLS A LES XARXES SOCIALS?

Aquests són alguns **consells bàsics** per prevenir els perills derivats de l'ús de les xarxes socials:

✔ Utilitza **protocols de seguretat** d'última generació.

✔ Protegeix les contrasenyes de tota la família. Per fer-ho, utilitza un **gestor de contrasenyes** que desi totes les claus en un lloc segur.

✔ Navega per internet amb una **VPN activada** i així podràs encaminar el teu tràfic de dades en línia.

Avís Legal

Aquest document conté informació pública.

El seu objectiu és la conscienciació en ciberseguretat pels ciutadans, empreses i entitats d'Andorra.