Definició i explicació dels termes que s'utilitzen en el llenguatge d'Internet i de les xarxes socials



PENSA

Connectar-se a Internet és una acció que realitzem gairebé diàriament. Internet és en realitat un conjunt descentralitzat de xarxes de comunicació interconnectades, que funciona com una xarxa única d'abast mundial.

Les possibilitats que ofereix Internet per accedir a informació, per a l'entreteniment, la comunicació i fins i tot la compra de qualsevol producte són importants, però també tenen dificultats i desavantatges. Per això cal que coneguem quins avantatges ens ofereix aquest sistema de comunicació, com utilitzar-los i com evitar-ne els possibles perills.

SABIES QUE...

INTERNET

Si internet fos un país, seria el sisè més contaminant del món. La petjada ecològica d'aquest tràfic digital immens equival a un consum aproximat del 7% de l'electricitat mundial. Sigues responsable amb l'ús que en fas, no n'abusis pel bé del planeta i pel bé de la teva salut física i mental.

Hi ha molts serveis i protocols a Internet, a part del web: l'enviament de correu electrònic, la transmissió i consulta d'arxius, les converses en línia, la missatgeria instantània, la comunicació multimèdia o els jocs en línia.

ACCÉS I CONNEXIONS:

Són diversos els criteris per classificar les connexions a Internet, almenys tants com tipus de xarxes a les quals podem connectar el nostre equip. Aquestes diferències poden ser tan físiques com del tipus de tecnologia de la qual se serveixen.

a) **Línia telefònica**: Es necessita un mòdem, que converteix els senyals digitals de l'ordinador en impulsos de so que es transmeten per la línia telefònica. Aquest sistema de connexió va caure en desús.

b) **Línia digital**

- **RDSI**: Es tracta d'una línia telefònica, però digital (en comptes d'analògic).
- **ADSL**: L'ADSL (Asymmetric Digital Subscriber Line) és una tecnologia d'accés a Internet de banda ampla i és el tipus de connexió favorit de llars i empreses.

c) **Cable**: Des del punt de vista físic, la xarxa de fibra òptica precisa d'una infraestructura nova i costosa, això explica que encara avui no estigui disponible a tot arreu.

d) **Satèl·lit**: Aquest tipus de connexió continua sent utilitzada en aquells casos en què no hi ha més opcions, per exemple en vaixells, avions o en zones molt aïllades on no arriba cap altre tipus de xarxa o connexió a Internet.



e) **Xarxes sense fil**: Les xarxes sense fil o wireless difereixen de totes les connexions anteriors, i la més coneguda i utilitzada és la WI-FI.

WI-FI: És un mecanisme de connexió de dispositius electrònics sense fil. Lesxarxes Wi-Fi posseeixen una sèrie d'avantatges, entre els quals destaca lacomoditat.

Però, de la mateixa manera que la xarxa sense fil, la tecnologia Wi-Fi presenta els seus propis problemes intrínsecs. Alguns dels desavantatges són:

1. **Manca de seguretat**. Moltes d'aquestes xarxes es converteixen en xarxes obertes, no protegeixen la informació que hi circula.

2. **Menor velocitat** en comparació amb una connexió per cable, a causa de les interferències.

f) **Telefonia mòbil**: La connexió a Internet, dins de la tecnologia mòbil, utilitza diferents sistemes derivats del GSM (Global System Mobile).

INFORMACIÓ D'INTERÈS

Per a accedir a internet, hem de recórrer a proveïdors, és a dir, a companyies que creen una connexió directa i permanent i que ens ofereixen la possibilitat d'accés en contractar un compte a canvi d'un pagament per aquest servei. Convé, com en tots els contractes, llegir-ne atentament les condicions.

En què ens hem de fixar quan contractem una connexió a Internet:



Cobertura del lloc de la connexió: D’ofertes n'hi ha moltes, però és molt probable que, si no vivim en grans ciutats, no puguem accedir a totes.

Promocions i velocitat: el preu final, no sol coincidir amb el que s'anuncia, i moltes vegades tampoc la velocitat, assabenta-te'n bé abans de contractar el servei.

No et refiïs només de la publicitat i contracta només el que necessitis, a fi de tenir la possibilitat de contractar una velocitat més gran no és obligatori contractar-la.

Informa't si té cap clàusula de permanència

Servei tècnic: És recomanable que comprovis en la mesura del possible com funcionen els serveis d'atenció al client.

ASPECTES ÈTICS, LEGALS I DE SEGURETAT



Tots coneixem els avantatges de la xarxa Internet, però pel fet de ser una xarxa oberta i universal, està subjecta a diferents riscos relacionats amb el seu propi funcionament i amb l'ús que en fem. A Internet hem d'utilitzar la lògica i el sentit comú, com ho faríem en la vida real.

Igual que ocorre en les activitats que realitzem en el món físic, totes les funcionalitats d'Internet poden comportar algun risc, entre els quals podem destacar:

Relacionats amb el funcionament: Problemes d'accessibilitat, de connexió a determinades webs o serveis d'Internet, virus, spams, etc.

Relacionats amb la informació: Hi ha molta informació poc fiable ja que qualsevol pot pujar continguts a la xarxa.

Accés a informació inapropiada: Informació perillosa (violència, immoral o il·lícita) sobretot per al col·lectiu menor d'edat.

Relacionats amb la comunicació interpersonal: Bloqueig del correu electrònic, missatges brossa i ofensius, pèrdua d'intimitat personal i de tercers, accions il·legals com ara plagis, difamacions, amenaces, etc.

Relacionats amb activitats econòmiques: Compres induïdes, publicitat, despesa telefònica desorbitada, estafes, robatoris o descàrregues il·legals.

Relacionats amb les addiccions: Existeixen riscos relacionats amb l'abús de determinades pràctiques com el joc, les compres compulsives, l'addicció a entorns socials com xats, videojocs en línia...

El correu electrònic també pot causar molts problemes. Podem ser bombardejats per correu brossa (publicitat no sol·licitada), ser enganyats amb falses cadenes de solidaritat o diferents mètodes d'estafa, així com rebre virus que afectin el nostre ordinador. (Vegeu la fitxa «Correu electrònic»)

RECOMANACIONS

Tria un navegador segur: La majoria de les activitats que desenvolupem per Internet se centren en el nostre navegador.

Cal tenir en compte també el nivell de seguretat que aquest ens pot proporcionar.

Protegeix el teu equip: Instal·la un antivirus en el sistema operatiu,

Comprova la configuració dels teus perfils: És important revisar el grau de privacitat que has triat per al teu perfil a les xarxes socials en què participes.

Si navegues des d'un PC compartit, recorda tancar la sessió de tots els teus comptes de correu electrònic o pàgines en què estiguis registrat cada vegada que t'hi connectis. I, per descomptat, mai comparteixis les teves contrasenyes ni perfils. Si cal, canvia-les amb freqüència per evitar que algú pugui utilitzar-les.

Si comparteixes imatges o informació d'altres persones a través d'Internet, assegura't que les dades o fotografies no perjudiquin ni molestin el seu protagonista, ni estiguin envaint la seva privacitat o violant la seva intimitat.

No reenviïs cadenes: Mai reenviïs a tots els teus contactes les famoses cadenes, ja que sovint contenen virus, fins i tot quan procedeixen d'un contacte de confiança.

Recorda que Internet «no oblida» fàcilment la informació, expressions o imatges que tu o persones del teu entorn, empreses i pàgines de tot tipus, pengen a la xarxa sobre tu.

Només amics de veritat. Abans d'acceptar una petició d'amistat o d'agregar algú a qualsevol de les teves xarxes socials, pensa si de veritat el coneixes i si no hi ha cap inconvenient perquè accedeixi a les teves dades, al teu entorn i a la teva vida íntima.

No publiquis contingut personal: aquest és un dels grans errors que es cometen, sobretot a les xarxes socials.

Exposar massa les activitats diàries i la teva família és perillós. Un exemple de mal ús de lesxarxes socials pot ser consultat amb molta freqüència a Instagram.

Aquesta xarxa té una eina anomenada Stories. En ella, pots publicar imatges o vídeos 15 segons que mostren què estàs fent en aquell moment i queda a disposició dels usuaris de la xarxa durant 24 hores.

No comparteixis informació provinent d'altres persones: No has de divulgar imatges, missatges o testimonis de tercers sense que ells ho permetin. A més no has de compartir continguts que puguin denigrar la imatge de ningú.

No exposis la teva seguretat: Informacions com són les dades bancàries, la ubicació i les compres de béns no han de ser mai compartides a les xarxes socials.

No facis clic a tot el que vegis: Sabem que per realitzar diverses accions a Internet hem de seleccionar diversos enllaços, i això no és un problema. El veritable error està en accedir a tots els enllaços que es suggereixen, sense tan sols saber abans si són segurs. Tot i que moltes persones conegudes suggereixen que facis clic a certs vincles, no creguis tot el que llegeixes.

Protegeix les teves dades personals: abans d'acceptar o rebutjar la proposta d'utilització de les teves dades personals per a comunicacions comercials, pensa què suposarà per a tu l'allau d'informació de terceres empreses que rebràs.

XARXES SOCIALS

Una xarxa social és una pàgina web o aplicació que serveix com a eina de comunicació entre els usuaris que la fan servir. Principalment s'hi comparteix informació en format de text, imatges i vídeos, encara que en els darrers anys s'ha vist un gran augment del format en àudio

A Espanya hi ha 29 milions de persones que utilitzen de manera activa les seves xarxes socials segons l'estudi sobre l'ús d'aquestes plataformes a Espanya de The Social Media Family.

Les xarxes socials s'han convertit en una de les principals vies de comunicació i interacció dels joves. De vegades, a causa d'això, s'empobreixen les relacions socials del dia a dia, podríem dir que com a conseqüència de l'ús excessiu de les xarxes socials, les persones interaccionen menys en el dia a dia. (Per exemple: vas a un restaurant amb la família o els amics i comproves que cada persona està consultant el seu telèfon sense parlar entre ells).

Amb l'augment de l'ús de les xarxes socials han aparegut amenaces i riscos deguts al seu mal ús. Com a persones consumidores i usuàries de les xarxes socials hem d'adquirir hàbits per a un ús responsable de les xarxes. Hi ha aspectes que convé tenir molt clars: cal respectar totes les persones, no s'ha de publicar informació personal d'interès (localització, residència, la teva escola o institut, els teus futurs viatges, etc.).

En primer lloc, quan una persona decideix entrar a formar part d'una xarxa social, pot trobar-se amb **diverses situacions conflictives**:

a) Per poder accedir a la xarxa, cal acceptar les condicions d'ús de la pàgina i la seva política de privacitat. Aquesta informació no sempre és directament visible i cal descarregar-la per poder accedir-hi. No obstant això, és possible acceptar-la assenyalant la opció de «accepto» sense necessitat de llegir-la. Això és molt freqüent i pot suposar un risc ja que, en acceptar aquestes condicions, estem donant el nostre consentiment a l'administrador de la pàgina perquè disposi de les nostres dades i de les nostres imatges.

b) En molts formularis de registre es demanen excessives dades de caràcter personal, com, per exemple, les creences religioses, la ideologia política, l'orientació sexual, etc. Habitualment aquestes dades no es sol·liciten com a «imprescindibles», i NO hem de facilitar-les.

c) La persona usuària decideix qui pot accedir al seu perfil i veure les seves dades personals. Per seguretat, és necessari que només acceptis a les teves xarxes socials les persones que coneguis i siguin del teu entorn proper. Has d'utilitzar SEMPRE un perfil privat per relacionar-te en una xarxa social que només permeti als teus amics/seguidors/subscriptors veure la informació i les publicacions que fas.

Després d'entrar a formar part de la xarxa, ens podem trobar amb **noves situacions**:

a) Les persones usuàries de les xarxes socials utilitzen aquests espais per compartir informació: comentaris d'experiències personals, fotografies, vídeos... Moltes vegades tota aquesta informació pot ser excessiva. NO hem de facilitar dades personals que permetin la nostra localització ni obtenir informació sobre la nostra família, amics, escola, etc.

b) Molts motors de cerca indexen els continguts.

c) Un gran nombre de pàgines requereixen la instal·lació de cookies per poder funcionar. Aquests dispositius, instal·lats al disc dur de l'usuari, recullen informació sobre els llocs web que es visiten i poden obtenir informació sobre els gustos i les preferències de l'usuari per personalitzar el contingut de la seva pàgina per ajustar-s'hi, amb finalitats publicitàries cada vegada que s'hi accedeix.

d) Si, per exemple, decidim pujar una foto personal al nostre perfil en una xarxa social, és possible que aquesta foto deixi de pertànyer només a nosaltres i a partir d'aquest moment els drets siguin compartits amb l'entitat que l'allotja, que pot utilitzar-la per a diverses finalitats.

Després d'haver participat en una xarxa social, quan la persona usuària es planteja deixar de formar-ne part, pot sorgir una nova dificultat. El risc principal en aquest moment és la impossibilitat de dur a terme una baixa efectiva. Tot i que el perfil estigui tancat i no es pugui accedir-hi, les dades de registre segueixen estant a disposició dels responsables de la xarxa social. La persona interessada ha de saber que té dret a obtenir, sense dilació per part del responsable del tractament, la supressió de les dades personals que li concerneixin.

Una de les principals preocupacions que també sorgeixen respecte a l'ús que els menors fan de les xarxes socials, és la possibilitat que siguin víctimes d'algun tipus d'assetjament. Actualment, quan parlem d'assetjament a través de la xarxa, en funció dels protagonistes de la situació, podem diferenciar dos tipus d'assetjament: cyberbullying i grooming.

El **cyberbullying**, o assetjament escolar a través d'Internet, és un problema que es produeix entre iguals o, de vegades, d'alumnes cap a professors.

Els grups de WhatsApp s'empren en moltes ocasions com a mitjà per a insultar i desvaloritzar un dels membres. Sempre ha existit el bullying als centres escolars, però no haver de donar la cara per desvaloritzar i fer patir una persona és molt més senzill.

El **grooming**, o assetjament sexual a través d'Internet, ve donat per part d'un adult, que actua contra una persona menor amb finalitat sexual. La facilitat i la immediatesa amb la qual, actualment, es comparteixen imatges del dia a dia, pot ser un punt molt important que cal tenir en compte en aquest tema.

Cap dels dos problemes no és nou ni ha sorgit amb les xarxes socials, però l'anonimat, la rapidesa i la sensació d'immunitat que proporcionen les comunicacions a través de les xarxes socials, han contribuït a agreujar-los.

TIPOS DE XARXES SOCIALS

Hi ha xarxes socials que reuneixen els usuaris sense tenir en compte una temàtica concreta, xarxes socials generalistes i d'altres que estan especialitzades en un interès o tema en comú, xarxes socials especialitzades:

Les xarxes socials generalistes més conegudes i utilitzades són: WhatsApp, Facebook, Twitter, Instagram, TikTok, Snapchat i VKontakte.

Xarxes socials especialitzades: LinkedIn, InfoJobs, 21Buttons, Spotify, Pinterest, Flickr.

Abonament d'una contraprestació per a dades personals

Es tracta d'un contracte com la resta, però en aquest cas, en lloc de diners com a contraprestació, es paga amb dades. La Directiva 2019/770 ha estat la primera norma a reconèixer la possibilitat que hi hagi un contracte en què el consumidor pugui explotar les seves dades personals i utilitzar-les com a moneda de canvi en el mercat digital [1].

Suposa un avenç important per a la protecció dels consumidors ja que els mecanismes de protecció legalment previstos s'estenen als supòsits en què el consumidor no ha de pagar un preu sinó que ha de cedir les seves dades personals.

Per això, en haver-hi una relació de consum, el consumidor té l'obligació de reclamar-ne els drets.

A INTERNET, NO ET CREGUIS TOT EL QUE HI VEUS

Un ús responsable d'internet en un entorn escolar, familiar i social implica tenir presents les qüestions següents:

Publicitat encoberta

Youtubers o influencers publiciten als mitjans digitals i xarxes socials, a canvi d'una contraprestació econòmica o en forma de productes (estratègia anomenada product placement) aquests articles o serveis. Per això, convé tenir presents que molts dels seus missatges són simplement reclams publicitaris per als seguidors.

Publicitat enganyosa a internet

Vegeu fitxa compres segures a internet.

Correus electrònics fraudulents

Amb aquests, intenten vendre'ns productes.

Amb aquests, intenten accedir a les nostres dades personals.

Vegeu Fitxa compres segures a internet.

Smishing i vishing

Dues de les noves estafes que s'han detectat en els últims temps, a més de les assenyalades a la fitxa compres segures a internet, són l'smishing i el vishing.

Smishing és una tècnica que consisteix en enviar un SMS per part d'un ciberdelinqüent a un usuari simulant que és una entitat legítima —xarxa social, banc, institució pública, etc.— amb l'objectiu de robar informació privada o efectuar-li un càrrec econòmic. Generalment, el missatge convida a trucar a un número de tarifació especial o accedir a un enllaç d'un web fals amb un pretext[2].

Vishing és un tipus de frau basat en l'enginyeria social i la suplantació d'identitat. Es fa mitjançant trucades telefòniques en què l'atacant suplanta la identitat d'una empresa, organització o, fins i tot, alguna persona de confiança, per a obtenir informació personal de les víctimes. Primer, l'atacant ha d'haver obtingut informació confidencial sobre la víctima, com el nom i els cognoms, el correu, el domicili, part de les dades de la targeta de crèdit, etc. Això ho obté gràcies a altres atacs fets

sobre les víctimes, com el phishing o pesca informàtica (vegeu fitxa compres segures a internet). Un cop s'ha obtingut aquesta informació, és el moment de fer una trucada telefònica al client, fer-se passar pel seu banc, una empresa de missatgeria o un servei tècnic a fi d'utilitzar la informació anterior i que la víctima hi confiï. Després d'això, intentarà obtenir més informació, aconseguir que l'usuari instal·li algun programari maliciós (programari hostil i intrusiu, com un virus, etc.) al seu equip o faci algun tipus de pagament.

[1] INDRET

[2] INCIBE

PER SABER-NE MÉS...

- INCIBE (Institut Nacional de Ciberseguretat)
- OSI (Oficina de Seguretat de l'Internauta)
- AEPD (Agència Espanyola de Protecció de Dades)
- Brigada de Recerca Tecnològica de la Policia
- Grup de Delictes Telemàtics de la Guàrdia Civil
- Educlic: Riesgos en Internet
- Instituto Nacional de Tecnologías Educativas y Formación del Profesorado
- MSCBS

Materials didàctics:

- Guia d´ús segur i responsable d´Internet per a professionals de serveis de protecció a la infància
- Guia per a la comunitat educativa de prevenció i suport a les víctimes de ciberassetjament en el context escolar
- SEDE EDUCACIÓN
- EDUCACIÓN Y FP
- Guía S.O.S. contra el Ciberbullying
- Guía S.O.S. contra el Ciberbullying. Padres
- EDUCA TOLERANCIA
- INCIBE

Guía de actuación contra el ciberacoso:

- INJUVE. Guía de actuación contra el ciberacoso

- Internet segura
- AEPD
- Compra segura a INTERNET GUIA PRÀCTICA
- Joguines connectades

Guies per a un bon ús del mòbil i les xarxes socials:

- Guia d'actuació per prevenir i solucionar l'abús dels mòbils
- Aprendre a conviure amb el mòbil
- Guia per a pares i educadors sobre ús segur d'Internet, mòbils i videojocs
- Guia per a joves i adolescents sobre bon ús de les tecnologies
- Guia de seguretat a les xarxes socials
- Servei d'atenció a addiccions tecnològiques (Madrid)
- Agencia Española de Protección de datos
- Brigada Central de Investigación Tecnológica de la Policía
- Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF)
- INCIBE (Institut Nacional de Ciberseguretat)
- Com evitar la publicitat no desitjada
- Exerceix els teus drets
- Guia de privadesa i seguretat a internet
- Tu decideixes a internet
- Observatorio de la infancia
- Guia per a joves i adolescents sobre bon ús de les tecnologies