Definició i explicació dels térmens que s'utilisen en el llenguage d'internet i de les Rets Socials



PENSA

Connectar-se a Internet és una acció que fem quasi 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 a accedir a informació, per a l'entreteniment, la comunicació i fins i tot la compra de qualsevol producte són importants, però també amaga 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...

Si internet fora un país, seria el sisé 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'abuses pel bé del planeta i pel bé de la teua salut física i mental.

Hi ha molts serveis i protocols en Internet, a part de la 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 a classificar les connexions a Internet, almenys tants com tipus de xarxes a què podem connectar el nostre equip. Aquestes diferències es poden trobar en el nivell físic i el tipus de tecnologia de què se serveixen.

a) **Línia telefònica**: es necessita un mòdem, el qual 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 compte d'analògica).
- **ADSL**: l'ADSL (Asymmetric Digital Subscriber Line) és una tecnologia d'accés a Internet de banda ampla i és el tipus de connexió preferit en llars i empreses.

c) **Cable**: des del punt de vista físic, la xarxa de fibra òptica necessita una infraestructura nova i costosa, i això explica que encara hui no estiga 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



e) **Xarxes sense fil**:

les xarxes sense fil (o *Wireless*) difereixen de totes les connexions anteriors, i la més coneguda i utilitzada és la xarxa WI-FI.

- És un mecanisme de connexió de dispositius electrònics sense fil. Les xarxes Wi-Fi posseeixen una sèrie d'avantatges, entre els quals destaca la comoditat.

Però, igual que la xarxa sense fil, la tecnologia Wi-Fi presenta els seus propis problemes intrínsecs. Alguns d'aquests desavantatges són:

Falta de seguretat. Moltes d'aquestes xarxes es converteixen en xarxes obertes, sense protegir la informació que circula per elles.

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 distints sistemes derivats del GSM (Global System Mobile).

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 hem de fixar-nos quan contractem una connexió a Internet:

Cobertura del lloc de la connexió: ofertes n'hi ha moltes, però és molt probable que, de no viure en grans ciutats, no podem accedir a totes elles.

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 refies només de la publicitat i contracta només el que necessites, per tindre 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 comproves en la mesura que siga possible com funcionen els serveis d'atenció al client.

Aspectes ètics, legals i de seguretat



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

Igual que passa 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 seu funcionament: problemes amb l'accessibilitat, la connexió a determinades webs o serveis d'Internet, virus, correu brossa (spam), 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 activitsts econòmiques: compres induïdes, publicitat, despesa telefònica desorbitada, estafes, robatoris o descàrregues il·legals.

Relacionats amb les addiccions: hi ha riscos relacionats amb l'abús de determinades pràctiques com el joc, compres compulsives, addicció a entorns

socials com ara xats, videojocs en línia...



El correu electrònic també pot causar-nos molts problemes. Ens podem vore bombardejats per spam (publicitat nosol·licitada), ser enganyats amb falses cadenes de solidaritat o diferents mètodes d'estafa,i també rebre virus que afecten el nostre ordinador. (Vegeu la fitxa Correu electrònic).

RECOMANACIONS

Tria un navegador segur: la major part de les activitats que exercim per Internet se centren en el nostre navegador. Haurem de tindre en compte també el nivell de seguretat que aquests ens pot proporcionar.

Tingues cura de la protecció del teu equip: hem de tenir instal·lat un antivirus en el nostre sistema operatiu.

Comprova la configuració dels teus perfils: és important revisar el grau de privacitat que has triat per al teu perfil en les xarxes socials en què participes. Si navegues des d'un PC compartit, recorda't de tancar la sessió de tots els teus comptes d'adreça electrònica o pàgines en què estigues registrat cada vegada que et connectes. I, per descomptat, no compartisques mai les teues contrasenyes ni perfils. Si cal, canvia-les ben sovint per evitar que algú puga utilitzar-les. Si comparteixes imatges o informació d'altres persones a través d'Internet, assegura't que aqueixes dades o fotografies no perjudiquen o molesten el seu protagonista, ni envaïsquen la seua privacitat o violen la seua intimitat.

No reenvies cadenes: no reenvies mai a tots els teus contactes les famoses cadenes, ja que ben 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 qualsevol tipus, pengen en la web sobre tu. Només amics verdaders: abans d'acceptar una petició d'amistat o d'agregar tu a algú en qualsevol de les xarxes socials, pensa si de veritat coneixes la persona i no hi ha cap inconvenient que accedisca a les teues dades, al teu entorn i a la teua vida íntima.

Publicar contingut personal: aquest és un dels errors més grans que es duen a terme, sobretot en xarxes socials. Exposar massa les activitats diàries i la teua família és quelcom perillós. Un exemple de mal ús de les xarxes socials es pot vore amb molta freqüència en Instagram. Aquesta xarxa té una eina denominada Stories. Hi pots publicar imatges o vídeos de 15 segons que mostren allò que estàs fent en aqueix moment i queda a disposició dels usuaris de la xarxa durant 24 hores.

Compartir informació provinent d'altres persones: no has de divulgar imatges, missatges o testimonis de tercers sense que ells ho permeten. A més, no has de compartir continguts que puguen denigrar la imatge d'algú. El ciberassetjament (cyberbullying) és una práctica considerada com a assetjament virtual.

Exposar la seguretat: informacions com ara dades bancàries, ubicació i compres de béns no han de ser mai compartides en les xarxes socials.

Fer clic en tot allò que es veu: sabem que per a realitzar diverses accions en Internet necessitem fer clic en diversos enllaços, i això no és un problema. El vertader error està en el fet d'accedir a tots els enllaços que se suggereixen, sense saber abans si són segurs. A pesar que moltes persones conegudes suggereixen que no cregues en tot allò que lliges.



Protegeix les teues dades personals: abans d'acceptar o rebutjar la proposta d'utilització de les teues dades personals per a comunicacions comercials, pensa el que 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 últims 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. En ocasions, a causa d'això, es veuen empobrides les relacions socials del dia a dia, diguem que com a conseqüència de l'ús excessiu d'aquestes xarxes socials, les persones interactuen menys en el dia a dia. (Per exemple: vas a un restaurant amb la teua família o els teus amics i es pot comprovar que cada persona està consultant el seu telèfon i no parlen entre ells).

Amb l'augment de l'ús de les xarxes socials han aparegut amenaces i riscos a causa de la mala utilització d'aquestes. Com a persones consumidores i usuàries de les xarxes socials se n'han d'adquirir hàbits per a un ús responsable. Hi ha aspectes que convé tenir molt clars: s'ha de respectar totes les persones, no s'ha de publicar informació personal d'interés (localització, residència, el teu col·legi o institut, els



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

a) Per a poder accedir a la xarxa, cal acceptar les condicions d'ús de la pàgina i la seua política de privacitat. Aquesta informació no sempre és directament visible i resulta necessari descarregar-se-la per a poder accedir-hi. No obstant això, és possible acceptar-la assenyalant l'opció d'«accepte» sense necessitat de llegir-la. Açò és una cosa molt freqüent i pot suposar un risc ja que, en acceptar aqueixes condicions, donem el nostre consentiment a l'administrador de la pàgina perquè

dispose de les nostres dades i les nostres imatges.

b) En molts formularis de registre se sol·liciten excessives dades de caràcter personal, com, per exemple, les creences religioses, la ideologia política, l'orientació sexual, etc. Habitualment, aquestes dades no se 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 seues dades personals. És necessari, per seguretat, que només acceptes en les teues xarxes socials persones que conegues i siguen del teu entorn pròxim. Hem d'utilitzar SEMPRE un perfil privat per a relacionar-nos en una xarxa social que només permeta veure la informació i les publicacions que fas als teus amics/seguidors/subscriptors.

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

a) **Les persones usuàries de les xarxes socials utilitzen aquests espais per a compartir informació**: comentaris d'experiències personals, fotografies, vídeos... Moltes vegades tota aqueixa informació pot ser excessiva. NO hem de facilitar dades personals que permeten la nostra localització o obtindre informació sobre la nostra família, els nostres amics, el col·legi, etc.

b) **Molts motors de busca indaguen en els continguts**.

c) **Un gran nombre de pàgines requereixen la instal·lació de galletes** (cookies) per a poder funcionaR. Aquests dispositius, instal·lats en el disc dur de l'usuari, arrepleguen informació sobre els llocs web que es visiten i poden obtenir informació sobre els gustos i les preferències de l'usuari per a personalitzar el contingut de la seua pàgina i mostrar-lo d'acord amb aquests, amb fins publicitaris 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 aqueixa foto deixe de pertànyer-nos només a nosaltres i a partir d'queix moment els drets siguen compartits amb l'entitat que l'allotja, que pot utilitzar-la per a diversos fins.



Després d'haver participat en una xarxa social, quan la persona usuària es planteja deixar de pertànyer a la xarxa, pot sorgir una nova dificultat. El risc principal en aqueix moment és la impossibilitat de dur a terme una baixa efectiva. Encara que el perfil estiga tancat i no es puga accedir-hi, les dades de registre continuen estant a disposició dels responsables de la xarxa social. La persona interessada ha de saber que té dret a obtindre, sense dilació per part del responsable del tractament, la supressió de les dades personals que li concernisquen.

Una de les majors preocupacions que també sorgeixen respecte a l'ús que els menors fan de les xarxes socials, és la possibilitat que siguen 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: ciberassetjament escolar (cyberbullying) i ciberassetjament pedòfil (grooming).

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

Els grups de WhatsApp s'usen en moltes ocasions com a mitjà per a insultar i desvalorar un dels membres. Sempre ha existit el bullying en els centres escolars, però no haver de donar la cara per a desvalorar i fer sofrir 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 un fi sexual. La facilitat i la immediatesa amb què, a hores d'ara, es comparteixen imatges del nostre dia a dia, pot ser un punt molt important a tindre en compte en aquest tema.

Ambdós problemes no són nous i no sorgeixen 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 l'agreujament d'quest tipus de problemes.

TIPOS DE XARXES SOCIALS

Hi ha xarxes socials que reuneixen els usuaris sense tindre en compte una temàtica concreta, xarxes socials generalistes i d'altres que estan especialitzades en un interés 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 comptes de diners com a contraprestació, es paga amb dades. La Directiva 2019/770 ha sigut la primera norma a reconéixer la possibilitat que hi haja un contracte en què el consumidor puga explotar les seues dades personals i utilitzar-les com a moneda de canvi en el mercat digital [1].

Suposa un avanç 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 seues dades personals.

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

EN INTERNET, NO ET CREGUES TOT EL QUE HI VEUS

Un ús responsable d'internet en un entorn escolar, familiar i social implica tindre 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 tindre presents que molts dels seus missatges són simplement reclams publicitaris per als seguidors.

Publicitat enganyosa en internet

Vegeu fitxa compres segures en internet.

Correus electrònics fraudulents

Amb aquests, intenten vendre'ns productes.

Amb aquests, intenten accedir a les nostres dades personals.

Vegeu Fitxa compres segures en internet.

Smishing i vishing

Dues de les noves estafes que s'han detectat en els últims temps, a més de les assenyalades en la fitxa compres segures en 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 telefonar 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 telefonades en què l'atacant suplanta la identitat d'una empresa, organització o, fins i tot, alguna persona de confiança, per a obtindre 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 en internet). Una vegada s'ha obtingut aquesta informació, és el moment de fer una telefonada 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 confie. Després d'això, intentarà obtindre més informació, aconseguir que l'usuari instal·le algun programari maliciós (programari hostil i intrusiu, com un virus, etc.) al seu equip o faça algun tipus de pagament.

[1] INDRET

[2] INCIBE: Smishing

PER A SABER-NE MÉS

Vegeu fitxa «Internet. Aspectes ètics, legals i de seguretat

- 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

Guia d'actuació contra el ciberassetjament:

- INJUVE. Guía de actuación contra el ciberacoso
- Internet segura
- AEPD
- Compra segura en INTERNET GUÍA PRÁCTICA
- Juguetes conectados

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

- Aprendre a conviure amb el mòbil
- Guia per a pares i educadors sobre l'ús segur d'Internet, mòbils i videojocs
- Guia per a joves i adolescents sobre un bon ús de les tecnologies
- Guia de seguretat a xarxes socials
- Servei d'atenció a addiccions tecnològiques (Madrid)
- Agència Espanyola de Protecció de Dades
- Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF)
- Brigada Central de Recerca Tecnològica de la Policia
- Cómo evitar la publicidad no deseada
- Ejerce tus derechos
- Tu decides en Internet
- Observatorio de la infancia
- Portal web Pantalles amigues