Interneten eta Sare Sozialen hizkuntzan erabiltzen diren terminoen definizioa eta azalpena (RRSS)



PENTSATU

Internetera konektatzea egunero egiten dugun ekintza da. Internet, egiatan, elkarrekin konektatuta dauden komunikazio-sareen multzo deszentralizatua da, mundu guztira heltzen den sare bakar gisa funtzionatzen duena.

Internetek aukera ugari eskaintzen ditu informazioa jasotzeko, entretenitzeko, komunikatzeko eta edozein produktu erosteko, baina zailtasunak eta desabantailak ere badauzka. Hori dela eta, jakin behar dugu zer abantaila eskaintzen digun komunikazio-sistema horrek, nola erabil dezakegun eta nola saihestu ditzakegun egon daitezkeen arriskuak.

BAZENEKIEN...

Internet sarea herrialde bat balitz, munduko kutsatzaile handien artean seigarrena izango litzateke. Trafiko digital itzel horren aztarna ekologikoa munduko elektrizitate-kontsumoaren % 7ren baliokidea da. Izan arduratsu egiten duzun erabilerarekin; ez abusatu planetaren eta zure osasun fisiko eta mentalaren hobe beharrez.

Interneten zerbitzu eta protokolo asko daude, webguneez gain: posta elektronikoaren bidalketa, fitxategien transmisioa eta kontsulta, lineako elkarrizketak, bat-bateko mezularitza, multimedia komunikazioa eta lineako jolasak.

SARBIDEA ETA KONEXIOAK:

Zenbait irizpide daude Internet konexioak sailkatzeko; gure ekipamendua konektatu ahal dugun sare-mota adina irizpide, gutxienez. Desberdintasun horiek alderdi fisikoan edo baliatzen duten teknologia-motan oinarritu daitezke.

a) **Telefono-linea**: modem bat behar da, ordenagailuaren seinale digitalak telefono-linearen bidez transmititzen diren soinu-pultsu bihurtzen dituena. Konexio-sistema hau jadanik ez da erabiltzen.

b) **Linea digitala**:

- **RDSI**: telefono-linea da, baina digitala (ez analogikoa).
- **ADSL**: ADSL (Asymmetric Digital Subscriber Line) Interneten sartzeko banda zabaleko teknologia da eta konexio-mota gogokoena da etxeetan eta enpresetan.

c) **Kablea**: ikuspuntu fisikotik, zuntz optikoko sareak azpiegitura berria eta garestia eskatzen du, horregatik oraindik ez dago erabilgarri leku guztietan.

d) **Satelitea**: konexio-mota hau oraindik erabiltzen da beste aukerarik ez dagoen kasuetan; adibidez, itsasontzietan, hegazkinetan edo oso gune isolatuetan, zeinetara bestelako sarerik edo Internet konexiorik iristen ez den.



e) **Hari gabeko sarea**k: hari gabeko edo *wireless* sareak aurreko sare guztietatik desberdinak dira; wifia da ezagunena eta erabiliena.

Gailu elektronikoak haririk gabe konektatzeko mekanismoa da. Wifi-sareek abantaila batzuk dituzte, batez ere erosotasuna.

Baina, hari gabeko sareak bezala, wifi-teknologiak berezko arazoak dauzka. Hauek dira desabantailetako batzuk:

Segurtasun-falta. Sare horietako asko sare ireki bihurtzen dira, haietatik zirkulatzen den informazioa babestu gabe.

Abiadura txikiagoa kable bidezko konexioekin erkatuta, interferentziak direla eta.

f) **Telefonia mugikorra**: Internet konexioak, teknologia mugikorraren barruan, GSM (Global System Mobile) delakotik eratorritako zenbait sistema erabiltzen ditu.

INFORMAZIO INTERESGARRIA

Internet erabili ahal izateko, hornitzaileengana jo behar dugu; zuzeneko konexio iraunkorra sortzen duten konpainiak dira, eta, zerbitzua ordainduta kontu bat kontratatzen badugu, sarean ibiltzeko aukera eskaintzen digute. Kontratu guztietan bezala, komeni da baldintzak arretaz irakurtzea.

Zertan jarri behar dugun arreta Internet konexio bat kontratatzerakoan:

Konexioaren tokiko estaldura: eskaintza asko daude, baina litekeena da, hiri handietan bizi ezean, guztietarako sarbiderik ez izatea.

Eskaintzak eta abiadura: azken prezioa eta, askotan, abiadura normalean ez datoz bat iragarkian agertzen direnekin; kontratatu aurretik, galdetu; ez fidatu publizitateaz bakarrik eta soilik behar duzuna kontratatu; abiadura handiagoa kontratatzeko aukera izateko, ez da nahitaezkoa hori kontratatzea.

Galdetu zerbitzuan jarraitzeko konpromisoari buruzko klausularik dagoen.

Zerbitzu teknikoa: gomendagarria da bezeroarentzako arreta-zerbitzuek nola funtzionatzen duten egiaztatzea, ahal den neurrian.

Etikari, legeari eta segurtasunari lotutako alderdiak

Denok ezagutzen ditugu Internet sarearen abantailak, baina, sare ireki eta unibertsala denez, haren funtzionamenduarekin eta ematen diogun erabilerarekin

zerikusia duten zenbait arrisku dauzka. Interneten,h logika eta zentzu komuna erabili behar ditugu, bizitza errealean egingo genukeen bezala.

Mundu fisikoan egiten ditugun jardueretan gertatzen den moduan, Interneten funtzionaltasun guztiek arriskuren bat ekar dezakete. Hauek azpimarra ditzakegu:

- **Funtzionamenduari lotutakoak**:  arazoak irisgarritasunarekin, webgune edo Interneteko zerbitzu jakin batzuetarako konexioarekin, birusekin, spamarekin eta abarrekin.
- **Informazioari lotutakoak**: oso fidagarria ez den informazio ugari dago, edonork igo ditzakeelako edukiak sarera.
- **Informazio desegokirako sarbidea**: informazio arriskutsua (indarkeriazkoa, immorala edo legez kontrakoa), batez ere adingabeentzat.
- **Pertsonen arteko komunikazioarekin zerikusia dutenak**: posta elektronikoaren blokeoa, zabor-mezuak eta mezu iraingarriak, norberaren eta hirugarrenen intimitate-galera, legez kontrako ekintzak (hala nola plagioak, difamazioak, mehatxuak eta abar).
- **Jarduera ekonomikoei lotutakoak**: eragindako erosketak, telefono-gastu neurrigabea, iruzurrak, lapurretak edo legez kontrako deskargak.
- **Jabetza industrial eta intelektualari lotutakoak**: marka bat edo egile-eskubideak pirateatzen direnean, musika, joko bat, liburu bat edo pelikula bat bidegabe jaisten dugunean.
- **Adikzioei lotutakoak**: praktika jakin batzuen abusuari lotutako arriskuak daude; esate baterako, jokoa, erosketa konpultsiboak, ingurune sozial batzuekiko adikzioa (txat, bideo-joko eta horrelakoak).



INFORMAZIO INTERESGARRIA

Posta elektronikoak ere arazo asko sor diezazkiguke. Spamez (eskatu gabeko publizitateaz) josi ahal gaituzte, solidaritate-kate faltsuez edo maula-metodo desberdinez engainatu ahal gaituzte eta gure ordenagailuari eragiten dioten birusak jaso ahal ditugu (ikusi posta elektronikoari buruzko fitxa).

ZER EGIN DEZAKET NIK…?

- **Aukeratu nabigatzaile seguru bat:** Interneten gauzatzen ditugun jarduera gehienak gure nabigatzailean ardazten dira. Beraz, horrek eman ahal digun segurtasun-maila ere kontuan hartu beharko dugu.
- **Zaindu zure ekipamenduaren babesa**: gure sistema eragilean antibirus bat instalatuta eduki behar dugu.
- **Egiaztatu zure profilen konfigurazioa**: garrantzitsua da parte hartzen duzun gizarte-sareetako zure profilerako hautatu duzun pribatutasun-maila berrikustea. Ordenagailu partekatu batean nabigatzen baduzu, gogoratu zure posta elektronikoko kontu guztietako eta erregistratuta zauden web-orri guztietako saioa itxi behar duzula konektatzen zaren bakoitzean. Eta, noski, ez partekatu inoiz zure pasahitzak edo profilak. Beharrezkoa bada, aldatu maiz, inork erabili ezin izateko. Interneten bidez beste pertsona batzuen irudiak edo informazioa partekatzen badituzu, ziurtatu datu edo argazki horiek beren protagonistari kalterik edo eragozpenik ekarriko ez diotela, haren pribatutasuna inbaditzen ez dutela eta haren intimitatea urratzen ez dutela.
- **Ez birbidali kateak**: ez bidali zure kontaktu guztiei zorioneko kate horiek, askotan birusak dauzkate-eta, nahiz eta konfiantzazko kontaktu batengandik etorri. Gogoratu Internetek «ez dituela ahazten» modu errazean zuk edo zure inguruneko pertsonek, enpresek edo nolanahiko weborriek zuri buruz sarean esekitzen dituzuen informazioa, adierazpenak eta irudiak.
- **Benetako adiskideak bakarrik**. Adiskidetasun-gonbidapen bat onartu edo zuk gizarte-sareetako inor gehitu baino lehen, pentsatu benetan ezagutzen duzun eta oztoporik ez dagoen hark zure datuetarako, zure ingurunerako eta zure bizitza intimorako sarbidea izan dezan.
- **Eduki pertsonala argitaratzea**: hori da batez ere gizarte-sareetan egiten diren akats handienetako bat. Eguneroko jarduerak eta zure familia gehiegi erakustea arriskutsua da. Gizarte-sareen erabilera desegokiaren adibide bat Instagramen ikus daiteke oso sarritan. Sare horrek Stories izeneko tresna bat dauka. Bertan, irudiak edo 15 segundoko bideoak argitara ditzakezu; horiek une horretan egiten ari zarena erakusten dute eta 24 orduz sarearen erabiltzaileen esku geratzen da.
- **Beste pertsona batzuengandik datorren informazioa partekatzea**: ez duzu hirugarrenen irudirik, mezurik edo lekukotzarik zabaldu behar, haiek baimentzen ez badute. Gainera, ez duzu inoren irudia belztu dezakeen edukirik partekatu behar. Cyberbullyinga jazarpen birtualtzat jotzen den praktika da.

- **Segurtasuna arriskuan jartzea**: gizarte-sareetan ez da inoiz banku-daturik, kokapenik, ondasunen erosketarik e iorik partekatu behar.



- **Ikusten den guztian klik egitea**: badakigu Interneten zenbait ekintza egiteko esteka batzuetan klik egin behar dugula, eta hori ez da arazoa. Benetako akatsa da iradokitzen diren esteka guztietan sartzea, aldez aurretik seguruak diren ere jakin gabe. Ezagun askok esteka batzuetan klik egin dezazun iradokitzen duten arren, ez sinetsi irakurtzen duzun guztia.
- **Babestu zure datu pertsonalak**: zure datu pertsonalak komunikazio komertzialetarako erabiltzeko proposamena onartu edo baztertu baino lehen, pentsatu nola eragingo dizun hirugarren enpresetatik jasoko duzun informazio mordoak.

Gizarte-sareak

Gizarte-sarea erabiltzaileen artean komunikatzeko tresna gisa erabiltzen den web orri edo aplikazio bat da. Informazioa testu, irudi eta bideo formatuan partekatzen da nagusiki, azken urteotan audio formatuaren erabilera areagotu bada ere.

Espainian 29 milioi pertsonak erabiltzen dituzte beren gizarte-sareak era aktiboan, The Social Media Family-k Espainian plataforma horien erabilerari buruz egin duen azterketaren arabera.

Gizarte-sareak gazteen komunikaziorako eta elkarrekintzarako bide nagusiak bihurtu dira. Batzuetan, egoera horren ondorioz, eguneroko gizarte-harremanak eskastu egiten dira, hau da, gizarte-sareak gehiegi erabiltzen direnez, pertsonek egunerokoan elkarrekintza gutxiago dute. (Esaterako: jatetetxe batera bazoaz zure familia edo lagunekin, gerta liteke pertsona bakoitza bere telefonoa kontsultatzen aritzea, elkarren artean hitz egin gabe.)
Gizarte-sareen erabilera igotzean, gainera, mehatxuak eta arriskuak agertu dira, horien erabilera txarra dela eta. Gizarte-sareen kontsumitzaile eta erabiltzaileek ohitura onak hartu behar dituzte, horien erabilera arduratsua izan dadin. Kontu batzuk oso argi izan behar dira: pertsona guztiak errespetatu behar dira, eta ezin da argitaratu interesa piztu dezakeen informazio pertsonalik (zure kokapena, bizilekua,

ikastetxea edo institutua, etorkizuneko bidaiak eta abar).

Lehenik eta behin, pertsona batek gizarte-sare batean sartzea erabakitzen duenean, hainbat egoera gatazkatsu aurki ditzake:



a) **Sarera sartu ahal izateko**, beharrezkoa da webgunea erabiltzeko baldintzak eta haren pribatutasun-politika onartzea. Informazio hori ez da beti ikusteko moduan agertzen, eta deskargatu egin behar da, ikusi ahal izateko. Hala ere, "onartu" egin daiteke, irakurri behar izanik gabe. Oso sarri gertatzen da hori, eta arriskuak eragin ditzake. Izan ere, baldintza horiek onartzean, baimena ematen diogu webgunearen administrariari, gure datuak eta gure irudiak eduki ditzan.

b) **Erregistro-inprimaki askotan**, datu personal gehiegi eskatzen da; adibidez, erlijio-sinesmenak, ideologia politikoa, sexu-orientazioa eta abar. Normalean, datu horiek ez dira "ezinbestekoak" izaten, **eta EZ ditugu eman behar**.

c) Erabiltzaileak erabakitzen du zein sar daitekeen bere profilera eta zeinek ikus ditzakeen bere datu pertsonalak. Segurtasun-arrazoiak direla-eta, zure gizarte-sareetan onartu soilik ezagutzen dituzun eta zure inguru hurbilekoak diren pertsonak. Erabili BETI profil pribatu bat gizarte-sareetan harremanak izateko, zure lagun/jarratzaile/harpidedunek soilik ikus ditzaten jartzen dituzun datuak eta egiten dituzun argitalpenak.

Sarean sartu zarenean, egoera berriak aurkituko dituzu:

a) Gizarte-sareen erabiltzaileek espazio horiek informazioa partekatzeko erabiltzen dituzte: esperientzia pertsonalen iruzkinak, argazkiak, bideoak... Sarritan, informazio hori gehiegizkoa izan daiteke. EZ dugu eman behar gure kokapenaren berri ematen duen datu pertsonalik, edo gure familiari, lagunei, ikastetxeari eta abarri buruzko daturik.

b) Bilaketa-motor askok eduki horiek arakatzen dituzte.

c)



Webgune askok cookie-ak instalatu behar dituzte funtzionatu ahal izateko. Erabiltzailearen disko gogorrean instalatzen diren gailu horiek, zehazki, bisitatzen ditugun webguneei buruzko informazioa jasotzen dute, eta erabiltzailearen gustu eta lehentasunei buruzko informazioa jaso dezakete, beren webgunearen edukia horien arabera pertsonalizatu eta erakusteko, publizitate-xedeak betez, bertara sartzen den bakoitzean.

d) Gizarte-sare batean gure profilera argazki bat igotzea erabakitzen badugu (adibide bat ematearren), argazki horrek gurea izateari utz diezaioke, eta une horretatik aurrera, eskubideak hura duen erakundearekin batera partekatuko ditugu. Beraz, azken horrek hainbat helburutarako erabili ahal izango du.

Gizarte-sare batean parte hartu ondoren, erabiltzaileak bertatik kendu nahi duela erabakitzen badu, beste zailtasun bat aurki dezake. Une horretan sortzen den zailtasun nagusia baja eraginkorra emateko ezintasuna da. Profila itxita egon arren eta bertara sartzea ezinezkoa izan arren, erregistro-datuak oraindik ere gizarte-sarearen arduradunen esku daude. Interesdunak, beraz, jakin beharra dauka berari dagozkion datu pertsonal guztiak ezabatzeko eska diezaiokeela haien tratamenduaren arduradunari, eta hark hala egin beharko duela, atzerapenik gabe.

Adingabeek gizarte-sareak erabiltzen dituztenean sortzen den kezka nagusietako bat jazarpen bat jasateko arriskua da. Gaur egun, sarearen bidez egindako jazarpenari buruz hitz egiten dugunean, egoeraren protagonisten arabera, bi jazarpen mota bereiz ditzakegu: **cyberbullyinga eta groominga**.

Cyberbullyinga internet bidezko eskola-jazarpena da; berdinen artean gertatzen da edo, batzuetan, ikasleen aldetik irakasleenganako.



WhatsApp taldeak, gainera, taldekideetako bat iraintzeko eta gutxiesteko erabiltzen dira sarritan. Beti egin izan da bullyinga ikastetxeetan, baina pertsona bat iraintzeko eta sufriarazteko aurpegia eman behar ez izatea askoz errazagoa da.

Groominga internet bidezko sexu-jazarpena da, heldu batek adingabe baten aurka egiten duena, sexu-xedeak lortzeko. Gaur egun, erraztasun eta berehalakotasun osoz partekatzen ditugu gure egunerokoaren irudiak, eta, beraz, gai hau oso kontuan eduki beharko genuke.

Bi arazo horiek ez dira berriak, eta ez dira gizarte-sareetan sortu, baina gizarte-sareen bidezko komunikazioek ematen dizkiguten anonimotasunak, azkartasunak eta immunitate-sentsazioak halako arazoak larriagotzen lagundu dute.

Gizarte-sareen motak

Gizarte-sare batzuek gai zehatz bat kontuan izan gabe elkartzen dituzte erabiltzaileak, sare sozial orokorrak direlakoak; beste batzuek, aldiz, interes edo gai komun batean espezializatuta daude, eta gizarte-sare espezializatuak dira:

Gizarte-sare orokor ezagunenak eta erabilienak honako hauek dira: WhatsApp, Facebook, Twitter, Instagram, TikTok, Snapchat, VKontakte

Gizarte-sare espezializatuak: LinkedIn, InfoJobs, 21Buttons, Spotify, Pinterest, Flickr.

Datu pertsonalen truke kontraprestazio bat ordaintzea

Gainerakoak bezalako kontratu bat da, baina, kasu honetan, dirua ordaindu beharrean, datuekin ordaintzen da. 2019/770 Zuzentaraua kontsumitzaileari bere datu pertsonalak ustiatzeko eta merkatu digitalean diru-truke gisa erabiltzeko aukera ematen dion kontratua egotea onartu zuen lehenengo araua izan da [1].

Aurrerapen garrantzitsua izan da kontsumitzaileak babesteko, legez aurreikusitako babes-mekanismoak beste kasu batzuetan ere aplikatzea ahalbidetu duelako: hain zuzen, kontsumitzaileak prezio bat ordaindu beharrean, bere datu pertsonalak eman behar dituenean.

Hori dela eta, kontsumo-harreman bat dagoenez, kontsumitzaileak bere eskubideak erreklamatu behar ditu.

INTERNETEN, EZ SINETSI IKUSTEN DUZUN GUZTIA

Internet sarea ikastetxean, familian eta gizartean arduraz erabiltzeko, honako hauek izan behar dira kontuan:

Ezkutuko publizitatea

Youtuberrek edo influencerrek beren hedabide digitaletan eta sare sozialetan produktu edo zerbitzu batzuen publizitatea egiten dute, prestazio ekonomiko baten edo produktu horien truke (product placement delako estrategia). Hori dela eta, kontuan izan behar da haien mezu asko jarraitzaileei zuzendutako publizitate-iragarki hutsak direla.

Iruzurrezko publizitatea Interneten

Ikus "Erosketa seguruak Interneten" fitxa.

Iruzurrezko mezu elektronikoak

Horien bidez, produktuak saldu nahi dizkigute.

Horien bidez, gure datu pertsonalak ezagutu nahi dituzte.

Ikus "Erosketa seguruak Interneten" fitxa.

Smishing eta Vishing

Azkenaldian detektatu diren bi maula berri, "Erosketa seguruak Interneten" fitxan aipatutakoez gain, smishing eta vishing dira.

Smishing teknikari dagokionez, ziberdelitugileak SMS bat bidaltzen dio erabiltzaileari eta egiazko erakunde baten plantak egiten ditu –sare soziala, bankua, erakunde publikoa eta abar–, informazio pribatua lapurtzeko edo kargu ekonomiko bat

ordainarazteko. Oro har, mezuak tarifa bereziko zenbaki batera deitzeko edo –aitzakia batez– webgune faltsu batean sartzeko agintzen du [2].

Vishing, aldiz, ingeniaritza sozialean eta identitatea ordeztean oinarritutako iruzur mota da. Telefono-deien bidez egiten da; izan ere, iruzurgileak enpresa edo erakunde baten edota konfiantzako pertsona baten plantak egiten ditu, bere biktimaren informazio pertsonala lortzeko. Lehenik, iruzurgileak biktimari buruzko isilpeko informazioa lortu behar du: izen-abizenak, e-maila, helbidea, kreditu-txartelaren datu batzuk eta abar. Biktimei egindako beste eraso batzuetan lortzen ditu datu horiek, adibidez, phishing bidez (ikus "Erosketa seguruak Interneten" fitxa). Informazio hori eskuratu ondoren, biktimari telefono-deia egiteko ordua da; bere bankua, mezularitza-enpresa edo zerbitzu teknikoa dela esaten diote, aurreko informazioa erabiltzeko eta biktimaren konfiantza lortzeko. Ondoren, iruzurgileak ahaleginak egingo ditu informazio gehiago lortzeko edo erabiltzailea bere ordenagailuan malware bat instalatzera (software gaiztoa eta intrusiboa, birus bat eta abar) edo ordainketaren bat egitera behartzeko.

[1] INDRET

[2] INCIBE

GEHIAGO JAKITEKO...

- INCIBE (Zibersegurtasun Institutu Nazionala)
- OSI (Internatuaren Segurtasun Bulegoa)
- AEPD (Datuak Babesteko Espainiako Agentzia)
- Poliziaren Ikerketa Teknologikorako Brigada
- Guardia Zibilaren Delitu Telematikoen Taldea
- Educlic: Riesgos en Internet
- Instituto Nacional de Tecnologías Educativas y Formación del Profesorado
- MSCBS

Material hezigarriak

- Internet sarea segurtasunez eta erantzukizunez erabiltzeko gida, haurrak babesteko zerbitzuetan diharduten profesionalentzat
- Hezkuntza-komunitatearentzako gida, eskola-ingurunean ziberjazarpena prebenitzeko eta biktimak babesteko

- Gidak
- Ziberbullying-aren kontrako SOS gida
- Ziberbullying-aren kontrako SOS gida gurasoak
- INCIBE

Ziberjazarpenaren kontra jarduteko gida

- INJUVE
- Internet segurua
- Pribatutasuna eta segurtasuna Interneten
- Erosketa segurua INTERNET-EN, GIDA PRAKTIKOA
- Jostailu konektatuak

Mugikorra eta sare sozialak ondo erabiltzeko gidak

- Mugikorrarekin bizitzen ikasi
- Guraso eta hezitzaileentzako gida, Internet, mugikorrak eta bideojokoak segurtasunez erabiltzeko
- Observatorio de la infancia
- Gazte eta nerabeentzako gida, teknologiak ondo erabiltzeko,
- Sare sozialetan seguru ibiltzeko gida
- Adikzio teknologien kasuetan laguntzeko zerbitzua (Madril)
- Datuak Babesteko Espainiako Agentzia
- Poliziaren Ikerketa Teknologikorako Brigada Nagusia
- Nola saihestu nahi ez den publizitatea
- Zure eskubideak erabili
- Interneten erabakitzen duzu