



PRIBATUTASUNA ETA SEGURTASUNA INTERNETEN

Aurkibidea eta edukien lizentzia

Aurkibidea

- ◆ **1. fitxa** Informazio pribatu asko gordetzen duzu zure gailuetan? Inoiz pentsatu duzu horretan?
- ◆ **2. fitxa** Pasahitzak zergatik dira hain garrantzitsuak?
- ◆ **3. fitxa** Pasahitzak izatea nahikoa da?
- ◆ **4. fitxa** Egin segurtasun kopiak lehenengotik, arazoak agertu aurretik
- ◆ **5. fitxa** Fidagarria ote da orrialde hau?
- ◆ **6. fitxa** Eman egin behar ditut nire datuak, eskatzen dizkidatenean?
- ◆ **7. fitxa** Nola ezabatu ditzaket bilatzaile baten emaitzetan dauden nire datu pertsonalak?
- ◆ **8. fitxa** Nola erabili behar dut nabigatzailea, ez ditzan gorde Interneten ematen ditudan urratsak?
- ◆ **9. fitxa** Nork ikus dezake sare sozialetan argitaratzen dudana?
- ◆ **10. fitxa** Iruzurrak eta bestelako arriskuak antzematen bat-bateko mezularitzan
- ◆ **11. fitxa** Interneten argitaratzen den informazio guztia egia da?
- ◆ **12. fitxa** Phishinga: gure datu pertsonalak eta bankuko datuak lapurtzen saiatzen den iruzurra
- ◆ **13. fitxa** Zer gertatzen zaio nire Interneteko konexioari?
- ◆ **14. fitxa** Nire posta elektronikoa babestu nahi dut
- ◆ **15. fitxa** Zer hartu behar dut kontutan nire informazio pertsonala hodeian gordetzen badut?
- ◆ **16. fitxa** Partekatu al ditut fitxategiak Interneten modu seguruan?
- ◆ **17. fitxa** Ez daukat argi zertarako ari den semea Internet erabiltzen, zer egin dezaket?
- ◆ **18. fitxa** Seguruak dira jarduera fisikoa neurtzen duten eskumuturrekoak eta erlojuak?

Edukien lizentzia

Argitalpen hau taldean egin dute. Jabeak honako hauek dira: Datuak Babesteko Espainiako Agentzia (AEPD) eta Zibersegurtasunerako Institutu Nazionala (INCIBE), eta honako Creative Commons lizentzia du: Aitortu - Ez Komertziala - Lan Eratorririk Gabe 3.0 Espainia. Hori dela eta, baimena dago lana kopiatzeko, banatzeko eta komunikatzeko edozein bitarteko edo formatu bidez, honako baldintzekin:

◆ Aitortu

Hirugarrenek erreproduzitu dezakete lanaren edukia osorik edo partzialki, lanaren jatorria aipatzu eta berariaz adieraziz AEPD eta INCIBE eta horien web guneak. Baina, lanaren aitortzatik ezin izango da ondorioztatu AEPDk edo INCIBEk hirugarren horri laguntzen diotenik edo hirugarren horrek lana nola erabiltzen duen babesten dutenik.

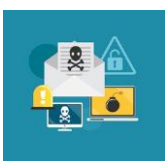
◆ Erabilera EZ Komertziala

Lana banatu, kopiatu eta erakutsi ahal izango da, ez bada merkataritza xedeetarako erabiltzen. Lana berrerabiltzean edo banatzean, argi utzi behar dira lanaren lizentziaren baldintzak. Baina, gerta daiteke baldintza horietako batzuk ez aplikatu behar izatea, AEPDren eta INCIBEn baimena eskuratuz gero, egile eskubideen titularrak direlako. Lizentziaren testua osorik: <http://creativecommons.org/licenses/by-nc-nd/3.0/legalcode>

◆ Lan Eratorririk Gabe

Ez da onartzen lana nahastea, eraldatzea eta jatorrizko lanaren gainean lan eratorririk egitea, ez eta aldatutako materiala hedatzea ere.





Internet eta Internet bidez ematen diren zerbitzuak funtsezkoak bihurtu dira gure bizitzan. Gainera, gailu mugikor adimentsuen erabilera masiboaren ondorioz -batez ere smartphoneak-, eta datu mugikorraren sare gero eta azkarragoen eraginez, eztanda egin duen konektibitate ubikuoaren ondorioz, Interneteko zerbitzu horiek edonon eta edonoiz kontsumitu daitezke, gauez nahiz egunez. Beraz, esan dezakegu “pertsonak daudela konektatua”, ez hainbeste gailuak eta ordenagailuak.

Interneteko zerbitzuak gure egunerokotasunean txertatuta daude: informatzen garenean, harremanak ditugunean informazioa beste pertsona batzuekin partekatuz, argazkiak edo bideoak argitaratzen ditugunean, bideo-jokoekin jolasten dugunean, musika entzun, pelikulak ikusi edo erosketak egiten ditugunean linean. Aukerak eta abantailak ikaragarriak dira, eta betiko etorri dira.

Kasu gehienetan esan daiteke sarean gehien erabiltzen diren zerbitzuak ematen direla, erabiltzaileok, zerbitzuak ematen dituzten enpresei eta beste erabiltzaileei ematen dizkiegun datuei eta informazio andanari esker. Beraz, argi izan behar dugu hori arriskutsua izan daitekeela gure segurtasunerako eta pribatutasunerako.

Argitalpen hau [Datuk Babesteko Espainiako Agentziaren \(AEPD\)](#) eta [Zibersegurtasunerako Institutu Nazionalaren \(INCIBE\)](#) arteko lankidetzaren emaitza da, eta bere helburua da Interneten erabilera segurua eta arduratsua sustatzea, arriskuak zein diren ondo azalduz, eta, gure segurtasuna eta pribatutasuna atakan jarri gabe, zerbitzuei etekina ateratzeko jarraibideak emanez.

Honako gaiak lantzen ditu: pasahitz sendoak izatea garrantzitsua dela, segurtasun kopiak egin behar direla, aholkuak ematen ditu linean erosketak egiteko, programa gaiztoak saihesteko, pribatutasunaren eta hodeiko zerbitzuen inguruko hainbat aholku, gurasoen bitartekaritzan aipatzen du, eta orokorrean nola babestu gure datu pertsonalak.

Gai horietako bakoitzak fitxa bat du, eta fitxa bakoitzean jaso dira informazio garrantzitsuena eta egileen web orrietan garatuta dauden edukietara jotzeko estekak: [Zibersegurtasunerako Institutu Nazionala \(INCIBE\)](#), [Datuk Babesteko Espainiako Agentzia \(AEPD\)](#) eta [Datuk Babesteko Euskal Bulegoa \(DBEB\)](#).

Horiez gain, bideo batzuk ere egin dira, gidaren osagarri, azaltzeko nola konfiguratu pribatutasuna sare sozial erabilienean zerbitzuetan: Instagram, Facebook, Twitter, Whatsapp, Snapchat eta YouTube.

INCIBEk eta AEPDk espero dute ekimena erabilgarria izatea Internet erabiltzen dutenentzat, eta baliokoa izatea bi erakundeei prestakuntza, prebentzioa eta laguntza emateko asmoarekin garatu dituzten edukietara modu praktikoan gerturatzeko.

Informazio pribatu asko gordetzen duzu zure gailuetan? Inoiz pentsatu duzu horretan?

“Trenean nentorren, lanetik bueltan, eta ate ondoan nengoen. Bidaia aprobetxatu nahi nuen bankuko gestio batzuk egiteko, bankuko app-arekin ari nintzen. Bat-batean tren geltutik egin zen geltoki batean, eta berriro martxan hasi zenean, atea ixten hasi ziren unean, baten batek mugikorra kendu zidan esku artetik.”



Gure gailu mugikorrak babesteko arrazoi nagusia da babestu egin behar dugula gure informazio pertsonala eta gurekin komunikatzen diren pertsonena: kontaktuak, argazkiak, bideoak, mezu elektronikoak eta abar, ez dugulako hori guzti hori galdu nahi edo hirugarrenek eskuratzetik nahi.

Behar bezala babestu behar dituzu zure gailuak. Badakizu zergatik?



- Argi dago mugikorra **galtzen baduzu edo lapurtzen badizute**, informaziorik gabe geratuko zarela.
- App gaizto bat** zure datuak ezabatzeko edo erabiltzeko gai da, zu konturatu ere egin gabe.
- Wifi sare publikoak** (aireportuak, kafetegiak, liburutegiak, eta abar) ez dira beti seguruak; alde batetik, ez dutelako zifratzen transmititzen duten informazioa, eta, ondorioz, informazioa eskuratzeko dakien edonork hartu egin dezakeelako; eta, bestetik, ez dakigulako nor gehiago dagoen sarera konektatuta eta ze asmorekin.

Aholkuak eta gomendioak



informazio zifratua



segurtasuneko tresnak



segurtasun kopiak



deskarga seguruak



esandakoak berrikustea



antibirusak ipintzea

Beti egongo da gailua galdu edo lapurtzeko arriskua. Beraz:

- Erabili pantaila desblokeatzeko kodea (zenbakizko kodea edo patroia) eta **zifratu informazioa**, halakorik gertatuz gero, trabak jartzeko zure gailua hartzen duen edonori.
- Erabili **segurtasuneko tresnak**, lagunduko dizutelako gailua lokalizatzen eta blokeatzen, bai eta bertan jasotako informazioa ezabatzen ere.
- Egin **segurtasun kopiak**, baina beste euskarri batean, horrela, edozer gertatuta ere, ez galtzeko mugikorrean edo tabletean duzun informazioa.

Gailuan eduki bakar-bakarrik aplikazio seguruak:

- Deskargatu aplikazioak egileen kanal ofizialetatik bakarrik. Horrela seguru jakingo duzu egileek eta erabiltzaileek ere berrikusi dituztela aplikazioak.
- Aldez aurretik beti ikusi erabiltzaileek **zer balorazio egin duten eta zer iritziz duten** dena delako aplikazioari (app) buruz. Aplikazio mugikorra txarto edo modu susmagarrian badabil, erabiltzaileek iritzia ematen dute eta oharrak egiten dituzte.
 - Ipini **antibirusak**, zure gailuan sartu nahi duten app maltzurak antzemateko.



Kontuz **wifi sare publikoekin** eta non konektatzen zaren. Erabiltzen badituzu:

- Ez trukatu informazio pribaturik edo konfidentzialik.
- Ez konektatu lineako bankuko zerbitzuarekin. ♦ Ez egin erosketarik.

Zergatik dira hain **garrantzitsuak** pasahitzak?

“Eroten ari naiz! Zerbitzu berri batean erregistratzen naizen bakoitzean pasahitz bat eman behar dut, eta zerbitzu pilo bat erabiltzen ditudanez (Facebook, Instagram, PayPal, Gmail...), ez naiz gai sarbide-pasahitzak ondo erabiltzeko, eta azkenean beti pasahitz bera erabiltzen dut neure burua ez estutzeko, nahiz eta jakin ez dela jokabide egokia. Zer egin dezaket?”



Egia da. Ez da oso zuzena pasahitz bera erabiltzea zerbitzu bat baino gehiagotan sartzeko. Izan ere, zure pasahitzari zerbait gertatzen bazaio, zure informazioa ere kinka larrian egongo delako: alde batetik, ezingo duzu dena delako zerbitzuan sartu; eta bestetik, sarbide-pasahitz bera duten beste zerbitzu guztietan ere ezingo duzu sartu.

Pasahitz sendoak erabili behar ditugu eta babestu egin behar ditugu. Badakizu zergatik?

Pasahitzak giltzak dira, zure zerbitzuetan sartzeko balio dutenak, eta zure informazio pertsonalean ere bai. Beraz, baten batek eskuratuz gero, zure pribatutasuna kolokan jar dezake:

Gauzak argitaratu ditzakeelako zure izenean sare sozialetan

Mezu elektronikoak irakurri eta erantzun ditzakeelako zure izenean

Zure lineako bankura sar daitekeelako

Erosketak egin ditzakeelako zure izenean, ordaintzeko moduren bat baduzu atxikita zerbitzuko kontuari.

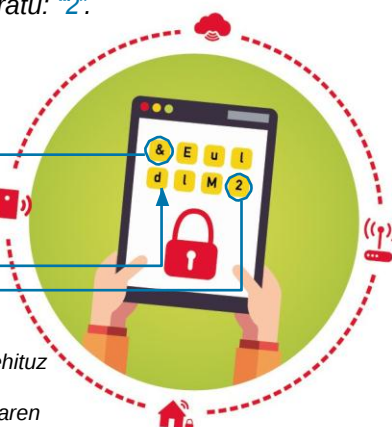
Aholkuak eta gomendioak

Inork ez ditzala asmatu zure pasahitzak

- ♦ Aukeratu **pasahitz irmoak** edo sendoak, gutxienez 8 karaktereak eta beste honakoak dituztenak:
 - ♦ letra larriak (A, B, C...)
 - ♦ letra xeheak (a, b, c...)
 - ♦ zenbakiak (1, 2, 3...)
 - ♦ eta karaktere bereziak (\$, &, #...)
- ♦ **EZ** erabili asmatzen errazak diren pasahitzak, adibidez, honakoak: “12345678”, “qwerty”, “aaaaa”, etxeko izenak, ibilgailuen matrikulak, eta abar.
- ♦ **EZ** partekatu zure pasahitzak. Partekatzen baduzu, ez delako gehiago sekretua izango, eta beste pertsona batzuei zure pribatutasunean sartzen utziko diezulako.
- ♦ **EZ** erabili pasahitz bera zerbitzu bat baino gehiagotan.

Erabili patroiak gako berriak sortzeko eta gogoratzeko

- ♦ Aukeratu sinbolo berezi bat: “&”.
 - ♦ Pentsatu esaldi bat, ahaztuko ez zaizun horietakoa, eta hartu gogoan esaldiaren inizialak: “Maritxu nora zoaz Eder galant hori” -> “MnzEgh”.
 - ♦ Segidan, zenbaki bat aukeratu: “2”.
 - ♦ Lotu bata bestearekin eta pasahitz sendo bat izango duzu:
ADIBIDEA : &EulDIM2
 - ♦ Sinbolo berezia: &
 - ♦ Erregela nemoteknikoa: “Maritxu nora zoaz Eder galant hori”
EulDIM
 - ♦ Zenbakia 2
 - TRIKIMAILUA:
- Patroiari elementu bereizgarri bat gehituz gero: web gunearen, produktuaren, aplikazioaren, jokoaren edo zerbitzuaren iniziala, pasahitz bat izango duzu zerbitzu bakoitzeko!



Ahazkorra bazara, erabili pasahitzak kudeatzeko tresna bat

Pasahitz asko erabiltzen badituzu, eta ez bazara gai denak gogoratzeko, erabili **pasahitzen kudeatzaile bat**. Halako programek laguntzen dute zerbitzuetan sartzeko norbere pasahitzak modu seguruan gordetzen.

- ♦ Pasahitzen kudeatzailean sartzeko pasahitza bakarrik gogoratu beharko duzu. Pasahitz nagusia edo gakoa deituko diogu, eta gainontzeko pasahitzak gogoratzeko balio du.
- ♦ Baina, kontuz, ahazten bazaizu ezin izango dituzulako besteak gogoratu. Beraz, ondo gorde buruan.

Lau urtaro, lau pasahitz

Pasahitza oso sendoa bada ere, denborarekin makaldu egin daiteke.

- ♦ Aldatu aldiro-aldi pasahitzak.

“Pasahitz sendoa erabiltzen dut, baina beldur naiz, baten batek eskuratu, eta nire lineako zerbitzuetan sartzea: sare sozialetan, lineako bankuan, posta elektronikoan... Pasahitza erabiltzeaz gain, badago erabiltzaile kontuak beste mekanismo batekin babesterik?”



Pasahitz batekin bakarrik babestuta dagoen zerbitzu baten segurtasuna pasahitzaren menpe dago, eta horrek esan nahi du segurtasuna arriskuan dagoela, hain zuzen ere, baten batek pasahitza eskuratu gero, erabiltzaile-kontuan sartzeaz gain, iruzurrezko jarduerak egin ditzakeelako neure izenean, edo neure informazio pertsonalean kuxkuxean ibili.

Pasahitz sendoa ez da nahikoa segurtasuna guztiz bermatzeko. Badakizu zergatik?

Ziberdelitugileak

pasahitzak lapurtzen saiatzen dira, gure zerbitzuetan sartzeko, eta nahierara erabiltzeko, honako tekniken bidez:



- ♦ **Phishing erako erasoak** edo ingeniari-tza soziala erabiliz.
- ♦ Berariaz helburu horrekin diseinatutako birusak erabiliz.
- ♦ Baimenik gabe sartuz erabiltzaileen pasahitzak gordetzen dituen dena delako zerbitzuaren zerbitzarian.
- ♦ Sareko komunikazioak zelatatuz.

Aholkuak eta gomendioak

Ez izan zalantzarik!

Gehitu segurtasun geruza osagarri bat zure kontuari

- ♦ Erabiltzaile kontuak babesteko modu bat da **bi urratseko egiaztapen** sistemak erabiltzea: hau da, dena delako lineako zerbitzuaren erregistro/login prozesuari segurtasun geruza osagarri bat gehitzea, hau da, zerbitzuan sartzeko, erabiltzaile-izenaz eta pasahitzaz gain, kode bat eman beharko duzu, zuk zeuk bakarrik dakizuna eta normalean gailu mugikorraren bidez lortzen dena.

Bi urratseko egiaztapena = faktore bikoitza = autentifikazio bikoitza = saioa hasteko baimena

■ Erabiltzailea

+

■ Pasahitza

+

■ Kodea



Zer lortzen duzu horrela?

Trabak jartzea beste pertsona batzuk ez sartzeko zure lineako zerbitzuetan: nahiz eta pasahitza lortu, beste kode bat beharko dutelako, eta kode hori jakiteko modu bakarra da zure telefono mugikorra edukitzea eskuartean.

Nola lor ditzakezu segurtasun kodeak?

- ♦ Zerbitzuaren arabera aukeratu dezakezu, baina gaur egun gehien erabiltzen den sistema da **SMS bidez kode bat bidaltzea** aldeztu aurretik konfiguratutako telefono zenbaki batera. Kodea jasotakoan, erabili egin behar da (bigarren urrats osagarria da), eta segidan zerbitzuan sartu.

Segurtasun neurri osagarriak:

Ausazko kodeak sortzen dituzten aplikazioak



SMS mezuak



Beste telefono zenbaki batzuk



- ♦ **Konfiantzazko gailuak** badituzu, ez duzu kodea sartu beharko dena delako zerbitzuan sartu nahi duzun bakoitzean. Eta noizean behin bakarrik sartu beharko duzunez, egiaztatze bikoitza egitea erraza izango da.
- ♦ Zerbitzu batzuek ez dute bi urratseko egiaztapenak egiteko aukerarik. Halakoetan ziurtatu **pasahitz sendoak** erabiltzen ari zarela eta behar bezala **kudeatu pasahitzok**, segurtasun eta pribatutasun arazorik ez izateko.

Arazoak eduki aurretik, egin **segurtasun kopiak**

“Aurreko batean ekipoko disko gogorra konektatzean, mezu bat agertu zitzaidan diskoa formateatzeari buruzko ez dakit zer zioena, eta onartu egin nuen nahi gabe. Ederra disgustua! Diskoko informazio guztia ezabatu dut eta azken 3 urteetako argazkiak galdu ditut, diskoan bakarrik neuzkalako gordeta, eta ez beste inon”.



Halakorik gertatzen bazaizu, eta segurtasun kopiarik ez baduzu egin, zure informazio guztia desagertu egingo da, eta, ondorioz, gerta daiteke oroitzenak eta une pertsonalak galtzea, berriro egin behar izatea hainbeste ahalegin eta denbora kostatutako lanak, eta abar. Informazioa gutxieneko bermearekin berreskuratzeko modu seguru bakarra da segurtasun kopia bat egitea.

Segurtasun kopiak egin behar dituzu. Badakizu zergatik?

Nahi gabe ezabatzea

izan ohi da informazioa galtzeko modurik ohikoena, baina ez da bakarra; izan ere, **birusak ere izan daitezke** informazioa zifratzeko edo ezabatzeko gai; edo gerta daiteke **galtzea, istripua izatea edo lapurtzea** informazioa duen gailua: smartphonea, tableta, ordenagailu eramangarria, kanpoko disko gogorra, pendrivea, DVDa, eta abar; edo gerta daiteke **gailua ez ibiltzea behar bezala**.



Aholkuak eta gomendioak

1 Aukeratu inondik inora galdu nahi ez duzun informazioa



Argazkiak



Bideoak



Dokumentuak



Fakturak



Bestelakoak

2 Aukeratu zein gailutan biltegitratuko duzun informazioa



USBa



Kanpoko disko gogorra



DVDa



Hodeia (cloud)



eta abar

3 Egin segurtasun kopia

Bikoiztu informazioa euskarri bitan edo gehiagotan. Adibidez, kopia bat kanpoko disko gogorrean gorde daiteke eta bestea ordenagailu eramangarriaren disko gogorrean, edo hodeiko zerbitzu batean (Drive, Dropbox, eta abar).



Ordenagailua



Android



iOS



Cloud

4 Errepikatu aldiro-aldiri kopia

Eguneratu aldi-an aldi-an zure segurtasun kopiak, eta egiaztatu, alde batetik, ea informazioa oraindik eskuragarri dagoen; eta, bestetik, segurtasun kopietan gehitu bien bitartean sortu duzun informazioa.



“Pozarren erabiliko nuke Internet bankuko mugimenduak kudeatzeko, linean saltzen duten dendetan erosketak egiteko, bai eta administrazio publikoekin izapideak egiteko ere; baina, ez dut halakorik egiten, ez naizelako seguru sentitzen. Zer egin dezaket konfiantza izateko?”



Ez bazaude teknologiak eta Internet erabiltzen ohituta, normala da zalantzak izatea lineako zenbait izapide egiteko orduan. Segurtasunari buruzko alderdi batzuk nola diren ez badakizu, gerta daiteke iruzurren bat jasatea edo zure aldetik ezer ez egitea, beldur zarela. Baina, ezintasun hori erraz gainditu dezakezu, ondoko aholkuei erreparatuz gero.

Ikasi egin behar duzu lineako izapideak modu seguruan egiten. Badakizu zergatik?

Lineako edozein izapide egin aurretik, ziurtatu behar duzu sartuko zaren web orria segurua dela, batez ere izapideak egiteko datu sentsibleak eman behar badituzu. Helburua da honakorik ez gertatzea:

- ♦ Enpresa eta zerbitzu ezagunen identitatea ordezkatzeko duten iruzurrezko web orrietan sartzea.
- ♦ Faltzifikatutako artikulua erostea, jatorrizkoen prezioa ordainduta.
- ♦ Dirua eta datu pertsonalak lapurtzea ahalbideratzen duten birusen edo iruzurren menpe erortzea.

Gailua sasoian duzu? Babestu ezazu behar bezala

Lehenengo eta behin ziurtatu behar duzu zure gailua prestatuta dagoela halako izapideak egiteko. Babestu ezazu behar bezala:

- ♦ Antibirus bat ipini eta mantendu eguneratuta ondo antzemateko azken mehatxuak sarean
- ♦ Zure ekipoa, programak eta nabigatzailea beti eduki behar dituzu eguneratuta eta behar bezala konfiguratuta.
- ♦ Sortu behar duzu erabiltzaile kontu bat pertsona bakoitzeko, hau da, gailua erabiliko duen bakoitzarentzat kontu bat.

Konexioak garrantzia du, kontuan hartu

Izapideak egin behar badituzu eta linean badira, ez erabili wifi sare publikorik. Hobe da konektatzea etxeko wifitik edo 3G/4G mugikorretik. Eta ez ahaztu egiaztatzea zure wifi sarea behar bezala konfiguratuta dagoela, inor ezezagunik ez konektatzeko zure sarera.

Aholkuak eta gomendioak

Ziurtatu zuk nahi duzun web orrian zaudela

Gune bat bisitatzen duzunean, egiaztatu benetan zaudela sartu nahi duzun tokian. Fijatu URLan, eta ikusi hasieran https agertzen dela eta giltzarrapo bat dagoela helbide-barran. Giltzarrapoaren gainean klikatu ostean, URLa ere ondo idatzita egon behar da.

Beste gomendio baliagarri batzuk...

Lineako bankan gestioak egiteko edo administrazio publikoarekin

- ♦ 1 Gorde sekretupean zure sarbide pasahitzak. Ez gorde idatzita eta ez partekatu inorekin.
- ♦ 2 Ez erantzun datu pertsonalak eta/edo bankuko datuak eskatzen dizkizuten mezu elektronikoak.
- ♦ 3 Zalantzarik baduzu, jarri harremanetan zuzenean bankuarekin edo zerbitzu publikoarekin, arazoa konpontzeko.



Bukatutakoan, ez ahaztu saioa itxi behar duzula

Sakatu saioa ixteko dioen tokian, saioa bukatzeko. Ez baduzu hori egiten, saioa zabalik geratuko da eta zure datu pertsonalak eta / edo bankukoak ikusi egin ahal izango dituzte Interneten sartzeko gailu bera erabiltzen dutenek.

Erosketak linean

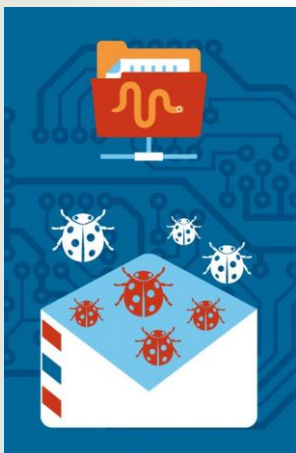
- ♦ 1 Egiaztatu ea agertzen den prezioa behin betikoa den ala beste zerga edo kargu osagarriren bat gehitu behar zaizkion.
- ♦ 2 Jakin zein diren baimendutako ordainketa moduak.
- ♦ 3 Ikusi beste erabiltzaile batzuek zer iritzi duten web orriaren edo saltzailearen gainean. Begiratu sarean.
- ♦ 4 Ondo aztertu bidalketa baldintzak eta ikusi itzulketen politika.

Eman egin behar ditut nire datuak eskatzen dizkidatenean?

“Web baten harpideduna egin naiz, eta hainbat orrialde bete behar izan ditut informazio pertsonalarekin. Hasiera batean ez diot garrantzi handirik eman, baina orain apur bar arduratuta nago. Uste dut informazio gehiegi eskatzen didatela eta ez dakit zertarako nahi dituzten nire datu pertsonalak”.

Normala da kezkatuta egotea. Zure datu pertsonalak eman aurretik, ondo begiratu behar duzu nork eskatu dizkizun eta zertarako, eta ea benetan behar duen informazio hori. Ez duzu informazio pertsonal bera eman behar mediku-aseguru bat kontratatzeko edo lineako erosketak egiteko web batean harpidetzeko. Seguruenez, aseguru egiteko, datu pertsonal asko eman beharko dituzu, beharbada familiako aurrekari buruzkoa ere bai; baina, web batean harpidetzeko, nahikoa izan behar da lineako erosketekin zer ikusia duten datuak betetzea (izena eta abizenak, NANA, fakturazio datuak, ordainketa modua, bidalketa helbidea ...).

Behar dena baino informazio gehiago ematea ez da ona. Badakizu zergatik?



- ♦ Spam-a jasoko duzu.
- ♦ Zure pribatutasuna eta identitatea ataka larrian gera daitezke.
- ♦ Xantaia egin ahal dizute edo estortsioa.
- ♦ Hirugarrenen datuak ematen badituzu, salatu egin ahal zaituzte.

Aholkuak eta gomendioak

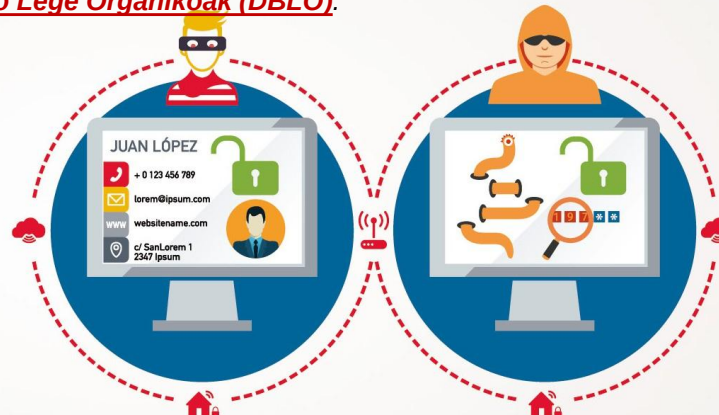
Zeuk erabaki zer egin zure datu pertsonalekin eta zure eskubideekin. Ezagutzen dituzu?

Zure datu pertsonalak babesteko eskubidea duzu. Horrek esan nahi du zure informazio pertsonala erabili dezakezula eta horren gaineko erabakiak hartu. Hala dela xedatzen dute Konstituzioak, Europako Zuzenbideak eta, bereziki, **Datu Pertsonalak Babesteari buruzko Lege Organikoak (DBLO)**.

Baten batek datu pertsonalak eskatzen badizkizu, esan egin behar dizu:

- ♦ Helburua: zertarako nahi dituen.
- ♦ Nola tratatuko dituzten:
Informazio eskubideak (aepd, dbep).
- ♦ Nola egikaritu zure AZETA eskubideak (**aepd, dbep**) (Datuak atzitzea, Zuzentzea, Ezerezte eta Aurka egitea).
- ♦ Nahiz eta pertsona edo erakunde bati baimena eman zure datu pertsonalak tratatu ditzan, **nahi duzunean esan dezakezu ezetz.** Adostasuna bertan behera utz dezakezu iritziz aldatzen baduzu.

- ♦ **Salbuespenak.** Zenbaitetan zure datuak tratatu ahal izango dira zure adostasunik gabe:
 - Zure bizi interesak babesteko.
 - Lege batek erakunde bat gaitzen badu horretarako.
 - Zure datuak jendearen eskurako iturrietan daudenean.



Datu pertsonala da identifikatutako edo identifikagarri diren pertsona fisikoei buruzko informazioa, adibidez, izena eta abizenak, NANA, posta elektronikoa edo IP helbidea.

Ez ahaztu besteek ere eskubideak dituztela

- ♦ Ez eman inoiz hirugarrenei buruzko informazio pertsonalik. Ezin duzu beste pertsona batzuei buruzko datu pertsonalen gaineko erabakirik hartu, ez badizute **baimenik eman** behintzat, edo horien tutorea edo legezko ordezkaria ez bazara.

Datuak babesteko eskubideari buruz informazio gehiago nahi baduzu, datu babesari buruzko **herritarren gida** liburua ikus dezakezu. Datu babesari buruzkoa da eta Datuak Babesteko Espainiako Agentziak argitaratua. Beste aukera bat da herritarrentzako kanaletara jotzea:

www.agpd.es eta
www.avpd.eus

Nola ezabatu ditzaket bilatzaile baten emaitzetan dauden nire datu pertsonalak?

“Kreditu pertsonalei buruzko informazioa eskatzeko web orri batean erregistratu nintzen, eta azkenean nomina eta etxeko eskuragarri eman nizkien. Ondorioz, informazio guztia eskuragarri geratu zen sarean. Nahikoa da nire izena idaztea Interneteko bilatzaile batean.”



Batzuetan, uste dugu web bat fidagarria dela eta helburua argi dagoela, bere itxuragatik, eta lasai asko ematen dugu gure informazio pertsonala, behar den bezala jakin gabe nola tratatuko duten eta zertarako erabiliko duten informazioa; eta hori ez da zuzena, informazioaren gaineko kontrola gal dezakegulako.

Ikasi behar duzu nola erabili zure eskubideak sarean Badakizu zergatik?

Web gune guztiek jaso behar dute tokiren batean **lege-oharra** eta **pribatutasun politika**. Hor adieraziko da zein pertsona edo erakunde den webaren eta eman dituzuen datuen tratamenduaren arduraduna. Gainera, zerbitzuaren arduradunek azaldu behar dizute nor diren, non dauden kokatuta eta nola jar zaitezkeen harremanetan beraiekin.

Beraz, webetan gutxienez honako informazioa agertu behar da:

- ♦ Izen soziala, IFK, sozietatearen helbidea (posta helbidea), merkataritza informazioa eta abar.
- ♦ Nola tratatuko dituzten zure datu pertsonalak eta nola baliatu ditzakezun **zure eskubideak** ([aepd](#), [ddeb](#)) datu pertsonalak direla eta.



Datu pertsonalak inori eman aurretik, enteratu ondo zertarako nahi dituzten, nork tratatuko dituen eta nola baliatu zure eskubideak.

Aholkuak eta gomendioak

- ♦ Datuak **atzitu**, **ezereztu**, **zuzendu** nahi baduzu, edo **aurka** ([aepd](#), [ddeb](#)) egin nahi badiozu datu tratamendu jakin bati, webaren titularraren aurrean egikaritu behar dituzu zure eskubideak. Lege-oharrak dio nor den titularra.
- ♦ Nahi baduzu zure informazio pertsonala ezabatu interneteko bilatzaileak eskubide hau baliatu dezakezu: **ahaztua izateko eskubidea** ([aepd](#), [ddeb](#))
- ♦ Zure eskubideak baliatu eta erantzunik ez baduzu jaso edo ez bazaude ados jasotako erantzunarekin, Datuak Babesteko Espainiako Agentziak (AEPD) lagunduko dizu **zure eskubideak** babesten ([aepd](#), [ddeb](#)).
- ♦ Datuak Babesteko eskubideari buruz gehiago jakin nahi baduzu, gida hau ikus dezakezu: **herritarrentzako gida**, Datu babesari buruzko oinarritzko eskubideari buruzkoa eta AEPDk egina.



Gogoan izan

Ez fidatu zure informazio pertsonala eskatzen dizuten web gunez, ez badizute esaten nor den tratamenduaren arduraduna, zertarako erabiliko dituzten datuak eta nola egikaritu ditzakezun zure eskubideak.

Nola erabili behar dut nabigatzailea, *ez ditzan gorde* Interneten ematen ditudan urratsak?

“Nabigatzaileek modu pribatuan nabigatzeko aukera ematen dute, baina zer esan nahi du horrek? Seguruagoa da horrela nabigatzea?”



Interneten nabigatzen duzunean, nabigatzailean egiten duzun guztia zuzenean gordetzen da ordenagailuaren edo gailuaren memorian, ez da desagertzen, eta, beraz, erraz jakin daitezke une jakin batean Interneten eman dituzun urratsak. Halakorik ez gertatzeko, eta batez ere gailu publikoak erabiltzen badituzu edo beste pertsona batzuekin partekatzen baduzu, nabigatzaileek honako aukera eskaintzen dute: “nabigazio pribatua”.

Jakin behar duzu zer nolako informazioa darabilten nabigatzaileek. Badakizu zergatik?

Garrantzitsua da jakitea nabigatzaileek zuri buruzko zein informazio duten eta informazioa behar bezala kudeatzeko eskaintzen dituzten aukerak, honakorik ez baduzu nahi:

- ♦ Interneten zertan ibili zaren jakitea nabigatzaile berbera erabiltzen duen edonork.
- ♦ Agerian uztea Interneten zertan ibiltzen zaren eta zure zaletasunak sarean.
- ♦ Web gune jakin batean saio bat hasia eta zabalik geratuz gero nabigatzailean, baten batek zure identitatea ordezkatzeari.



Nabigazio pribatuari esker, inork ezin du jakin zein orritan ibili zaren, zer erosi duzun, zer publizitateri erreparatu diozun, eta abar.

Aholkuak eta gomendioak

Berdin dio zein nabigatzaile erabiltzen duzun, kontua da beti hartu behar dituzula neurriak ahalik eta arrisku gutxien izateko Interneten nabigatzen duzunean.

Beti egongo da gailua galdu edo lapurtzeko arriskua. Beraz:

- ♦ Eduki nabigatzailea eguneratuta. Beti azken bertsioa.
- ♦ **Aukeratu konfiantzazko osagarriak eta pluginak.** Deskargatu konfiantzazko eta ospe ona duten lekuetatik bakarrik, adibidez, nabigatzaileen orrialde ofizialetatik.
- ♦ Instalatu web orrien egiaztatzaile bat. Normalean antibirus ezagunenean eskaintzen dute.
- ♦ Berrikusi konfigurazio aukerak nabigatzailean, eta gaitu interesgarrienak iruditzen zaizkizunak zure pribatutasuna babesteko eta seguruago egoteko.
- ♦ Ezabatu nabigazio historiala ez duzunean behar.
- ♦ **Ezabatu cookieak.** Bisitatzen dituzun tokiei buruzko informazioa gordetzen duten fitxategi txikiak dira.
- ♦ Erabili pasahitzen kudeatzaile bat zure sarbide gakoak gordetzeko eta babesteko. Horrela, behintzat, zure nabigatzaileek ez dituzte zure pasahitzak kudeatuko.
- ♦ **Itxi beti saioa**, web batean sartu bazara eta erabiltzailearekin eta pasahitzarekin autentifikatu baduzu zeure burua. Saioa ixten baduzu eta baten batek erabiltzen badu zure ordenagailua edo gailu mugikorra, ezin izango du zure informazio pertsonalik ikusi. Bai, ordea, saioa zabalik badago.



Nork ikus dezake sare sozialetan **argitaratzen** dudana?

“Sare sozialean dudan profila konfiguratut, bakar-bakarrik lagunek ikus dezaten, baina ez daukat argi beste pertsona batzuk ere ikus dezaketen zer argitaratzen dudan.”



Jakin behar duzun lehenengo gauza da sare sozialek hainbat baliabide jartzen dizkizutela eskura, beste pertsona batzuekin zure bizitza pertsonalari edo profesionalari buruzko informazioa zabaltzeko edo partekatzeko. Baina, kontuan izan, ezabatzen baduzu ere, erregistratuta geratuko dela gutxienez sare sozialaren zerbitzarietan, eta ikusi duen orok erabili ahal izan duela, kopiatuz edo zabalduz.

Ondo pentsatu, sarean informazioa argitaratu aurretik. Badakizu zergatik?

Argi izan behar duzu sare sozial batean partekatzen duzun informazioa **beste pertsona batzuek** ikus dezaketela, zuk jakin gabe. Hori gerta daiteke zuk zure gauzetan sarbidea ematen diezulako pertsona batzuei eta horiek aldi berean beste batzuei: lagunei, lagunak lagunei edo mundu guztiari. Beraz, itxura batean kontrolpean duzula badirudi ere norekin partekatzen dituzun zure bizitza pribatuko kontuak, gerta ahal zaizu informazioaren gaineko kontrola galtzea. Adibidez, argazki bat partekatu duzu zure kontaktuekin, eta batek “Atsegin dut” klikatu du. Orain ez dakizu zure lagun horren beste lagun batek ikus dezakeen zure argazkia.



Sare sozialetan informazioa argitaratu aurretik, ondo pentsatu zer partekatu nahi duzun eta norekin

Aholkuak eta gomendioak

Beharrezkoa den informazioa argitaratu, gehiago ez!

Sare sozial batzuek datu asko eskatzen dituzte erregistratzeko: helbidea, lantokia, eskola, gustuak, zaletasunak. senideak eta abar, eta ez dira beharrezkoak. Ondo pentsatu zein informazio pertsonal eman nahi duzun.

Komeni da **datu batzuk ez argitaratzea zure profiletan**, ez baduzu nahi zure pribatutasuna kaltetzea eta argitaratutakoa zure kontra etortzea edo arazo pertsonalak eta laneko arazoak ekartzea.

- ♦ Datu pertsonalak
- ♦ Pasahitzak
- ♦ Bankuko datuak
- ♦ Telefono mugikorra
- ♦ Oporretako planak
- ♦ Portaera desegokiak
- ♦ Irainak, hitz itsusiak
- ♦ Medikatuak edo osasunari buruzkoak



Sare sozial batean duzun profila ez da izan behar ate bat zabalik zure intimitatean

Gainera, urteak igaro ahala, Interneten argitaratzen duzunak **zure ospe digitala** eratzen du. Gerta daiteke enpresek, lagunek eta abarrek zuri buruzko irudi bat egin izana, argitaratuta ikusi duten zure informazioaren ondorioz.

Zure informazioa, zuk nahi duzunak bakarrik ikus dezala!

Berrikusi **konfigurazioko aukerak** sare sozial guztietan, eta horrela kontrolpean izango dituzu pribatutasunaren eta segurtasunaren alderdi garrantzitsuenak:

- ♦ Jakitea ea nork ikus ditzakeen zure argitalpenak
- ♦ Jakitea ea nork etiketatu ahal zaituen
- ♦ Jakitea ea zure profila ikusgai dagoen Interneteko bilatzaileetan
- ♦ Jakitea argitalpenen eta abarren geokopakena

Ez badakizu nola egin, ikusi sare sozialetako segurtasunari buruzko bideoak. Bideoetan dago azalduta urratsez urrats nola konfiguratzea pribatutasuneko eta segurtasuneko aukerak (**bideotutorialak**):

- ♦ [Instagram](#)
- ♦ [Facebook](#)
- ♦ [Twitter](#)
- ♦ [Snapchat](#)
- ♦ [Whatsapp](#)
- ♦ [Youtube](#)



Zure ospe pertsonala edo soziala eta zure ospe digitala batera doaz



“WhatsAppeko mezu bat jaso dut eta dio 50 €-ko kupoi bat irabaz dezakedala denda ospetsu batean gastatzeko. Dirudienez, kupoia jasotzeko, galde-sorta txiki bat bete behar dut eta sustapena bidali 10 laguni. Sinetsi egin behar dut?”

Nola antzeman elementu susmagarriak eta erne ibili

Komeni da jakitea nolako **iruzur estrategiak** erabiltzen dituzten ziberdelitugileak, horrela erne egongo zara. Adi egon honakoak jasotzen badituzu:

- ♦ **Kontaktu ezezagunen mezuak**
 - Ez badakizu nor den, hobe da ez gehitzea kontaktueta.
- ♦ **Web orrietan sartzeko estekak**
 - Ez egin klik ez badakizu zein orritara bidali behar zaituen; eta are gutxiago **esteka hautsita** badago.
- ♦ **Gezurrak eta mezuak bata bestearen segidan**
 - Ez birbidali. Informazioa egiaztatu, eta ziurtatu jaso duzun informazioa egiazkoa dela. Jarri arreta berezia mezuan:
- ♦ **Alarmista bada**
 - Esaten dizutena egin ezean, zerbait gertatuko bada.
- ♦ **Informazio pribatua eskatzen badu**
 - Datu pertsonalak, bankukoak eta abar.
- ♦ **Sariak / kupoiak / zozketak badauzka**
 - Zer edo zer agintzen badizute inkesta bat betetzeagatik, aplikazio bat jaisteagatik, telefono zenbakia emateagatik eta abar.



WhatsAppek eta berehalako mezularitzako gainontzeko aplikazioek funtzionalitate asko dituzte: testu-mezuak, bideoak, argazkiak eta abar jaso eta bidaltzea...; eta Interneteko beste zerbitzuek (adibidez, posta elektronikoa eta sare sozialak) dituzten arrisku bera dute: spamak, gezurrak, azpilapurretak, iruzurak, malwarea eta abar.

Aholkuak eta gomendioak

Zein arrisku gehiagoren eraginpean zaude berehalako mezularitzako aplikazioak erabiltzen badituzu?

Arriskuak pribatutasunerako

- ♦ Ez baduzu nahi zuri buruzko informazioa publikoa egitea, hobe da txat bidez ez baduzu zabaltzen, ez dakizulako zure kontaktuek zertarako erabili dezaket. **Bizpahiru aholku:**
- ♦ **Profileko argazkia**
 - Aukeratu berezitasunik ez duen argazki bat.
- ♦ **Erabiltzaileak blokeatu**
 - Zeuk erabaki norekin komunikatu nahi duzun eta norekin ez.
- ♦ **Egoerari buruzko informazioa**
 - Ez erabili egoera zuri buruzko informazio pribatua eskueran jartzeko.



Profileko argazkia



Erabiltzaileak blokeatzea



Egoerari buruzko informazioa

- ♦ Ziurtatu **mezu trukea zifratuta dagoela**, horrela, edozeinek antzemanda ere, ezin izango ditu ulertu.
- ♦ Erabili **txat pribatuaren eta ledo sekretuaren aukera** eta ez utzi elkarriketarekin zer ikusirik ez duen inori zelatan ibiltzea.
- ♦ Egin **segurtasun kopiak** ez badituzu galdu nahi txateko mezuak.

Nortasuna faltsutzea

Smartphonetako berehalako mezularitzako aplikazioek (**app-ek**) ez dute erabiltzailea eta pasahitza eskatzen erabiltzen ditugun bakoitzean. Horrek esan nahi du smartphonea galtzen badugu edo lapurtzen badigute, aurkitzen duenak mezuak bidali ahal dizkiela biktimaren kontaktu guztiei, biktima ordezkatzuz.



- ♦ Ezarri **blokeo pasahitz** bat smartphonean, eta horrela ezin izango dute erabili zure baimenik gabe.

Interneten argitaratzen den **informazio guztia** egia da?

“WhatsAppen alerta bat jaso dut sarean dabilen uestezko iruzur bati buruzko informazioa lortzeko, baina klikatu dudanean bidali didaten estekan, app bat hasi da bera bakarrik instalatzen.”



Ziberdelitugileak nahi zutena lortu dute: zure arreta. Sinestarazi dizute klik egin eta informazioa jasoko zenuela, eta benetan gertatu dena izan da gezurra zela eta lortu dutela zuk zeuk instalatzea app gaizto bat zure gailuan. Antzekorik gertatuz gero, aplikazioa instalatzea onartu aurretik, begiratu Interneten eta enteratu ea zer dioten horri buruz. Batzuetan bilaketa txiki bat eginda, izena adibidez, informazio baliagarria jasotzen da.

Zer jakin behar duzun Interneten dabilen informazioari buruz

Sarean **gezur ugari eta egiazkoak ez diren berri** asko dabil, eta halako berriak jasotzen dituzten pertsonak sinetsi eta arduratu egiten dira. Askotan, gezurrezko berri horien helburua da **zu engainatzea** eta lortzea birus batekin kutsatutako web batean sar zaitezen, software gaiztoa zabaltzeko. Beste zenbaitetan gezurrezko berrien helburua da dena delako web batek jasotzen dituen bisita kopurua handitzea, lortzeko web horrek diru-sarrera gehiago izatea, edo zure datu pertsonalak edo pasahitzak biltzea, besteak beste.

Beraz, kontuan izan:

- ♦ Mezu horien atzean ezkutuan egon daitezke **phishing kanpainak**.
- ♦ Mota horretako mezu segida batean klikatzen baduzu edo birbidaltzen baduzu, zuri buruzko edo hirugarrenei buruzko informazio pertsonala bidaltzen diezu pertsona ezezagunei.
- ♦ Askotan helbide elektronikoak, datu pertsonalak, kontaktuen zerrendak, zein gailu mota erabili den, eta abar lortu nahi izaten dituzte, eta dirua irabazteko erabiltzen dute informazioa.

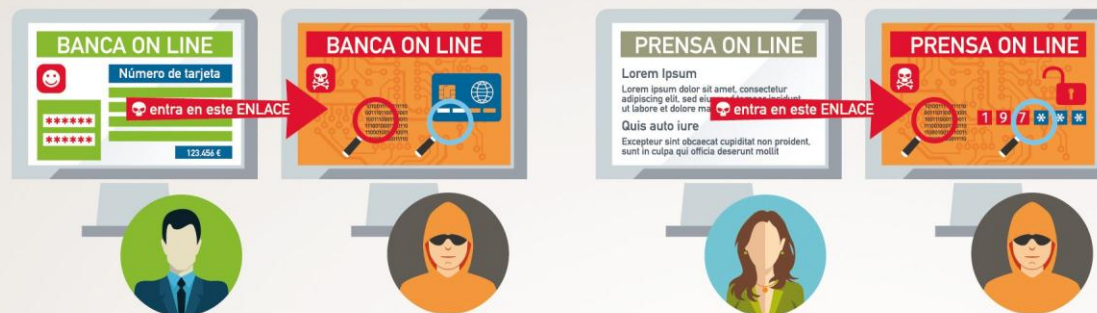


Ez zaitez fidatu mezu segidez

Ez klikatu mezu horietako estekarik

Ez instalatu aplikaziorik (app) berri bat ikusteagatik

Aholkuak eta gomendioak



- ♦ Ospe oneko erakundeek euren web orriak eta komunikabide ofizialak erabiltzen dituzte bezeroekin komunikatzeko. Besteak beste, sare sozial bateko, bankuko edo beste edozein zerbitzu ezaguneko mezurik jasotzen baduzu, ez ireki mezurik eta sartu zuzenean web orrian, nabigatzailean URLa idatzita.
- ♦ Garrantzi handiko benetako alerta bat jasotzen baduzu, komunikabideetan ere ikusi edo entzungo zenuen. Begiratu komunikabide garrantzitsuenen web orrietan.
- ♦ Ez baduzu argi mezu bat egiazkoa den ala ez, zuzenean galdetu tartean dagoenari.
- ♦ **Ez ezazu birbidali mezu segida alarmistarik**, batez ere mezuaren estekak bidaltzen bazaitu ezagutzen ez ditugun aplikazioak dauden webetara edo deskarga-webetara.
- ♦ Berrikusi zure mezularitza-aplikazioen eta sare sozialen konfigurazioa, beti jakiteko nor jar daitekeen zurekin harremanetan.

“Mezu elektronikoa bat jaso dut eta mezuak dio nire kontu korrontea eguneratu behar dudala, eta, horretarako, esteka bat klikatu behar dudala. Baina, susmagarria egin zait bankuko URLa betikoa ez izatea. Bankura deitu dut eta esan didate phishing izena duen iruzur ezagun bat dela”.



Internet erabiltzen dugunean arrisku askorekin egin dezakegu topo. Horietako bat phishinga da. Ziberdelitugileek teknika hau erabili ohi dute erabiltzaileen datu pertsonalak eta bankuko datuak lortzeko, eta, horretarako legezko erakundeak ordezkatzan dituzte, adibidez, bankuak, sare sozialak, erakunde publikoak eta abar.

Nahitaez jakin behar duzu zer den phishinga

Esan behar da **phishinga** abian jartzen **duten** ziberdelitugileek **ingeniaritza soziala** erabiltzen dutela guri buruzko informazio pribatua eskuratzeko. Gure arreta bereganatzen dute edozein aitzakia erabilita, eta itxura batean enpresa edo zerbitzu jakin bateko benetako web orriak diruditen iruzurrezko web orrietara bideratzen gaituzte.

Mezuak bidaltzea ahalbideratzen duen sistema oro erabil daiteke gure informazio pribatua lapurtzeko tresna gisa. Batzuetan gure informazio pertsonala lapurtzen saia daitezke mezu elektronikoen bidez, SMS edo MMS mezuen bidez (**smishing**), bai eta berehalako mezularitzako bestelako tresnen bidez (WhatsApp, LINE, eta abar).



Aholkuak eta gomendioak

Hona hainbat trikimailu phishinga saihesteko

- ♦ Zuhur jokatu banku edo zerbitzu ezagunen itxura duten mezuekin, batez ere honako gaiak aipatzen badituzte:
 - ♦ Ordezkatu duten erakundearen arazo teknikoak.
 - ♦ Erabiltzailearen kontuan segurtasun eta pribatutasun arazoak.
 - ♦ Iruzurrak saihesteko segurtasun gomendioak.
 - ♦ Erakundearen segurtasun politika aldatzea.
 - ♦ Produktu berrien sustapena.
 - ♦ Deskontu baleak, sariak edo opariak.
 - ♦ Zerbitzua eten edo desaktibatuko dutela.
- ♦ Hartu susmo txarra testuak akats gramatikalak baditu.
- ♦ Erne komunikazio anonimoak jasotzen badituzu eta hartzailearen lekuan honakoak badatoz: “Bezero estimatua”, “Jakinarazpena erabiltzaileari” edo “Lagun hori”.
- ♦ Mezuak badio erabaki potolo bat hartu behar dugula oso denbora tarte txikian, hori seinale txarra da. Jarri harremanetan zerbitzuarekin beste kanalen bat erabiliz, eta galdetu ea presa egiazkoa den ala ez.
- ♦ Begiratu ondo ea estekan idatzita dagoena bat datorren hor agertu beharko zen helbidearekin.
- ♦ Ospe ona duten zerbitzuek euren domeinuak izan ohi dituzte posta elektronikoko korporatiboaren helbideetarako. Erne, era honetako postontzietatik komunikaziorik jasoz gero: @gmail.com edo @hotmail.com.

Zer egin behar duzu phishing saiakera bat atzematen baduzu?

- ♦ Ez erantzun sekula halako mezuei. Zalantzarik baduzu, galdetu zuzenean enpresari edo zerbitzuari edo **jarri gurekin harremanetan** eta galdetu guri.
- ♦ Ez sartu mezuan jasotako esteketan, eta ez jaitsi mezuari atxikitako dokumenturik..
- ♦ Ezabatu, eta nahi baduzu, eman iruzur saiakeraren berri kontaktuei.



Ez egin klik mezu bidez jasotako esteketan, identifikatu egin behar bazara edo informazio pertsonala eman behar baduzu, dena delako web gune batean sartzeko

Zer gertatzen zaio nire *Interneteko konexioari!*

“Etxeko wifia gero eta astiroago dabil, nahiz eta inor ez egon konektatuta, baina routerra itxuraz badabil. Zerbitzu teknikora deitu dut eta esan didate konexioa ondo dabilela. Auzokoa konektatu ote da?”



Gero eta etxeko tresna gehiagok dute wifi konexioa: hozkailuek, telebistek, inprimagailuek eta abar. Gainera, etxean gero eta gailu eramangarri eta ordenagailu gehiago ditugu. Beraz, etxea babestu behar dugu “lapur zibernetikoak” ez daitezen sartu konexioaren bidez.

Jakin egin behar duzu zer arrisku dakarren baten batek zure wifia erabiltzea zure baimenik gabe

♦ Banda zabalera murriztea

Norberaren gailuen konexioa trabatu dezakete gailu arrotz asko konektatzen badira eta sarea erabiltzen badute.

♦ Transmittutako informazioa lapurtzea

Konfigurazioa ez badago ondo eginda, erasotzaileek erraz lapurtu dezakete bidaltzen ari zaren informazioa.

♦ Gure gailuekin konektatzea zuzenean

Erraza da ezezagunen bat sartzea konektatua dauden gailuetan, behar besteko prestakuntza badauka eta gailuek segurtasun arazoak badituzte edo instalazioek ez badute segurtasun nahikorik.

♦ Legez kanpoko ekintzengatik erantzukizuna

Interneteko konexio bat kontratatzen duzunean zerbitzuen hornitzaile batekin, konexioa zure izenari lotzen zaio, eta IP helbide bat esleitzen zaizu, Interneten identifikatzen zaituena. IP horretatik burutzen den edozein ekintza zuri lotuta agertzen da.

Aholkuak eta gomendioak

Ondo konfiguratu wifi konexioa:

- 1 Enteratu zein den zure routerarren IP helbidea.
- 2 Sartu routerarren administrazio orrian.
- 3 Aldatu defektuz dakarren administrazio-sarbideko pasahitza.
- 4 Aldatu wifiaren edo SSID sarearen izena.
- 5 Konfiguratu wifia WP2 erako zifratua erabil dezan.
- 6 Sortu pasahitz sendo bat wifi-sarbiderako.
- 7 Begiratu zure gailuen MAC helbidea eta ezarri. Mac bidezko iragazketa routerrean.
- 8 Itzali routerra ez baduzu erabili behar.



Halako gauzak beti inori gertatzen zaizkiola uste baduzu eta zure wifi sarea sekula ez dutela erasoko, kontuz ibili behar duzu, eta zure esku dituzun segurtasun neurri guztiak erabili, inork ez dezan zure konexioa erabili eta arazorik ekarri.

Eta, horrez gain, babestu zure gailuak:

- ♦ Ziurtatu eguneratuta daudela eta azken bertsioa direla.
- ♦ Instalatu antibirusa.
- ♦ Ohiko zereginetarako ez nabigatu eta ez erabili ordenagailua administrariaren erabiltzailearekin.
- ♦ Erabili pasahitz onak.
- ♦ Ez exekutatu programarik eta ez jarraitu estekarik posta elektronikoz heldu bazaizu eta edukia eta IP helbide bat esleitzen zaizu, Interneten identifikatzen zaituena. IP horretatik burutzen bada, iruzurrak edo malwarea saihesteko.
- ♦ Ez konektatu gailu aldagarriak, ez badakizu zer daukan barruan edo nondik datorren.
- ♦ Gailuak kamera badauka, estali, ez baduzu erabili behar.



Nire **posta elektronikoa** babestu nahi dut

“Lagun baten mezu bat jaso dut esanez mezu elektroniko bat bidali diodala eta mezuari atxikita birus bat. Baina, nik ez diot bidali. Posible da norbait nire postontzian sartu izana? Zer gertatu ote da?”



Norbaitek gure helbide elektronikoa lortzen badu —blog edo foro batean argitaratuta zegoelako, edo mezu elektronikoaren segidak bidali ditugulako, edo gezurrezko lehiaketak, sustapenak eta sariak eskaintzen dituzten web orrietan parte hartu dugulako, halakoetan parte hartzeko helbide elektronikoa bezalako datuak eman behar izaten direlako, edo birus bat sartu zaigulako eta abar—; eta gainera postontzian sartzeko erabiltzen dugun pasahitza ez bada oso segurua, nahikoa erraza da norbait sartzea gure postontzian eta mezu pribatuak irakurtzea, aldatzea edo ezabatzea, mezu elektronikoak bidaltzea gure izenean, postari lotutako pribatutasun eta segurtasun aukerak aldatzea eta abar.

Zer gerta daiteke norbait sartzen bada zure posta elektronikoan?

Pribatutasuna galtzea

Zure elkarrizketa pribatuak agerian geratuko dira.

Zure kontaktuak eta bidali eta jaso duzun dokumentazio garrantzitsua lortu ditzakete:

- ♦ Ordainagiriak
- ♦ Nominak
- ♦ NANA
- ♦ Argazkiak
- ♦ Bideoak
- ♦ eta abar.

Segurtasun arazoak

Ezin izango zara zuren kontuan sartu, norbaitek zure pasahitza edo kontua berreskuratzeko bestelako aukerak aldatzen baditu:

- ♦ Beste helbide elektroniko bat, telefono zenbaki bat eta abar.

Beste zerbitzu batzuk badituzu helbide elektroniko berera atxikita, horiek ere kalteren bat jasan dezakete:

- ♦ PayPal
- ♦ Amazon
- ♦ Facebook
- ♦ Dropbox
- ♦ eta abar.

Nortasuna faltsutzea

Edonolako mezu elektronikoak bidali ditzakete zure izenean:

- ♦ Zure ospea kaltetzeko
- ♦ Beste pertsona batzuk ziberjazartzeko
- ♦ **Iruzurrezko mezu** elektronikoak bidaltzeko: **phishinga**, malwarea, scam-a, eta abar.

- ♦ Gezurrak / hoax-ak eta spama / gogoz kontrako publizitatea jartzea abian.



Aholkuak eta gomendioak

Posta elektronikoa tresna zoragarria da, eta aukera asko eskaintzen dizkizu lanean zein esparru pribatuan. Baina, zuhur jokatu behar duzu erabiltzen duzunean. Beraz, kontuz ibili eta egin kasu honako aholku hauei:

- ♦ Ziurtatu **pasahitz sendoa** duzula eta ez duzula beste zerbitzu baterako erabiltzen.
- ♦ Zerbitzu batek eskaintzen badizu, aktiba ezazu **bi urratseko egiaztapena** segurtasun geruza osagarri bat gehitzeko autentifikazio prozesuari.
- ♦ Ahal bada ez eman zure pribatutasuna kaltetu dezakeen informaziorik; baina, beste aukerarik ez baduzu, **zifratu edo konprimatu fitxategiak pasahitz bat ipinita**, eta zuk eta mezu elektronikoa jasoko duenak bakarrik jakin behar duzue.
- ♦ Ez ireki erabiltzaile ezezagunen mezurik eta ezabatu: malware-dun fitxategiak izan daitezke, orri gaiztoetara bidaltzen duten estekak eduki ditzakete edo norbaiten identitatea ordezkatu dezakete eta abar.
- ♦ Mezuaren bidaltzailea ezaguna bada ere, mezua susmagarria iruditzen bazaizu, galdetu zuzenean bidaltzaileari ea ez ote duten faltsutu bere **e-postaren helbidea**.
- ♦ Ez ahaztu segurtasun kopiak egitea ez galtzeko balioko informazioa, gerta daitekeelako posta zerbitzariarekin arazoak egotea.



Zer hartu behar dut kontuan nire informazio pertsonala **hodeian** gordetzen badut?

“Bigarren eskuko tablet bat erosi dut, eta etxera heldu naizenean eta wifia konektatu dudanean konturatu naiz saldu didanak ez dituela ezabatu instalatuta zeuzkan aplikazio batzuen konfigurazioak, adibidez: Google Drive eta Dropbox. Beraz, hodeian gordeta daukan informazio pertsonalean sar naiteke.”

Informazio pertsonala gorde nahi baduzu hodeian, zer egin behar duzu?

Hodeiak abantaila handiak ditu inondik ere:

- ♦ Zure informazioa eskuragarri edukiko duzu beti, Interneteko sarbidea duzun edozein tokitan.
- ♦ Ez da galduko, nahiz eta mugikorra edo tableta galdu edo lapurtu. Informazioa zerbitzuaren zerbitzarietan gordetzen da. Segurtasun kopiak bezalakoak dira.
- ♦ Informazioa erraz partekatu dezakegu nahi dugunekin, pendriverik, disko gogorrik eta halakorik erabili beharrik gabe.
- ♦ Gailu mugikorrek ordenagailuarekin sinkronizatu ditzakezu, guztietatik izateko sarbidea zure informazioan.

Ez ipini arriskuan zure informazioa. Kontuan izan informazioa **ondo babestuta eduki ez**, eta zerbitzuan sartzeko pasahitza ahula delako, zerbitzarian segurtasun huts bat gertatu delako, hacker batek eraso egin duelako edo gailua lapurtu dizutelako, zure informazioa baimenik ez duten pertsonak ikusteko moduan gera daitekeela edo desagertu egin daitekeela, bereziki zerbitzua ixten badute eta **segurtasun kopiarik ez baduzu beste euskarri batean.**

Hodeiko biltegi-zerbitzuak aproposak dira gure fitxategietan sartzeko edozein lekutatik eta edozein gailurekin, smartphoneak eta tabletak barne; eta horrez gain, informazioa antolatzeak karpetak sor ditzakegu eta fitxategiak partekatu era bai, behar izanez gero. Gainera, aukera dugu gure gailuko karpeta bat hautatzeko eta, automatikoki hodeiko zerbitzuarekin sinkronizatzeko; horrela, gure informazioaren segurtasun kopia bat sor dezakegu linean. Hala ere, abantailak batzuetan arazo bihur daitezke. Beraz, hobe segurtasun eta pribatutasun neurri egokiak hartzea.

Aholkuak eta gomendioak

Aukeratu **zure beharretara ondoen egokitzen diren biltegiaratzeko aukerak eta zerbitzuak**, irakurri ondo baldintzak eta betebeharrak, onartu aurretik, eta zerbitzuak erabiltzen badituzu, kontuan hartu honako aholkuak:

- ♦ Ziurtatu hodeiko zerbitzurako sarbidea HTTPS protokoloarekin dela.
- ♦ Konfiguratu ondo zerbitzuak ematen dituen pribatutasuneko eta segurtasuneko aukerak.
- ♦ Segurtasun hobia izateko, **zifratu zure datu** konfidentzialenak, hodeiko zerbitzura igo aurretik.
- ♦ Erabili sarbideko **pasahitz sendo bat** eta ez partekatu inorekin.
- ♦ Egin **segurtasun kopiak** beste euskarri batzuetan.
- ♦ Eta **fitxategiak** partekatzen badituzu, ziurtatu hartzaila benetan dela uste duzuna.



**zerbitzurako
sarbideak
https://
protokoloarekin**



**konfiguratu
segurtasun
aukerak**



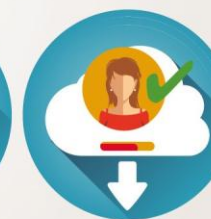
**zifratu zure
datuak igo
aurretik**



**erabili
pasahitz
sendoak**



**segurtasun
kopiak beste
euskarri
batzuetan**



**ezagunekin
bakarrik
partekatu
fitxategiak**

Partekatu ditzaket fitxategiak Interneten ?

“Emule instalatu nuen ordenagailuan, eta ohartu gabe karpetak partekatzeko “c:\” aukera hautatu nuen. Ondorioz, aspaldi honetan nire disko gogorra partekatu dut eta informazio asko egon da edonoren eskura...”



P2P motako aplikazioak instalatzen badituzu, adibidez, eMule, Ares edo BitTorrent bezalakoak, egiaztatu nahitaezkoak diren direktorioak bakarrik partekatzen ari zarela (hau da, fitxategiak deskargatzeko behar direnak) eta ez besterik. Hori egin ezean, sarean konektatuta dauden erabiltzaile guztien eskura jartzen ari zara agian pribatuak diren fitxategiak, eta zeure burua estutasunen jar dezakezu.

Jakin egin behar duzu nola konfiguratzen diren ondo P2P erako aplikazioak Badakizu zergatik?

Esan behar da fitxategien transferentziak egiteko, hau da, hirugarrenekin informazioa partekatzeko erabiltzen diren fitxategi guztiek dutela hutsak egiteko aukera eta gailuaren karpeta edo fitxategi bateko informazioa agerian uzteko arriskua (argazkiak, bideoak, ordainagiriak, e-posta, lanak, softwarea, proiektuak eta abar). Beraz, P2P erako aplikazioak erabili aurretik, egiaztatu ea ondo konfiguratu dituzun.



Aholkuak eta gomendioak

- 1 Lehenengo eta behin, ahal bada, erabili ordenagailu desberdinak lanerako eta norberaren gauzetarako edo aisialdirako. Ezinezkoa bada, beste aukera bat dago, oso erraza, eta da erabiltzaile profil bana sortzea, gailua zertarako erabiliko duzun kontuan hartuta. Arazorik egonez gero, kaltea txikiagoa izango da.
- 2 Zifratu informazioa konfidentziala. Konponbide ona izan daiteke. Nahi gabe informazioa partekatzen baduzu, informazioa zifratuta badago, kaltea txikiagoa izango da, informazioa jasotzen duenak ezin izango duelako irakurri deszifratzeko gakorik gabe.
- 3 Egiaztatu sarbide baimenak informazioan sartzeko. Berdin dio gailuaren bidez partekatzen duzun, hodeian partekatzen duzun ala fitxategiak bidaltzeko zerbitzuen bidez egiten duzun. Egiaztatu ea informazioa jasotzeko baimendu dituzun hartzaileak benetan direla informazioa jasoko dutenak.



Erantzukizun-ohar bat jar dezakezu, informazioa jasotzen duenaren erantzukizunari buruz, hain zuzen ere!

Ahal denean, txertatu mezuetan edo dokumentuetan hartzaileak duen erantzukizunari buruzko ohar bat. Hona adibide bat: **“KONFIDENTZIALTASUNA: Mezu hau pribatua da eta atxikitako fitxategiak konfidentzialak dira, eta adierazitako jasotzaileari beste inori ez dagokio. Jasotzaileetako inor ez bazara, jakinaraz iezaguzu, mesedez, eta eskatu nahi dizugu edukia ez koptatzeko eta inori ez jakinarazteko.”**

Oharra ez du esan nahi akatsik ez duzunik egingo, baina, egiten baduzu, eta jaso behar duen hirugarren batek jasotzen badu informazioa, zuk esan diozu zer egin zuzen jokatzeko.

Ez daukat argi zertarako ari den erabiltzen **semea Internet**, zer egin dezaket?

“Azken boladan semea/alaba arraro dabil. Uste dut ordenagailua eta mugikorra semea/alaba aldatzen ari dela, eta ez dakit zer egin jakiteko zertan dabilen eta norekin. Zer egin dezaket?”

Gazteen umore edo aldarte aldaketen oinarrian arrazoi bat baino gehiago egon daitezke: estres emozionala, adinerako egokiak ez diren irudiak ikustegatik edo jazarpen egoerak.

Zergatik da garrantzitsua jakitea zer egiten duten gure seme-alabek Interneten?

Internetek onura asko dakartza seme-alabentzat, eta euren esku jartzen ditu ikasketetarako lagungarri diren lineako hainbat informazio, tresna eta zerbitzu; aisialdirako aukerak ere eskaintzen dizkie eta harremanak izaten ere laguntzen die. Baina, Interneten dabiltzanean arriskuak daude eta jakin egin behar da zer nolakoak diren:

♦ **Eduki desegokiak**

Informazio edo irudi desegokiak, haurren adina, heldutasuna edo sentsibiltatea kontuan hartuta, edo gaigatik edo tratamenduagatik.

♦ **Pribatutasuna galtzea**

Informazio pribatu gehiegi argitaratzea eta haien kontra erabiltzeko arriskua.

♦ **Txarto kudeatzea hirugarrenen informazioa**

Arazoak, baimenik gabe beste pertsona batzuen informazioa argitaratzeagatik edo birbidaltzeagatik.

♦ **Identitatea faltsutzea**

Norbaitek adingabearen nortasuna ordeztu dezake eta bere benetako profilak erabili, edo faltsu bat sortu kalte egiteko.

♦ **Sextinga**

Sexu izaerako norberaren irudiak, bideoak edo testuak bidaltzea.

♦ **Ciberbullyinga**

Nahita egiten den kaltea, behin eta berriz egiten dena berdinen artean, eta bitarteko digitalen bidez egiten dena.

♦ **Groominga**

Heldu bat adingabe batengana hurbiltzea da, Internet bidez, sexu-gogobetetzea lortzeko.



Aholkuak eta gomendioak

Gurasoek gainbegiratzea, laguntzea eta aholkua ematea funtsezkoa da adingabeek Internet modu seguruan eta arduratsuan erabiltzen ikasteko. **Seme-alabei Internet erabiltzen laguntzeko** modurik onena da jaramon egitea konektatuta daudenean. Hona zer egin dezakegun:

- ♦ Jakin zein lagun dituzten Interneten, zein aplikazio erabiltzen duten eta zein zaletasun dituzten.
- ♦ Hitz egin elkarrekin Interneti buruz dakizuenaz eta esperientziak partekatu elkarrekin; horrela, errazagoa izango da seme-alabentzat gurasoei galderak egitea eta kezkak azaltzea.
- ♦ Haiekin batera ibili Interneten. Adibidez, sare sozialetako pribatutasun aukerak konfiguratzeko laguntzea edo Interneten partida bat jokatzea primeran datoz ikusteko zer egiten duten Interneten eta beste ikuspegi batzuk ere azaltzeko, eta sentsibilizatzeko.
- ♦ Gauza bakoitza bere garaian. Egokitu arauak eta mugak haurren adinaren arabera eta haiengan duzun konfiantzaren arabera. Lineako hainbat zerbitzu erabiltzeko, adibidez, sare sozialak, heldutasuna behar da.

Informazio gehiago nahi izanez gero, honako web hauetara jo dezakezu: **Adingabeak OSI** eta **Interneten zeuk erabaki**. Beste gida hau ere gomendatzen dugu: **Garbi jokatu Interneten** (helburua da adingabeari laguntzea jazarpen egoerak antzematen) eta **Erakutsi seme-alabei garbi jokatzen Interneten** (helburu bera du, baina gurasoei eta hezitzaileei zuzenduta).

Guzti horren osagarri, **gurasoen kontrol tresnak** ere erabil daitezke. Hona horien funtzionaltasun aipagarrienak:

- ♦ Ez uztea adingabeari eduki desegokietara sartzen.
- ♦ Mugatzea gailuak eta zenbait aplikazio erabiltzeko denbora.
- ♦ Ez dezala erabili hiztegi desegokia.
- ♦ Monitorizazio lanak egitea, jakiteko zein web orritan ibili diren.

Halakorik erabiltzea erabakitzen baduzu, kontuan izan **seme-alabekin ados jartzea** eta zure erabakiaren berri ematea, haiek uler dezaten zergatik egin duzun.

Adingabearen eta senide eta hezitzaileen arteko harremana eta hezkuntza dira tresnarik onenak. Ezerk ezin ditu ordeztu.



Seguruak dira jarduera fisikoa neurtzen duten **eskumuturrekoak eta erlojuak**?

“Nire kirol jarduera monitorizatzeko eskumuturreko bat erosi dut. Bluetooth bidez konektatzen da nire mugikorrarekin, eta hainbat egunetan soinean eramanez eta gero, ikusi dut nire sare sozialean agertu direla zein ibilbide egin ditudan, nire kokapena eta eguneroko jarduerari buruzko beste datu batzuk. Zer egin dezaket halakorik ez gertatzeko?”

Jakin egin behar duzu zein informazio jasotzen duten wearable deritzen soineko teknologiek. Badakizu zergatik?

Azken boladan merkatuak gainezka egin du soinean eramateko tresnak direla eta. Tresna horiek guri buruzko datu pertsonal mordoa biltzen dituzte eta erraza izan ohi da beste pertsona batzuek jakitea non egon garen une jakin batean, gure adina, egoera fisikoa, ohiturak (noiz joaten garen lotara, jatera, kirola egitera eta abar), eta egunean zehar gure aldarteak izan ditzakeen gorabeheren gaineko balorazioak eskura ditzakete ere bai.

Gainera, gailu horiek eskuratzen duten informazioa sare sozialetan ere argitaratu daiteke; beraz, norbaitek edo erakunde batek nahi izanez gero zuri buruzko informazioa, erraz eskura dezake eta erabili ere bai, profilak behar bezala konfiguraturik eduki ezean.



Erne egon behar duzu, sentore biometrikoek bereziki sentsibleak diren datuak atzematen dituztelako, eta zure osasun egoeraren berri ematen dutelako hain zuzen ere.



Gailu mugikorrek, sentore biometrikoek eta oro har “wearables” deritzen gailu guztiek, bai eta telefono mugikorrean instalaturik dituzun aplikazioek (app) ere, denek dute fabrikatzaileak jarritako konfigurazioa, zuk hobeto kudeatzeko; baina, aldi berean, haiek jaso egiten dute, zuk erabiltzen duzun bitartean, sortzen duzun informazioa. Beraz, kontuz ibili, batzuetan ez daudelako modurik egokienean konfiguraturik.

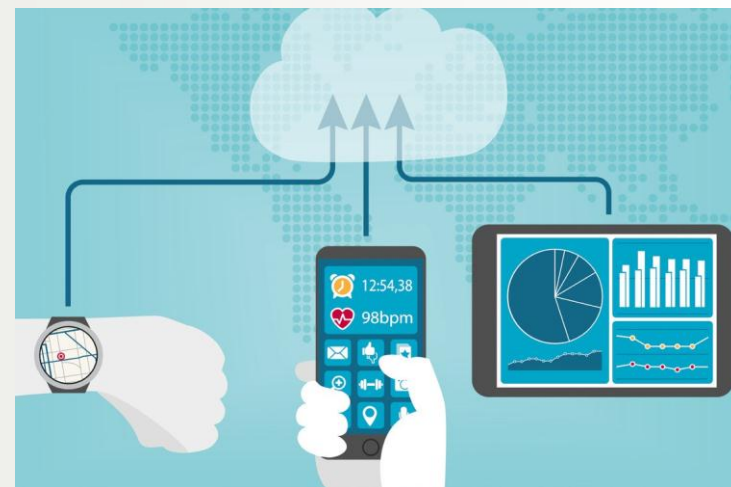
Aholkuak eta gomendioak

Wearableak: erabili aurretik, zer da jakin behar duzuna?

- ♦ Erabiltzen duzu **zifratzeko mekanismorik** zure informazioaren konfidentziasuna bermatzeko?
- ♦ Nork du **sarbidea zure informazio pertsonalean**?
- ♦ Zein **baimen** behar du zure datu pertsonalak tratatzeko dituen aplikazioak (app)?
- ♦ Zein informazio ari zara partekatzen sare sozialetan?
- ♦ **Zuri buruzko informazioa hodeian** biltegitratzen da?
- ♦ Nork eskuratu dezake?
- ♦ Zenbat **denboran gorde nahi dituzu** zure datuak?

Zuretzat wearable egokiena aukeratu.

Nahi baduzu zure jarduera pertsonal guztia monitorizatzeko duen sentore bat erosi, aukeratu aurretik, bilatu prestazio onenak dituenak, eta ez ahaztu ahalik eta segurtasun eta pribatutasun bermerik onenak dituenak aukeratzea, zure informazioa behar bezala erabili eta tratatu dezan.



Kontuan hartzeko oinarritzko konfigurazioak

Berrikusi wearablearekin sinkronizatu nahi duzun sare sozialaren **pribatutasuneko eta segurtasuneko aukerak**, eta **gailuak** dituen konfigurazioak ere bai. Eta hori guzti hori egiteaz gain, gogoratu konfiguratu egin behar dituzula dena delako **wearablea** kudeatzen duen aplikazioaren babes mekanismoak ere.



AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



OSI Oficina
de Seguridad
del Internauta



incibe
2015-2016 TRABAJANDO POR
LA CONFIANZA DIGITAL

Laguntzaileak:

GOBIERNO
DE ESPAÑA

MINISTERIO
DE SANIDAD, SERVICIOS SOCIALES
E IGUALDAD

aecosan
agencia española
de consumo,
seguridad alimentaria y nutrición



Telefonica

Egokitzapena eta itzulpena:

Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos