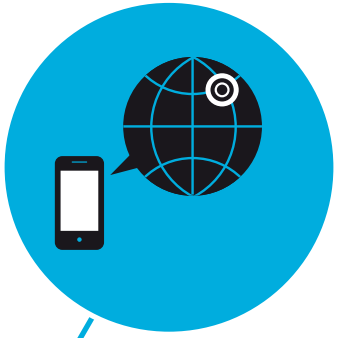
Eusko Jaurlaritzan gailu elektronikoak eta gizarte sareak SEGURTASUNEZ erabiltzeko gomendioak

EUSKO JAURLARITZA
GOBIERNO VASCO

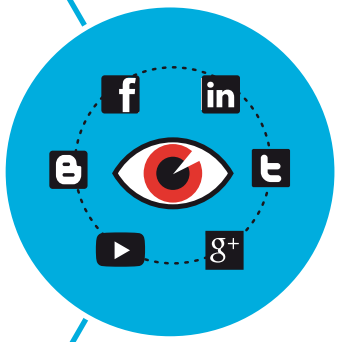
Badakizu geokokapena noiz eta zergatik aktibatu behar duzun?



Zure pasahitz eta ziurtagiri digitalak era egokian erabiltzen dituzu?

Zure aisialdian, zure segurtasunaz arduratzen zara?

Baduzu galdera hauentzat erantzun ziurrik?



Gizarte sareetan segurtasun eta pribatutasun jarraibideak betetzen dituzu?

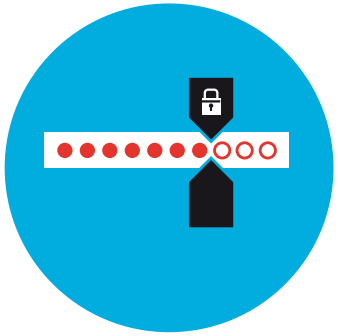
Bidaltzen duzu bereziki babestutako informaziorik WhatsApp-en edo WiFi publiko baten bidez?

Zure gailu mugikorrak eguneratu eta babesten dituzu?

EUSKO JAURLARITZA
GOBIERNO VASCO

Zure pasahitz eta ziurtagiri digitalak era egokian erabiltzen dituzu?

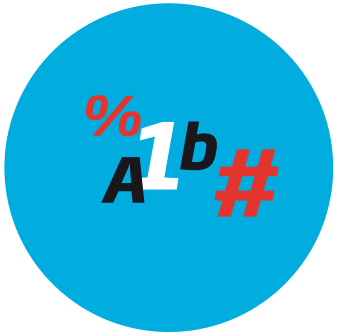
Pasahitz seguru bat izateko baldintzak



Gutxienez, 8 karaktere

Ez erabili 123456, 1q2w3e, 123QWEasd, password, zure izena, beste edozein hizkuntzatan existitzen den hitzik edo zurekin erlaziona daitezken hitzik (zure maskotaren izena, ondorengoenak, etab.).

AEBetako presidenteordetzarako hautagai izandako batek, pasahitz ahula zuen yahoo-ko kontu bat erabiltzen omen zuen bere mezu ofizialetarako, eta ikasle batek kontu hori urratu zuen (2008ko iraila).



Erabili zenbakiak, hizkiak (letra larriz eta xehez) eta ikurrak ($, @, &, #, etab.).

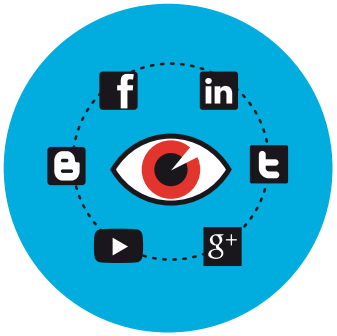
Zuk bakarrik ezagutzen duzun esaldi bat erabili.

EUSKO JAURLARITZA
GOBIERNO VASCO

Zure pasahitz eta ziurtagiri digitalak era egokian erabiltzen dituzu?

Pasahitza zuzen erabili:

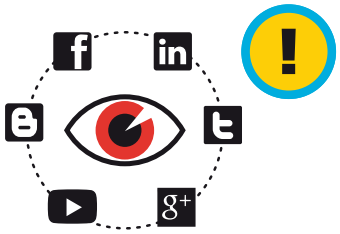
Zure pasahitza nabigatzailean edo mugikorreko aplikazioetan sartzen duzun bakoitzean, gorde nahi duzun galdetzen dizute. Zure gailua beste norbaitek erabiltzen badu, erosotasun horrek segurtasun eza eragin dezake.



Kontuz ibili zure pasahitza zurea ez den ordenagailuren batean sartzerakoan.

Erabili ziurtagiri elektronikoak *(info.+: www.izenpe.com)* ***edo NAN elektronikoa agiriak sinatzeko edo onarpen segurua eskatzen duten prozeduretarako.***

EUSKO JAURLARITZA
GOBIERNO VASCO



Gizarte sareetan segurtasun eta pribatutasun jarraibideak betetzen dituzu?

Segurtasuna eta pribatutasuna gizarte sareetan

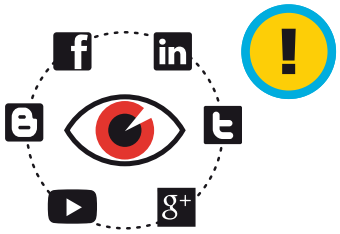
Gizarte sareetan pribatutasuna ziurtatzeko erarik egokiena da gizarte sareetako orrialde hauetan sartzea (beti egoten dira eguneratuta):

Aholkulari famatu batek bere alabari joko baten bidez erakutsi zion zein garrantzitsua den pribatutasuna egoki konfiguratua izatea: bere "laguna" izan gabe, berak aurkitzea nahi izango ez zukeen informazio pertsonala eskuratu zuen (2013ko urtarrila).

- ***Facebook***
- ***Twitter***
- ***LinkedIn***
- ***Google Plus***

Erabili Eusko Jaurlaritzaren Gizarte Sareetako Gida (Irekia) gizarte sareak egoki erabiltzearen inguruan zalantzak dituzun guztietan.

EUSKO JAURLARITZA
GOBIERNO VASCO



Gizarte sareetan segurtasun eta pribatutasun jarraibideak betetzen dituzu?

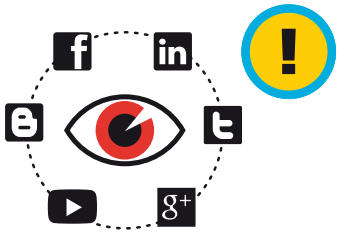
Segurtasuna eta pribatutasuna Facebook-en

Zure kontuaren inguruko aholkuak

- Gida azkarra (Irekia)
- Konfigurazioa
- Babesa
- Lagunak bilatzea eta iradokizunen funtzioa
- Erabiltzaileak blokeatzea
- Bilaketa motorren emaitzetan agertzea
- Aplikazioekin partekatutako informazioa
- Aplikazio bati baja ematea

Bideotutorialak (DBEB)

- Pribatutasun aukerak I
- Pribatutasun aukerak II
- Zerrendak sortu eta kudeatzea
- Kontrolatu "timeline" berria



Gizarte sareetan segurtasun eta pribatutasun jarraibideak betetzen dituzu?

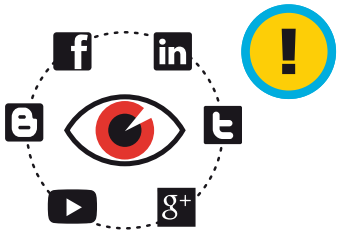
Segurtasuna eta pribatutasuna Twitter-en

Zure kontuaren inguruko aholkuak

- Gida azkarra (Irekia)
- Konfigurazioa
- Babesa
- Txioak ezabatzea
- Kontua ezabatzea
- SPAMaren berri ematea

Bideotutorialak (DBEB)

- Pribatutasun ohar orokorrak
- Pribatutasun aukerak
- Geokokapenaren arazoak

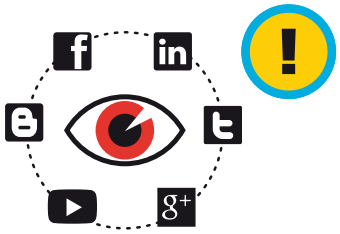


Gizarte sareetan segurtasun eta pribatutasun jarraibideak betetzen dituzu?

Segurtasuna eta pribatutasuna LinkedIn-en

Zure kontuaren inguruko aholkuak

- Konfigurazioa
- Laguntza
- Segurtasun zentroa
- Babestu zure nortasuna
- Babestu zure kontua
- Babestu zure pribatutasuna



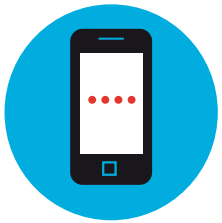
Gizarte sareetan segurtasun eta pribatutasun jarraibideak betetzen dituzu?

Segurtasuna eta pribatutasuna Google Plus-en

Zure kontuaren inguruko aholkuak

- Gida azkarra (Irekia)
- Konfigurazioa
- Zure kontuaren pribatutasuna
- Segurtasuna
- Besteek zure profilarekin eragitea

Zure gailu mugikorrak eguneratu eta babesten dituzu?



Erabili beti SIM txartelaren PINa gailu mugikorretan, eta, badaezpada, aldatu aldizka.

Aktibatu blokeo automatikoaren aukera (Adib.: hatzamarrarekin aktibatu beharreko patroia/PINa/ Pasahitza/blokeo biometrikoa).

Kodetu bereziki babestutako datuak.

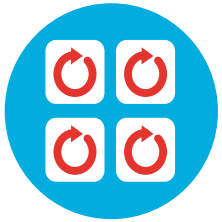
Erabiltzen ez duzunean, itzali pantaila: blokeatu gailu mugikorra. Segurtasuna areagotzeaz gain, bateria aurreztuko duzu.

Lana bukatutakoan, itzali gailu mugikorra. Etenaldietan, hasi eta itxi saioa.

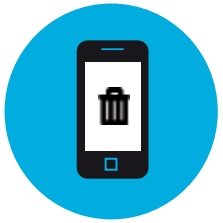
Ez partekatu hirugarrenekin zure informazio pertsonala, ez argitaratu eta ez bidali posta elektronikoz edo berehalako mezularitza bidez.

Egoki konfiguratu haririk gabeko konexioak, erabiltzen direnean bakarrik egon daitezen aktibatuta.

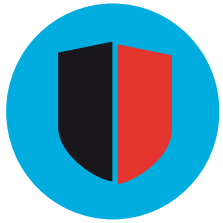
Zure gailu mugikorrak eguneratu eta babesten dituzu?



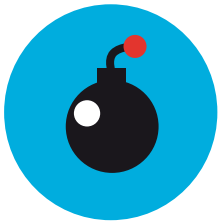
*Gorde zure gailu mugikorraren IMEI zenbakia, gailua galtzen baduzu eskura izateko (markatu *#06#).*



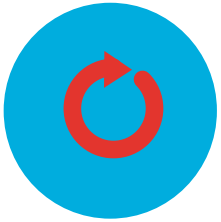
Eusko Jaurlaritzaren terminal bati baja ematen zaionean, telefono-operadoreak informazio guztia ezabatzen du, eta ez dago berreskuratzeko modurik.



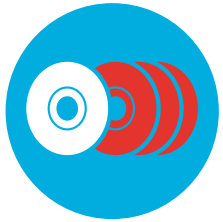
Erabili segurtasun programak: antibirusak, etab. (beti hornitzaile fidagarrienak).



Adi ibili gizarte sareetan argitaraturiko edo masiboki bidalitako mezuen estekekin edo fitxategi erantsiekin, SPAMa edo malwarea izan baitezakete.



Eguneratuta eduki programa, aplikazio eta sistema eragileak. Horiek eguneratzeko mezuak jaso ohi ditugu (baieztapena eskatzen dute).



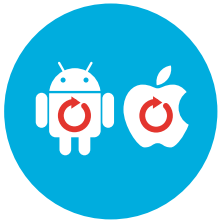
Egin segurtasun kopiak aldizka, prozesu hori automatikoki burutzeko era asko dago.

EUSKO JAURLARITZA
GOBIERNO VASCO

Zure gailu mugikorrak eguneratu eta babesten dituzu?

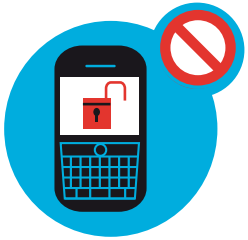
Kontuz ibili ezezagunengandik jasotako SMS, mezu elektroniko eta estekekin.

Ez instalatu jatorri ezezagunetako aplikaziorik (soilik jatorri ofizialetakoak, adib.: Apple Store, Google Play...).



Automatikoki eguneratu sistema eragilea (Android, iOS...) azken bertsioarekin.

Gailu mugikorretan aplikazioak instalatzean, maiz, datu pribatuak atzitzeko baimena ematen dugu; egitekotan, ziurtatu badakizula zertarako baimena ematen ari zaren.



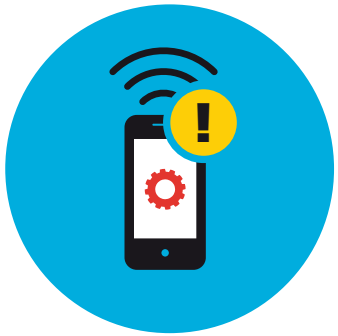
Errespetatu terminalaren bermea. Ez desblokeatu.

Automatikoki eguneratu instalatuta dituzun aplikazioak.

EUSKO JAURLARITZA
GOBIERNO VASCO

Bidaltzen duzu bereziki babestutako informaziorik WhatsApp-en edo WiFi publiko baten bidez?

Ez bidali inoiz bereziki babestutako informaziorik WiFi publikoen bidez.



Eusko Jaurlaritzako langileen telefono mugikorrek SIM txartelak eskainitako garraio-zerbitzuak erabiliko dituzte beti, ezin da telefonoen konfigurazioa aldatu.

Kontuan izan informazioa WiFi publikoen bidez transmititzean igorpena publikoa dela eta, hortaz, ez dela segurua.

"Seguridad ofensiva" blogeko segurtasun aditu bik ariketa praktiko baten bidez erakutsi dute WhatsApp ez dela segurua eta, hortaz, blindatu beharko litzatekeela (2013ko azaroa).

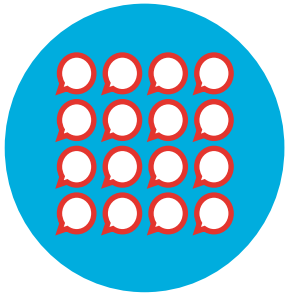
EUSKO JAURLARITZA
GOBIERNO VASCO

Bidaltzen duzu bereziki babestutako informaziorik WhatsApp-en edo WiFi publiko baten bidez?

WhatsApp-en arriskuak

Nortasuna ordezkatzea.

"Phishing" mezuak bidaltzea.



Mezuak masiboki bidaltzea.

Zerbitzua ezeztatzea.

Erabiltzaileak zerrendatzea.

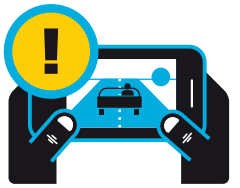
Pasahitzak erauztea.

Elkarrizketak erauztea.

Gomendatzen da tresna hori lanerako ez erabiltzea eta administrazioaren gailu mugikorretan ez instalatzea.

EUSKO JAURLARITZA
GOBIERNO VASCO

Zure aisialdian, zure segurtasunaz arduratzen zara?



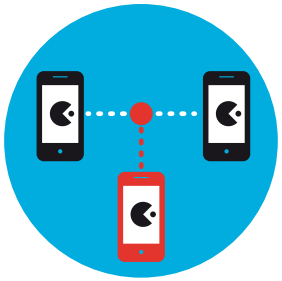
Segurtasun aholkuak

Ziberkriminalek ez zaitzatela engaina.

Kontuz erabili zure erabiltzaile kontua: ez eman ezezagunei zure datu pertsonalak.

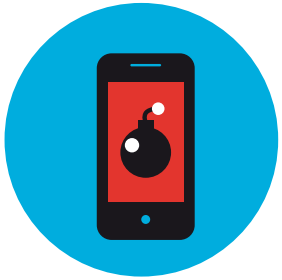
Erantzukizun handiko kargudun baten mugikorrean instalaturiko joko sozial batek haren twitter profilean automatikoki publizitate mezuak argitaratu zituen, eta horrek egunkarietan oihartzun handia izanzuen (2012ko uztaila).

Joko sozialen arriskuak



Datuak atzitzea pertsonekin harremanetan jartzen zarenean.

Nortasuna ordezkatzea.



Malwarea bidaltzea.

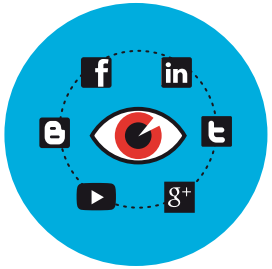
EUSKO JAURLARITZA
GOBIERNO VASCO

Badakizu geokokapena noiz eta zergatik aktibatu behar duzun?

Arretaz irakurri geokokapeneko zerbitzuen eta gizarte sareen pribatutasun baldintzak eta saiatu ulertzen.

Kontuz ibili argitaratzen dituzun edo zu etiketatuta azaltzen zaren argazkiekin eta bideoekin, non zauden jakiteko arrastoak eman baititzakete.

Orokorrean, ez fidatu ezagunak ez diren pertsonekin.



Egoki konfiguratu zure kokapena azaltzen duten loturak, eta ahalik eta gehien murriztu publikoki ematen duzun informazioa.

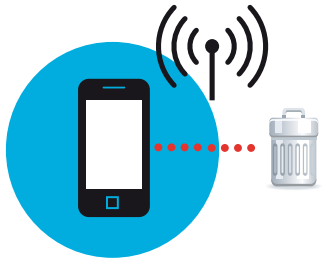
Konfiguratu geokokapeneko sare edo aplikazioek sortutako informazioa ikusi ahal izango duten erabiltzaileen taldea.

Zure gailu mugikorra galdu baduzu edo lapurtu badizute

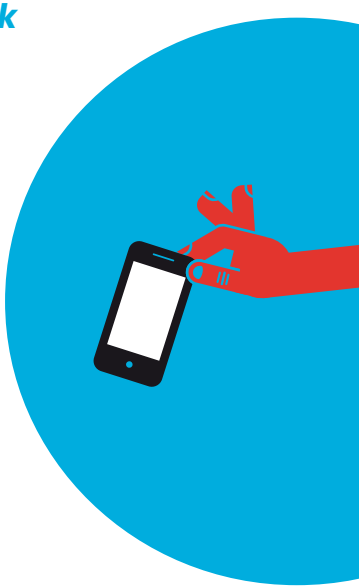
Jarri harremanetan Erabiltzaileen Arretarako Zerbitzuarekin (EAZ) ***400*** *zenbakian edo, barne saretik kanpo deitzen baduzu,* ***+34 945 016 400*** *zenbakian.*

Aktibatu arakatze eta bilaketa aplikazioak.

Aldatu, lehenbailehen, mugikorrean instalaturiko zerbitzuetarako sarbide gakoak.



Ezabatu datuak urrunetik (ziur bazaude ez duzula berreskuratuko).



Iruzur, nortasun ordezte edo lapurretaren bat jasaten baduzu,

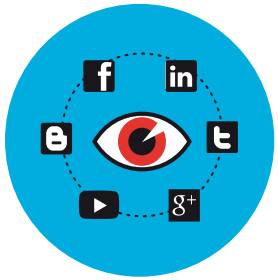
SALATU Ertzaintzan edo Polizian

delituinformatikoak@ertzaintza.net

EUSKO JAURLARITZA
GOBIERNO VASCO

Segurtasuneko oinarrizko hamar aholkuak

Ondo aukeratu pasahitzak eta era seguruan erabili.



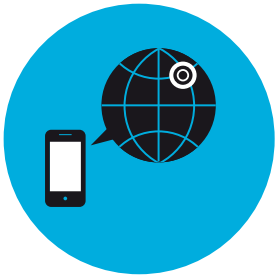
Zaindu eta bermatu zure pribatutasuna gizarte sareetan.

Eguneratuta eduki sistema eragileak eta aplikazioak, eta babestu segurtasun softwarearekin.

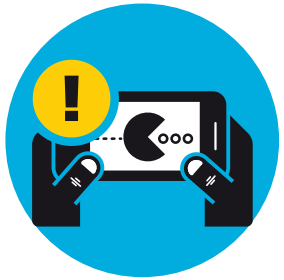
Adi ibili estekak eta atxikitako fitxategiak jasotzen dituzunean.

Ez bidali inoiz bereziki babestutako informaziorik WhatsApp bidez.

Zure gailuak eskainitako zerbitzuen bitartez konektatu eta ez bidali bereziki babestutako informaziorik WiFi publikoak erabilita.

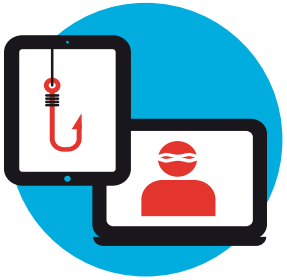


Zure beharren arabera aktibatu edo desaktibatu geokokapena.



Aisialdian, arduraz erabili zure gailu mugikorra.

Ez argitaratu une jakin batean non zauden jakiteko baliagarria izan daitekeen informaziorik.



Iruzur, nortasun ordezte edo lapurretaren bat jasaten baduzu, salatu Ertzaintzan edo Polizian.

EUSKO JAURLARITZA
GOBIERNO VASCO

Terminoen glosarioa

Apple Store: Apple (iOS) aplikazioen ataria.

DBEB: Datuak Babesteko Euskal Bulegoa (http://www.avpd.euskadi.net).

Geokokapena: geoerreferentziazioa ere deitua, kokapen geografikoa automatikoki ezagutzeko balio du, eta objektu batek koordenatu sistema batean duen kokapen zehatza adierazten du.

Google Play: lehen "*Android Market*" deitzen zen, eta Android sistema eragilea duten gailu mugikorretarako "*software*" produktuen online denda da.

IMEI: *"International Mobile Equipment Identity",* Gailu Mugikorraren Nazioarteko Nortasunaren ingelesezko sigla. Sarera konektatzen den gailu mugikor fisikoa okerrik gabe identifikatzeko kodea da, eta lapurreta kasuetan hura blokeatzeko aukera ematen du.

Irekia: Euskadiko gobernu irekiaren ataria (www.irekia.euskadi.net).

Phishing: ingelesezko *"fishing"* hitzetik (arrantza). Erabiltzaileen informazio sekretua lortzeko, amuak erabiliz "arrantzatzean" datza. *"Password harvesting fishing"* hitzen laburdura dela ere esan da (gakoak jasoeta arrantzatzea).

PIN: "*Personal Identification Number*"en sigla (Identifikazio Zenbaki Pertsonala ingelesez). Orokorrean, 4 digitu izaten ditu, eta gailu mugikorra erabili eta blokeatzeko aukera ematen du.

Sare geosozialak: sarea osatzen duten kideei elkarri eragiteko aukera ematen dieten eta kokalekua oinarri hartzen duten sare sozialak.

SIM: tamaina txikiko "txip" adimendun desmuntagarria da eta zerbitzuaren harpidedunak sarean identifikatzeko darabilen informazio osoa gordetzen du, aukera emanez linea terminal batetik bestera aldatzeko, txartela aldatze hutsarekin.

WiFi: uhin bidez eta haririk gabe komunikatzeko teknologia da. IEEE 802.11 estandarrean oinarritzen da, eta Internetera haririk gabe konektatzeko erabiltzen da.

Oharra: marka bakoitza bere jabearena da: Google, Facebook, LinkedIn, Twitter, WhatsApp, etab.

1go edizioa, 2013ko abendua

EUSKO JAURLARITZA
GOBIERNO VASCO