ZIBERSEGURTASUNEKO JARDUNBIDE EGOKIAK SARE SOZIALETAN

NORI ZUZENDUTA DAGO?

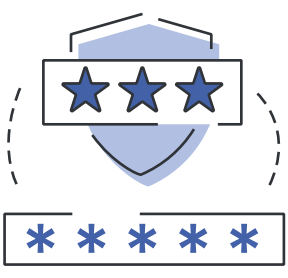
Zibersegurtasunaren arloan erakundeko goi-zuzendaritzarekin komunikazioa hobetu nahi duten erakunde publiko zein pribatuetako profesionalei zuzenduta dago.

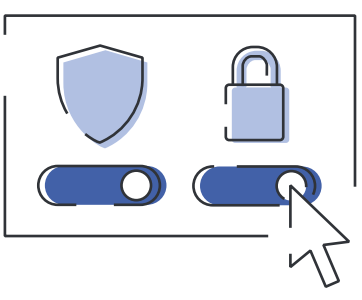
ZIBERSEGURTASUNEKO JARDUNBIDE EGOKIAK ERAKUNDEAN

Sare sozialak garatzeko edo hedatzeko ibilgailu gisa erabiltzen dituzten eraso informatikoen etengabeko hazkundea dela eta, oinarrizko emaitza horiek erabiltzean babestu eta ingurune seguru bat edukitzea da:

Lehen babes-ezkutua, pasahitz sendoa

Sare sozialen kontua indartzeko pasahitz bakarra, sendoa eta asmatzeko zaila sortu behar da (gomendagarria da letra larriak eta minuskulak, zenbakiak eta ikurren konbinazioa erabiltzea, etab.).



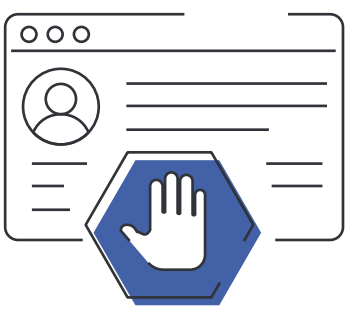


Erabili pribatutasun eta segurtasun aukerak babesa bermatzeko

Egiaztatu sare sozialetako edukia lagunek eta senideek soilik ikusten dutela. Datu pertsonalak ez dira ezezagunekin partekatu behar.

Mantendu pribatutasunean, informazio pribatua

Beharrezkoa da gure profilen pribatutasun-aukerak behar bezala konfiguratzea. Horrela definitzen ditugun pertsonei soilik baimenduko diegu gure datuetarako sarbidea. Ondorioz, helburu maltzurrekin erabiltzeko arriskua murriztuko da.

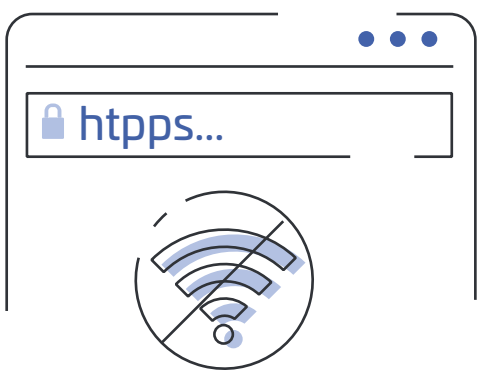


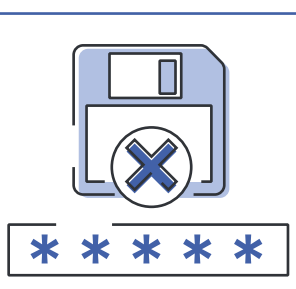
Zenbat eta informazio gutxiago azaldu, orduan eta hobeto

Denbora-lerroa (arbel, horma, etab.) kontu horren jabe den pertsonaren ispilu/errepresentazioa izan daiteke. Horregatik, garrantzitsua da bertan zer informazio argitaratzen den kontrolatzea. Mugatu zer partekatzen den eta nori ematen zaion sarbidea.

Sarbide segurua

Egiaztatu gune zuzena sartzen ari dela eta komunikazioa HTTPS bidez babestuta dagoela komunikazioa enkriptatuta dagoela ziurtatzeko. Ez dira sare sozialetara sartu behar ordenagailu partekatu edo publikoetatik eta fidagarriak ez diren Wi-Fi sareetatik. Bide hauetatik sartzen bazara, beti itxi behar duzu saioa amaitzean eta ez utzi arakatzaileari pasahitza gogoratzen utzi.



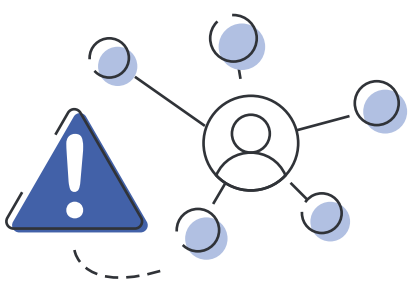


Ez gorde pasahitzak

Gomendio hau errespetatzen ez badugu, gure gailuan fisikoki sartzen den edonork arazorik gabe sar lezake gure kontuetara.

Kontuz estekekin

Kontuz ibili behar duzu jasotzen dituzun estekekin, nahiz eta lagun edo ezagun batengandik etorri. Estekan arreta handiz jarri behar da eta ezezaguna edo/eta susmagarria bada, ez duzu klik egin behar.



Kontuz partekatzen duzunarekin

Sare sozialetan zerbait argitaratzen denean, argitaratutakoaren kontrola galtzen da. Gerora ezabatzen baduzu ere, ziberespazioaren memorian geratuko da betirako.

Segurtasun sistema

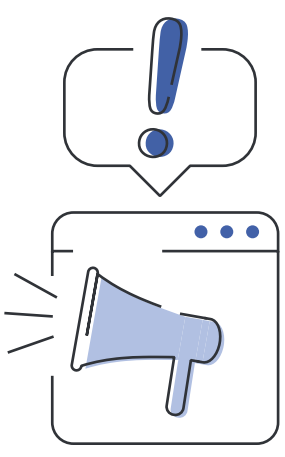
Zure ordenagailuan segurtasun-programak eta tresnak instalatuta izan behar dituzu, adibidez, malwarearen aurkako programak.

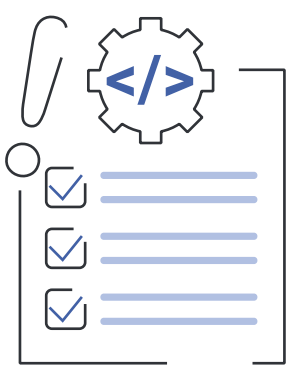
Kontuz GPSarekin eta kokapenarekin

Gailu askok eskaintzen duten GPS funtzionalitatearekin, edozein streaming euskarriek kokapenaren informazioa eduki dezakete. Ziberkriminalek informazio horren bidez ondoriozta ditzakete gure eguneroko ohiturak, maiz joaten garen lekuak eta, oro har, gure bizi-ohiturak.

Zabalkundea

Ez duzu sare sozialetan ikusten duzun guztia sinetsi behar eta zabaldu aurretik edozein albiste egiaztatzea beharrezkoa da. Ziberkriminalak, ingeniaritza sozialeko taktikak erabiliz, erabiltzaileak engainatzen saiatuko dira agertoki faltsuak edo simulatuak erabiliz: sare sozialetako iragarkiak, klik eginez gero, malwarea deskargatzen dutenak, iruzurrezko oharrak banku-entitateen itxurak egiten dituztenak, lapurreta egiteko diseinatutako formularioak eramaten dituztenak. kreditu-txartelen kredentzialak, publizitate-trikimailuak erabiltzailea iruzurrez harpidetzeko SMS zerbitzuetara fakturatzeko, etab.





Kontuz ibili aplikazioen baimenekin

Sare sozialetan joko eta aplikazio asko daude. Horiek deskargatzeko, batzuetan baldintza batzuk eta gure profilera sartzeko baimenak onartu behar ditugu. Une honetan, beharrezkoa da ematen ditugun baimen hauek arretaz berrikusi horiek onartu aurretik.