SEGURTASUNA

BABESTU ZURE GAILUAK

Ordenagailua, sakelako telefonoa eta tableta babesteko neurriak.

Ordenagailua

- Noizean behin, eguneratu erabiltzen dituzun programa guztiak. Egin hori sistema eragileetatik (Windows, Mac OS, Linux…). Gainera, birusen eta espioien kontrako programak zein Interneteko nabigatzaileak (Internet Explorer, Google Chrome, Mozilla Firefox, Safari, Opera, etab.) ere eguneratu behar dituzu.
- Ez erabili ezagunak eta konfiantzazkoak ez diren programa, zerbitzu edo webguneak.
- Adi egon mezu elektronikoetan erantsitako fitxategiak behera kargatzean edo dokumentuak irekitzean eta esteketan klik egitean. Jatorri ezaguna dutela iruditzen bazaizu ere, ez ireki, ez bazaude erabat ziur seguruak direla, edo egiaztatu bidaltzailearekin.
- Interneteko nabigatzaileek pasahitzak gordetzeko edo testua automatikoki osatzeko aukera ematen dute. Desaktibatu aukera horiek.
- Ez onartu konfiantzazkoak ez diren webguneetako ustekabeko abisurik edo leihorik.
- Ez konektatu flash unitate –USB memoria– ezezagunik zure ordenagailuan, birusik edo malwarerik ez hartzeko.
- Babestu zure datu pertsonalak, kontaktuak eta finantza-datuak. Pasahitz seguruenek letrak, zenbakiak eta ikurrak konbinatzen dituzte.
- Ez erabili pasahitz bera leku guztietan. Pasahitz hori osten badizute, haren bidez babesten duzun informazio guztia arriskuan egongo da.
- Ez eman pasahitzak inori.
- Ez utzi ordenagailua piztuta bertan ez zaudenean.
- Ordenagailua beste pertsona batzuekin partekatzen baduzu, itxi beti saioak eta ezabatu Interneteko nabigatzaileen cache memoria.
- Ez eman daturik webguneetan, baldin eta ez badute webgune seguruaren ziurtagiria (SSL) edo ez badute identitatea egiaztatuta (giltzarrapo baten irudia nabigatzailean).
- Ez gorde segurtasun-kopiak ordenagailua daukazun leku berean.

Sakelako telefonoa eta tableta

Ordenagailua babesteko aipatu ditugun neurriez gain, neurri hauek espezifikoagoak dira zure gailu mugikorrak babesteko:
- Instalatu aplikazio ezagunak zure gailuaren sistema eragileari dagozkion denda ofizialetatik edo marketetatik (Google Play, App Store…). Arduradunek etengabe egiaztatzen dituzte dendetako aplikazioak, eta beraz, zailagoa da haietan programa kaltegarriak egotea. Halaber, gomendagarria da jendeak dendetan aplikazioei buruz idazten dituen iruzkinak idaztea; horri esker, ziur egongo gara bilatzen ari garen aplikazioa lortuko dugula.
- Instalatu antibirusa sakelako telefonoan edo tabletan.
- Erabili kode bat edo keinu bidezko patroi bat sakelako telefonoa blokeatzeko, erabiltzen ez duzunean.
- Ez gorde informazio konprometiturik sakelako telefonoan; esate baterako, PIN

zenbakirik eta pasahitzik.
- Finantza-informazioa eskatzen duen SMSrik jasotzen baduzu, ez erantzun telefonotik.
- Aktibatu telefonoko urruneko ezabaketa funtzioa, telefonoa galtzen duzunerako edo osten dizutenerako. Zenbait Android, iPhone eta Windows Phone telefonok kokatzeko funtzioa dute, galtzen direnean erabiltzeko. Gainera, sakelako telefonoaren edukia urrunetik ezabatzeko edo blokeatzeko aukera dute, beharrezkoa izanez gero.
- Eguneratu sakelako telefonoko aplikazioak eta sistema eragilea.
- Aldian behin, egin sakelako telefonoaren edo tabletaren edukiaren segurtasun-kopia (kontaktuak, egutegiak, programak, etab.).
- Aplikazioak erabiltzen amaitzean, itxi saioak.
- Ahal izanez gero, erabili sare mugikorrak (3G eta 4G) edo sarbide publikokoak ez diren WiFi sareak. Ez utzi WiFia eta Bluetootha etengabe aktibatuta.