Mondragon Unibertsitatea

Biblioteka

Konpetentzia digitalak

Graduko ikasleentzako formakuntza materialak

4. Segurtasuna

4.1. Gailuen babesa:

4.1.3. Gailuen babesa

CRUE-REBIUNek egindako eta Mondragon Unibertsitateko Bibliotekak moldatutako materiala

Segurtasuna.
Gailuen babesa.

GAILUEN BABESA

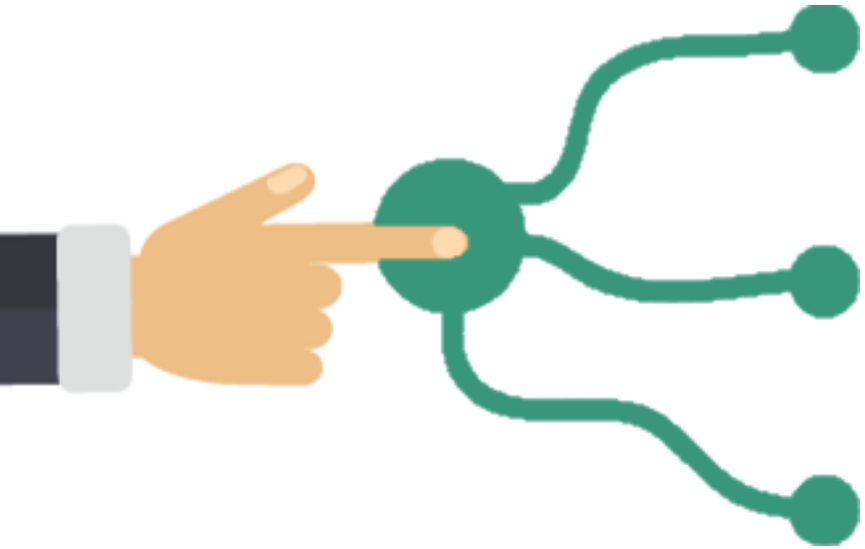
CRUE REBIUN
Red de Bibliotecas Universitarias

LABURPENA

- Gailuen babesa
  - Gailura sarbidea
  - Sistema eragilea
  - Aplikazio eta programak
  - Fitxategiak eta karpetak
  - Web-nabigazioa
  - Haririk gabeko konexioak
  - Geolokalizazioa
  - Babes-sistemak
  - Informazio-kanalak
  - Sen ona

HELBURUAK

Jarduera hau egin ondoren, gaitasun hauek lortu behar zenituzke:



- Gailuak babesteko hainbat modu ezagutzea.
- Gailuak erabiltzeak dituen arriskuez ohartzea.
- Gailuen erabilera arduratsua eta segurua egitea.

GAILUEN BABESA

Sarera konektatutako gailu mugikorren garapenak lan egiteko eta besteekin harremanak izateko modua aldatu du. Etengabe erabiltzen ditugu nabigatzeko, aplikazioak instalatzeko, linean kolaboratzeko edo komunikatzeko, eta horien erabileraren onurak egunerokoan ikus ditzakegu.

Gure mugikorren, eramangarrien eta gainerako gailuen bidez, aplikazio, fitxategi eta informazio sentikor ugari trukatzen eta biltegiratzen dugu. Horregatik, garrantzitsua da babes-neurriak ezagutzea eta gailuak babesteko oinarrizko segurtasun-gomendioak jarraitzea.

Arreta berezia jarri behar zaie alderdi hauei:

- Gailura sarbidea
- Sistema eragilea
- Aplikazio eta programak
- Fitxategiak eta karpetak
- Web-nabigazioa
- Haririk gabeko konexioak
- Geolokalizazioa
- Babes-sistema

Instalatutako segurtasun-sistemek eta aplikazioek ez dute gailuen erabilera arduratsua eta segurua ordezten.

GAILURA SARBIDEA

$4FtAm3!

Gailura sartzeko kode bat ezartzea

Gure gailuen, ordenagailuen edo gailu mugikorren, segurtasuna bermatzeko blokeatze-pantailari lotutako kode edo pasahitz sendo baten bidez sartzea komeni da, eta baita, telefono mugikorren kasuan, SIM txartela desblokeatzeko PIN kode bat ezartzea ere.

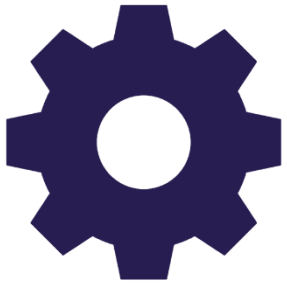
Gailuaren edukiak segurtasunean eta pribatutasunean dituen ondorioak kontuan hartuta, ez da gomendagarria gailua desblokeatzeko pantaila irristatzea bezalako sarbide-metodoak erabiltzea, ez dira oso seguruak.

Hauek dira sartzeko babes-sistema ohikoenak:

- **PINa**: zenbakizko kodea. Gutxienez 8 digitu izatea gomendatzen da.
- **Patroia**: puntu-matrize baten gaineko mugimendu-sekuentzia, non gutxienez 4 puntu lotu behar diren. Alfabetoaren letren antzekoak diren patroiak ez erabiltzea, eta marraztutako patroia erakusteko aukera desaktibatzea gomendatzen da.
- **Pasahitza:** gehienez 16 karaktereko sekuentzia alfanumerikoa. Sartzeko aukerarik egokiena, gutxienez 8 karaktereko pasahitz sendoa erabiltzea da.

Halakorik ez bada, ahal den guztietan, segurtasuneko sistema biometrikoak erabil daitezke, hala nola hatz-marka duen sarbidea edo aurpegiko desblokeoa.

SISTEMA ERAGILEA



Gailuen sistema eragilea eguneratuta izatea

Gailuen segurtasunaren zutabeetako bat horiei eragin diezaieketen segurtasun-ahultasunak ezabatzea da. Segurtasun-arrakala kritikoenek sistema eragilearen kodeari eragiten diote.

Garatzaileek eskainitako aldizkako eguneratzeek, besteak beste, akatsen zuzenketak eta azken **segurtasun-adabakiak** dituzte, bereziki izaera kritikoa dutenak. Horregatik, eguneratze horiek aldizka egiaztatzea komeni da.

Eguneratze horiek eskuz instalatzea komeni da, sistema automatikoki eguneratzeko aukerak desaktibatuz, eta, aldez aurretik, fitxategien segurtasun-kopia egitea, informazioa gal ez dadin.

APLIKAZIOAK ETA PROGRAMAK

Gailuetan instalatutako aplikazioak eta programak eguneratuta edukitzea

Programa edo aplikazio berriak instalatzeak eragina izan dezake gailuen errendimenduan eta segurtasunean.

Ekipoan instalatutako aplikazioen **eguneratzeak** maiz egiaztatzea gomendatzen da, ahultasun posibleetatik babesteko.

Aplikazioak biltegi ofizialetatik instalatzea

Babes-neurri gisa, funtsezkoa da aplikazioak edo programak **konfiantzazko guneetatik** soilik instalatzea, segurtasun-arazo bat sor dezaketen ordezkapenak saihesteko.

Aplikazioen biltegi ofizialak instalazioetarako leku seguruak dira, aplikazioek hainbat egiaztatze-iragazki pasatzen baitituzte.

Google Play
Android aplikazioen biltegia

App Store
iOS aplikazioen biltegia

Microsoft Store
Windows aplikazioen biltegia

FITXATEGIAK ETA KARPETAK

Gailuen edukiaren segurtasun-kopiak egitea

Gailuetako informazioaren eta datuen babesa kontuan hartu behar da, gailua lapurtu edo desagertzen bada, nahi ez diren datuak galtzeko arriskua saihesteko.

Horregatik, **segurtasun-kopiak** egin behar dira aldizka, eta, ahal bada, automatikoki programatu. Kopia bat hodeiko biltegiratze tresnetan egitea gomendatzen da, hala nola Dropbox edo Google Drive, eta beste bat Interneteko konexiorik gabeko gailu fisiko batean, hala nola USB memoria edo kanpoko diskoa.

Segurtasun-kopiak erabiltzeak eraso arriskutsu batek eragin dezakeen kaltearen eta horren ondorioz informazioa galtzeko aukera murrizten du, adibidez *ransomware* bidez egindako eraso baten aurrean.

Hauek dira banakako segurtasun-kopiak egin daitezkeen elementurik sentikorrenak:

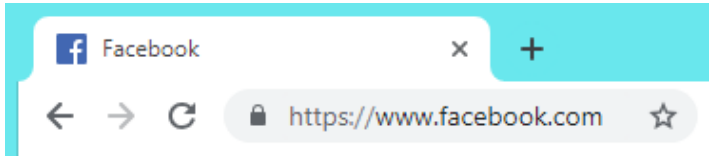
- Fitxategi eta karpetak
- Kontaktuak
- Argazki eta bideoak
- Aplikazioen datuak
- Sistemaren doikuntzak

WEB-NABIGAZIOA

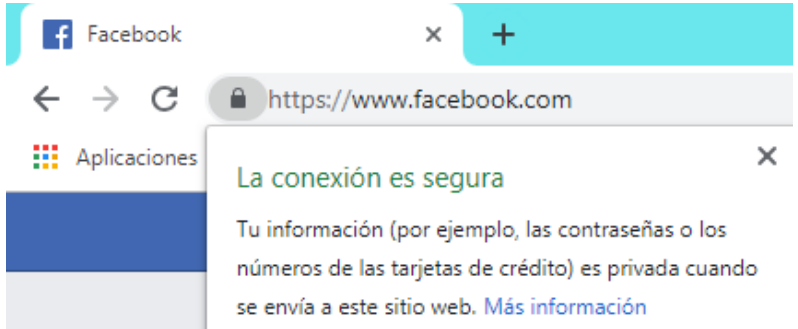
HTTPS:// Nabigazio segurua duten web orriak aukeratu

Ahal den guztietan, Hipertestua Transferitzeko Protokolo Segurua edo **HTTPS** ezarri duten orrietan nabigatzea gomendatzen da. Sistema horrek zifratze-kanal bat du, SSL/TLS izenarekin ezagutzen diren protokoloetan oinarritua, horrek datu sentikorren trafikoaren segurtasuna bermatzen duelarik. Hau funtsezkoa da informazio pribatua trukatzeko zerbitzuak erabiliko baditugu, hala nola posta elektronikoa, sare sozialak edo banku elektronikoa.

Segurtasun-geruzarik ez duen HTTP protokolotik bereizteko, nahikoa da nabigatzailearen helbide-barra kontsultatzea eta URL helbidearen hasiera https:// dela ikustea. Ikusizko errefortzu gisa, nabigatzaile guztiek leku seguru batean nabigatzen ari garela adierazten laguntzen digun giltzarrapo itxiaren ikonoa dute.



Gainera, segurtasun-ziurtagiria nabigatzailearen bidez egiaztatzea gomendatzen da. Horretarako, nahikoa da giltzarrapoaren ikonoa sakatzea, leku seguru baten aurrean gaudela dioen baieztapena jasotzeko.



HARIRIK GABEKO KONEXIOAK

Gailuak WiFi sare publiko irekietara ez konektatzea

WiFi sare publiko irekiek ez dute sarbide-pasahitzik behar, eta konexio azkarra ahalbidetzen digute. Hala ere, sare horietako batera konektatzean, gure gailuen segurtasuna arriskuan jartzen ari gara, sare horietan dabilen edukia ez baita zifratzen. Gauza bera gerta daiteke erabiltzaile asko konektatuta dituzten sareekin (taberna, hotela, etab.). sarbide-pasahitza izan arren, ezin dugulako jakin nor konektatzen den eta informazioa nola transmititzen den.

Sare horietako batera konektatu behar izanez gero, hau gomendatzen da:

- Datu sentikorrak transmititzen dituzten zerbitzuetara kredentzial pribatuekin sartzea saihestea, hala nola, banku elektronikora edo lineako merkataritzara.
- Datuak edo irudiak trukatzeko zerbitzuen sinkronizazioak geldiaraztea, hala nola posta elektronikoa edo hodeian biltegiratzeko zerbitzuak.
- Sare publikoaren datuak ez memorizatzea, gailua etorkizunean baimenik gabe berriro konektatu ez dadin.

Haririk gabeko konexioak desgaitu (WiFi, Bluetooth, NFC...)

Gailuak nahi ez diren urruneko sarbideez babesteko, erabili ondoren, haririk gabeko konexio mota guztiak desgaitzea gomendatzen da.

Datu mugikorren konexioa soilik aktibatuta edukitzea gomendatzen da, gailua galduz gero lokalizatu ahal izateko.

GEOLOKALIZAZIOA

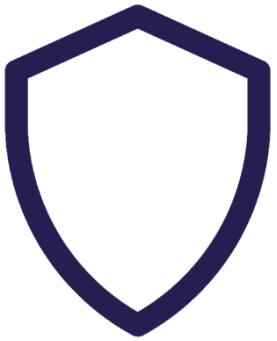
Gailuak aurkitzeko zerbitzuak desgaitu

Gailuek jasotzen duten datu pribatu sentikorrenetako bat denbora errealeko kokapenarena da. Lokalizazioa hirugarrenen esku gera daiteke, eta beste parametro batzuekin erlaziona daitekeenez, gailuen eta pertsonen segurtasuna arriskuan jartzen duen informazio gehigarria lortu daiteke.

Gailu baten kokapena helburu maltzurrekin arakatu daiteke, gailuaren GPS moduluaren bidez, baina baita WiFi sareen, zuntz optikozko sareen edo telefonia mugikorreko seinalearen bidez ere.

Hori dela eta, eginkizun nagusitzat kokalekuaren berariazko funtzionaltasunik ez duten aplikazio, programa edo web orri guztien lokalizazioa desgaitzea gomendatzen da, baita kokalekuaren etiketatzea desaktibatzea ere, argazki aplikazio nahiz sare sozialetan.

BABES-SISTEMAK



Antibirus eta antimalware-tresnak erabiltzea

Gailuak malware edo software maltzurra bezalako **lineako mehatxuetatik** babesteko babes-tresna espezifikoak erabiltzea gomendatzen da.

Suebakia edo firewall	Gailuaren sarrerako eta irteerako konexioak monitorizatzen dituen tresna. Baimenik gabeko sarbideak blokeatzeko balio du. Oro har, ez da iturri ezezagunen konexiorik onartu behar.
Antibirusa	Software maltzurretik babesten gaituen programa, gailuen segurtasun-ahultasunak aprobetxatzen dituzten mehatxuak detektatuz, geldiaraziz eta ezabatuz. Osoenek tresna bakar batean malware, antispyware eta adwareak ezabatzeko sistemak dituzte.

Mehatxuetatik babesteko tresnak automatikoki eguneratzea komeni da, etengabe aldatzen baitoaz.

Babes-neurriak hartu behar dira, gailuak erabiltzen duen sistema eragilea edozein dela ere.

INFORMAZIO-KANALAK

Egungo mehatxu eta arriskuen berri izatea

Zibermehatxu berriak sortzen dira egunero; beraz, **kanal ofizial espezializatuen** bidez informatuta egotea komeni da, gure gailuen segurtasunari eusteko eta zibersegurtasunari buruzko prestakuntza lortzeko.

Internautaren segurtasun-bulegoa
https://www.osi.es/es

Zentro Kriptologiko Nazionala
https://www.ccn-cert.cni.es/

Internauten Elkartea
https://www.internautas.org/

Sareen eta Informazioaren Segurtasunerako Europako Agentzia (ENISA)
https://www.enisa.europa.eu/

SEN ONA

- Gailura sartzeko kode bat ezartzea
- Gailuen sistema eragilea eguneratuta izatea
- Instalatutako aplikazio eta programak eguneratuta edukitzea
- Aplikazioak biltegi ofizialetatik instalatzea
- Gailuen edukiaren segurtasun-kopiak egitea
- HTTPS:// nabigazio segurua duten web orriak aukeratzea
- Gailuak WiFi sare publiko irekietara ez konektatzea
- Haririk gabeko konexioak desgaitzea (WiFi, Bluetooth, NFC...)
- Gailuak aurkitzeko zerbitzuak desgaitzea
- Antibirus eta antimalware-tresnak erabiltzea
- Egungo mehatxu eta arriskuen berri izatea

Mondragon Unibertsitatea

Biblioteka

Zalantzarik baduzu, galdetu zure bibliotekan:

Basque Culinary Center
Biblioteka
Juan Abelino Barriola pasealekua, 101
20009, Donostia, Gipuzkoa.
T. 943574514
biblioteca@bculinary.com

Enpresa Zientzien Fakultatea
Biblioteka
Ibarra Zelaia, 2
20560, Oñati, Gipuzkoa.
T. 943718009
biblioteka.enpresagintza@mondragon.edu

Humanitate eta Hezkuntza Zientzien Fakultatea

Biblioteka

Dorleta, z/g.

20540, Eskoriatza, Gipuzkoa.

T. 943714157

biblioteka.huhezi@mondragon.edu

Goi Eskola Politeknikoa
Biblioteka
Campus Iturripe. Loramendi, 4. 20500 Arrasate – Mondragon, Gipuzkoa.
Campus Orona Ideo. Fundazioa eraikuntza, Jauregi Bailara, z/g. 20120 Hernani, Gipuzkoa.
T. 943794700
biblioteka.mgep@mondragon.edu