

2. Komunikazioa eta lankidetzatza

2.5. Identitate digitalaren kudeaketa:

2.5.4. Identitate digitalaren arriskuak

CRUE-REBIUNek egindako eta Mondragon Unibertsitateko Bibliotekak moldatutako materiala

**Komunikazioa eta
lankidetzak.
Identitate digitalaren
kudeaketa**

Identitate digitalaren arriskuak



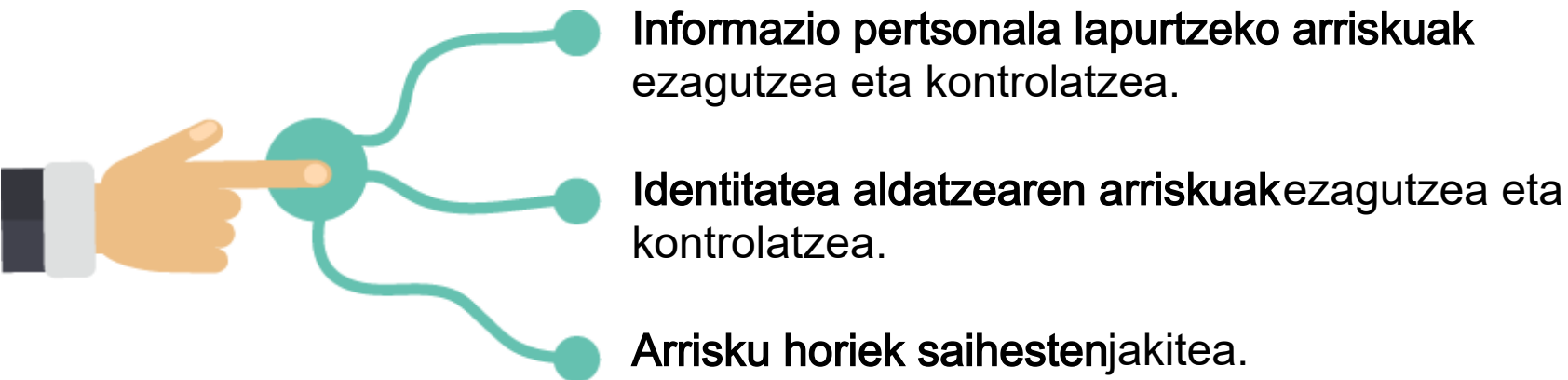
CRUE

REBIUN

Red de Bibliotecas Universitarias

HELBURUA

Jarduera hau amaitzean, gaitasun hauek lortu behar zenituzke:



AURKIBIDEA

- Informazio pertsonala lapurtzea
- Identitatea aldatzea
 - Identitate digitala ordeztzea
 - Pribatutasunerako mehatxuak
 - Erasoak irudiari eta online ospeari
- Gomendioak
- Gehiago jakiteko...

OHIKO ARRISKUA

1. INFORMAZIO PERTSONALA LAPURTZEA

Hauek dira informazio pertsonalaren datuak eskuratzeko metodoetariko batzuk:

- **Programa maltzurak (malware):** haien helburu nagusia erabiltzaileen datuak ezabatzea, blokeatzea, aldatzea edo kopiatzea da (birusak, harrak, troiarrak...).
- **Phishing-a:** informazio pertsonala (pasahitzak, kreditu-txartelen datuak...) iruzur bidez (e-mailez, telefono-deien bidez...) eskuratzeko erabiltzen den metodoa.
- **Pharming-a:** webgune bat beste webgune faltsu batera birbideratzeko iruzurrezko jardunbidea. Webgune faltsu hori itxuraz oso antzekoa da, bisitariaren ordenagailuan software maltzurra instalatzen du, edo erabiltzailearen datu pertsonalak miatzen ditu.

GOMENDIOAK

*Ez baduzu nahi
informazio
pertsonalik
lapur
diezazuten...*



Zalantzarik txikienaren aurrean, izan zentzuduna eta ez arriskatu.

- Ez ireki edo irakurri posta elektronikorik haren jatorria eta egiazkotasuna baieztatu gabe.
- Sartu zure ezkutuko datuak protokolo segurua duten webetan soilik, hala nola https-etan, eta ez http-etan.
- Ez sartu informazio pribatua duten webetan (bankuak...) posta elektronikoetan datozen loturen bidez.
- Ez jakinarazi inori zure gakoak eta pasahitzak, eta aldatu maiztasunez.
- Babestu zure ordenagailua antibirusarekin.
- Ahal dela, ez erabili wifi sare publikorik eragiketa pribatuak egiteko.

OHIKO ARRISKUA

2. IDENTITATEA ALDATZEA

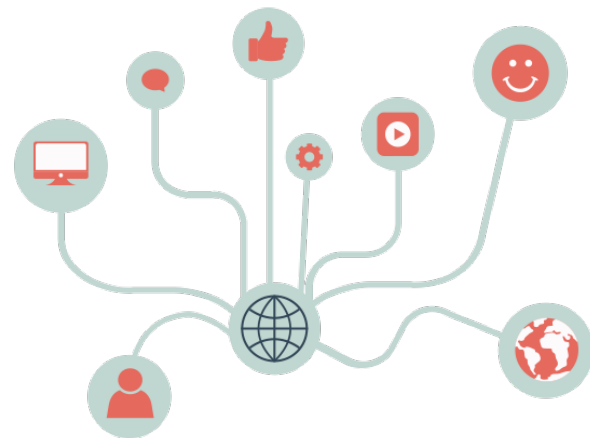
- 1 Identitate digitala ordeztea
- 2 Pribatutasunerako mehatxuak
- 3 Erasoak irudiari eta ospeari

1

IDENTITATE DIGITALA ORDEZTEA

Asmo gaiztoko norbait beste pertsona baten identitate digitalaz behar ez bezala jabetzen denean eta haren izenean jarduten duenean gertatzen da. Modu askotara egin dezake hori:

- ✓ Profil faltsu bat erregistratuz, faltsututako pertsonaren informazio pertsonalik erabili gabe. Adibidez, pertsonaia publikoen profil karikaturizatuak.
- ✓ Profil faltsu bat sortuz, beste pertsona baten datuekin.
- ✓ Baimenik gabe sartuz norbaiten profilean Interneteko zerbitzu batean, norbait horren itxurak eginez.



2

PRIBATUTASUNERAKO MEHATXUAK

Komunikabide sozialetan parte hartzean, argitaratzen duzun informazioaren hedapenari buruzko kontrola galtzen duzu, eta beste pertsona batzuek modu desegokian erabil dezakete informazio hori.

Honako hauek dira pribatutasunerako mehatxu izan daitezkeen arrazoi nagusiak:

- Behar beste ez konfiguratzea darabilzun bitartekoaren pribatutasun-aukerak.
- Zenbait komunikabideren arteko sinkronizaziotik eratorritako pribatutasuna aldatzea.
- Sare sozialetako etiketatzea.

- Sexting-a (sexu-izaeradun edukiak bidaltzea mugikor bidez).
- Cookieak erabiltzea erabiltzaileak jakin gabe.
- Hirugarren pertsoneri eragiten dien informazioa partekatzea.

3

ERASOAK IRUDIARI ETA OSPEARI

Interneten, ohorearen edo ospearen aurkako eraso bat jasateko arriskua areagotzen da; izan ere, edukiak zabaltzerakoan izandako biraltasunak zaildu egiten du jabeak bere informazio pertsonala kontrolatzea.

Hona hemen online ospearen eta irudiaren aurkako mehatxuaren kausa nagusiak:

- ✓ Informazio-askatasuna baino haratago doazen argitalpenen eragina.
- ✓ Argitalpen faltsuen, irainen eta gezurren ondorioz ospeari egindako kaltea.
- ✓ Testuinguruz kanpoko informazioak.
- ✓ Jabetza intelektualaren eskubideak baimenik gabe erabiltzea.

GOMENDIOAK



*Segurtasun- eta
pribatutasun-aukerak
egoki konfiguratzeko
eta berrikusten ikasi
behar duzu, zure
informazio
pertsonalaren gaineko
kontrola ahalik gehien
bermatzeko.*

- Balioetsi argitaratuko duzun informazioa, eta hori egin aurretik:
 - Bereziki zuhurra izan Interneten argitaratuko dituzun argazki edo bideoekin, fisikoki identifikatuko baitzaituzte.
 - Mugatu ezazu kokapen-datuen erabilera hertsiki beharrezkoak diren aplikazioetarako.
 - Egokitu ezazu zure informazio pertsonalaren hedapen-maila beste pertsona batzuekiko harreman motara.



GOMENDIOAK

- Konfiguratu ongi pribatutasun-eta segurtasun-parametroak.
- Amaitzean, itxi egoki profileko edo zerbitzuko saioa.
- Berrikusi aldian-aldian zure profilak.

- Konfiantzazkoak diren hirugarrenen aplikazioei soilik eman sarbidea:
 - Egiaztatu ahalik ongien zein den identitate-datuak erabiltzea baimendu zaion aplikazioaren titularra, zer datu dituen eta zertarako behar dituen.
 - Soilik nahitaezko datuetara sartzeko muga jarri.



GEHIAGO JAKITEKO...

Kontsultatu [Erabiltzaileentzako gida: identitate digitala eta online ospea](#)ren 4. kapitulua.

Kontsultatu OCDEren

[At a Crossroads: Personhood and Digital Identity in the Information Society - OECD.org](#) dokumentua

Honi buruzko informazioa:

[Datuak zuzentzeko eskubideari buruzko araudia](#)



**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
biblioteca.enpresagintza@mondragon.edu

Humanitate eta Hezkuntza Zientzien Fakultatea

Biblioteka

Dorleta, z/g.
20540, Eskoriatza, Gipuzkoa.
T. 943714157
biblioteca.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
biblioteca.mgep@mondragon.edu