Mondragon Unibertsitatea

Biblioteka

Konpetentzia digitalak

Graduko ikasleentzako formakuntza materialak

4. Segurtasuna

4.1. Gailuen babesa:

4.1.2. Pasahitz seguruak

CRUE-REBIUNek egindako eta Mondragon Unibertsitateko Bibliotekak moldatutako materiala

Segurtasuna.
Gailuen babesa.

PASAHITZ SEGURUAK

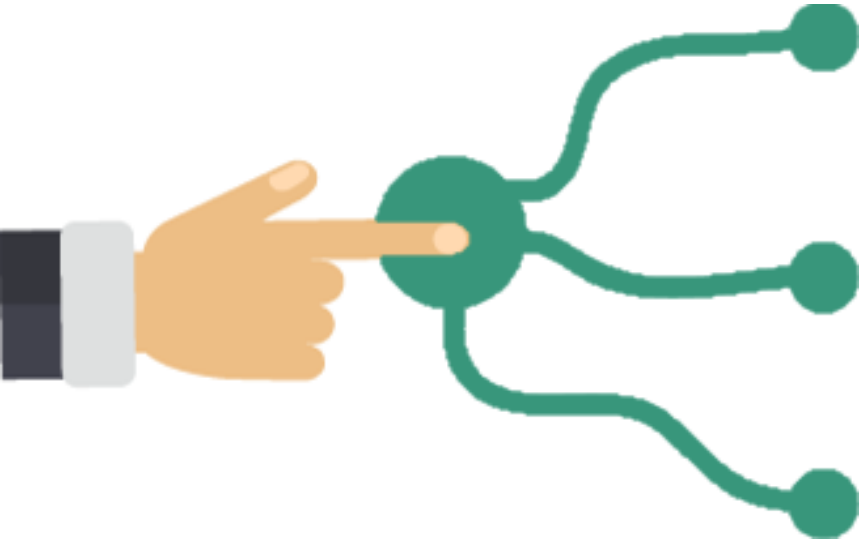
CRUE REBIUN
Red de Bibliotecas Universitarias

LABURPENA

- Pasahitzen erabilera
- Pasahitzen erabileraren arriskuak
- Pasahitz seguruak sortu
- Pasahitzen kudeaketa
- Autentifikazio bikoitza

HELBURUAK

Jarduera hau egin ondoren, gaitasun hauek lortu behar zenituzke:



- Lineako zerbitzuetara sartzeko pasahitzak erabiltzearen abantailak ezagutzea
- Ingurune digitalean pasahitzak erabiltzeak dituen arriskuak ulertzea
- Pasahitz seguruak sortzen ikastea

PASAHITZEN ERABILERA

Pasahitzak gure gailuetako eta lineako zerbitzuen kontu pertsonaletako (posta elektronikoa, lineako bankuak edo sare sozialak) informazio eta fitxategiak **eskuratzeko** aukera **mugatu** ahal izateko erabiltzen dugun babes-metodo bat dira.

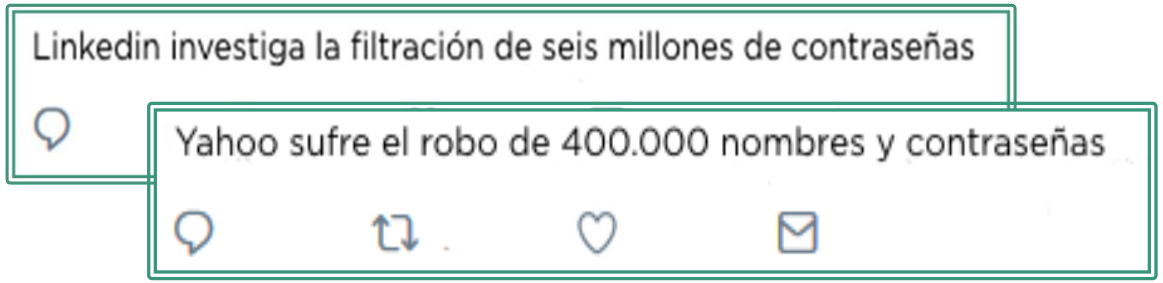
Honetarako balio dute:

- Gure informazio pertsonala babesteko
- Txat, mezu, argazki edo artxiboak bezalako edukien pribatutasuna bermatzeko
- Gailu edo kontu pertsonaletara sarbideak saihesteko

Lineako zerbitzu gehienek erabiltzen dute erabiltzaile eta pasahitz batean oinarritutako sarbidearen bidez autentifikatzeko sistema, baina ahuleziak ere baditu:

- Pasahitz konplexu ugari buruz ikasteko zailtasuna
- Zibergaizkileek pasahitzak lapurtzeko erabiltzen dituzten teknikekiko zaurgarritasuna

PASAHITZEN ERABILERAREN ARRISKUAK



Zibergaizkileek hainbat eraso mota erabiltzen dituzte pasahitzak lapurtzeko eta gure gailu eta kontu pertsonaletan helburu maltzurrak lortzeko.

Eraso mota	Ezaugarriak
Indarrez	Saiatu eta huts eginez, pasahitza asmatzean datza. Zibergaizkileek hainbat konbinazio probatzen dituzte, eredu zuzenarekin bat egiten duten arte.
Hiztegi-erasoa	Software bat pasahitza automatikoki lortzen saiatzeaz da, letrak eta hitzen konbinazioekin probatuz.
Phising	Engainu-teknika bat da, non banku elektronikoa bezalako lineako zerbitzu baten interfazea simulatu edo ordezkatzen den, guk gure gakoak sartzea eginez eta horrela datuak erraz lortu ahal izateko.
Keylogger	Teklatuaren pultsazio guztiak atzematen ditu, pasahitzak barne. Spyware motako software maltzurra da.

Internautaren Segurtasun Bulego-tik egokitua (2019). Pasahitzei erasoa. https://www.osi.es/es/campanas/contrasenas-seguras/ataques-contrasenas-tik berreskuratua

Pasahitz sendoak eta seguruak erabiltzeak, nahi ez diren sarbideen, datuen manipulazioaren edo suntsiketaren eta informazio edo artxibo pertsonalen baimenik gabeko hedapenaren arriskuak murriztu egiten ditu.

PASAHITZ SEGURUAK SORTU

Pasahitz bat sortzen dugunean kontu handiz jokatu behar dugu, eta zibergaizkileei lana zaildu:

- Gutxienez 8 karakteretako luzera duen pasahitza aukeratu.
- Izena, NAN, jaioteguna, telefono-zenbakia edo posta helbidea bezalako datu pertsonalak erabili.
- Teklatuko letra-segida bat sortu (qwerty, 1234…) edo karaktere bera pasahitzean errepikatu (11ee44).
- Letra larriak eta xeheak zenbaki eta karaktere bereziekin (sinboloak) konbinatu.

Pasahitza	Zenbat denboran izango litzatekeen asmatua
123456	Segundo bat baino gutxiago
asdfghjk	Segundo bat baino gutxiago
551882342	Segundo bat baino gutxiago
alcala13	Minutu bat
Tokio2020	4 egun
Era$e1vez!	6 urte

https://howsecureismypassword.net-etik jasotako kalkuluen arabera

PASAHITZ SEGURUAK SORTU

Pasahitzak sortu eta erabiltzerakoan segurtasuna hobetzeko, pasahitz sendoak erabiltzeak eta jardunbide egokiak jarraitzeko neurriak hartzeak duen garrantziaz jabetu behar dugu:

- Erraz gogoratzeko moduko pasahitza aukeratzea
- Teklatuari begiratu gabe azkar idatz daitekeen pasahitz bat erabiltzea
- Zerbitzu bakoitzerako pasahitz bat sortzea
- Pasahitza aldizka aldatzea
- Pasahitzak paperean edo fitxategi batean apuntatzea saihestu
- Pasahitzak ez partekatu, edo zabaldu bitarteko elektronikoen bidez

Pasahitz asko erabiliz gero, pasahitzen kudeatzaile bat erabiltzea komeni da.

PASAHITZEN KUDEAKETA

Pasahitzen kudeatzaileak, hainbat zerbitzutarako sarbide-gakoak gordetzeko tresnak dira, gakoak buruz ikasteko beharrik gabe. Gainera, pasahitz konplexuak sortzeko aukera ematen dute.

Tresna horiek Interneteko gailuetan eta nabigatzaileetan integratuta egon ohi dira, edo aplikazio independente gisa ere instalatzen dira.

Horien erabilera gomendagarria da:

- Ausaz pasahitz sendoak sortzeko
- Hainbat zerbitzuri lotutako pasahitzak gordetzeko
- Gakoak maiz aldatzearen garrantzia gogoratzeko
- Pasahitz bera behin eta berriz erabiltzen dela ohartarazteko

Pasahitzen kudeatzaile bat erabiltzeak phising-erasoetatik babesten gaitu, jatorrizko sarbide-orria eta ordezko bat bereizteko gai izango baita, nahiz eta interfaze bera izan.

AUTENTIFIKAZIO BIKOITZA

Lineako zerbitzuetara sartzeko pasahitzak erabiltzeak hainbat arrisku ditu, eta, beraz, horietako batzuek (posta, merkataritza edo banka elektronikoa) bi urratsetan identitatea **egiaztatzeko sistema** bat erabiltzea gomendatzen diete erabiltzaileei: **autentifikazio bikoitza**.

Sistema honen bidez, erabiltzailea eta pasahitzaz gain, gure nortasuna egiaztatu behar dugu, informazio osagarria emanez:

- SMS bidez edo telefono-dei bidez jasotako kodea sartuta
- Aztarna digital edo aurpegi-azterketa bezalako gailuari lotutako azterketa-sistema biometrikoen bidezko egiaztapen bidez
- Zenbaki-txartel edo kriptokalkulagailu moduko gailu zehatz batek emandako erabilera bakarreko kodea

Lineako zerbitzu askok, batez ere hodeian oinarritutakoek, autentifikazioa bi urratsetan aktibatzeko aukera ematen dute.

Beste modu bat, bigarren segurtasun-geruza erabiltzeko aukera ematen duten aplikazioak dira:

Google Authenticator

Latch

GEHIAGO JAKITEKO...

Eman begirada bat honako artikuluari:

¡Pasahitza seguruak!

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