

ZURE SEGURTASUNA PASAHITZEN BITARTEZ

Zenbatetan ahantzi duzu pasahitza eta **“Pasahitza ahaztu dut”** botoiari eman behar izan diozu? Segurtasun informatikoa dela medio, zure informazio pertsonal guztia zaintzeko ardura hartu behar duzu.

Gaur egun, **pasahitz segurua** letra larriak, xeheak, zenbakiak eta karaktere bereziak dituena da. Letra edo zenbaki gehigarri bakoitzak esponentzialki handituko du segurtasuna. Gainera, ez da komeni informazio pertsonalik erabiltzea, ez eta teklatu-patroirik edo segidako zenbakirik ere, erraz asmatu ahal badira.



PASAHITZ LAPURRETA OHIKOENAK



Keylogger

Gailu mugikor edo ordenagailu batean instala daitekeen malware bat da. Sisteman sartutakoan, pantailetan edo botoietan egiten diren tekla-argitalpen guztiak biltzen ditu.



Spyware

Pantaila grabatzeko gai den beste malware mota bat da. Horrela, hor ageri den guztia biltzen du.



Plataformetan pasahitzak iragaztea

Batzuetan, segurtasun akatsak izaten dira, eta horiek erabil ditzakete erasotzaileek gako eta erabiltzaile horietara sartzeko.

JARDUNBIDE EGOKIAK LAPURRETEN AURREAN



Aldatu pasahitzak aldizka

Pasahitzen bat zure taldekoa ez den ekipo batean gorde bada, ezingo da erabili.



Berrikusi pasahitz zentroak

Era horretan gure pasahitzen bat konprometitu den egiaztatuko dugu.



Maiz eguneratu aplikazioak

Era berean, garrantzitsua da sistema eragilea eta erabiltzen dugun edozein programa eguneratzea.

BABESTUTA MANTENDU ZURE PASAHITZAK



Kontu, aplikazio eta zerbitzu bakoitzerako pasahitzak erabiltzea kaosa izan daiteke; horregatik, **pasahitzen administratzaileek** lana erraztu ahal digute. Memoria pribilegiaturik ez baduzu, ia ezinezkoa da pasahitz guztiak gogoratzea!

Pasahitzak modu seguruan gordetzeko, erabili **pasahitzen kudeatzaile edo administratzaile** bat. Aplikazio horiek gure egiaztatgiri guztiak **datu base zifratu** batean gordetzen laguntzen digute. Horrela, gure kontu guztiak tresna beretik kudeatu ditzakegu.