4. Segurtasuna

4.1. Gailuen babesa

1. Alderdi hauetako zeini erreparatu behar diogu gure gailuak babesteko? [Aukeratu erantzun zuzena]

a. Sistema eragilea
b. Hari gabeko konexioak
c. Aplikazioak eta programak
d. Guztiak dira zuzenak

2. Gailuetara sartzeko babes-sistemak dira [Aukeratu erantzun zuzena/k. Bat baino gehiago egon daiteke]

a. Pantailaren horma
b. PIN codea
c. Bluetooth
d. Pasahitza

3. Sartzeko babes-sistema hauetatik, zein da gomendagarriena? [Aukeratu erantzun zuzena]

a. Hatz-marka
b. 4 digituko PIN kodea
c. 8 karaktereko pasahitz alfanumerikoa
d. Puntuen patroia

4. Gure gailurako azken segurtasun-adabakiak izan ahal izateko, gomendagarria da… [hautatu erantzun zuzena]

a. Mezularitzako aplikazioak instalatzea
b. Gailua telefonia-sare batera konektatzea
c. Sistema eragilea eguneratzea
d. Gailuaren kokapena desaktibatzea

5. Adierazi gailu pertsonal bati eragin diezaioketen segurtasun-mehatxuak [Aukeratu erantzun zuzena/k. Bat baino gehiago egon daiteke]

a. Malware
b. Webmail
c. Freeware
d. Spam

6. Adierazi baieztapen bakoitzerako aukera zuzena.

	Egia	Gezurra
a. Pasahitzetan datu pertsonalak erabiltzea gomendatzen da, eraso batean aurkitzerik ez izateko.		
b. Pasahitzak babes-metodo bat dira, eta gure gailu eta kontu pertsonaletan dauden informaziorako eta artxiboetarako sarbidea mugatzeko erabiltzen ditugu.		
c. Pasahitz asko erabiliz gero, gomendagarria da paper batean idaztea.		
d. Pasahitzen kudeatzaileek zerbitzu askotara sartzeko gakoak gordetzeko aukera ematen digute, hauek buruz ikasi beharrik gabe.		

7. Zer eratako erasoak egiten dira pasahitzak aurkitzeko? [Lotu eraso mota bakoitza bere ezaugarriekin]

	Indar basatia	Phising	Keyblogger	Hiztegiaren erasoa
Online zerbitzu baten interfazea simulatzen edo ordezten duen engainu-teknika bat da, banka elektronikoa bezala, gure gakoak sar ditzagun eta horrela erraz lortu.				
Spyware motako software maltzurra da, teklatuko pultsazio guztiak atzematen dituena, pasahitzak barne.				
Software bat pasahitza automatikoki lortzen saiatzeaz arduratzen da, letren eta hitzen konbinazioekin probatuz.				
Pasahitza saiakuntza eta errore bidez asmatzean datza. Zibergaizkileek konbinazio desberdinak probatzen dituzte patroi zuzena aurkitu arte.				

8. Pasahitzak sortzeko jardunbide egokien neurriak dira [Aukeratu erantzun zuzena/k. Bat baino gehiago egon daiteke]

a. Pasahitz gisa datu pertsonalak erabiltzea
b. Gutxienez 8 karaktere luze dituen pasahitza aukeratu
c. Errepikatu karaktere bera pasahitzean
d. Letra larriak eta xeheak zenbaki eta karaktere bereziekin konbinatu

9. Pasahitzak erabiltzeko jardunbide egokien neurriak dira [Aukeratu erantzun zuzena/k. Bat baino gehiago egon daiteke]

a. Erraz gogoratzeko pasahitza aukeratu
b. Pasahitzak partekatzea edo bitarteko elektronikoen bidez zabaltzea
c. Pasahitza aldizka aldatu
d. Erabili pasahitz bera zerbitzu bakoitzean

10. Pasahitzen kudeatzaile bat erabiltzea gomendagarria da honetarako: [aukeratu erantzun zuzena/k. Bat baino gehiago egon daiteke]

a. Ausazko pasahitz sendoak sortzea
b. Instalatutako aplikazioak eta programak eguneratuta edukitzea
c. Hainbat zerbitzuri lotutako pasahitz ugari gordetzea
d. Lineako zerbitzu baten interfazea simulatzea edo ordezkatzea

11. Hari gabeko konexioen segurtasuna bermatzeko neurriak [Aukeratu erantzun zuzena/k. Bat baino gehiago egon daiteke]

a. Bluetooth-a konektatu WiFi erabiltzen dugun guztietan
b. Ez konektatu gailuak WiFi sare publiko irekietara
c. Konektatu WiFi publikoetara fitxategiak hodeian sinkronizatu behar ditugunean bakarrik
d. Hari gabeko konexioak desgaitu (WiFi, Bluetooth, NFC)

12. Gailuak babesteko moduak [Aukeratu erantzun zuzena/k. Bat baino gehiago egon daiteke]

a. Sarbide-kode bat ezartzea
b. Instalatutako aplikazioak eta programak eguneratuta edukitzea
c. Lokalizazio-zerbitzuak desgaitzea
d. Aplikazioak biltegi ofizialetatik ez instalatzea

13. HTTP web nabigazioko protokolo segurua	Egia	Gezurra
a. Zifratze-kanal bat du, datu sentikorren trafikoaren segurtasuna bermatzen duena		
b. Nabigatzaile mugikorretan bakarrik funtzionatzen du		
c. Segurtasun-ziurtagiri bat du, nabigatzailearen bidez egiazta daitekeena		
d. Saihestu egin beharko litzateke informazio pribatua trukatzeko zerbitzuak erabiliko baditugu, hala nola posta elektronikoa, sare sozialak edo banka elektronikoa		

14. Adierazi baieztapen bakoitzerako aukera zuzena	Egia	Gezurra
a. Babeskopiak erabiltzeak eraso arriskutsu batek eragin dezakeen kaltea murrizten du, eta informazioa galtzea aurreikusten da		
b. Gomendagarria da kanal ofizial espezializatuen bidez informatuta egotea, gure gailuen segurtasuna mantentzeko eta zibersegurtasuneko prestakuntza lortzeko.		
c. Gomendagarria da gailura sartzeko metodoak erabiltzea, hala nola aparatua desblokeatzeko pantaila lerratzea		
d. Babes-neurriak eduki behar dira, gailuak erabiltzen duen sistema eragilea edozein dela ere		

15. Nahi ez den posta edo spama saihesteko, hau gomendatzen da: [aukeratu erantzun zuzena/k. Bat baino gehiago egon daiteke]

a. Posta-iragazki pertsonalizatuak sortzea
b. Aldez aurretik spam gisa kategorizatutako mezuak irekitzea
c. Erabili posta-kontu nagusia harpidetza-zerbitzuetarako
d. Susmagarria edo ezezaguna iruditzen zaigun igorlea duten mezuak ez irekitzea edo ez erantzutea

4. Segurtasuna

4.1. Gailuen babesa

1. Alderdi hauetako zeini erreparatu behar diogu gure gailuak babesteko? [Aukeratu erantzun zuzena]

a. Sistema eragilea
b. Hari gabeko konexioak
c. Aplikazioak eta programak
d. Guztiak dira zuzenak

2. Gailuetara sartzeko babes-sistemak dira [Aukeratu erantzun zuzena/k. Bat baino gehiago egon daiteke]

a. Pantailaren horma
b. PIN codea
c. Bluetooth
d. Pasahitza

3. Sartzeko babes-sistema hauetatik, zein da gomendagarriena? [Aukeratu erantzun zuzena]

a. Hatz-marka
b. 4 digituko PIN kodea
c. 8 karaktereko pasahitz alfanumerikoa
d. Puntuen patroia

4. Gure gailurako azken segurtasun-adabakiak izan ahal izateko, gomendagarria da… [hautatu erantzun zuzena]

a. Mezularitzako aplikazioak instalatzea
b. Gailua telefonia-sare batera konektatzea
c. Sistema eragilea eguneratzea
d. Gailuaren kokapena desaktibatzea

5. Adierazi gailu pertsonal bati eragin diezaioketen segurtasun-mehatxuak [Aukeratu erantzun zuzena/k. Bat baino gehiago egon daiteke]

a. Malware
b. Webmail
c. Freeware
d. Spam

6. Adierazi baieztapen bakoitzerako aukera zuzena.

	Egia	Gezurra
a. Pasahitzetan datu pertsonalak erabiltzea gomendatzen da, eraso batean aurkitzerik ez izateko.		
b. Pasahitzak babes-metodo bat dira, eta gure gailu eta kontu pertsonaletan dauden informaziorako eta artxiboetarako sarbidea mugatzeko erabiltzen ditugu.		
c. Pasahitz asko erabiliz gero, gomendagarria da paper batean idaztea.		
d. Pasahitzen kudeatzaileek zerbitzu askotara sartzeko gakoak gordetzeko aukera ematen digute, hauek buruz ikasi beharrik gabe.		

7. Zer eratako erasoak egiten dira pasahitzak aurkitzeko? [Lotu eraso mota bakoitza bere ezaugarriekin]

	Indar basatia	Phising	Keyblogger	Hiztegiaren erasoa
Online zerbitzu baten interfazea simulatzen edo ordezten duen engainu-teknika bat da, banka elektronikoa bezala, gure gakoak sar ditzagun eta horrela erraz lortu.				
Spyware motako software maltzurra da, teklatuko pultsazio guztiak atzematen dituena, pasahitzak barne.				
Software bat pasahitza automatikoki lortzen saiatzeaz arduratzen da, letren eta hitzen konbinazioekin probatuz.				
Pasahitza saiakuntza eta errore bidez asmatzean datza. Zibergaizkileek konbinazio desberdinak probatzen dituzte patroi zuzena aurkitu arte.				

8. Pasahitzak sortzeko jardunbide egokien neurriak dira [Aukeratu erantzun zuzena/k. Bat baino gehiago egon daiteke]

a. Pasahitz gisa datu pertsonalak erabiltzea
b. Gutxienez 8 karaktere luze dituen pasahitza aukeratu
c. Errepikatu karaktere bera pasahitzean
d. Letra larriak eta xeheak zenbaki eta karaktere bereziekin konbinatu

9. Pasahitzak erabiltzeko jardunbide egokien neurriak dira [Aukeratu erantzun zuzena/k. Bat baino gehiago egon daiteke]

a. Erraz gogoratzeko pasahitza aukeratu
b. Pasahitzak partekatzea edo bitarteko elektronikoen bidez zabaltzea
c. Pasahitza aldizka aldatu
d. Erabili pasahitz bera zerbitzu bakoitzean

10. Pasahitzen kudeatzaile bat erabiltzea gomendagarria da honetarako: [aukeratu erantzun zuzena/k. Bat baino gehiago egon daiteke]

a. Ausazko pasahitz sendoak sortzea
b. Instalatutako aplikazioak eta programak eguneratuta edukitzea
c. Hainbat zerbitzuri lotutako pasahitz ugari gordetzea
d. Lineako zerbitzu baten interfazea simulatzea edo ordezkatzea

11. Hari gabeko konexioen segurtasuna bermatzeko neurriak [Aukeratu erantzun zuzena/k. Bat baino gehiago egon daiteke]

a. Bluetooth-a konektatu WiFi erabiltzen dugun guztietan
b. Ez konektatu gailuak WiFi sare publiko irekietara
c. Konektatu WiFi publikoetara fitxategiak hodeian sinkronizatu behar ditugunean bakarrik
d. Hari gabeko konexioak desgaitu (WiFi, Bluetooth, NFC)

12. Gailuak babesteko moduak [Aukeratu erantzun zuzena/k. Bat baino gehiago egon daiteke]

a. Sarbide-kode bat ezartzea
b. Instalatutako aplikazioak eta programak eguneratuta edukitzea
c. Lokalizazio-zerbitzuak desgaitzea
d. Aplikazioak biltegi ofizialetatik ez instalatzea

13. HTTP web nabigazioko protokolo segurua	Egia	Gezurra
a. Zifratze-kanal bat du, datu sentikorren trafikoaren segurtasuna bermatzen duena		
b. Nabigatzaile mugikorretan bakarrik funtzionatzen du		
c. Segurtasun-ziurtagiri bat du, nabigatzailearen bidez egiazta daitekeena		
d. Saihestu egin beharko litzateke informazio pribatua trukatzeko zerbitzuak erabiliko baditugu, hala nola posta elektronikoa, sare sozialak edo banka elektronikoa		

14. Adierazi baieztapen bakoitzerako aukera zuzena	Egia	Gezurra
a. Babeskopiak erabiltzeak eraso arriskutsu batek eragin dezakeen kaltea murrizten du, eta informazioa galtzea aurreikusten da		
b. Gomendagarria da kanal ofizial espezializatuen bidez informatuta egotea, gure gailuen segurtasuna mantentzeko eta zibersegurtasuneko prestakuntza lortzeko.		
c. Gomendagarria da gailura sartzeko metodoak erabiltzea, hala nola aparatua desblokeatzeko pantaila lerratzea		
d. Babes-neurriak eduki behar dira, gailuak erabiltzen duen sistema eragilea edozein dela ere		

15. Nahi ez den posta edo spama saihesteko, hau gomendatzen da: [aukeratu erantzun zuzena/k. Bat baino gehiago egon daiteke]

a. Posta-iragazki pertsonalizatuak sortzea
b. Aldez aurretik spam gisa kategorizatutako mezuak irekitzea
c. Erabili posta-kontu nagusia harpidetza-zerbitzuetarako
d. Susmagarria edo ezezaguna iruditzen zaigun igorlea duten mezuak ez irekitzea edo ez erantzutea