Sareko segurtasuna

GIDA DIDAKTIKOA

01.AURKEZPENA

Dena aldatu da.

Argazki-kamera baztertu egin dugu, kontaktu-agendak gurekin bidaiatzen du eta erlojuak ordua esaten digu, egunero ibiltzera animatzen gaitu eta, ariketa egiten dugunean, ura edan behar dugula gogorarazten digu.

Alexa edo Sira gure bizitzan sartu dira, eta beraiek gomendatzen digute zer entzun, zer irakurri edo nora joan behar dugun bazkaltzera.

Teknologia harrigarria da, azkarra eta erabilerraza. Hori dela eta, **natibo digitalek** ez dute beren burua arriskuan ikusten hura erabiltzen dutenean, eta **sinetsita** daude beren informazioaren gaineko kontrol osoa dutela.

Baina, benetan uste al dugu badakitela non dauden arriskuak eta nola babestu behar duten haietatik?

Programa hau komunikazio-eredu berri baterako biziraupen-eskuliburua da. Izan ere, haren pantaila eta jardueren bidez, ikasleek beren datuak eta intimitatea babesteko eskura dituzten tresnak ezagutu ahal izango dituzte: pribatutasun-iragazkiak, antibirusak, gako eta pasahitzen kudeaketa zuzena, web-kameraren erabilera arduratsua eta, azkenik, hodeiko zerbitzuen erabilera segurua.

Labur esanda: oso tresna erabilgarria da mundu interkonektatu batean segurtasunez mugitzeko.

02.PROIEKTUAREN FORMATUA: ESCAPE ROOM

Hezkuntza-arloko onlineko ihes-gela bat gamifikazio-teknika bat da, eta ikasle talde bat abentura baten barruan alegiazko egoera baten aurrean jartzean datza. Abenturaren amaierara iristeko, proiektuaren hezkuntza-edukiekin zerikusia duten proba batzuk gainditu beharko dituzte ikasleek.

Esperientzia motibagarria da, eta adimen anizkoitzak zein funtsezko konpetentziak behar bezala lantzeko aukera ematen du.

Lehentasunak:

- Talde-lana.
- Sormena.
- Erabakiak hartzea.
- Lidergoa.
- Komunikazioa.
- Pentsamendu kritikoa.

Garapena:

Ikastetxe batean gertatzen da abentura. Ikasle batek laguntza eskatu dio informatikako irakasleari, ikaskide bat jazartzen ari den pertsona aurkitzeko.

Une horretatik aurrera, 35 minutu izango ditu pertsona hori aurkitzeko, ikastetxeko wifitik deskonektatu baino lehen.

03.HELBURUAK

3.1

Interneten nabigatzea eta informazioa bilatzea, informazioa iragaziz eta ikuspegi kritikoarekin kudeatuz haren baliozkotasunari eta sinesgarritasunari dagokienez.

3.2

Jasotako komunikazio-motak kudeatzeko gai izatea, eta komunikazio-formak eta -modalitateak hartzaile-motaren arabera egokitzen jakitea (mezu elektronikoak, txatak, SMSak, bat-bateko mezularitza, blogak, foroak, Instagram, Tik Tok).

3.3

Sare sozialetan eta onlineko komunitateetan nola parte hartu jakitea, edukiak eta informazioa partekatzeko. Horretarako, sareko etiketa-arauak ulertu behar dira, eta testuinguru pertsonalera aplikatzeko gai izan, norberaren identitate digitala sortzeko.

3.4

Edukia sortzea: informazioari buruzko lizentzia-mota guztiak eta erabiltzen diren bitartekoak ezagutzea.

3.5

Sareko arriskuak eta mehatxuak ezagutzea, norberaren gailu digitalak babesten jakitea eta oinarrizko segurtasun-estrategiak eguneratzea.

04.EDUKIAK

1. Identitate digitala eta ospe digitala.
2. Datu pertsonalak eta pribatutasunaren babesa.
   Aztarna digitala.
3. Sare sozialak
4. Webgune eta gune arriskutsuak
   4.1. Pornografía
   4.2. Eduki arriskutsuak
   4.3. Online jokoa
5. Ziberjazarpena eta indarkeria digitala.
6. Sareko segurtasuna

Beste eduki batzuk:

› Interneten ezaugarriak: anonimotasuna, deskolakizazioa, publizitatea eta denborazkanpokotasuna.
› Netiketa: sarean zuzen jokatzeko arauak.
› Glosarioa
› Irakasleentzako jarduerak eta tutorialak

Hona hemen zeharka garatzen diren edukiak:

› Informazio-iturrien eta informazioaren beraren egokitasunaren ebaluazioa.
› Pertsonen arteko harremanak eta komunikazioa garatzea (enpatia, entzute aktiboa eta asertibitatea).
› Sare sozialak, aukerak, ezarpenak, babesa, kudeaketa egokia.
› Ingurune birtual seguruak. Onlineko zerbitzuak erabiltzeko baldintzak.
› Prestakuntzako eta aisialdiko baliabide eta plataformetarako sarbidea.
› Segurtasun-arriskuak eta babes-sistemak. Segurtasun-neurri aktiboak eta pasiboak.
› Teknologiaren erabilerari lotutako osasun-arriskuak. Ongizate fisiko eta psikologikoa. Adikzioak, arreta-galtzeak eta oreka emozionala.

05.NABIGAZIOA:

› Sarbide-gakoari buruzko sarreraren pantaila
› 2 aurkezpen-pantaila, eta, horiez gain, eduki gehigarriak eta pdf-ko gida.
› Beste pertsonaia batzuen deskribapenaren pantaila.

› Hemendik aurrera, Escape Room-aren egiturarekin egingo dugu topo: antolamendu bera duten 6 misio interaktibo:

» Argibideak
» Sarrera
» Galde-erantzunak
» Maila horretako gakoa lortzea
» Hurrengo mailara igarotzea

› Abenturaren amaierako pantaila.
› Gomendioen dekalogoa
› Escape Room-a amaitu izana egiaztatzen duen diploma sortzeko aukera.

06.IRAKASLEENTZAKO

JARDUERAK ETA TUTORIALAK

6.1. Pentsamendu kritikoa.

Informazio asko jasotzen dugu Interneten nabigatzen dugunean, eta gazteentzat ez da erraza informazio hori kudeatzea. Interneten bitartez jasotzen dituzten eduki asko ez dira egiazkoak edo seguruak. Hori dela eta, garrantzitsua da eduki horiek pentsamendu kritikoarekin aztertzen jakitea.

Zer da FAKE bat?

Fake: benetakoaren itxurarekin ematen den, baina erreala edo egiazkoa ez den informazioa.

Deepfake: pertsona baten bideoak, irudiak edo ahotsa aldatzeko eta, era horretan, haren mezua edo ekintzak manipulatzeko aukera. Eduki faltsu horren helburua da pertsona jakin batek adierazpen faltsu batzuk egin zituela edo errealak ez diren ekintzak gertatu zirela sinestaraztea.

6.1 Jarduera

Banatu ikasleak 4 taldetan, eta eskatu Interneten bideo faltsuak bilatzeko (bat baino gehiago, errepikatuko balira ere).

Talde bakoitzak berea erakutsiko die gainerakoei, eta azalduko die nola egiaztatu duen faltsua dela.

Pentsamendu kritikoa lantzea:

› **Informazioaren analisia.** Pentsamendu kritikoa ikasleek mezu, meme edo albiste bat jasotzen duten bakoitzean praktikan jarri beharreko trebetasun bat da, eta haren egiazkotasunari eta helburuari buruzko gogoetan datza.

› **Funtsezko puntuak: iturria, erreferentziak eta idazketa.** *Fake new* izenekoen ezaugarriak ezagutzeko modua: jatorria ez da iturri aintzatetsi edo ofizial bat izaten, eta, askotan, hizkuntza profesionaltasun urrikoa izan ohi da.

› **Informazioa bilatu eta kontrastatzea.** Eduki bera hainbat informazio-iturritan bilatu behar da.

› **Segurtasuna egiaztatzea klik egin aurretik.** Oso garrantzitsua da webgune edo eduki baten fidagarritasuna egiaztatzea fitxategiak deskargatu edo esteketara jo aurretik.

› **Eduki faltsuak edo engainagarriak zabaltzen ez parte hartzea.** Egiaztatu gabeko eduki bat berehala birbidaltzeak gezur baten konplize inkontziente bihurtzen gaitu.

Esteka interesgarriak:

☞ DEEP FAKE-A

☞ FAKE NEW-AK

Oharra: ikasgelako aniztasunarekin eta gustuekin bat datozen bideo gehiago bilatu ditzakezu gaiari buruz YOUTUBEn.

6.2. Pribatutasunaren babesa.

Pribatutasunaren kudeaketa

Interneten borondatez argitaratzen dugun informazio pertsonal guztia erabiltzeko moduari pribatutasunaren kudeaketa deitzen zaio. Ezinbestekoa da oreka bat bilatzea gure informazio pertsonala agerian jartzeak eskaintzen dizkigun onuren eta lotutako arriskuen artean.

Gure pribatutasuna zaintzea gure online ospea zaintzea da, hau da, Interneten dugun irudia positiboa izan dadin saiatzea, inplikazio larriak izan baititzake gure bizitza errealean.

6.2 Jarduera

Eskatu ikasleei Instagramen beren pribatutasunari buruzko informazioa ematen duten argazkiak eta mezuak bilatzeko.

Erakutsi argazki horiek eta haiei erantsitako mezuak. Zer informazio pribatu biltzen dute?

Gure pribatutasunaren kudeaketa lantzea:

› **Argitalpen inkontzientea.** Norberaren argitalpen batetik ondoriozta daitekeen informazioa.

› **Beste batzuen argitalpena.** Erabiltzaile baten datuak, beste pertsona batzuek Interneten argitaratuak.

› **Argitalpen automatikoa.** Automatikoki sortutako eta argitaratutako informazioa. Adibideak: azken konexioaren ordua, bisitatutako webguneak, geolokalizazioa eta abar.

6.3. Gehiegizko erabilera

Haurrek eta nerabeek gero eta denbora gehiago ematen dute pantailen aurrean. Portaera horrek eragin negatiboa du beren harreman sozialetan, jokabidean eta emozioak kudeatzeko gaitasunean.

6.3 Jarduera

Gailu teknologikoen erabilerari buruzko testa.

- Inprimatu paper-orri batean honako galdera hauek, eta eskatu zintzotasunez erantzun dezaten:
  - › Lagunekin edo senideekin zaudenean, beste pertsona batzuekin txatean aritzen al zara haiek hitz egiten ari diren bitartean?
  - › Egunean bi ordu baino gehiago ematen al dituzu pantailen aurrean?
  - › Zure sare sozialetan gertatzen denari adi egoten al zara etengabe?
  - › Asko kezkatzen al zara bateriarik gabe geratu behar duzunean?
  - › Etxetik kanpo, norabait joaten zarenean wifi konexioa duzula egiaztatzen al duzu lehenik eta behin? Eta haserretu egiten al zara estaldurarik ez duzunean?

  Galdera horiei baietz erantzuten badiete, gehiegizko erabilera baten aurrean gaude seguruenik. Proposatu esperimentu bat: egun oso bat mugikorrik gabe ematea.
- Mugikorrak emango dizkizute, eta kutxa batean gordeko dituzu, giltzarrapo batekin. Hurrengo egunean, smartphonerik gabeko egunaren esperientzia azaldu beharko diete ikasgelako gainerako kideei.
  - › Mugikorraren falta sentitu al dute? Zenbat aldiz?
  - › Nola komunikatu dira beste pertsona batzuekin?
  - › Nolako sentsazioak izan dituzte?
  - › Bizi al litezke smartphonerik gabe?
  - › Zer ikasi dute telefono mugikorrarekin duten erlazioaren inguruan?

Adikzio digitalak lantzea:

Kontuz honako hauekin:

- › Interneten edo bideojokoetan gero eta denbora-tarte handiagoan konektatuta egoteko **irrika bizia edo premia kontrolaezina**. Tolerantzia deitzen zaio.
- › **Abstinentzia-sindromearen** agerpena. Kontakturik edo estaldurarik ez dagoenean haserrea eta suminkortasuna sentitzea.
- › **Taldearekiko mendekotasun soziala.** Gurekin elkarreragiten duten adiskide birtualen berehalako oniritzia eta onarpen soziala behar dugunean.
- › **Ohiko interesez eta jarduerez** (eskolakoez zein pertsonalez) **ez arduratzea.**
- › Norberaren jokabidearen gaineko **gero eta kontrol txikiagoa**: norberaren portaera kudeatzeko gai ez izatea, eta, deskonektatu nahi izanik ere, ezin izatea.

6.4. Webgune arriskutsuak

Zer dira?

Internet oso tresna baliagarria da haurrek eta gazteek kirolei, musikari, jokoei, modari eta abarri buruzko interesak edo kezkak partekatzeko edo zabaltzeko. Baina, era berean, haurren eta gazteen garapenerako kaltegarriak diren inguruneak daude, haien adinerako arriskutsuak edo desegokiak diren gaiak lantzen baitituzte.

› **Estremismoa, gorrotoa eta indarkeria:** intolerantziaren sustapena, gorroto-diskurtsoak, etniari, erlijioari, generoari, sexu-identitateari eta abarri lotutako arrazoiek eragindako diskriminazioa eta indarkeria.

› **Jokoa eta adikzioa:** esperientzien bitartez pertsonaren adikzioa (gero eta denbora gehiago ematea konektatuta, emozioen edo irabazi ekonomikoen bila) bilatzen duten online jokoen inguruneak.

› **Osasunerako arriskuak:** anorexiaren eta bulimiaren aldeko webguneak, drogak sustatzen dituztenak, erronka arriskutsuetan parte hartzera bultzatzen dutenak, autolesioa eta suizidioa sustatzen dutenak eta abar.

› **Adingabeen sexu-abusua:** adingabeen sexu-abusua bultzatzea, jokabide horien justifikazioa, adingabeen sentsibilizaziorik eza eduki sexual eta pornografikoen aurrean, eta biktimak erakartzeko ahaleginak.

6.4 Jarduera:

Asier 13 urteko mutila da, eta izugarri gustatzen zaio futbola. Adiskideekin futbolean aritzeaz gain, bere talderik gogokoenaren partidu guztiak ikusten ditu. Familiak tablet bat oparitu zion urtebetetze-egunean, eta liga birtual batean bere talde propioa kudeatzea ahalbidetzen dion joko batean aritzeko erabiltzen du. Oso ona da, eta jokalari anitzeko moduan konektatzen denean, ia beti irabazten du.

Inoiz ez du arazorik izan eskolan, baina duela astebetez geroztik etxean dago, gaixorik omen baitago. Haren medikuak ez dio ezer aurkitu, eta, beraz, ez diote garrantzi handirik eman, adinaren gorabeherak izango direlakoan.

Gaur goizean, ikaskide baten amak Asierren etxera deitu du, aitarekin hitz egiteko asmoz. Alaba kezkatuta dago, eta kontatu dio Asierrek kreditu-txartel baten datuak sartu zituela online joko batean, konektatu ahal izateko. Hasieran ez zioten ezer kobratzen, baina hilabete igaro ondoren astero bitcoin izeneko monetan kargu bat zuela konturatu zen. Ez zen hutsegiteaz jabetu aitari VISAn kargu arraro batzuk zituela esaten entzun zion arte. Ia 200 euro hilabete batean!

Hasi irakurri duten testuari buruzko eztabaida.

› Zergatik sartu da Asier arazo horretan?
› Saihestu al zezakeen?
› Ongi egin al du ikaskideak amari kontatzean?
› Zure ustez, zer esango diote gurasoek Asierri, eta zer egingo dute?

6.5. Ziberjazarpena

Zer da?

Ziberjazarpena errealitate bat da ikasgeletan, gero eta kasu gehiago ateratzen dira argitara, eta adin eta giro desberdineko haurrak eta gazteak hartzen ditu eraginpean. Jazarpen-mota horretan, baliabide digitalak erabiltzen dira biktimari jakinaren gainean eta behin eta berriz kalte egiteko.

6.5 a Jarduera

Amina ikasturtea hasita zegoela iritsi zen ikasle berria da, 14 urtekoa. Hasieran, oso pozik zegoen eta haren errendimendu akademikoa nabarmen hobetu zen hilabete gutxiren buruan. Amina, gainerako ikaskide guztiak bezala, WhatsApp talde batean sartuta zegoen, halako batean taldetik kanpo utzi zutela konturatu zen arte. Aminak ez zuen ulertzen zer gertatu zen, baina inork ez zion azalpenik ematen, eta barre egiten zioten ezkutuan.

Handik gutxira, ezagutzen ez zituen profil batzuetatik iraintzen zuten mezu batzuk hasi zen jasotzen bere sare sozialetan. Mezuak egunero eta edozein ordutan iristen ziren (jaiki berritan, eskola batetik besterako tartean, arratsaldean, oheratu aurretik…, eta gau batzuetan ere mezu berrien hotsarekin esnatzen zen).

Hurrengo astean, ukituak zituzten Aminaren argazki batzuk zabaldu ziren, Amina barregarri uzteko asmoz. Horrez gain, argazki horietako asko biltzen zituen kontu faltsu bat ireki zuten Instagramen, edonork iruzkin desatseginak egin ahal izateko.

Aminak ez zekien zer egin egoera hori gelditzeko.

Hasi irakurri duten testuari buruzko eztabaida.

Eztabaidaren lehen zatia:

› Zure ustez, zer egin du Aminak WhatsApp-etik kanpo geratzeko?
› Nork erabakitzen du nor sartzen den WhatsApp talde batean eta nor irteten den bertatik?
› Zergatik bidaltzen dizkiote mezuak ezagutzen ez dituen pertsonen profiletatik?
› Aminak zergatik ez du itzaltzen bere mugikorra mezu gehiago ez jasotzeko?
› Zer egin behar du Aminak? Barkamena eskatu behar al du WhatsApp taldean berriz sartzeko?
› Zure ustez, aurre egin beharko al lieke jazartzen ari zaizkionei?

Ziberjazarpena lantzea:

› **Asmo txarrez egindako kaltea:** jazarpenaren bidez kalte psikologikoa, emozionala eta soziala egin nahi zaio biktimari.
› Mota askotakoa izan daiteke: isekak, umiliazioak, irainak, zurrumurruak zabaltzea, adiskideengan eragitea isolatuta uzteko eta abar.
› **Errepikatua:** kaltea ohikoa izaten da, eta egunerokoa ere izan daiteke. Ez da gorabehera bakana.
› **Adingabeen artean:** ohikoena da ziberjazarpena adingabe batek edo adingabe-talde batek beste adingabe bati egitea, eta biktimarekin nagusitasun- edo botere-rol bat hartzea.
› **Baliabide digitalen bidez:** mugikorrak, sare sozialak, argazkiak, bideoak, online jokoak, posta elektronikoa eta abar erabiltzen dituzte tresna gisa.

6.5 b Jarduera

Zergatik da hain kaltegarria eta konplexua ziberjazarpena?
Gailu teknologikoen erabilerarekin, **portaeraren desinhibizioa** gertatu da. Jazarleak jardutera (aurrez aurre egingo ez luketena) edo modu oldarkorragoan edo agresiboagoan jardutera ausartu daitezke:

Egin 4 talde ikasgelan; bakoitzak honako gai hauetako bat garatu beharko du:

› Anonimatua Interneten.

› Biktimarekiko enpatiarik eza. Txantxa baino ez da.

› Mezuen berehalakotasuna. Zergatik da arriskutsua?

› Jazarpen aktiboa eta pasiboa. Taldearen presioa.

Aurkezpenak ebaluatzeko elementuak:

› Sareak eskaintzen duen **ustezko anonimatuak** zigorgabetasunaren eta erantzukizunik ezaren sentsazio faltsua sorrarazten du. Gainera, jazarleak harrapatuko ez dutela sentitzen du.

› Biktimarekiko **distantzia fisiko** errealak harekiko enpatia murrizten du, eta eragindako kaltearen inguruan kontzientziatzea eragozten du. Biktimaren mina ikusten ez denez gero, aurrez aurre aspalditik egingo ez liratekeen portaerek iraun egin dezakete.

› Ziberjazarpenaren lekukoek errazago egin dezakete bat, taldearen presioaren ondorioz. Ez da beharrezkoa biktimari zuzenean erasotzea; nahikoa da beste pertsona baten jazarpen-mezuak partekatzea edo «gustatzen zait» sakatzea.

› Komunikazioen **berehalakotasunak** erantzun bizkorrak eta oldartsuak emateko arriskua dakar, eta baliteke bidalitako mezu batzuez edo gogoetarik egin gabe agertutako jarrerez damutzea.

6.6. Sareko segurtasuna

Gure gailuetan, informazio pertsonal asko, mezuak, argazkiak, pasahitzak eta abar daude biltegiratuta. Inork informazio hori eskuratuko balu, gure ospe digitala eta gure bizitza erreala kaltetzeko adina tresna izango lituzke.

Hori dela eta, guztiz beharrezkoa da gure gailuak eta gure pasahitzak sare sozialetan eta Interneten gainerako zerbitzuetan babestea.

6.6 Jarduera

Amaia oso neska alaia da, baina nortasun handikoa. Ez zaizkio gustatzen ikasgelako adarjotzeak, eta ikasgelan aurre egin dion ikaskide bat Amaiari min emateko modua bilatzen ari da.
Gaur, ikastetxeko jangelan, Amaiak mahai gainean utzi du motxila une batez, janari bila joateko. Amaia ikusi ezin duen ikaskideak berehala hartu du haren telefonoa, eta hainbat pasahitzekin saiatu da. Oso erraza izan da asmatzea! 123456 zenbakia zen. 2 minututan, Amaiaren adiskiderik onenari buruzko oso mezu desatsegina idatzi du, eta kontaktu guztiei bidali die. Adiskiderik onena ez du Amaiarekin hitz egin nahi orain, eta ez du sinetsi nahi ez dela Amaia izan.

Sareko segurtasuna lantzea.

› Berrikusi ikasleekin gailuak erabiltzeko oinarrizko segurtasun-sistemak.

› Erabili SAREKO SEGURTASUNA programa lan-tresna gisa.

07.EBALUAZIOA

Ebaluazio-irizpideetan, batez ere, Internetekin eta sareko segurtasunarekin lotutako gaien inguruko sentsibilizazioa hartuko da kontuan.

› Pasahitzak erabiltzeko politika seguruak erabiltzen ditu, informazio pertsonala babesteko.

› Gailu fisikoen segurtasun-arriskuak aztertzen eta ezagutzen ditu, eta babes-ohitura egokien jakitun da.

› Segurtasun-jokabide aktibo eta pasiboak ditu datuak babesteko eta informazioa trukatzeko.

› Hirugarrenekiko begirunez jarduten du norberak edo beste norbaitek ekoiztutako edukiak erabili eta trukatzean.

› Hainbat informazio-iturri erabiltzen ditu eta nabigatzen duenean badaki zein garrantzitsua den identitate digitala eta webean dauden iruzur-mota guztiak ezagutzea.

› Jabetza intelektuala errespetatzen du informazioa trukatzen duenean.

› Segurtasun informatikoari lotutako eguneratzeak, birusen aurkako softwareak, suebakiak eta bestelako iragazkiak instalatzeko gai da.

› Enpatia erakusten du sareko jazarpenaren eta bestelako delituen biktimekin.

08.GLOSARIOA

› **Antibirusa**
Antibirusaren funtzioa da malware bidezko infekzioari aurrea hartzea eta, infektatuz gero, malware horren aurka jardutea.

› **Bibrazio faltsuaren sindromea (vibranxiety)**
Gure garunean sortzen den eta jasotako bulkada oro telefono mugikorraren soinuarekin edo bibrazioarekin lotzen duen estres-egoera.

› **Birus informatikoa**
Edozein sistema eragile, programa edo gailuren funtzionamendua baimenik gabe aldatzeko edo hondatzeko helburua duen programa.

› **Check bikoitzaren sindromea**
Larritasuna sortzen du whatsapp-a bidali diogun pertsona linean zegoela edo mezua jaso duela dakigunean, baina erantzun ez duenean.

› **Fomo sindromea**
Gure adiskideek planak islatzen dituztenean eta gonbidatzen ez gaituztenean sortzen den ezinegona.

› **Google efektua**
Ikasteko edo buruz ikasteko interesik eza dakarren nahasmendua. Horren ondorioz, informazioa ahaztu egiten da, eta ez da egituratzen aurrerago gogoratzeko.

› **Harrak**
Fitxategiak infektatzeaz gain, zabaldu egin daitezke; horretarako, kontaktuen zerrendaren bitartez birbidali ohi dira.

› **Hijacker**
Guk eskatu gabe irekitzen diren programak eta tresnak (pop-up motakoak edo leiho emergenteak) instalatzen ditu, eta alarma faltsuak dituzten iragarkiak agertzen dituzte, programak deskargatu ditzagun (ordainpeko ustezko antibirusak).

› **Hikikomori sindromea**
Borondatezko eta muturreko isolamendua aldi luze batean; kanpoko munduarekiko sentimendu negatiboak eta, zenbaitetan, indarkeriazkoak sorrarazten ditu.

› **Infosurfing-a**
Helburu argirik gabe nabigatzea.

08.GLOSARIOA

› **Internet Rage**
Erabiltzen ari garen sarearen abiadurarik ezak edo komunikatzea eragozten diguten akats teknikoek sorrarazten diguten estresa. Sorrarazitako amorruaren ondorioz, modu txarrak erabiltzen dira konpondu beharreko arazoarekin zerikusirik ez duten pertsonen aurka.

› **Keyloogger**
Edozein teklatutako teklen pultsazioa erregistratzen eta atzematen duen programa gaiztoa. Informazioa fitxategi batean gordetzen da, ondoren administratzailearengana itzultzen da, eta erabiltzaile-izenak, pasahitzak, kreditu-txartelen zenbakiak eta mota guztietako datu pertsonalak eta pribatuak lapurtzeko balio du.

› **Malwarea**
Programa gaiztoak, oro har.

› **Nomofobia**
Telefono mugikorra erabiltzerik ez dagoenean edo estaldurarik ez dagoenean sortzen den beldur irrazionala, ziurgabetasuna eta larritasuna.

› **Phubbing-a**
Mugikorraren pantailari oso adi egotea eta, horren ondorioz, gurekin dauden pertsonei arretarik ez eskaintzea.

› **Porno revenge edo mendeku-pornoa**
«Porno revenge» (edo mendeku-porno) terminoak sarean sexu-edukiko argazkiak edo bideoak bertan agertzen diren pertsonen baimenik gabe zabaltzeko ekintza adierazten du.

› **Ransomware, kriptobirus, cryptowall edo cryptolocker izeneko malwareak**
Edozein gailuren memorian dagoen informazioaren zati bat bahitzeko edo mugatzeko funtzioa duten malwareak.

Ekipamendua blokeatu eta informazioa enkriptatzen dute, eta pantaila emergente baten bidez gure datuak bahitu dituztela eta erreskate bat ordaindu behar dela (normalean moneta birtualean, arrastorik ez uzteko) jakinarazten digute.

› **Rogue softwarea**
Detektatutako akats edo birus bat desagerrarazteko laguntza eskaintzen du. Antibirus faltsua da. Webgune arriskutsuak, legez kanpoko deskargak edo doako programak bisitatzean instala daiteke.

08.GLOSARIOA

› **Spyware edo software espioia**
Ekipamendu batean egindako jarduera zelatatzen edo atzematen du, online zein offline.
Spyware Adware edo publizitate-software espioia: instalatzeko baimena eskatzen du, eta nabigazio-ohiturak jasotzea du helburu, publizitate pertsonalizatua bidaltzeko.
Spyware gaiztoa: jasotzen diren datuek delitu-izaerako asmoak ezkutatzen dituzte.

› **Stealer**
Gailuan sartzen da, eta programetan, sare sozialetan eta banka elektronikoan sartzeko gure pasahitzak eta datuak baino ez ditu lapurtzen.

› **Suebakia edo firewall**
Babesten dituen ekipamenduetan sartzen diren eta bertatik irteten diren datuen trafikoa aztertzen eta iragazten du.

› **Troiarrak**
Legezko programa baten itxurapean, infektatutako ekipamendu edo sistemaren urruneko kontrola eskuratzen du.

› **Vamping-a**
Gauez gailu elektronikoak erabiltzeko ohitura. Lorik ezaren ondorioz, nekea, suminkortasuna, loezina eta ikusmen-nekea sortzen da.

› **Ziberadikzioa**
Sarea etengabe kontsultatzeko eta erabiltzeko premia kontrolaezina.

› **Ziberludopatia edo gambling-a**
Online jokoarekiko adikzioa; ordainpekoak, apustuak edo joko indibidualetan edo jokalari anitzekoetan denbora inbertitzea eskatzen dutenak izan daitezke.

09.LINKS

- www.incibe.es
  Zibersegurtasuneko Institutu Nazionala.
- www.osi.es
  Internautaren Segurtasun Bulegoa.
- www.red.es
  Red.es proiektua.
- www.pantallasamigas.net
  “Pantaila lagunak” hezkuntza-proiektua.
- www.is4K.es
  Haurrentzako Internet seguruaren proiektua.
- www.padres20.org
  Pares 2.0
- www.aepd.es
  Datuak Babesteko Espainiako Bulegoa.
- www.avpd.euskadi.eus
  Datuak Babesteko Euskal Bulegoa.
- www.basquecybersecurity.eus
  Zibersegurtasunaren Euskal Zentroa.
- www.ertzaintza.euskadi.eus/lfr/eu/web/ertzaintza/-/talde-espezializatua
  Delitu informatikoen salaketa Ertzaintzan.