



“SEGURTASUNA ETA KONFIDENTZIALTASUNA INTERNETEN”



AURKIBIDEA

1. Sarrera.....	4
2. Birus informatikoak	4
Birusen bizitza	4
Sorrera	4
Eratzea	4
Kopiatzea.....	5
Aktibazioa.....	5
Aurkikuntza	5
Asimilazioa.....	5
Ezabatzea	5
Birusen sarbideak	7
Disko-unitate aldagarriak	7
Ordenagailu-sareak.....	8
Internet.....	8
Birusek infektatzen dituzten ordenagailuko elementuak.....	10
Hedapena	11
Eragindako kalteak eta ondorioak	12
Antzematea	13
Babes-neurriak.....	15
3. Segurtasuna merkataritza elektronikoan.....	24
Zerbitzari seguruak	24
Gune seguru bat nola antzeman.....	25
Segurtasun-ziurtagiria.....	30
Segurtasun-ziurtagiria nola ikusi	32
Merkataritza elektroniko segururako aholkuak	36
4. Posta elektronikoa	37
PGP.....	37
Sinadura digitala	38
5. Chat-eko bezeroen arriskuak	39
6. Firewall edo suebakia.....	39
7. Spam-a: mezu baztergarria	41
Nola lortzen dituzte helbide-zerrendak?.....	42
Nahi ez ditugun e-mail komertzialen aurrean zer egin?	43
Spam-aren aurrean nola jardun.....	43



8. Interneteko 10 maula ezagunenak	44
9. 906 telefono-zenbakien iruzurra	46
Iruzur honen aurrean egon daitezkeen irtenbideak	47
10. Helbide interesgarriak	48



1. SARRERA

Internet segurua al da? Erosketak edo banku-transakzioak beldurrik gabe egin al ditzakegu? Nola ekidin birus batek gure datuak suntsitzea? Gure posta elektronikoa benetan konfidentziala al da? Inork eskura al ditzake gure ordenagailuko datuak Interneten konektatuta gauden bitartean?

Aurreko horiek bezalako galderak egiten ditugu Interneteko erabiltzaile guztiok, hacker (pirata informatikoa) batek ustez erakunde seguru edo enpresa garrantzitsuen hainbat sekretu eskuratu dituela bezalako berriak entzuten ditugunean.

2. BIRUS INFORMATIKOAK

Birusak, nahi ez ditugun ondorio kaltegarriak eragiteko gure ordenagailutan hainbat modutara sartzen diren programa informatikoak dira. Birus bat gure PCan sartzen den bakoitzean, infekzio bat gertatu dela esango dugu.

“Birus ideala” (birus-egileen ikuspuntutik) ezkutuan hedatzen da, inork antzeman gabe, eta ordenagailuak jada kutsatuta daudenean hasten dute euren ekintza suntsitzailea.

BIRUSEN BIZITZA

Birus informatikoek, sortzen direnean hasi eta erabat erauzten dituztenean amaitzen da. Ondoko laburpen honek etapa bakoitza laburtzen du:

Sorrera

Duela zenbait urte arte, birus bat sortzeko assembler programazioaren lengoia ezagutu behar zen. Gaur egun, programazio-arloan ezagutzaren bat duen edozeinek birus bat sor dezake. Orokorrean, birusak, ordenagailuak kaltetu nahi dituzten pertsona maltzurak dira.

Eratzea



Birusa sortu ondoren, programatzaileak kopiak egiten ditu barreiatzen direla ziurtatzeko. Orokorrean hori, programa ezagun bat infektatuz edo kopiak bulego, ikastetxe edo beste edozein erakundetan banatuz lortzen da.

Kopiatzea

Birusak naturalki kopiatzen dira. Ondo diseinatutako birus bat, aktibatu aurretik luzaroan kopiatuko da. Horri esker, alde guztietatik barrea daiteke.

Aktibazioa

Errutina kaltegarriak dituzten birusak, hainbat baldintza emanez gero aktibatuko dira, adibidez, egun jakin batean edo erabiltzaileak gauza zehatzen bat egiten duenean. Errutina kaltegarririk ez duten birusak ez dira aktibatzen baina kalteak eragiten dituzte diskoan espazioa hartuz.

Aurkikuntza

Fase hori normalean, aktibatu ondoren dator. Birus bat aurkitu eta isolatzen denean, Washington DCn dagoen International Security Association elkartera igortzen da, bertan dokumentatu egingo da biruskontrako produktuak garatzen dituztenei banatzeko. Aurkikuntza normalean, birusa komunitate informatikorako mehatxu bihurtu baino urte bete lehenago ematen da.

Asimilazioa

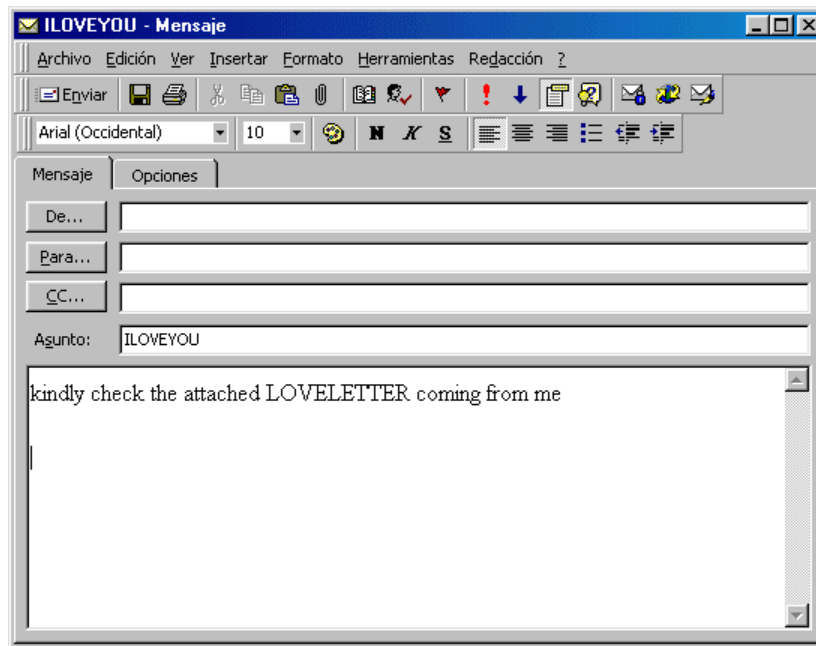
Puntu honetan, biruskontrako produktuak garatzen dituztenek euren programak birus berriak antzemateko aldatzen dituzte. Horrek, egun batetik sei hilabetera eman dezake, nork garatzen dituen eta birus-motaren arabera.

Ezabatzea

Gutxieneko erabiltzaile-kopuruak biruskontrako eguneratua instalatzen badu, edozein birus ezaba dezake. Orain arte, birus bat bera ere ez da erabat desagertu, baina zenbaitek mehatxu izateari utzi diote.

Horietako bat, dauden milaka biruskontrakoen artean adibide bezala, VBS/Love Letter (I LOVE YOU) da. Biruskontrako honek ordu gutxi behar izan zituen mundu osoan milaka ordenagailu infektatzeko. Ikus dezagun birus honek nola funtzionatzen duen:

1. Posta elektronikoko mezu bat jasotzen da eta bertan **LOVE-LETTER-FOR-YOU.TXT.VBS** izeneko fitxategia erantsita dakar; edo, **LOVE-LETTER-FOR-YOU.HTM** fitxategia, IRC (Chat –Internet idatzitako elkarrizketak) motako kanal baten bidez konektatuta egongo bagina.



2. Klik bikoitza eginez fitxategia exekututzen bada, birusa aktibatu egingo da.
3. Orduan posta elektroniko bidez norberaren helbidera (**LOVE-LETTER-FOR-YOU.TXT.VBS** fitxategia) eta Outlook Expresseko Helbide Liburuan gordetako helbide guztietara bidaltzen du.
4. Infektatutako PCa, Chat kanal batera konektatuta badago (IRC), birusak **LOVE-LETTER-FOR-YOU.HTM** fitxategia kanal horretara konektatutako lagun guztiei bidaliko die.
5. Oso denbora-tarte laburrean I LOVE YOU birusa mundu osoko ehunka edo milaka ordenagailutan sartuko litzateke.
6. Birusak, hainbat fitxategitako edukiak behin betiko ezabatzen ditu: **VBS** (Visual Basic Script), **VBE**, **JS** (Java Script), **JSE**, **CSS** (estilo-fitxategia), **WSH**, **SCT**, **HTA** **JPG** (irudiak), **JPEG** (irudiak), **MP3** (soinua) edo **MP2** (soinua).
7. VBS/LoveLetter-ek telefono-konexio baten (Internet adibidez) bidez sare batean sartzeko ez du pasahitza aldatzen uzten.
8. Erabilizailearen eta infektatutako ordenagailuaren informazio konfidentziala lortzen da (infekzio-data, infektatutako ordenagailuaren helbidea, infektatutako



ordenagailuaren izena, erabiltzailearen izena, sarerako telefono-sarbideari dagokion pasahitza, konexio hori egiten den telefono-zenbakia, eta abar) eta Filipinetako posta elektronikoko helbide batera igortzen da.

BIRUSEN SARBIDEAK

Gure ordenagailua birus batekin infektatzeko, birusaren kodea gure ordenagailuan grabatu behar da. Birus batek horretarako bide errazena fitxategiak kopiazen ditugunean da, kopiazen ari garen fitxategiaren barruan ezkutatu besterik ez baitu egin behar.



Informazioa bakarrik irakurtzen badugu ezin dugu infektatu, adibidez, CD baten edukia irakurtzen badugu edo Web orri bat bisitatzen badugu ez dago infektatzeko arriskua. Hori arau orokorra da, baina, aurrerago ikusiko dugun bezala, salbuespenak daude; zenbaitetan gerta daiteke, gu jabetu gabe, gure ordenagailuan gauzak grabatzen egotea.

Exekutatzeko hainbat modu daude, adibidez, guk geuk exekuta dezakegu postako fitxategi erantsia irekitzean. Auto-exekutatzeko beste modu bat da, ordenagailua abian jartzen dugun bakoitzean exekutatzeko ordenagailuaren konfigurazioa aldatzea.

Birusak gure ordenagailuan, informazioa trukatzeko erabiltzen ditugun hainbat modutan sar daitezke. Funtsean bitarteko horiek hiru taldetan banatzen dira:

- ✓ Disko-unitate aldagarriak.
- ✓ Ordenagailu-sareak.
- ✓ Internet.

Disko-unitate aldagarriak

Informazioa trukatzeko edo gordetzeko erabiltzen diren gure ordenagailutik kanpo dauden unitate fisikoak dira: disketeak, CD-ROM eta DVD-ROM. Disko-unitate batean



gordetako programa, fitxategi, posta-mezu eta antzeko bat infektatuta badago, gure ordenagailuan sartzean hau ere infekta dezake.

Garai batean infekzio-iturri garrantzitsu izan ziren disketeek gaur egun infekzio guztien %10 eragiten dute besterik gabe.

I LOVE YOU birusak disketea baino askoz ere azkarragoko hedapen-metodo bat erabiltzen du (posta elektronikoa), baina infekzioa eragiten duen fitxategia diskete, CD-ROM edo beste edozein unitatetan egon daiteke.

Ordenagailu-sareak

Sare bat, elkarren artean fisikoki konektatutako (kable, modem, router, eta abar bidez) ordenagailu-multzo bat da, ordenagailu horien artean, disko-unitate aldagarriak erabiltzeko beharrik gabe informazioa transferitu ahal izateko.

Sareko ordenagailu batek birusa duen informazioa badu, gainerakoek informazio hori eskuratzen dutenean infektatu egin daitezke, guztiak katean eroriz (enpresa osoen jarduera gelditu duten duela gutxi izandako infekzioen kasuan bezala).

Infekzioa eragiten duen fitxategia, I LOVE YOU birusaren kasuan, ordenagailu batetik bestera oso erraz igaro daiteke.

Internet

Sarea, ordenagailuen artean informazioa transferitzeko bitarteko garrantzitsuena bihurtu da, eta ondorioz, gaur egun birus gehienak bertatik sartzen dira. Hala ere, Internetek informazioa trukatzeko modu ugari ematen ditu, eta bakoitzak ezaugarri eta arrisku-potentzial diferenteak ditu.

Posta elektronikoa

Gaur egun dagoen infekzio-metodo garrantzitsuena da. Birusei oso azkar hedatzeko aukera ematen die egunero milioika posta igortzen baitira.

Postaren arrisku handiena bere ezaugarrien ondorioz ematen da:

- ✓ Erantzuteko eta hedatzeko izugarriko gaitasuna (posta infektatu bat zenbait minututan mundu osoko milaka ordenagailutara hel daiteke).
- ✓ Posta-sistemarako bereziki diseinatuta ez dauden biruskontrakoentzat aztertzeo zailtasun handia.



- ✓ Ordenagailuen artean konektatzeko ahalmen handia (ia edozein motako ordenagailu edo plataforma bidez mezuak bidali eta jaso daitezke).
- ✓ Birus horietako askok, erabiltzaileak bere Helbide Liburuan sartuta dituen pertsona guztien helbidetara autobidaltzeko duten ahalmena.

Zehazki I LOVE YOU birusak, berehala mundu osoan hedatzeko bitarteko hau erabiltzen du: ordenagailu bat infektatzean, zuzenean Outlook Expresseko Helbide Liburura doa eta liburu horretan dauden helbide guztietara autobidaltzen da.

Web orriak

Normalean Web orriek testua, grafikoak, soinua, animazioak eta bideoak dituzte. Nabigatzaileak, elementu horiek irakurri eta pantailan bistaratzeko dituzte bakarrik. Horrenbestez, Web orriek ezin dituzte ordenagailuak infektatu, ez baitute gure ordenagailuan exekutatu den programarik izaten.

Hala ere hainbat Web orriek ActiveX eta Applets Java kontrolen bidez gure ordenagailuan informazioa graba dezakete gu horretaz jabetu gabe. Hori, oraindik oso gutxi erabili den infektatzeko bitarteko bat da. Noski, Sareko orri gehienetan lasai nabigatu dezakegu. Ia %100eko zerbitzariak biruskontrakoak dituzte, eta eurei esker bertako Web orrien bidez infektatzeko arriskua ekiditen dute.

Behera kargatzea (Download)

Esteka batean klik eginez fitxategiak beheara kargatzeko aukera ematen duten Web ugari daude. Elkarrizketa-koadroa irekitzen da gure disko gogorreko zein karpetan fitxategia jarri nahi dugun galdetzeko eta beheara kargatzen hasteko. Behera kargatzen hasten garen fitxategia infektatuta bada, gure ordenagailua infekta dezake.

Fitxategien transferentzia (FTP)

Gure dokumentuak, munduko edozein tokitan dauden beste hainbat ordenagailutan ipintzeko (upload) edo ordenagailu horietatik gurera fitxategiak kopiatzeko (download) balio duen sistema da. Fitxategi bat deskargatzean, zuzenean gure ordenagailuan kopiatzen dugu; fitxategi horrek birusa izan dezake.

Demagun horietako batean I LOVE YOU birusaren zati den **LETTER-FOR-YOU.TXT.VBS** fitxategia dagoela. Fitxategia beste ordenagailu batean kopiatu eta exekutatu bada, infektatu egingo da.

Berri-taldeak, banaketa-zerrendak, foroak



Eztabaida-foreok, banaketa-zerrendek eta berri-taldeek posta jaso eta bidali, albisteak argitaratu eta Interneten bidez beste hainbat lagunekin zenbait gairi buruz eztabaidatzeko aukera ematen dute. Bakoitzak dokumentazio erantsia izan dezake (**LETTER-FOR-YOU.TXT.VBS** bezalako fitxategi infektatuak barne). Era berean, berri-talde jakin batean harpidetutako erabiltzaile bat infektatzen egon daiteke eta (berak jakin eta baimendu gabe) mezu infektatua taldeko lagun guztiei bidal diezaieke.

Fitxategiak transmititzeko edozein bide potentzialki birus bat igortzeko erabil daiteke.

Mezuak bidaliz eta jasoz parte hartzeagatik bakarrik ezin da kutsatu.

IRC

IRC, Internet bidez idatziz komunikatzeko modu bat da. Zenbait kanal ezartzen dira, eta kanal horien bidez pertsona-kopuru zehaztugabeak elkarrizketan parte har dezake (testu idatzi bidez). Birus batek bitarteko hori erabil dezake norberari igortzeko edo kanal horretara konektatuta dagoen pertsona bakoitzari jada infektatuta dauden fitxategiak bidaltzeko.

Adibidez, kanalera konektatutako pertsona bat I LOVE YOU birusarekin infektatuta badago, horrek automatikoki **LOVE-LETTER-FOR-YOU.HTM** fitxategia kanal horretara konektatutako erabiltzaile GUZTIETARA bidaliko du.

BIRUSEK INFEKTATZEN DITUZTEN ORDENAGAILUKO ELEMENTUAK

Helburu nagusi bezala, ordenagailuetan jasotako informazioa dute, hots, fitxategiak (testuak, irudiak, datu-baseak, kalkulu-orriak, eta abar) edo ordenagailuan instalatutako programak. Birus batek infektatutako fitxategi bat zabaldu edo exekutatzeko denean, birusa aktibatu eta lanean hasten da. Beste hainbat kasutan, birusek baldintza jakin bat eman dadin, edo egun jakin bat hel dadin itxaroten dute aktibatuzeko.



Disko-unitateak (fitxategiak gordetzen diren tokia) ere izan daitezke birus baten beste helburu bat. Bertan, birusek ordenagailuaren abiatzeko sisteman (berari esker ordenagailu bat pizten da, diskoa dagoela antzematen du eta, ondorioz, bertan lan egiteko aukera ematen du) eta antolakuntzan (sistema horren bidez bertan jasotako informazioa, bertara nola heldu eta abar kontrolatzen dira) eragingo dute.

I LOVE YOU birusaren adibidearekin jarraituz, beste hainbat ekintza burutzeaz gain, ordenagailu osoan fitxategi jakinak aurkitu (soinu, irudi eta beste hainbat motakoak) eta bertako edukia atzerazina den moduan erabat ezabatzen du.

HEDAPENA

Birus batek arrakasta handiagoa edo txikiagoa izatea birus hedapena azkarrago edo motelago ematean dago. Birus-sortzaileek etengabe, antzematen gero eta zailagoak diren eta azkarrago hedatzen diren metodo berriak bilatzen jarraitzen dute.

Hedatze horren barne hainbat alderdi hartzen dira kontuan: ordenagailuan sartzeko puntua edo infektatzeko modua, fitxategia gordetzeko tokia eta fitxategi hori aktibatzeke modua:

- ✓ Sarrera-puntua oso komuna ez bada, ordenagailu gutxi infektatuko dira.
- ✓ Birusa duen fitxategia ez bada behar bezala ezkututzen, azkar aurkituko da eta ezingo da hedatu.



- ✓ Antzeman aurretik aktibatzen ez bada, ez da asko hedatuko.

Birusak gorde daitezkeen tokiak eta aktibatze moduak:

- ✓ **Postetan fitxategi erantsiak.** Fitxategi erantsia zabaltzean, birusa aktibatu egiten da.
- ✓ **Zenbait fitxategiren kodearen barne,** Word edo Excel dokumentuetako makroak bezala. Dokumentu horiek, dokumentuan bertan funtzio gehigarriak egiten dituzten makroak izan ditzakete; baina azken batean makro bat dokumentuari lotuta doan programa bat besterik ez da. Dokumentua irekitzean makroa exekutatu da eta birusa aktiba daiteke.
- ✓ **Ordenagailuaren memorian.** Memoriatik edozein unetan exekutatu eta beste fitxategi batean kopia daiteke.
- ✓ **Fitxategi exekutagarriak.** Fitxategi exekutagarri arruntentz .exe edo .com luzapena dute, eta programak dituzte. Fitxategi horiek, irekitzean exekutatu diren kodeak dituzte.
- ✓ **Diskoak abian jartzeko sektoretan.** Disko bat irakurtzen den bakoitzean, bere abian jartzeko sektorea irakurtzen da. Horrenbestez, birusaren kodea gordetzeko toki egokia da.

ERAGINDAKO KALTEAK ETA ONDORIOAK

Birus baten lehen helburua hedatzea da eta bigarrena agertzea, bertan dagoela erakustea. Birus bat agertzen ez bada beraz antzematea zailagoa izango da.

Bi modutan ager daiteke: suntsitzeko moduan eta txantxa moduan.

- ✓ **Suntsitzaileak** hainbat maila izan ditzake, programaren bat gauzaeztantzetik edo fitxategi jakin bat ezabatetik hasi, eta disko gogorra ezabatzeraz edo Sistema Eragilea blokeatzeraz heldu arte.
- ✓ **Txantxa** moduan azaltzeak esan nahi du mezuren bat azal daitekeela edo marrazki bat pantailan mugituz, soinuren bat eginez eta abar.

Hainbat birus-sortzailek euren gaitasuna, eta programa komertzialen ahuleziak aurkitzeko ahalmena dutela besterik ez dute erakutsi nahi. Ordenagailuek ia inoiz ez dute huts egiten, baina berauek funtzionarazten dituzten programak ez dira hutsezinak. Programa batek milioika kode-lerro izan ditzake. Beharbada programatzaileei xehetasun batek ihes egin die. Birus-sortzaileak, egoera jakinetan aurreikusi ez den moduan programak funtziona dezan aurkitzeko helburua du.



Birus-sortzaileek nabarmentzeko joera izan ohi dute: euren birusak ekintza suntsitzaile bat egiten badu, kalterik egiten ez badu baino ezagunagoa eta beldurgarriagoa izango da. Horrenbestez birus askok, fitxategi edo beste hainbat elementu infektatzeaz gain, ordenagailua erabiltezin utz dezaketen ekintza suntsitzaile gehigarriak egiten dituzte. Ordenagailua abian jartzea edo piztea eragozten dute, memoriaren edukia ezabatzen dute, erabiltzailearen informazioa eskuratzen dute, ezkutuko pasahitzak aurkitzen dituzte, informazioa ezabatzen dute, gure programek funtziona dezaten edo zuzen funtziona dezaten eragozten dute, eta abar.

Hori nabarmena da fitxategi-mota jakinen edukia ezabatzen duen I LOVE YOU bezalako birus batean: irudiak, soinuak, kalkulu-orriak, datu-baseak, eta abar.

Bestalde, honako hauek bezalako beste hainbat kalte eragiten ditu:

- ✓ Karpeta eta direktorio askotan SCRIPT.INI izeneko fitxategia sortzen du.
- ✓ Interneten sartzeko pasahitza aurkitzen du eta pasahitz hori alda dadin eragozten du.
- ✓ Interneten sartzen da fitxategi jakin bat infektatutako ordenagailuan kopiatzeko.
- ✓ Infektatutako egunaren biharamunean, I LOVE YOU birusak, infektatutako erabiltzailearen datu pertsonal guztiak lortzen ditu (posta elektronikoko helbidea, infektatutako ordenagailuaren izena, telefono bidez sareratzeko pasahitza, izan daitezkeen pasahitz guztien zerrenda, eta abar) eta Filipinetan dagoen posta elektronikoko helbide jakin batera igortzen ditu (mailme@super.net.ph).

Zenbait kasutan eta herrialdetan legeak ez daude teknologia berrietara egokituak, eta horregatik delitu informatikoak tipifikatu gabe egon daitezke. Bestalde birus bat lege-hutsunea duen herrialde batean sortu eta bertatik mundu osora hedatu daiteke.

ANTZEMATEA

Nola jakin gure ordenagailuan birus bat dugun ala ez?

Jakiteko modu argi eta tamalgarriena, birusak eragindako kalteen ondorioz da.

Hala ere, hainbat sintomek birus bat dugula adieraz dezakete:

- ✓ **Memorian edo disko gogorrean espazio librea murriztea:**
Birus bat, ordenagailu batean sartzen denean, derrigorrez RAM memorian kokatu behar du eta horregatik haren zati bat hartzen du. Horrenbestez, memoriaren neurri operatibo erabilgarria, birusaren kodeak duen kopuru berean murrizten da.
- ✓ **Arruntak ez diren errore-mezuak azaltzen badira.**



- ✓ **Programak exekutatzeko akatsak ematean.**
- ✓ **Sistema maiz erortzea.**
- ✓ **Kargatzeko denbora handiagoa.**
- ✓ **Eragiketa arruntak ohi baino motelago egiten badira.**
- ✓ **Memorian programa egoiliar ezezagunak azaltzen badira.**
- ✓ **Pantailaren jokabidea ezohikoa bada:**
Birus askok bideo-sistema aukeratzen dute erabiltzaileari bere ordenagailuan daudela adierazteko. Pantailan edo bertako karakteretan emandako edozein aldaketak, ordenagailuak birusa duela adieraz dezake.
- ✓ **Disko gogorrek, hondatutako sektoreak ditu:**
Zenbait birusek diskoko sektoreak erabiltzen dituzte ezkutatzeko, eta ondorioz kaltetu edo lanerako balio ez dutela geratzen dira.
- ✓ **Fitxategi exekutagarrietan aldaketak:**
Fitxategiko ia birus guztiek fitxategi exekutagarri bateko tamaina handitzen dute infektatzen dutenean. Halaber, birusa aditu batek programatu ez badu, gerta daiteke fitxategiaren data infekzio-datara aldatzea.
- ✓ **Teklatuan anomaliak azaltzea:**
Hainbat birusek tekla jakin batzuk definitzen dituzte; tekla horiek sakatzen diren unean, ordenagailuan kalteak eragiten dituzte. Halaber sarritan teklen konfigurazioa birusa programatu zen herrialdearen arabera konfiguratu da.

Halako seinaleren bat emateak esan nahi du jada kalteak sortu direla, adibidez, fitxategiak desagertu direla ikustea; dena den beti garrantzitsua da lehenbailehen gertatutakoaz jabetzea.

Laburtuz, beste edozein arrazoiri lotu ezin diogun edozein ekintza, birus batek sortutakoa izan daiteke.

Informatikan ezagutarik ez duten erabiltzaileentzako birus bat antzemateko ezagutzen den modu egokiena, adibidez “Panda Antivirus” bezalako biruskontrako programa exekutatzea da (birusak antzeman eta ezabatzeke diseinatutako programa).

BABES-NEURRIAK

Atal honetan, birusek zure ordenagailua kaltetu ez dezaten 15 gomendio baliagarri eskainiko dizkizugu.

- ✓ **Biruskontrako ona erabili eta maiz eguneratu.**



Birusetatik babestuta egoteko modurik aproposena zure ordenagailuan biruskontrako egokia instalatzea da, birusak antzeman eta ezabatzeko espezifikoki diseinatutako programa da.

Ezagutzen dituelako, nola jarduten duten badakielako eta haiek ezabatzeko gaitasuna duelako.

Hala ere egunero, biruskontrakoak harrapatzeko gai ez diren 20 birus berri baino gehiago azaltzen dira. Birus horiek antzeman eta ezabatzeko gure biruskontrakoa etengabe eguneratu behar dugu. Biruskontrako baten eraginkortasuna, neurri handi batean, eguneratzeko duen gaitasunaren arabera da, ahal izanez gero egunero eguneratu beharko luke.

Oso informatika-ezagutza oinarrikoak badituzu ere, biruskontrako programa erraza eta intuitibo bat “Panda Antivirus Titanium” da. Zure ordenagailura informazioa Internet edo disko-unitate aldagarrien bidez bakarrik heltzen bada, “Panda Antivirus Titanium” biruskontrakoarekin babes zaitetz. Bestalde, Sare batera konektatuta bazaude, “Panda Antivirus Platinum” edo “Panda Seguro Antivirus Global” probatu.

- ✓ **Egiaztatu zure biruskontrakoak euskarri teknikoak, birus berrien aurkako premiazko soluzioa eta alerta-zerbitzuak.**



Behar bezala eguneratutako biruskontrakoa birusetatik babesteko arma onena den arren, zerbitzu gehigarriak ezartzea gomendatzen da.

Euskarri teknikoko zerbitzua, posta elektronikoa edo telefono bidez, birusarekin edo biruskontrakoren funtzionamenduarekin lotuta sor daitekeen edozein arazo edo zalantzaren aurrean oso lagungarria da.

Birus berri batek zure ordenagailua infektatzen badu, birus berrien aurkako premiazko soluzioa emango dizun zerbitzua beharko duzu, birus hori ahalik eta denbora laburrenean ezabatuko duen zerbitzua (Panda enpresak zerbitzu hori eskaintzen du).

Beste funtsezko zerbitzua, birus arriskutsu berriei buruzko alertak dira, adibidez, posta-zerrenden bidez.

✓ **Zure biruskontrakoa beti aktibo egongo dela ziurtatu.**



Biruskontrako bat aktibo dago, ordenagailuan egindako eragiketa guztiak etengabe zaintzeko gai den babes iraunkorra duenean.

Babes iraunkor hori aktibo dagoela egiaztatzeko bi modu daude: ataza-barran ikono finko baten bidez (erlojuaren ondoan) edo biruskontrakoren konfigurazioan bertan.

Birusetatik babestuta egoteak etengabeko babesa eskatzen du, fitxategiena zein posta elektrikoarena.

- ✓ **Zabaldu aurretik, jasotako posta elektronikoko mezu bakoitza egiaztatu.**



Posta elektronikoa, transmititzeko birusek duten bitarteko egokiena da; horregatik kontu berezia izan behar da erabiltzean.

Jasotako edozein postak birusa izan dezake, datu erantsien sinboloa ez badu ere (ohiko "klipa"). Bestalde, ez da behar posta-mezu bateko fitxategi erantsia exekutatzeko infektatzeko. Hainbat sistematan nahikoa da mezua ireki edo "aurrebista" bidez ikustearekin.

Horretaz babesteko, onena, espero ez diren edo ezohiko iturri batetik datozen mezuak egiaztatzea da. Mezuak birusa daramala susmatzeko modu bat mezuaren gaia igorleak erabiltzen ez duen hizkuntza batean idatzita egotea da.

- ✓ **Saihestu Interneten seguruak ez diren tokitatik programak deskargatzea.**



Interneteko orri askok, birusez infektatuta egon daitezkeen programa eta fitxategiak deskargatzen uzten dute.

Euren fidagarritasuna bermatuko duten adierazle argirik ez dagoenez, bermagarriak ez diren Webguneetatik programak deskargatzea ekidin behar dugu. Orokorrean,

euren jarduerari, eta eskaintzen dituzten produktu edo zerbitzuei buruzko informazio argia erakusten duten guneak seguruak dira. Halaber seguruak dira editorial eta erakunde ofizialak bezalako orriak.

- ✓ **Chat edo berri-taldetan (news) zaudenean eskatu ez dituzun fitxategiak ez onartu.**



Interneti esker, berri-talde eta chaten bidez hainbat gairi buruz denbora errealean informazioa trukatu eta mintza daiteke hurrenez hurren. Berri-taldeak edo “news” izenekoak posta-zerrendak ez direnez eta Internet bidez transmititzeko euren sistema (NNTP) erabiltzen dutenez, etengabeko babes eraginkorra ere behar dute.

Bi sistemek, beste hainbat pertsonekin komunikatzeko aukera emateaz gain, fitxategiak transferitzeko aukera ematen dute. Bertan kontu berezia izan behar da, eta igorle ezagun eta konfiantzazko batengandik heltzen direnak bakarrik onartu behar dira.

- ✓ **Beti, biruskontrako egoki batekin zure ordenagailuan erabiliko dituzun disketeak aztertu.**



Internetez gain, birus ugari disketeen bidez infektatzen dira. Egokia da, biruskontrako egoki bat erabiliz, gure ordenagailura sartzen diren eta bertatik irteten diren diskete guztiak aztertzea.

Bestalde, gure disketeak beste hainbat ordenagailutan erabiltzean bertan idatzi ez dadin, disketearen atzealdean, eskuin behealdean dagoen erlaitza jaitsi.

- ✓ **Ordenagailua itzali edo berrabiaraztean disketeak diskete-unitatetik atera.**



Biruskontrako baten bidez, erabilitako diskete guztiak aztertzeaz gain, “boot birus” edo “abio-birus” ezagunak aktiba daitezen ekiditeko modu bat, ordenagailua itzali edo berrabiaraztean diskete-unitatetik disketeak kentzea da.

Egitea ahazten bazaigu, kasu horietan infektatutako disketeak daudela egiaztatzeko gai den biruskontrako bat izan behar da.

- ✓ **Konprimitutako fitxategien edukia aztertu.**



Fitxategi konprimituak, oso erabilgarriak fitxategi asko dituztelako eta espazio txikiagoa hartzen dutelako, birusak hedatzeko lagungarri dira. Lehendabizi, gure biruskontrakoari, ahal dituen formatu konprimitu kopuru handiena antzeman dezan eskatu behar diogu.

ZIP formatukoak bezalako fitxategi horietako bat zabaldu aurretik, Windows, Mis Documentos, Idazmahaia, eta abar karpeta bezalako laneko direktoriotan zabaldu beharrean, aldi baterako karpetatantzerabiltzaileek sortuak eta bertako fitxategiak aurrerago ezaba daitezkeenak gordetzea gomendatzen da.

- ✓ **Birusak izan daitezkeen ekintza susmagarrien aurrean adi-adi egon.**



Birus berriak daudela antzeman dezaketen seinale ugari daude: fitxategien tamaina handitzea, berez izan behar ez luketen Word edo Excel dokumentuetan makroen oharrak, beste hainbat pertsonak guk bidali ez dugun postako mezuak jasotzea, eta abar.

Ustezko infekzio horien irtenbide egokien bezala, gure biruskontrako konpainiak birus berrietarako dituen premiazko zerbitzuetara jo behar dugu.

- ✓ **Birusetatik babesteko politikarako normalean erabiltzen dituzun aplikazioen segurtasun-aukerak gehitu.**



Gehien erabilitako informatikako programak, arrazoi horrengatik hain zuzen ere, birus-egileen helburu bihurtzen dira. Fabrikatzaileek programa horietan birusen aurkako segurtasun-aukerak sartu ohi dituzte.

Hori da Interneteko nabigatzaile, testu-prozesadore, postako programa, eta abarren kasua; eurek, informazioa pixka bat gehiago ziurtatzeko ezaugarriak dituzte. Haiek ondo ezagutzen ez baditugu, programak berak emandako laguntzan sar gaitzke eta “seguridad” hitzaren bilaketa egin dezakegu programa horiek nola erabili jakiteko.

Egokia da segurtasuneko aukera espezifiko horiek aprobetxatzea, bai eta etengabe eguneratzen den biruskontrakoa izatea ere.

✓ **Aldizka, segurtasun-kopiak egin.**



Birus baten eragina txikitzeko oso modu egokia, korporazio zein norberarentzat, gure informazioko segurtasun-kopiak berritzea da.

Gure informazio garrantzitsuena aldizka eta maiz kopiatzea, segurtasun-politika egokia da. Modu horretan, adibidez birus batek eragindako datu-galera, azken kopia berriz ezarriz konpon daiteke.

✓ **Informatuta egon zaitez.**



Birus berrietatik babesteko modu egokia, informatikaren segurtasunaren sektorean gertatzen denaren berri etengabe jasotzea da.

Hala ere, hainbat bidetatik jasotako informazio zabalaren aurrean, datu horiek, konpainia eta erakunde jakinek zabalduko informazio oso, eguneratu eta adituarekin alderatzea gomendatzen da: biruskontrako konpainiak, segurtasunerako enpresa aholkulariak, alerta berriei buruz informatzen duten erakundeak, gobernu-erakundeak, unibertsitateak, eta abar.

✓ **Beti software legala erabili.**



Ordenagailuan programa berria ezartzean, infekzio-arriskua txikiagoa da software legala erabiltzen bada.

Hala ere, softwarea CD-ROM pirata batean badugu, edo fabrikatzaileen babesak kentzeko manipulatu den software legala bada, inork ezin du ziurtatu birusik ez duenik.

Bestalde, biruskontrako softwarea bada, bere legaltasunak, eraginkortasuna eta segurtasuna bermatzen duten zerbitzu gehigarri guztiak erabiltzeko aukera ematen digu.

- ✓ **Software-fabrikatzaile, Interneten sartzeko hornitzaile eta argitalpenen editoreei, birusen aurkako borrokan parte har dezaten exijitu.**



INTERNET SEGURUAGOAREN ALDE

Birusen aurkako borrokan, informatika-arloan inplikaturako agente guztiek parte har dezaten behar da: enpresak, azken erabiltzaileak, biruskontrako konpainiak, hedabideak, eta abar.

Birusak hedatzeko, Internet bitarteko erabilienez, Interneten sartzeko hornitzaileen lankidetzak oso garrantzitsua da. Halaber, software-fabrikatzaileek eta CD-ROM eskaintzen duten argitalpenek, birusa ez hedatzeko neurriak har ditzaten



komeni da. Guztion laguntzak, birusek eragindako infekzioen arazoa minimizatzen lagunduko du.



3. SEGURTASUNA MERKATARITZA ELEKTRONIKOAN

Merkataritza elektronikoa bezala ulertzen ditugu banku-eragiketak eta Internet bidez egiten ditugun erosketak.

Interneten erosteak ez du zertan mundu fisikoan baino arriskutsuagoa izan behar. Bitarteko berri honetan mugitzen besterik ez dugu ikasi behar.

Zerbitzari bat barraren atzean norberaren kreditu-txartelarekin desagertzeko eragozpenik ikusten ez duten erabiltzaileek, mesfidantza erakusten dute txartelaren zenbakia Interneten teklatu behar dutenean. Izan ere Sarea eta segurtasun faltaren lotura oso hedatuta dago. Ezezagunari beldurraren ondorioz, ezezaguna egiten zaien giro batean, kontsumitzaile askok ordaintzeko garaian atzera egiten dute. Mundu fisikoan guztiok joko-arauak ezagutzen ditugu; gakoak, arauak mundu berrira egokitzea da, mundu digitalera alegia.

Kontuan izan behar dugu azken urteetan diru-eragiketak bitarteko honetan egitea oso segurua dela. Ez da %100 fidagarria baina, orokorrean, maiz egiten ditugun beste hainbat eragiketa baino seguruagoa da: kutzazainetik dirua atera, jatetxe batean kreditu-txartelarekin ordaindu edo katalogo bidez erosi.

ZERBITZARI SEGUURUAK

Segurtasun “handi samar” hori, zerbitzari seguruak erabiltzen dituzten Web orriek aplikatzen zaie, baina, zer da zerbitzari seguruak? **Zerbitzari seguruak**, bezeroarekin konexioa ezartzen duen html orrien zerbitzaria da (World Wide Web motako zerbitzua); era horretan informazioa Interneten barrena doa, SSL (Secure Sockets Layer) protokoloari esker Webean sartzen den erabiltzaileak eta zerbitzariak bakarrik irakurri ahal izatea ziurtatuko duten algoritmo bidez enkriptatuta. Zerbitzari seguruak, konfidentzialtasuna babestu behar den informazio-transferentzia eragingo duten zerbitzuei buruzko konexio seguruak ezartzen uzten duen ezinbesteko plataforma da. Banku elektronikoko edo merkataritza elektronikoko zerbitzuak ezartzeko ezinbesteko baldintza da; izan ere zerbitzari seguru batekin lanean hasten garen uneetan, Internet bidez igortzen ditugun datuak (kontu-zenbakiak, txartelen datuak, gako pertsonalak, eta abar) enkriptatuak joango dira. Eragiketa horiek egiten ez baditugu, ez da beharrezkoa izango zerbitzari seguru batekin lan egitea.

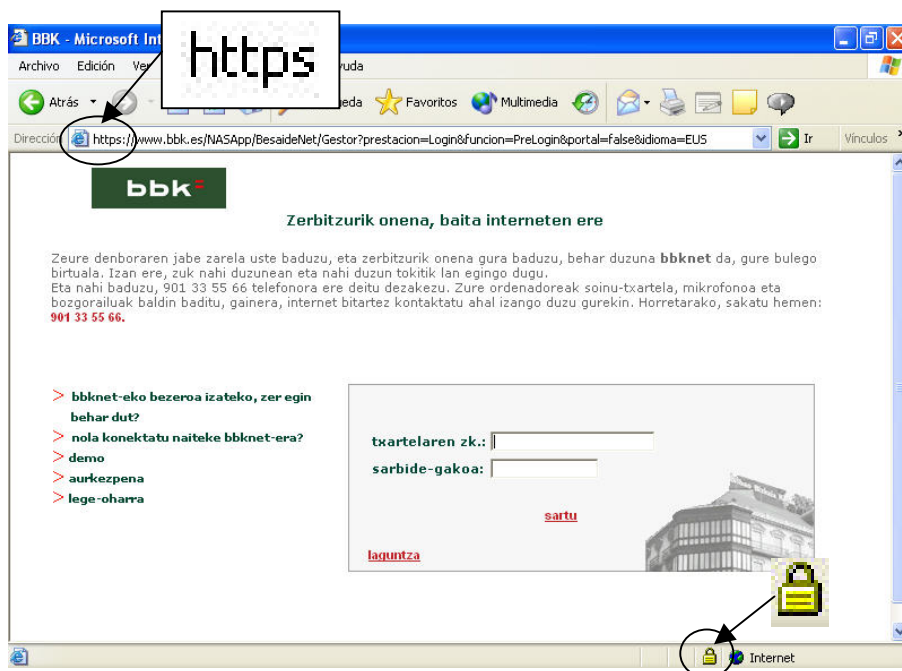
Zerbitzari seguru batek honako abantaila hauek eskaintzen ditu:




- ✓ **Identifikazioa eta baimentzea**, gure datuak berretsi aurretik, zerbitzari hori benetan enpresa horretakoa dela ziurtatzeko aukera ematen dute.
- ✓ **Datuen konfidentzialtasuna eta segurtasuna**. Zerbitzari seguru batek aurkeztutako formulario batean tekleatu ditugun datuak bidaltzen ditugunean, Interneten barrena igarotzea zenbaki bidez egiten da. Horrek esan nahi du erasotzaile batek haren ibilbidean harrapatuko balu, erasotzaileari ez liokeela ezertarako balio, ez baititu deskriptatzeko behar diren gakoak ezagutzen.

Gune seguru bat nola antzeman

Erraz jakin daiteke zerbitzari seguru batekin konektatu dugun. Lehendabizi, URLko helbidea http beharrean **https**-arekin hasten da (helbide honetara, zenbaitetan, erabiltzailea ezer egin gabe heltzen da, barne daraman hitz gako bat sakatzen delako, edo nahita, modu seguruan zerbitzari batean sartu nahi denean).

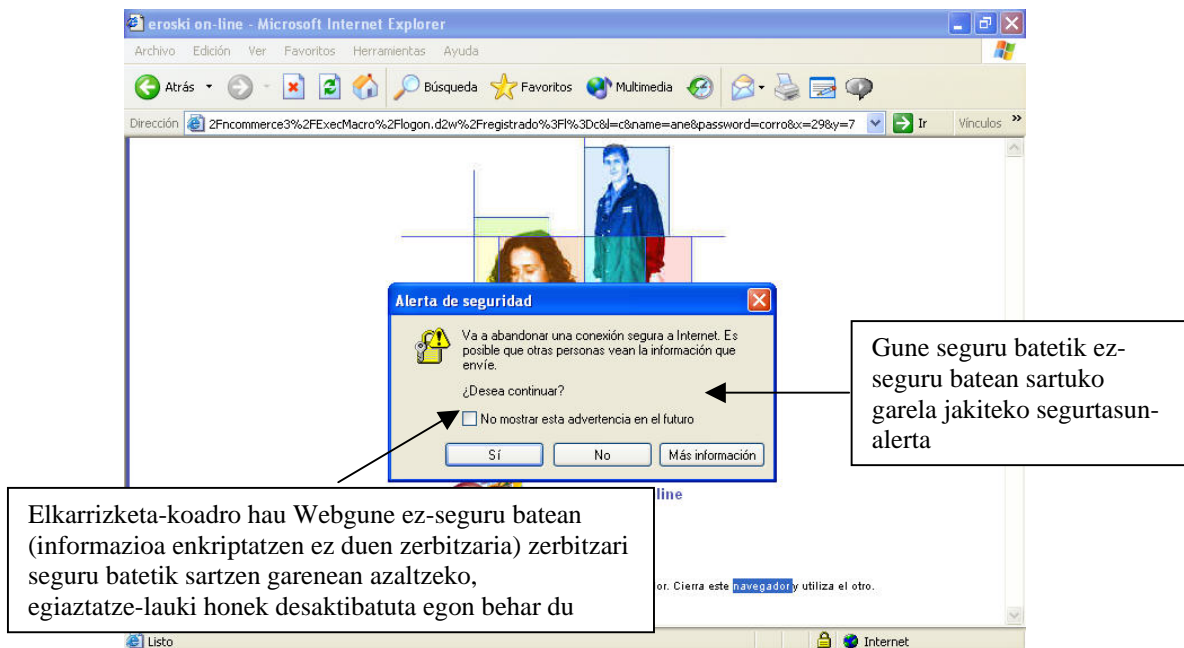


Bestalde, nabigatzaileek, konexio segurua ezarri denaren seinale bat dute. Horrenbestez, adibidez Internet Explorerrek, zerbitzari seguru batean sartzen ari garela ohartaraziko digu eta egoera-barran honako hau bezalako giltzarrapoa azalduko da: .

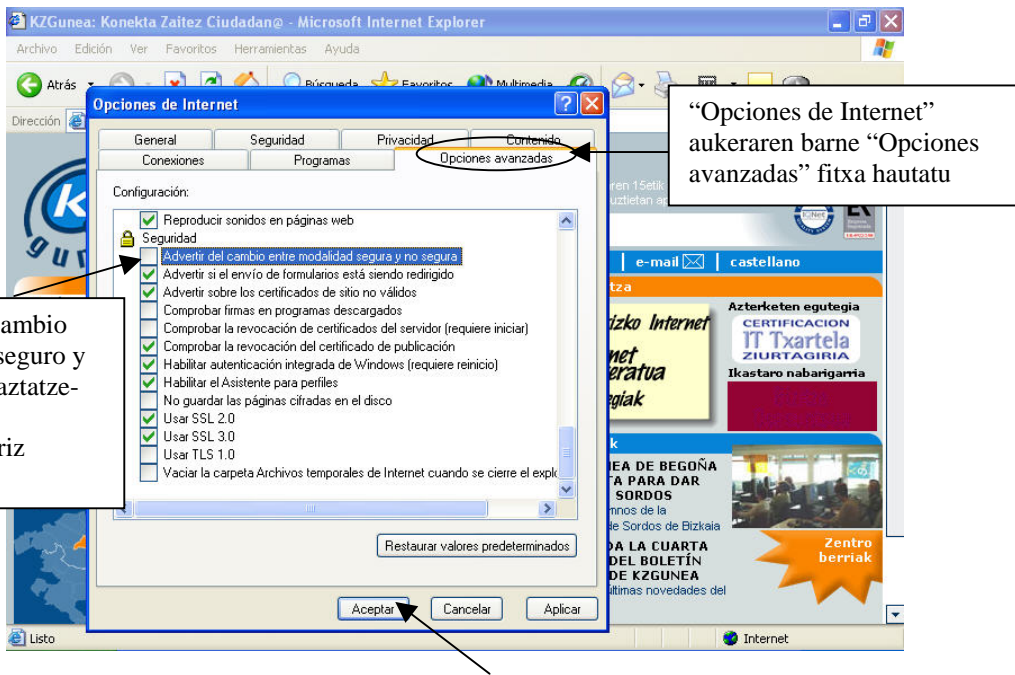


Garrantzitsua da jakitea, elkarrizketa-koadro hau, gune seguru batekin konektatzen dugun bakoitzean gure pantailan azaldu dadin, “No mostrar esta advertencia en el futuro” egiaztatze-laukiak desaktibatuta egon behar duela.

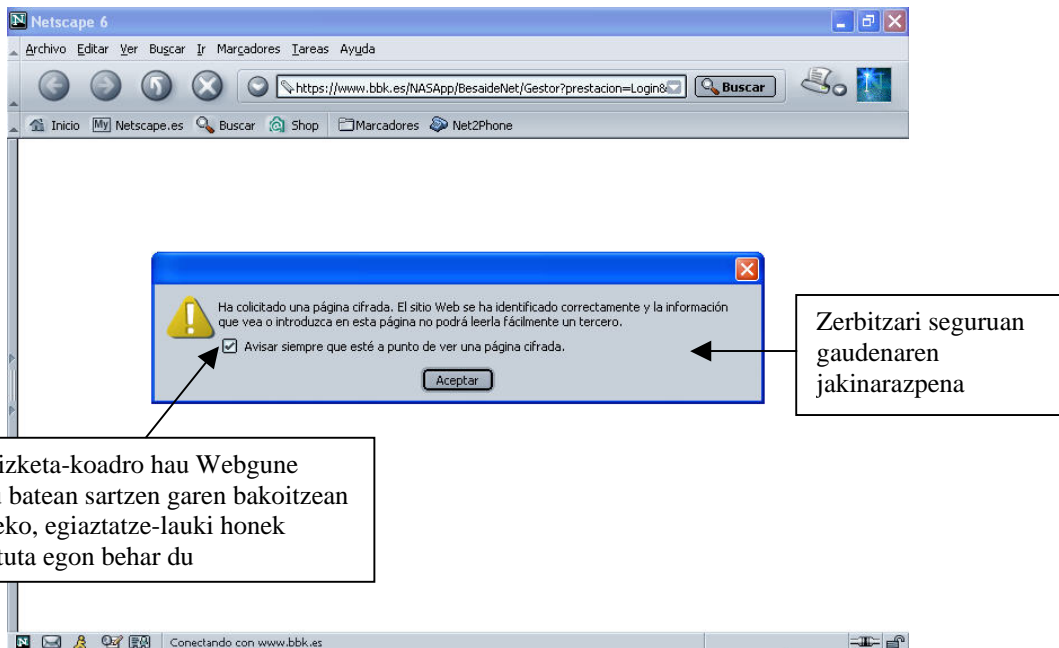
Webgune seguru batetik beste webgune ez-seguru batean sartzean (ez du segurtasun-protokolorik erabiltzen, eta horrenbestez, igorri edo jasoko dugun informazioa ez dago babestuta), Internet Explorerrek, hori adierazteko elkarrizketa-koadroa erakutsiko du. Guneari eta gure ekipoari buruz dakigunaren arabera, bisitatu nahi ote dugun erabaki beharko dugu. Gune honetan sartzeko zalantzan bagaude, “No” aukeran klik egin.

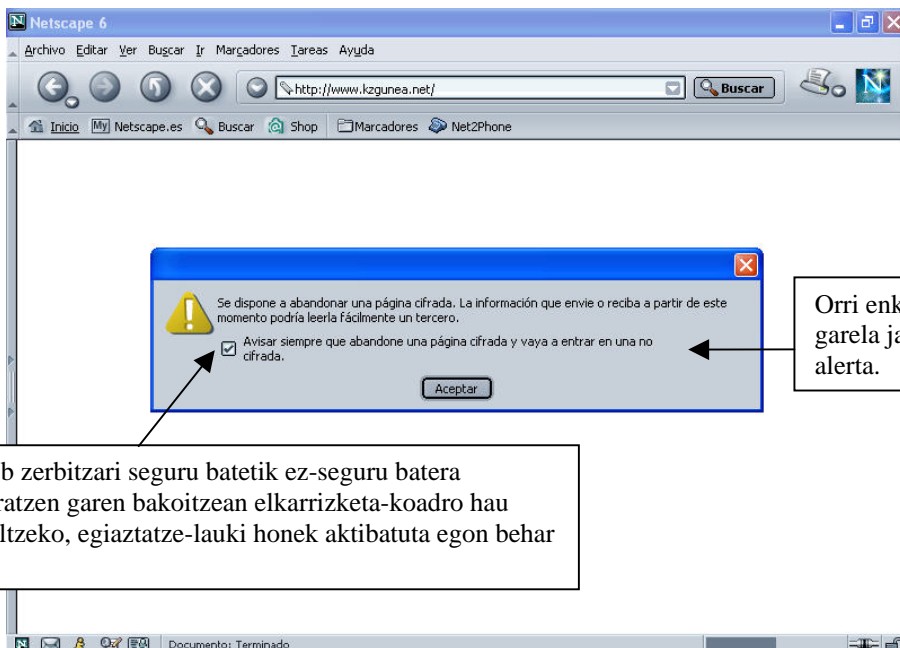
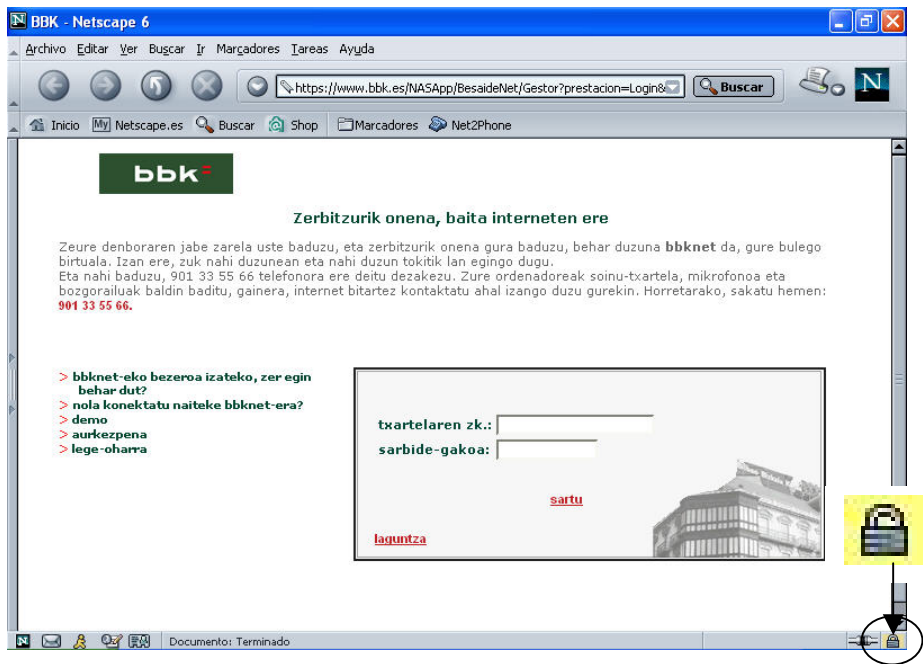


Gure nabigatzaileak, zerbitzari seguru batetik aterako gara guri jakinarazteko, “No mostrar esta advertencia en el futuro” (Aurrerantzean ez erakutsi ohar hau) egiaztatze-laukiak desaktibatuta egon behar du. Edozein arrazoirengatik laukia aktibatuko bagenu edo ordenagailuak zerbitzari seguruan sartuko gara jakinaraziko ez baligu, “Herramientas” (Tresnak) menuaren barne “Opciones de Internet” (Internet aukerak) hautatuko dugu, eta bertan zabalitzen den leihoan “Opciones avanzadas” (Aukera aurreratuak) fitxan sakatuko dugu. “Seguridad” (Segurtasuna) atala bilatu eta “Advertir del cambio entre servidor seguro y no seguro” (Zerbitzari seguru eta ez-seguruaren arteko aldaketa ohartarazi) egiaztatze-laukia aktibatuko dugu. “Aceptar” (Ados) sakatu, egindako aldaketak gordetzeko.



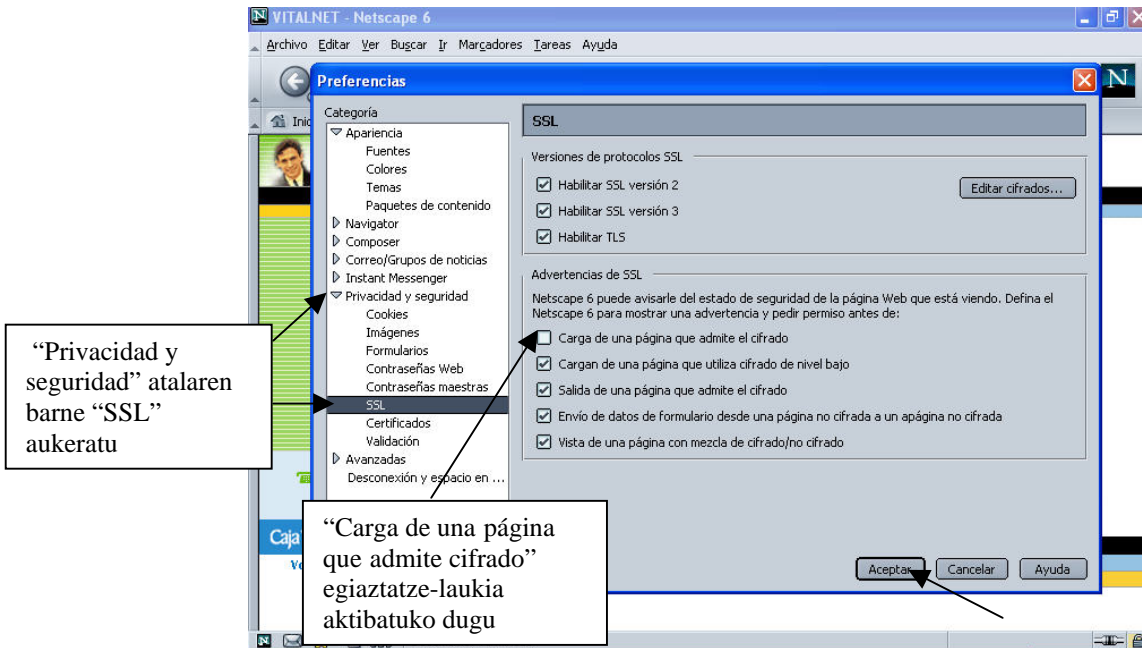
Netscape nabigatzailean badakigu orri enkriptatuarekin konektatu dugula elkarrizketa-koadro batek hala adierazten digulako. Webgune seguru batean sartzen garen bakoitzean koadro hori azaltzeko, “Avisar siempre que esté a punto de ver una página cifrada” (orri enkriptatua ikusteko dagoen bakoitzean gogoratu) egiaztatze-laukiak aktibatua egon behar du. Bestalde, egoera-barran normalean zabalik (🔒) dagoen giltzarrapoa itxita ikusiko da 📄.





Orri enkriptatu bat utzi behar dugun bakoitzean abisu hau azal dadin, “Avisar siempre que abandone una página cifrada y vaya a entrar en una no cifrada” (Orri enkriptatua utzi eta enkriptatu gabe batera sartzen den bakoitzean ohartu) egiaztatze-laukiak aktibatuta egon behar du. Edozein arrazoirengatik laukia desaktibatzen badugu edo ordenagailuak zerbitzari seguruan sartuko garelara ohartarazten ez badigu, “Editar” (Editatu) menuaren barne “Preferencias” aukeratu dugu, eta “Privacidad y seguridad” (Pribatutasuna eta segurtasuna) atalaren barne zabalten den leihoan “SSL” hautatuko

dugu, eta “Advertencias de SSL” (SSLko oharrak) atalean dagoen “Carga de una página que admite cifrado” (Enkriptatzea onartzen duen orri bat kargatu) egiaztatze-laukia aktibatuko dugu. Amaitzeko “Aceptar” (Ados) sakatuko dugu egindako aldaketak gordetzeko.



Zerbitzari seguru batek, nabigatzailearekin gune seguru batean gaudenean, RSA enkriptatze-sistemaren bidez bidaltzen ditugun datuak enkriptatuz funtzionatzen du.

Gure nabigatzaileak, Internet Explorer edo Netscape, deitzen dion zerbitzari seguruarekin batera lanean, datuak enkriptatzen ditu; ondorioz, transmisio-prozesuan norbait datu horien jabetuz gero, ezingo ditu irakurri beharrezkoa den gakorik ez duelako. Bestalde, konexio bakoitzean zerbitzari seguruak eta gure nabigatzaileak gako diferente eta aleatorioa sortzen dute, eta horrek zalantzarik gabe identifikatzen gaitu. Deskonektatu (orritik atera) ondoren, transmititutako datuak zerbitzarian bakarrik geratu dira.

Enkriptatze hau, Netscape Communications enpresak Internet bidez informazio segurua transferitzeko Secure Socket Layer, SSL, estandarrean oinarritu da.

SEGURTASUN-ZIURTAGIRIA

Merkataritza elektronikoa hasi nahi duen enpresa batek, beste hainbat gauzaren artean, zerbitzari segurua instalatu eta konfiguratu behar du. Prozesu horren ondorioz, enpresak bi gako eskuratuko ditu (publikoa eta pribatua). Gako horiek euren komunikazio seguruak enkriptatzeko erabiliko ditu.



Gakoak sortu ondoren, zerbitzari hori, zerbitzari seguru bezala egiaztatu beharko da; hau da, hiruren fidagarri batek zerbitzari zehatz horrek segurtasun-protokoloarekiko egiten duen inplementazioa egiazta dezan, eta digitalki zerbitzari seguru horren (bere gakoekin) eta berau duen enpresaren arteko erlazioa benetakoa dela bermatzea eskatzen da. Ziurtagiri digitalak emateaz arduratzen diren hirurenak, ziurtagiri-agintari bezala ezagutzen dira. Munduan gehien onartutako bat Verisign da. Espainian ere badira zenbait, adibidez, IPS eta Ziurtapen Elektronikoko Agentzia.

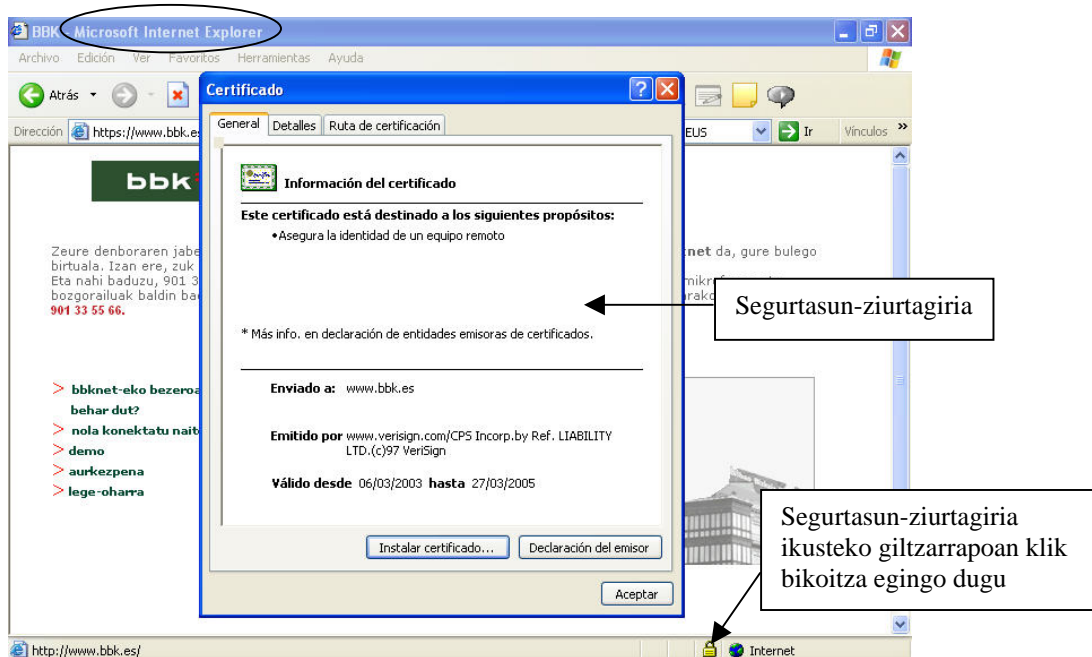
Halaber ziurtatu du **EZ** daudela bi zerbitzari seguru identitate berarekin, eta bezeroaren nabigatzaileari, haren behin-behineko baliagarritasuna berresteko baimena ematen dio.

Verising-ek ziurtatutako zerbitzari seguruak 128 bit-eko gakoa du, 40 bit-eko ezkutuko zati batekin.

Horrek esan nahi du sarkin bat sistema honekin transmititutako datuak desenkriptatzen saiatzen bada, 240 eragiketa zail egin beharko ditu datuak desenkriptatzeko, hau da, konputazio-denboran, merkatuko makina azkarrenetako batean milaka urte.

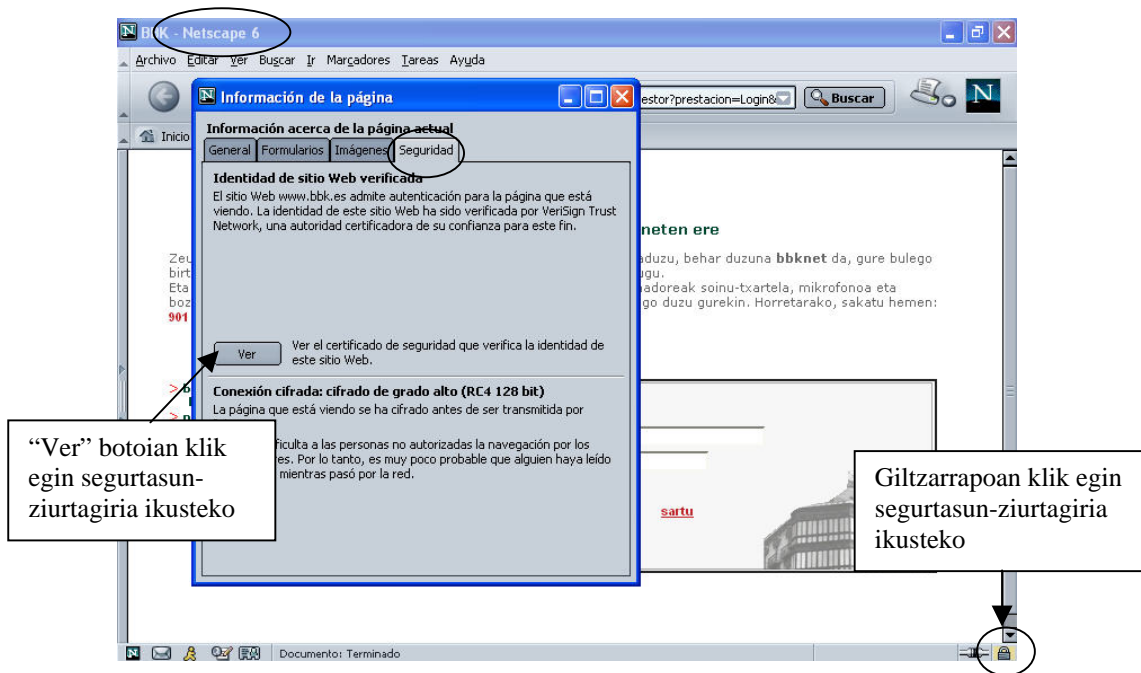
Segurtasun-ziurtagiria nola ikusi

Jakin badakigun bezala, gune seguru batean sartzean gure nabigatzaileak, Internet Explorer edo Netscapek, egoera-barran giltzarrapo itxi bat erakusten du. Bi kasuetan, ikono horietan sakatuta, gure nabigatzaileak, segurtasun-protokoloei buruz behar den informazio guztia zabalduko du.

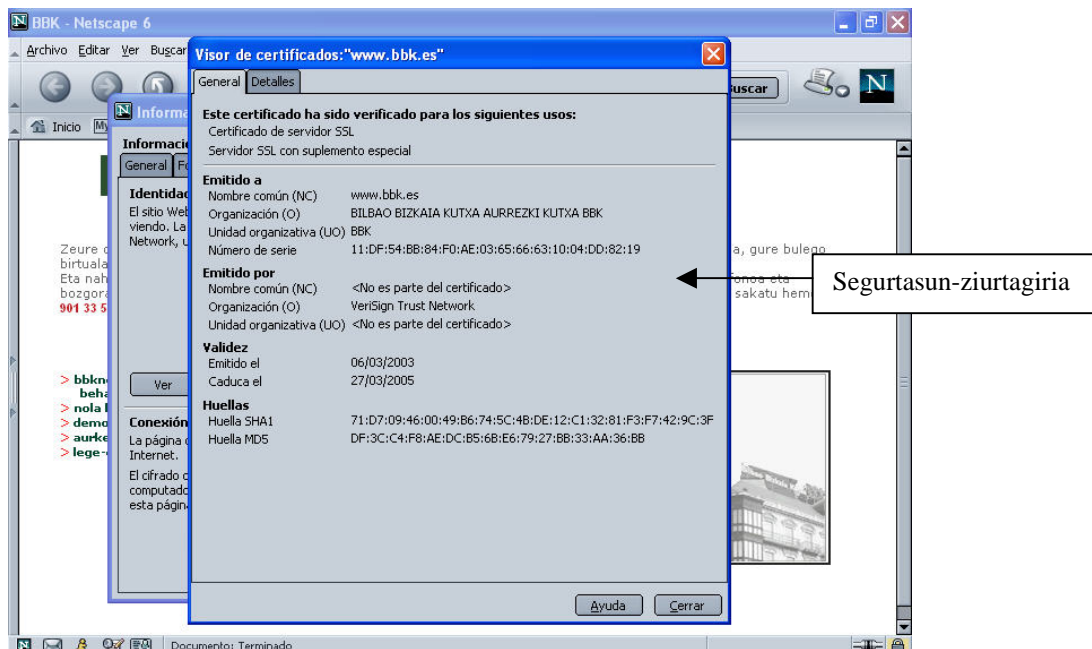


Segurtasun-ziurtagiri horrek honako informazio hau eskaintzen du:

- ✓ **“Enviado a”** (Nori bidalia): ziurtagiri honen jabea.
- ✓ **“Emitido por”** (Jaulkitzailea): erakunde ziurtatzailea.
- ✓ **“Validez”**(Baliozkotasuna): ziurtagiri hau indarrean egongo den denbora.



Segurtasun-zurtagiriari buruzko informazio gehiago lortzeko, “Ver” sakatu.



Segurtasun-zurtagiri honek ondoko informazio hau eskaintzen du:

- ✓ **“Emitido a”** (Jasotzailea): zurtagiriari buruz honako informazio hau laburtzen du:
“Nombre común” (Izen orokorra): zurtagiriak identifikatzen duen pertsona edo beste entitate baten izena.



“**Organización**”(erakundea): entitate hori sartuta dagoen erakundearen izena (adibidez, enpresa baten izena).

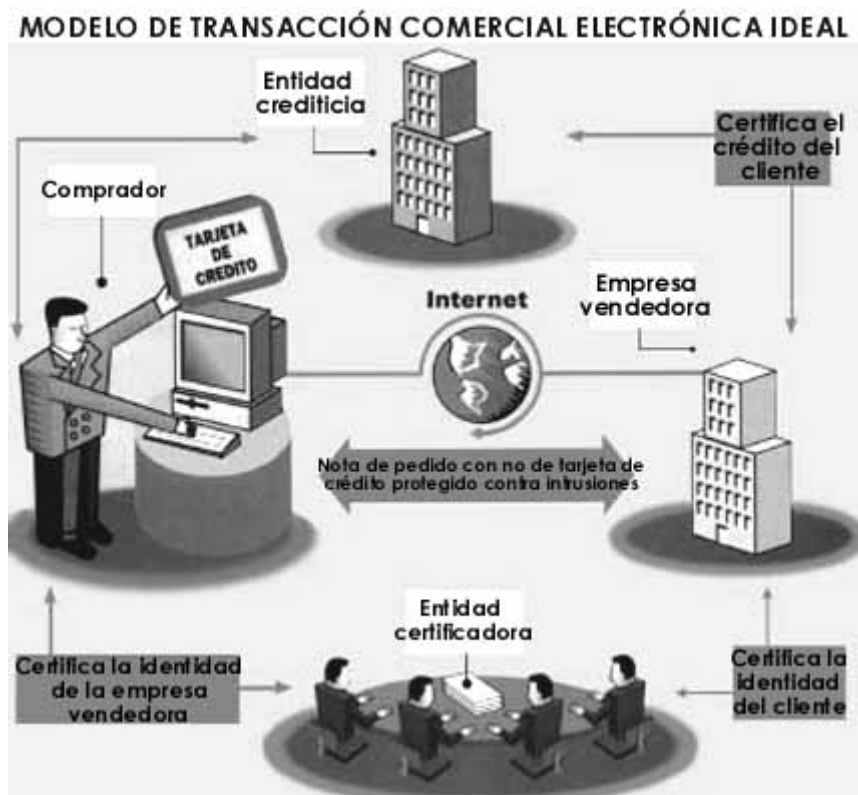
“**Unidad organizativa**” (Antolakuntza-unitatea): entitatea barne dagoen antolakuntza-unitatearen izena (adibidez, kontabilitate-saila).

“**Número de serie**” (Serie-zenbakia): ziurtagiriaren serie-zenbakia.

- ✓ “**Emitido por**” (Jaulkitzailea): Ziurtagiria luzatu zuen Agintaritza Ziurtatzaileari (AC) buruzko informazioa laburtzen du (“Emitido a” atalean eskaintzen zenaren antzekoa; ikusi gorago)
- ✓ “**Validez**” (Baliozkotasuna): ziurtagiria zenbat denboran dagoen indarrean adierazten du.
- ✓ “**Huellas**” (Aztarnak): ziurtagiriaren hatz-aztarnen zerrenda eskaintzen du. Hatz-aztarna bat, matematikako funtzio bat ziurtagiriaren edukietara aplikatzearen ondorioz ematen den zenbaki bakarra da. Hatz-aztarna, ziurtagiria manipulatu ez dela egiaztatzeko erabil daiteke.

Gunearen ziurtagiria kontu handiz aztertu behar dugu, pentsatzen dugun enpresari ote dagokion ikusteko, batez ere egiaztatuz helbidea edo URL zuzena eta zehatza dela (halaber nabigatzaileak, ziurtagiriaren helbidea, gu gauden gunearekin bat etortzen ote den egiaztatzen du). Ziurtagiria, ziurtatze ezaguneko autoritate batek luzatu bazuen, gure nabigatzaileak, edozein izanda ere, arazorik gabe baliozkotuko du.

Interneteko nabigatzaileek jatorriz, autoritate ziurtatzaile nagusien erroko gako publikoak (edo ziurtagiriak) dituzte. Era horretan, Verisign bidez ziurtatutako zerbitzari segurua bisitatzen dugunean, gure nabigatzaileak eta zerbitzari horrek truke enkriptatua has dezakete, nahikoa gako dituelako eta Verisign bat ziurtatze baliagarriko autoritate bezala onartzen duelako.



MERKATARITZAKO TRANSAKZIO ELEKTRONIKOKO EREDU EGOKIA

Hori guztiaz gain, merkataritza elektronikoko enpresaburuek, segurtasuneko neurri gehigarriak ezarri beharko lituzkete euren zerbitzarietan. Beste hainbaten artean honako neurri hauek azpimarratuko genituzke:

- ✓ Softwarea egunero gaurkotzea.
- ✓ Urrakortasun berrien aurrean arreta areagotzea.
- ✓ Erabiltzaileen datu konfidentzial guztien segurtasun-politika latza.

Neurri horiei esker Sarean segurtasuna ezarri ahal izango da eta erabiltzaile guztiok lasaiago nabigatuko dugu, gure datuak onik daudela ziur egonda.

Espanian gaur egun Merkataritza Elektronikoaren Legea dago. Lege horrek, duela gutxi arte zeuden ia hutsune guztiak betetzen ditu. Informazio gehiago lor daiteke Justizia Ministerioaren orrian: www.mju.es

Gure kreditu-txartelaren datuak edo bankuko beste edozein datu erosketak egiteko inork behar ez bezala erabiltzen baditu, dendak on-line erosketa hori egin zela eta guk erosi genuela egiaztatu beharko du. Baina eragiketa sinadura elektronikoa (dokumentu edo fitxategi batekin doan karaktere-multzoa, egilea nor den eta datuak manipulatu ez direla



egiaztatzen duena) batekin egiten bada gure nortasuna aurreuposatuko du eta guk egiaztatu beharko dugu ez genuela eragiketa hori egin.

Garrantzitsuena, iruzurra berehala salatzea izango da. Enpresei kexak aurkezteaz eta kontsumitzailearentzat konpentsazio ekonomikoak proposatzeaz arduratzen diren neurketa estrajudizialeko hainbat erakunde daude. Euren zeregina lekukotasunarena da eta saltzailearen ospearen gainean bakarrik presionatzen dute. Hainbat helbide interesgarri: www.ilevel.com eta www.isitsafe.com

Interneteko erabiltzaileen elkarteak (www.aui.es) saltzaile bati buruz salaketa asko dituenean, administrazioari jakinarazten dio.

Aurki, segurtasun-sistemak areagotu egingo dira identifikazio-forma berriei esker: iris, hatz-marka eta ahotsen irakurleak, txartel adimendunak, eta abar. Erosketak egiteko gero eta gutxiago mugitu beharko dugu eta, prezio eta kalitateen alderatzeak egiteko aukera dagoenez, erosketa horiek optimizatuak egongo dira.

MERKATARITZA ELEKTRONIKO SEGURURAKO AHOLKUAK

- ✓ Edozein banku-eragiketa edo erosketa egiteko zerbitzari seguruak bakarrik erabili (<https://> bidez bakarrik hasten direnak). Internet bidez inoiz ez zenuke inolako babesik gabe informazio konfidentziala eman beharko, bereziki datu finantzarioei dagokienean. Hala eginez gero, zure datuak Interneten barrena enkriptatu gabe joango dira, datuen ibilbide osoan arriskuan egonik.
- ✓ Erosi duzun produktua jasotzeko, ezinbestekoa den informazioa bakarrik eman.
- ✓ Zure datu finantzarioak inoiz ez bidali posta elektronikoko mezu batean. Gomendio honetarako salbuespen bakarra, aurrerago ikusiko dugun PGP bezalako hain sistema seguruarekin gure mezua enkriptatzea izango litzateke.
- ✓ Tarteka, konektatzen zaren gune seguruaren ziurtagiriak egiaztatu.
- ✓ Kontsumitzaile bezala zure eskubideak erreklamatu, prezioei, bidaltzeko modu eta kostu gehigarriari, eta berme- eta itzulpen-baldintzei buruzko informazio xehatua eta argia exijitu.
- ✓ Saltokiaren pribatutasun-politikari buruzko informazioa bilatu, zuzenean bildutako, formularioak betetzean emandako eta zure nabigazioagatik zeharka lortutako zure informazio pribatuarekin zer egiten den jakiteko. Ez baduzu aurkitzen, exijitu.
- ✓ Ez ordaindu esku-diru, txeke edo zordunketazko txartel bidez, hobe kreditu-txartelarekin egiten baduzu. Orokorrean uste dena baino seguruagoa da eta zuk erositakoa entregatzean irregulartasunak edo zure txartelarekin iruzurra eginez gero arazo gutxiago izango dituzu. Saltzailearekin eztabaidak konpontzeko baldintzak zure bankuarekin kontsultatu. Orokorrean, ordainbideen finantza-



erakundeak transakzioko dirua itzuliko dizu, kreditu-txartelarekin ordaindu baduzu, eta erreklamazioa, erosketa egin eta hurrengo hiru hilabetetan egiten baduzu.

- ✓ Merkataritza elektronikoari buruzko berrikuntzak arretaz jarraitu.

4. POSTA ELEKTRONIKOA

Posta elektronikoaren kasuan, oso kontuan hartu beharreko hainbat egoera topatzen ditugu. Mezuaren pribatutasunetik hasita. Gure ekipoan segurtasun-sistematik ezarri ez badugu, pentsatu behar dugu bidaltzen edo jasotzen ditugun posta elektronikoko mezuak, gu ez garen norbaitek irakur ditzakeela, horretarako baliabideak baditu.

Baina baieztapen erreal horrek ez gaitu mugatu behar zerbitzu hau erabiltzeko, nahiko arraroa baita horrelakorik gertatzea erabiltzaile “arrunt” baten kasuan. Interneten zirkulatzen duen informazio eta erabiltzaile-kopuru handiek babesten gaituzte.

Garrantzi handiko datu konfidentzialak bidaliko baditugu, Internet zerbitzuetako gure enpresa hornitzaileko (gure posta kudeatzen duen ekipoaren jabe den enpresa) administratzaileak edo teknikariak, nahi badu, gure posta kontsulta dezake. Halaber pentsa dezakegu harcker bat Pentagonoko ordenagailutan sartu bada ez lukeela gure posta-zerbitzarian sartzeko arazorik izango.

Konfidentzialtasun osoa behar badugu, gure posta elektronikoa enkriptatu dezakegu. Posta elektronikoko bateko informazioa kodifikatuko litzateke, Sarean batetik bestera doan bitartean hirugarren pertsona batek eskuratuz gero irakur ezin dezan. Mezua, deskodifikatzeko software-mota egokia duten pertsonak bakarrik desencriptatu ahal izango dute. Hori egin behar dugu, Internet bidez e-mail bat bidaltzea “postal” bat bidaltzea bezala delako, posta elektronikoa gutunazalik gabeko mezua da. Posta elektronikoko edozein mezu hasieratik amaierara atzeman, irakur eta/edo alda daiteke (horrek ez du esan nahi egingo denik, baina aukera hor dago, eta gainera, egin denaren inolako aztarnarik utzi gabe egin daiteke).

PGP

Gure e-maila enkriptatzeko modu egokiena “PGP Security” programaren doako bertsioa (norberak erabiltzeko) erabiltzea da.



Programa honek hiru zerbitzu eskaintzen ditu:

- ✓ **Konfidentzialtasuna.** Enkriptatzearen bidez, erabiltzaile bati, mezua hartzaileak bakarrik irakurriko duela bermatuko zaio.
- ✓ **Kautotzea.** Erabiltzaileari, bidali aurretik dokumentu bat sinatzeko aukera ematen dio, eta horrek, aldi berean ondoko honetarako bidea ematen dio:
 - ❖ Sinatu denez, dokumentua aldatu ez dela ziur egotea. Mezua aldatuko balitz, sinadurak ez luke baliorik izango.
 - ❖ Mezua pertsona jakin batek sinatu duela egiaztatzea.
- ✓ **Segurtasuna.** Goian adierazitako sinadurak, igorlearen nortasunarenpean egoteaz gain mezua edukiarenpean ere badago; horrenbestez, mezua aldatzen bada, sinadurak jada ez du baliorik izango.

SINADURA DIGITALA

Hala ere, enkriptatzeak ere arazoak ditu. Mundu guztia ez dago, heltzen zaion mezu bakoitza enkriptatu eta desenkriptatzeko eragozpenak jasateko prest. Horregatik, enkriptatze-programek, segurtasun osoaren (igorlea eta hartzailea, zein sistema erabiltzeari buruz ados jartzea inplikatzeko du gutxienez) eta gaur egun e-mail gehienak igortzen diren arduragabetasunaren artean erdiko bidean geratzeko aukera ematen dute. Erdi-bide horretan sinadura digitala dago. Posta elektronikoaren amaieran, mezu horretarako zehazki “da hor” sortutako hainbat zenbaki eta letra gehitzen dira. Aplikazio egokia erabiliz, hartzaileak egiazta dezake, igorlea, esaten ari dena ote den, eta oraindik garrantzitsuagoa dena, mezua, ziberespazioan egindako ibilbidean zehar manipulatu ote duten.

Mezuak enkriptatu edo digitalki sinatzea ez da erabiltzaile aurreratuen ondare bakarrik. Tutoretza egokiak dituen edonork (www.Kriptopolis.com helbidean oso dokumentazio praktikoa dago) mota horretako programa instalatu ahal izango du. Ondoren, mezu bat enkriptatu edo sinatzeko ekintza bera, posta elektronikoko aplikazio arrunteko botoi batean klik egitera mugatzen da.



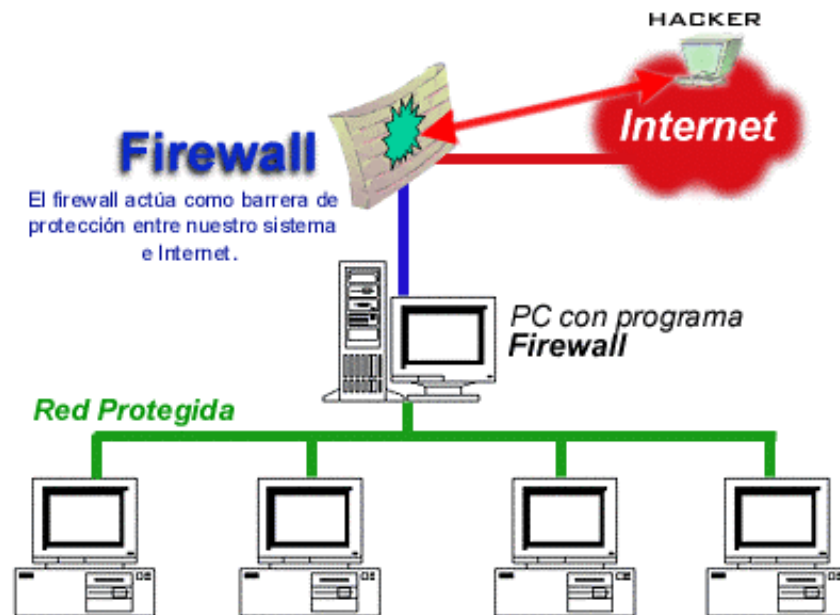
5. CHAT-EKO BEZEROEN ARRISKUAK

Chat-a fenomeno sozial bihurtzen ari da, komunikatzeko modu berria. Bisitariak elkarren artean txateatzeko kanal bat eskaintzen duten atari ugari daude, imajina daitekeen edozein gairi buruzko kanal tematikoak daude. Erabiltzen errazak, munduko edozein tokitako lagunekin bat-batean harremanetan jartzeko eta fitxategiak trukatzeko aukera, aurrez aurre aurpegiak ez ikustea, lengoaiaren malgutasuna dira, zerbitzu hau Interneten gehien erabiltzen denetako bat izateko arrazoiak. Hasieran kalterik eragin ezin duela iruditu arren, oso arriskutsua izan daiteke ekipoaren segurtasunerako, izan ere chat-inguruneek, orokorrean, sare-ingurunean arrisku handia eragiten duten fitxategi, URL, eta abar erraz transmititzen dituzte.

Kontuan izan beharreko gauzak: ezezagunen fitxategiak ez onartzea, eta iturri ezagunek eskatu eta bidalitakoez ez fidatzea. Neurri horri, noski, biruskontrako eguneratua gehitzen zaio; bere modulu egoiliarak fitxategi berrien sarrerak zaindu eta automatikoki aztertu beharko ditu. Puntu horretan, gogoratu behar dugu Web orri baten bidez txateatzeak, horretarako espezifikoki dagoen gune batean egitea baino arrisku txikiagoa duela, adibidez MIRCaren bidez, lehendabizikoak fitxategiak bidali eta jasotzea eragozten digulako.

6. FIREWALL EDO SUEBAKIA

Internetera konektatzeko erabili behar dugun segurtasuneko oinarritzko sistema, Firewall edo suebakia instalatzea da. Firewall, gure ordenagailuaren eta datu guztiek zirkulatzen duten Sarearen artean “hesia” instalatzean oinarritzen den defentsa-sistema bat da. Sarearen eta gure ordenagailuaren arteko trafiko hori firewall-ek (“hesia”) baimendu edo ukatzen du, konfiguratu dizkiogun aginduak jarraituz.



Firewall ekipoz eta programaz osatuta badago ere, etxeko erabiltzailearentzat haiek pixka bat urrun geratzen dira; beraz, deskribatutako funtzioak betetzen dituen programa bat (asko daude) azalduko dugu.

Programa-mota honen funtzionamendua “paketeak iragaztean” oinarritzen da. Gure ordenagailuaren eta Sarearen artean zirkulatzen duen edozein datu edo informazio, programak (firewall) aztertzen du, bi norabidetan pasatu dadin baimenduz edo eragotziz (Internet-->PC edo PC-->Internet).

Azken hori ulertzea oso garrantzitsua da, izan ere zerbitzu edo programa jakin bat baimentzen badugu, firewall-ek ez digu esango programa hori zuzena ala okerra den, edo, sartzen edo irteten ari diren paketeak zuzenak izanda ere, pakete horiek gure sistemarako edo Sarerako datu kaltegarriak izan ditzaketen; horregatik kontu handia izan behar da emango ditugun baimenetan.

Azken honen adibide bezala Posta Elektronikoa ipini dezakegu. Gure firewall-ean postako programa jakinen bat Internetera heltzeko baimena ematen badugu, eta gure posta jasotzean, hartutako mezu batean birusa badakar, adibidez har motakoa, firewall-ak ez gaitu birus horretatik babestuko, programa horri Sarean sartzeko baimena eman baitiogu. Hala ere firewall-ek, eranskina exekutatzearan harra, guk alde aurretik onartu ez dugun ataka batetik sarera sartzen saiatzen bada ez dio hedatzen utziko. Dena den, postako bezero bera erabiltzen badu hedatu egingo da. Firewall-en zeregina trafikoa onartu edo atzera botatzea da, baina ez bertako edukiarena. Kasu honetan, adibidez Panda bezalako Biruskontrako programa batetik babesteko zeregina dago (fitxategi erantsi bat besterik gabe ez exekutatzeko sen onaz gain).



Firewall batek, printzipioz, edozein trafiko eragotziz funtzionatzen du, gure ordenagailuko ataka guztiak itxiz. Zerbitzu edo programa zehatz bat Interneten edo gure ordenagailuan sartzen saiatzen den unean jakinaraziko digu. Une horretan, trafiko hori onartu edo atzera bota ahal izango dugu, eta halaber, erantzun “iraunkor” bihur dezakegu onartzeko gure politika aldatzen ez dugun arte (onartu edo atzera botatzeko eragiketa aldi bakoitzean ez errepikatu behar izateko).

Politika egokiak izan beharko luke, zalantza baten aurrean, sarbiderik ez onartzea, baldin eta erabili nahi dugun zerbitzuak behar bezala funtzionatzeko beharrezkoa ez dela eta printzipioz sistemarako arriskutsua ez dela egiaztatu arte. Sarrera debekatzen badugu eta gure sistemak ondo funtzionatzen jarraitzen badu, ez dugu behar, eta horrenbestez ez dugu ukatu behar.

Firewall bat ezarriz, bidegabe sartzeen aurrean gure sistema askoz ere sendoagoa egitea lortuko dugu.

Gehien erabilitako eta doako bertsio batean deskarga dezakegun programetako bat ZoneAlarm (www.zonelabs.com) da. Programa honi esker, gure ekiporako nahi dugun segurtasun-maila zehaztu dezakegu.

7. SPAM-A: MEZU BAZTERGARRIA

E-mail helbidea lanpostu askotan tresna komun, eta gure etxeetako ordenagailutik ezarritako pertsonen arteko komunikazioetarako oso tresna erabilgarri bihurtu da.

Aurki edozein hiritarrek posta elektronikoaren aurrean, bizitza osoan izandako tresna batekin ariko balitz bezala jardungo du; halaxe gertatzen ari da telefono mugikorren hedapen zabalarekin. Baina, telefono-zenbakia interesatzen zaizkigunei bakarrik ematen diegun bezala, eta arrotzen eta telefono bidezko saltzaileen deiak oso desatseginak gertatzen zaizkigun bezala, helbide elektronikoa gune pribatua da eta, beraz, bertan sarrerak mugatuta egon behar du: mundu guztiak ezin dizkigu mezuak bidali.

Nahi ez ditugun gutunek gure ordenagailuan eta gure bizitzan sartu eta internauta gogaitzeaz gain, arazo larriak eragin ditzakete.



Adituen arabera, munduan 263 milioi posta-helbide inguru daude eta erabiltzaile bakoitzak batez beste egunean 30 mezu jasotzen ditu. Iaz mezu horien %70 spam edo publizitate-erauntsiak izan zirela kalkulatu da. Eta etorkizunean egoerak okerrera egitea espero da. Ondorioz, euren postontzi elektronikoa publizitate edo euren gustukoak ez diren mezuz beteta ikusi nahi ez duten zibernauten kezak oso ulergarriak dira; gainera mezu horiek Saretik “jaisteak” denbora (eta dirua, tarifa laua ez badugu behintzat) eskatzen du.

Gartner Group taldeak posta elektronikoko erabiltzaileen artean duela gutxi egindako azterketa batek erakusten du Interneteko hamar kontsumitzailetatik bederatzi spam-aren biktima direla astean behin gutxienez.

NOLA LORTZEN DITUZTE HELBIDE-ZERRENDAK?

Adituek ere galdera bera egiten dute. Hainbat erabiltzailek diote ez dakitela nola gertatzen den hori, beste hainbatek uste dute helbideak cookien (erabiltzailea Internetera konektatzen denean automatikoki sortzen diren kode-linea laburrak) bidez banatzen direla, erabiltzailearen identitatea xurgatzen dutela, eta informazio-mota hau bildu eta ordaintzen dutenek igortzen dizkietela.

Beste askok uste dute norberaren helbidea lortzen dutela erabiltzaile hori Webgune edo sarrera-hornitzaileen gune batean sartu eta nahita izena ematen duenean. Ondoren hornitzaile horiek euren bezeroen posta-helbideak enpresa interesatuei saltzen dizkiete.



Halaber diote, Interneten antolatzen diren hainbat zerbitzu, ekitaldi eta solasalditak jaso daitezkeela; bertan erabiltzaileari, lehiaketan parte hartzeko izena eman dezan eskatzen zaio.

NAHI EZ DITUGUN E-MAIL KOMERTZIALEN AURREAN ZER EGIN?

Erabiltzaile gehienek, euren gogoz kontra eta denbora asko galduz jasotako publizitate-mezu horiek ezabatu ondoren, lehenago edo beranduago norbaiten aurrean kexatzen dira. Zenbaitek spam-a igorri dienari irainduz erantzuten diete, beste hainbatek kexak Interneten sartzeko hornitzaileari luzatzen dizkiote, besteek jaso nahi ez duten mezuaren onurak jasoko dituen konpainiari idazten diote, eta gutxienez lagun eta ezagunei jakinarazten dizkiete; hala ere badira, euren kexa Administrazioaren aurrean aurkezten dutenak. Eskatu ez den posta komertzialeko bonbardaketa elektronikoen aurrean, hainbat enpresek irtenbideak eskaintzen dituzte. Adibidez, posta elektronikoko hainbat softwarek (programa informatikoak) spammerrek gehien erabilitako esaldiak iragazteko tresnak eranstzen dituzte, eta tresna horiek nahikoak ez badira, erabiltzaileak, Internetetik jaitziko beste hainbat tresna gehitu ditzake.

Spam Attack Pro www.sofwiz.com/html/spam_attack_pro.htm helbidean eskura daiteke; bertan, spam-zerrenda bat dago eta berriak gehitu daitezke. Exterminator spamak (www.unisyn.com/spamex) automatikoki postako karpeta aztertzen du jaso nahi ez diren mezu horien bila, bere gain dituen 17.000 helbideko datu-base baten arabera. Eta amaitzeko, Spamkiller (www.spamkiller.com) osatuenetako bat da eta hainbat iragazkirekin lan egin dezake, igorlearen, hitz gakoaren, izenburuaren edo erabiltzaileak espezifikatzen duen beste edozein aginduren arabera mezuak geratu arte.

Sokaren beste muturrean, mezu horiek diseinatu, landu eta igortzen dituzten, eta e-mail helbideen datu-basea erabili eta mantentzen duten enpresak daude. Konpainia horientzako, helburu komertzialekin posta-zerrenda batean parte hartzen duten pertsonak bazkideak edo bezeroak dira, biktimak inoiz ez. Funtsezkoena mezu gehiegi ez bidaltzea eta mezu horietan zerbait eskaintzea dela defendatzen dute. Eskaintakoak ez du bakarrik informazio komertzial izan behar, erabiltzaileak, zerrenda horietako batean egoteagatik onuraren bat jaso beharko luke. Hartzaileek, nahi dutenean zerrenda horietatik irteteko erraztasuna izan behar dutela ziurtatzen dute.

SPAM-AREN AURREAN NOLA JARDUN

- ✓ Inoiz ez erantzun eskatu ez den mezu bati. Zure helbidea aktibo dagoela berretsi besterik ez duzu egingo.



- ✓ Ez da gomendatzen mezu horietako bat bera ere irain edo antzeko zerbaiten bidez erantzutea. Zure aurka joan daiteke.
- ✓ Spama egin duen pertsonari buruz postmasterraren aurrean kexatzea.
- ✓ Helbide jakin batetik mezu gehiago ez jasotzeko, gure posta-programan mezu- edo erregela-iragazkiak konfiguratzeko.
- ✓ Zure mail-helbidea Interneteko edozein formulario edo forotan ez uztea.
- ✓ Zabor-mezu gehiegi jasotzen ari bazara, beharbada onena zure posta-helbidea jasotzea izango da.

8. INTERNETEKO 10 MAULA EZAGUNENAK

Egunero, Interneten ematen diren iruzurrei buruzko eskandaluzko albisteak entzun edo irakurtzen ditugu. Informazio ugari, askotan ez oso zehatza eta desitxuratua, baina Sarearen sinesgarritasunerako eta bertan aritzen garenontzat oso kaltegarriak.

Egia da maulak ematen direla, baina ez dira zibermerkatariak horren arduradun bakarrak; internauta askok, merkataritza elektronikoan dauden gabezia legalez baliatuta, legez kanpo horri etekina ateratzen diote. 2000ko maiatzean gertatutakoa ikusi besterik ez dugu egin behar American Expressek ofizialki helduentzako Webguneetan (gune pornografikoak), karguen baliogabetzeak transakzioen %40ko kopurua gainditu zuelako euren txarteletan on-line kobratzeko zerbitzuak eskaintzeari uzten ziola adierazi zuenean. Argiago esanda, sexuguneetara sartzeko American Express txartelarekin ordaintzen zuten bisitarien ia erdiak, biharamunean euren bankuari kargua baliogabetzeko eskatzen zion. Hori egin daiteke transakzioa ez bada SET protokoloan egin. Protokolo hori, txartelaren titularraren kautotzea eskatzen duenez, transakzioa ez onartzeko aukera ematen ez duen bakarra da.

Baina aipa ditzagun Sarean jarduten duten merkatariek egindako iruzurrak. Sarean ematen diren 10 iruzur nagusien zerrenda argitaratu da, internautak iruzur horietatik babestuta egon daitezten.

Honako hauek dira:

- ✓ **Iruzurrak enkantetan:** enkantean esleitu den dirua bidali ondoren, adierazitako ezaugarriak ez dituen produktu bat jasotzen da, bai eta inolako baliorik ez duen produktu bat ere.
- ✓ **ISPen (Internet Zerbitzuen Hornitzaileak) iruzurrak:** baliteke klausulen atala irakurri gabe on-line kontratuak izenpetzea; horrenbestez, hori egiten duten pertsonak libratu ezingo duten iraupen luzeko kontratuean egon daitezke, eta



aurretik kontratua eteteko isun handiak ordaintzera behartuta egon daitezke. Maiz ematen den beste kasu bat, domeinu-izenak erregistratzen dituzten ISPeK euren izenean egitea, eta horrela, euren domeinu-izena galduko luketelako zerbitzua utzi ezin duten bezeroak lotuta izateko.

- ✓ **Webguneen diseinua/promozioa:** telefono-fakturan, inoiz eskatu edo kontratatu ez ziren zerbitzuengatik ustekabeko karguak gertatu ohi dira.
- ✓ **Kreditu-txartelen gehiegikeria:** adina egiaztatzeko helburu bakarrarekin kreditu-txartelaren zenbakia eskatzen zaio, eta ondoren ezeztatzen zailak diren karguak egiten zaizkio.
- ✓ **Maila Anitzeko Marketinga edo Sare Piramidalak:** produktuak edo zerbitzuak komertzializatuz diru asko egingo dela agintzen da, norberaren edo guk geuk biltzen ditugun saltzaileen bidez; baina azkenean gure bezeroak inoiz ez dira azken kontsumitzaileak, banatzaileak baizik, eta horrenbestez katea apurtu egiten da eta irabaziak katean lehendabizi sartu zirenek bakarrik eskuratzen dituzte.
- ✓ **Negozio-aukerak eta “Zeure etxetik lan egin” bezalako iruzurrak:** etxetik bertatik lan egiteko eta norbera nagusi izateko aukera eskaintzen da oso sarrera-plan handiak erakutsiz. Baina noski hasteko, inoiz irteerarik ez duten makina edo produktutan inbertitu behar da.
- ✓ **Berehala aberasteko Inbertsio Planak:** oso errentagarritasun handiko agintzek eta merkatu bereziei buruzko segurtasun osoko finantza-aurreikuspenek iruzurrezko eragiketak estaltzen ohi dituzte.
- ✓ **Bidaia edo opor-paketetan iruzurrak:** azkenean eskainiko zaion zerbitzua baino kalitate handiagoko bidaiak eta ostatuak saltzean datza; halaber, kontratatu ez ziren kontzeptuengatik ordaindu beharra gerta daiteke.
- ✓ **Telefono-iruzurrak:** sexu guneetan bada nahiko zabaldua dagoen sistema bat. Webean doan sartzeko programa bat jaitsi eta gure ordenagailuan instalatzeko eskatzen zaigu. Baina, guk jakin gabe, ordaintzeko nazioarteko zenbaki bat markatzen du (Espainiako 906 motakoa), eta zenbaki horren bidez Webean sartzen dira. Horrenbestez, argazkiak eta bideoak ikusten dibertitzen ari garen bitartean gure telefono-faktura izugarri handitzen ari da.
- ✓ **Osasun-gomendioetan iruzurrak:** edozein gaixotasun sendatzeko errezeta miraritsuak maiz aurkitzen dira Sarean. Gehienak inolako babes mediku edo osasun-agintarien kontrolik gabe; horregatik, agindutako emaitzak ez dituztenez, maula izateaz gain, gaixoaren osasunerako beste arrisku bat suposa dezakete.

Ikus daitekeen bezala, ez dago alde handirik iruzurgileak Interneten egiten ari direnaren eta urtetan bizitza errealean egin dutenaren artean. Alde bakarra da Sarean gauzak aurpegia eman gabe egin daitezkeela, eta beraz, arriskua txikiagoa da eta desagertzea errazagoa.

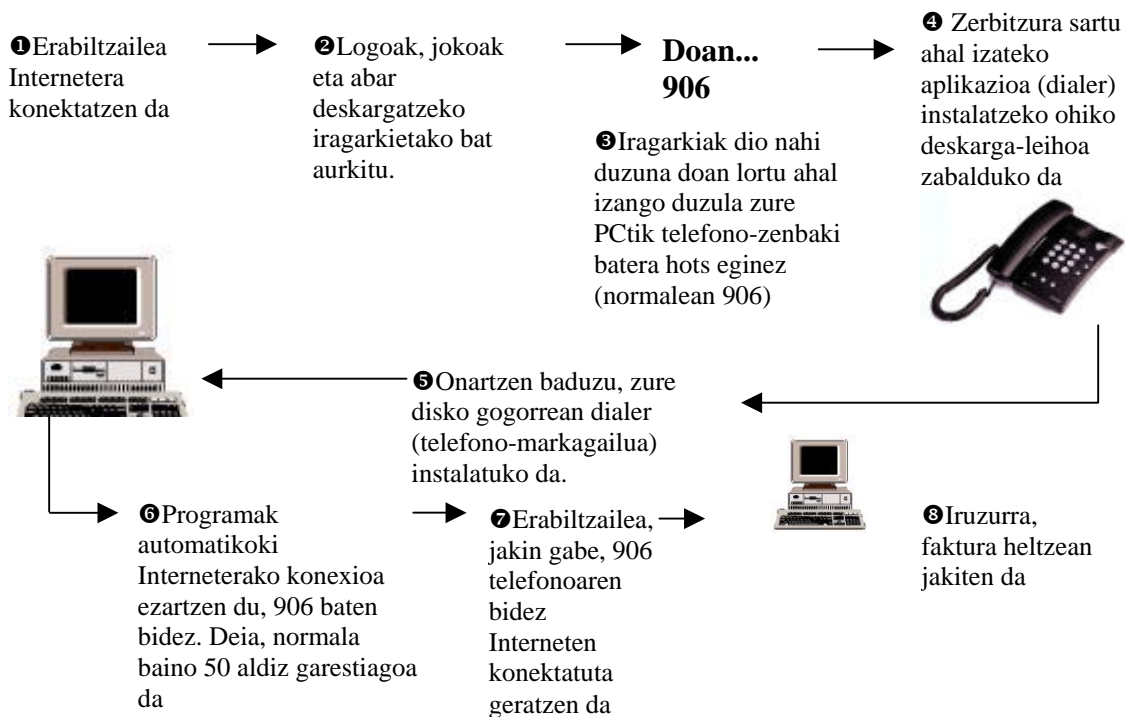
Pertsonaia maltzur horien esku ez erortzeko errezeta: konfiantzazko Webguneetan bakarrik erosi, eta benetako helbidea edo telefono-zenbakia ematen ez dutenetatik ihes egin.

9. 906 TELEFONO-ZENBAKIEN IRUZURRA

Egunez egun gero eta Webgune gehiagotan iragartzen dituzte eduki erotiko/pornografikoetarako doako sarrerak, edo kreditu-txartelen bidez erosi beharrik gabe telefono mugikorretarako logoak eta melodiak, edo ordenagailurako pantaila-babesak saltzen dituzten orriak. Eskaintza horietako askok erabiltzaileari, bezeroari edukiez gozatzeko aukera emango dion doako programa deskargatu eta instala dezan eskatzen diote.

Erabiltzaile gehienek, publizitate iruzurtiak bultzatuta edo programa horietan ezkututzen den letra txikia ez irakurtzeagatik, ez dakite 906 zenbakien bidez konektatzen dituzten markagailuak edo “dialer” erabiltzen ari direla (Espainian tarifatze berezia, kasu onenean 100 pezeta minutuko).

906 zenbakiaren iruzurrak honela funtzionatzen du:



Arazoa are larriagoa da “dialer” horietako zenbaitek erabilitako jardun-mota erasokorrak kontuan hartuta. “Dialer” horietako zenbait, deia, konexioak irauten duen



bitartean mantentzera mugatzen dira, hau da, ordenagailua itzaltzean deia amaitu egiten da, eta berriz konektatzean jatorrizko zenbakia erabiltzen da. Hainbat kasutan ordea, sistemaren konfigurazioa aldatzen dute; ondorioz, erabiltzailea Internetera konektatzen den bakoitzean 906 bidez egiten du. Gainera, erabiltzaileak tarifa laua badu (prezio finko batekin Internetera etengabe konektatuta egoteko aukera ematen du), kostuak, hots, telefono-fakturak, oso handiak dira. Zenbait kasutan ere “dialer” hori instalatzea baimentzeko sakatu behar diren botoien erantzuna aldatu egin da, hau da, utzi botoia sakatzen badugu, onartzen ari garela esaten ari gara.

Biktima gehienek Interneten egiten ari diren ohiko zereginekin jarraitzen dute, aldaketaz jabetu gabe. Telefono-faktura heltzen den arte. Lehen erreakzioa, akats bat dela pentsatzea da. Kaltetu gehienek, urdurituta, operadoreari hots egiten diote faktura berriz aztertzeko eskatzen. Ondoren ezustekoa dator: faktura zuzena da. Hurrengo pausoa, arazoa eragin duen 906 horren atzean nor dagoen aurkitzen saiatzea da. Baina operadoreek ezin dute informazio hori eskaini, gaur egungo arauak debekatu egiten baitute. Faktura izugarri horiek ordaintzeari uko egin dioten hainbat kaltetuk ikusi dute telefono-linea moztu diotela deiak ez ordaintzeagatik.

IRUZUR HONEN AURREAN EGON DAITEZKEEN IRTENBIDEAK

- ✓ Kaltetuek epaitegi hurbilenean salaketa jar dezakete, operadoreak datuak eman ahal izateko agindu judiziala behar delako. Horrek prozesu luzea eta garestia eragin dezake, eta erabiltzaileentzat berehalakoa eta premiazkoa den arazoa konpondu gabe utzi. Gaur egun, alabaina, operadoreek ezin dute zenbaki jakin bati dagozkion fakturen zatia ordaintzeari uko egiten dioten pertsonen horniketa moztu, beti ere gainerako zatia ordaintzen badute.
- ✓ Euren lineak tarifatze bereziko zenbakietarako deiak murriztea eska diezaiekete operadoreei, zenbaki horien artean 906arekin hasten direnak daude.
- ✓ Irtenbidea bilatzen, CheckDialer garatzen ari dira. Modem (edo RDSI) bidez egiten diren konexioak monitorizatzen dituen Windows sistemetarako programa.

Euren zeregina honako hau da: konexio bat saiatzean markatzen den telefono-zenbakia antzematea eta debekatutako zenbakien txantilo batekin (Zerrenda Beltza) alderatzea. Markatzen saiatzen ari den zenbakia Zerrenda Beltzeko patroiren batekin bat badator, programak erabiltzaileari jakinaraziko dio eta markatzea amaitu aurretik eten egingo da, Windowsen eta modemaren arteko komunikazioa geldiarazten baitu (serieko atakaren mailan).

Beste aukera, are murriztaileagoa eta seguruagoa, onartutako zenbakien zerrenda konfiguratzea da (Zerrenda Zuria); horrenbestez, CheckDialer-ek zenbaki horietako batzuekin konexioa bakarrik onartuko du eta gainerakoak atzera botako ditu.

Programa hori doan behera kargatzeko honako Web orri hau bisitatuko dugu:

<http://seguridad.internautas.org/checkdialer.php>



10. HELBIDE INTERESGARRIAK

✓ Birusei buruz:

www.rompecadenas.com.ar

Goiburuak argi adierazten du: “Guztia, e-mail bidez heltzen zaizkigun hoax, spam, birus eta beste hainbat zaborri buruz”. Mota guztietako zoritxarrekin mehatxatzen zuten garai bateko gutun/kateak Sarera egokitu dira. Orri honek haietaz babesten laguntzen du.

www.edata.es/Enciclop.html

Informatikako birusen laburpen osatua. Erabiltzaileak, alfabeto bidez antolatutako zerrenda zabal batean zein birus-mota duen aurki dezake eta, zenbait kasutan, birus hori ezabatzeko modua ere.

www.monografias.com/trabajos/estudiovirus/estudiovirus.shtml

Artikulu zabal eta luze honek birusen inguruko guztia argitzen du ez oso ikuspegi teknikitik, eta eskuragarri gertatzen da aditu ez direnentzat. Izurrite horien jatorria oso ondo dokumentatuta dago.

pauillac.inria.fr/~doligez/corewar/

Hasieran birusak, informatikako sistemen bihotzean garatzen ziren gerratan elkarren artean desafiitzen zuten denbora-pasak besterik ez ziren. Jolas hori, aurrerago sortu ziren birusak ez bezala, ez zen gaiztoa eta horretan aritzen direnek xakearekin alderatzen dute.

<http://tira.escomposlinux.org>

Ordenagailuak eragindako arazoak umorez hartu behar dira ez badugu haserre bukatu nahi. Ecol-en asteko komikiak, ordenagailuekin saltsan dabilzanek jasaten dituzten buruhaustek satirizatzen ditu, eta hainbeste kable eta sigla ulertezinaren alde alaiena erakusten du.

<http://www.privacy.org/>

Pribatutasunari buruzko webgunea.

Espanian dauden biruskontrako konpainiak:

www.pandasoftware.com

www.commandsoftware.com

www.cai.com

www.f-secure.com

www.avp.ru

www.nai.com

www.norman.com

www.sophos.com

www.symantec.com



www.trendmicro.com

Biruskontrako babesarekin lotutako beste hainbat erakunde eta Web:

www.eicar.com

European Institute for Computer Anti-virus Research erakundearen orria. Institutu honen lana, birusen eta mota guztietako kode kaltegarrien aurka borrokatzera bideratuta dago. Unibertsitate, segurtasun-aditu eta abarrez osatuta dago. Hizkuntza: ingelesa.

www.trusecure.com

Biruskontrako programen kalitatea ziurtatzeko erakundea. Hizkuntza: ingelesa.

www.wildlist.org

Orri honek, "In the wild" (arruntenak) dauden birus guztiei buruz informatzeko helburua du eta hileko zerrenda homonimoak argitaratzen ditu. Hizkuntza: ingelesa

www.westcoast.com

Biruskontrako programen kalitatea ziurtatzeko erakundea. Secure Computing Magazine aldizkariko editoreak. Hizkuntza: ingelesa.

✓ **Merkataritza elektronikoari buruz:**

www.mju.es

Justizia Ministerioaren webgunea. Bertan, indarrean den Merkatartza Elektronikoari buruzko Legearen inguruko informazioa aurki dezakegu.

✓ **Kriptologiari buruz**

www.kriptopolis.com

Sarean pribatutasunari buruzko gaztelaniazko web osatuenetako bat. Gaur egun, eraldaketa teknologikoan murgilduta dago, eta horregatik bertako zerbitzu askok ez dute behar bezala funtzionatzen.

www.pgp.com

Pribatutasun Nahiko Ona (Pretty Good Privacy). Izen bitxia, inoiz izan den dokumentuak enkriptatzeko sistema onenetako batentzat. PGP programaren jatorrizko kodea ezkutatzeko erabakiak erabiltzaile-talde handi baten errezeloak eragin ditu, eta hauek, GnuPG bezalako alternatiba libre eta gardenak sortu dituzte. GnuPG-ak gainera Alemaniako gobernuaren babesas jaso du.

✓ **Firewall edo suebakia:**

<http://www.zonelabs.com>

Trebeenek konfiguratzeko aukera badutela ere, internauta hasi berriek erraz erabiltzeko suebaki eraginkorra. Etxeko erabiltzaileentzako doan da.

✓ **Spam-ari buruz:**

www.sofwiz.com/html/spam_attack_pro.htm

www.unisyn.com/spamex

www.spamkiller.com



✓ **Datuen babesari buruz:**

www.eff.org

Zibernauten askatasun zibilak babesten dituen erakundea. Hasieratik, merkatu erraldoi bat beharrez, erabiltzaileen pribatutasunarekiko errespetua eta adierazpen-askatasuna nagusituko den foro komun bat izan nahi duen Sarea sustatzeagatik nabarmendu da.

<http://www.ulpiano.com/boletinprivacidad.html>

On line pribatutasun-buletina.

http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/

Datuen babesari buruzko Europako Kontseiluaren orria.