

**616 COMUNICACIONS****INTERNET****SEGURETAT****3641**

Existeixen diversos factors que poden inhibir els usuaris d'Internet:

#### ELS VIRUS

Són programes informàtics que ataquen la informació guardada a l'ordinador i que es poden traspasar voluntària o involuntàriament a d'altres ordinadors. Per això cal que instal·lem a l'ordinador programes de detecció de virus. També és recomanable, en qualsevol cas, efectuar còpies de seguretat de la informació continguda al nostre ordinador per evitar-ne el risc de destrucció.

#### LES GALETES O COOKIES

Són un conjunt de dades que el servidor d'una pàgina web grava en forma d'arxiu en la memòria de l'ordinador de l'usuari. Aquestes dades són informació relativa a les visites que l'usuari fa a una web i permet al seu autor saber quines seccions han estat consultades, conèixer les preferències i personalitzar els seus serveis en funció dels gustos de l'usuari. Les galetes (cookies) han arribat a ser un important instrument d'obtenció d'informació per l'administrador del servidor i pels departaments de màrqueting de les empreses que fan publicitat per Internet.

Quan el prestador del servei utilitzi aquests dispositius d'emmagatzematge i recuperació de dades ho ha d'informar al consumidor de manera clara i completa. Li ha d'indicar la finalitat de les dades i el seu ús. A més li ha de facilitar l'opció de refusar aquest tractament de les seves dades amb un procediment gratuït i senzill

Per evitar que es gravi cap cosa al disc dur de l'ordinador i que, en accedir a una pàgina web, s'envii informació al servidor, cal desactivar l'opció acceptar cookie. Una altra manera de controlar l'enviament de galetes (cookies) és fer que cada cop que s'envii una galeta (cookie), aparegui un missatge d'avís, de forma que l'usuari pugui decidir si vol que s'envii o no al disc dur del seu ordinador.

També hi ha programes que permeten filtrar o eliminar les galetes (cookies) que es van instal·lant al disc dur de l'ordinador de l'usuari. A Internet poden trobar-se també programes i servidors que permeten una navegació anònima a través de la xarxa, eliminant o substituint elements identificadors de l'usuari.

#### RECOMANACIONS ALS USUARIS D'INTERNET DAVANT EL PHISING (pesca de contrasenyes)

El "Phishing" és una tècnica informàtica d'enginyeria social, a través de la qual s'utilitza il·lícitament un duplicat fals d'una pàgina web amb la finalitat d'aconseguir, de manera fraudulenta, les dades confidencials de la persona destinatària del correu electrònic (contrasenyes i claus bancàries, números de compte i de targetes de crèdit, dates de caducitat...) per tal de fer-ne ús.

- Podem arribar a rebre a la nostra adreça electrònica determinats correus electrònics fraudulents, contingut il·lícit, enviats massivament sota una aparença simulada d'una entitat bancària o financera, de que ens demana les nostres dades personals i confidencials d'accés a serveis bancaris (contrasenyes de comptes bancaris, claus bancàries, números de targetes de crèdit, dates de caducitat...) de manera fraudulenta amb falsos pretextos (verificar les dades, actualitzar el sistema, reactivar el compte, problemes de caràcter tècnic...) i amb la intenció d'apropiar-se de les nostres dades confidencials.
- Desconfiem d'aquest tipus de correus electrònics indiscriminats i no els contestem en cap concepte, encara que reproduïxin perfectament el logotip i les senyes d'identitat o la signatura de l'entitat bancària, i imitin l'original, ja que tenen la intenció de capturar les nostres dades bancàries de manera fraudulenta.
- És una pràctica fraudulenta a Internet; és un correu trampa on hi ha voluntat d'enganyar-nos, com a usuaris/destinatària d'aquest correu, per tal d'aconseguir de manera fraudulenta la nostra informació

*Aquesta fitxa es informativa i no té cap valor jurídic vinculant*



bancària secreta, personal i confidencial i poder fer-ne ús.

- Vigilem! No facilitem les nostres dades personals, privades i confidencials d'accés als serveis bancaris (contrasenyes de comptes bancaris, claus bancàries, números de targetes de crèdit...) per correu electrònic.
- Els bancs i les caixes mai no ens demanaran que els informem de les nostres claus i informacions secretes i confidencials a través del correu electrònic.
- No hem d'emplenar el formulari que ens adjunten per enviar les dades que ens sol·liciten.
- No hem d'accedir a la pàgina web falsa que inclou aquest correu electrònic, no és la web real i oficial de l'entitat bancària, per més que s'assembli i ens vulguin fer creure que és la pàgina web original.
- Sapiguem identificar una pàgina web segura quan la seva adreça electrònica comença per "https" en lloc de "http".
- No n'hem de fer cas, ni tan sols davant les amenaces de bloquejar-nos el compte, si no facilitem la informació que ens demanen i encara que ens assegurin que la intenció del correu és "evitar el frau".
- No hem de contestar aquest tipus de correus electrònics.
- Eliminem els correus electrònics d'aquest tipus.
- Comprovem sempre l'adreça del remitent; desconfiem si és un remitent fals i fixem-nos si el correu electrònic està personalitzat: mai no ho està en aquests tipus de correus electrònics indiscriminats.
- Si aconseguixen fraudulentament les nostres dades personals (pesca de contrasenyes), les utilitzaran per realitzar operacions per Internet i suplantaràn la nostra identitat.
- Reconeguem, rebutgem i denunciem els correus electrònics que ens conviden a facilitar informació confidencial d'una manera fraudulenta.

#### OFERTES FALSES DE TREBALL

Hem d'anar amb compte si rebem un correu electrònic d'una oferta falsa de treball amb la intenció fictícia de contractar personal laboral i d'apropiar-se de les nostres dades bancàries per a finalitats fraudulentament.

És una modalitat de Phishing a través de la qual una empresa fraudulenta ens comunica que cerca personal de confiança per a un lloc de comandament o similar, amb uns ingressos alts i ràpids dins d'un horari flexible (temps parcial) i des de casa.

En aquest correu de falsa oferta de treball ens sol·liciten, amb engany, les dades del nostre compte bancari per a finalitats fraudulentament sota l'aparença d'una oferta de treball ben pagat que consistirà a rebre girs bancaris, transferències bancàries i posteriorment enviar aquests diners a l'estranger.

Vigilem si estem cercant treball en els portals d'Internet perquè, aleshores, podem rebre correus personalitzats amb la mateixa intenció fraudulenta.

Seguim les recomanacions esmentades a dalt: recordem que és una pràctica fraudulenta a Internet; és un correu trampa on hi ha voluntat d'enganyar-nos, com a usuaris/destinatari d'aquest correu, per tal d'aconseguir de manera fraudulenta la nostra informació bancària secreta, personal i confidencial i poder fer-ne ús.

On denunciar-ho?

- A la Brigada d'Investigació Tecnològica (BIT), cos de la Policia Nacional que investiga els delictes comesos a través d'Internet <http://mailto:fraudeinternet@policia.es>.

-A la Comissaria dels Mossos d'Esquadra: en el cas que la persona consumidora hagi estat víctima d'un delicte informàtic.

#### SPAM O CORREU BROSSA

El "Spam" o correu brossa és tot tipus de comunicació no sol·licitada, realitzada per via electrònica.

*Aquesta fitxa es informativa i no té cap valor jurídic vinculant*

Tinguem en compte que la nostra adreça electrònica és una dada de caràcter personal; recordem que tenim reconegut el dret fonamental a la protecció de dades personals.

- Està prohibit l'enviament de comunicacions publicitàries o promocionals no sol·licitades, realitzades a través de correus electrònics o altres mitjans de comunicació electrònica equivalents, que no haguessin estat prèviament sol·licitades o expressament autoritzades pels seus destinataris. Això no serà necessari, en canvi, quan existeixi una relació contractual prèvia, sempre que el prestador hagi obtingut de manera lícita les dades de contacte del/de la destinatari/ària i les utilitzi per a l'enviament de comunicacions comercials referents a productes o serveis de la seva pròpia empresa, que siguin similars als que inicialment hagin estat objecte de contractació amb el/la client. En tot cas, el prestador ha d'oferir al/a la destinatari/ària la possibilitat d'oposar-se al tractament de les seves dades amb finalitats promocionals mitjançant un procediment senzill i gratuït, tant en el moment de recollida de les dades, com en cadascuna de les comunicacions comercials que li dirigeixi.
- Podem utilitzar programes de filtratge en el nostre equip.

#### L'ACCÈS A PÀGINES DE PAGAMENT

Sovint us podeu trobar que quan navegueu per Internet és una pràctica comuna l'oferiment de descarregar-vos determinats programes o continguts dels quals no coneixeu la procedència.

És recomanable vigilar molt bé abans d'acceptar aquests productes ja que molts cops per accedir a determinades temàtiques (premis, concursos, casinos, pornografia, eròtica, etc.) en moltes pàgines web s'ha d'accedir a través de números de telèfon de cost elevat (907). Aleshores en lloc de connectar a Internet pel nostre número de node de tarifa metropolitana hi accedim a través d'aquest telèfons, el cost dels quals és molt més car ja que paguem el servei que ens estan oferint a través la pàgina web.

L'accés a aquest tipus de pàgines es realitza a través dels anomenats serveis de tarificació addicional.

Els serveis de tarificació addicional que s'ofereixen a Internet són aquells que, a través d'un determinat prefix (907), comporten una retribució per la prestació d'uns serveis d'informació o entreteniment i, en conseqüència, a l'usuari se li repercuteix un cost addicional a part del de la pròpia trucada. Per a més informació consulteu el tema de consum Serveis de tarificació addicional (803, 806, 807, 907 i 905i SMS Premium).

Teniu dret a sol·licitar de la vostra companyia telefònica la desconexió als telèfons que comencen per aquests prefixos.

No obstant amb l'actual normativa, des del 22 d'agost de 2004, ja no són de lliure accés els números de serveis de tarificació addicional que comencen per 907 (d'accés a través d'Internet)

Les trucades a aquests prefixos han de venir desglossades a les factures de telèfon on podeu comprovar-ne el cost econòmic. Podeu demanar a la companyia telefònica que identifiqui l'empresa titular del servei per si voleu reclamar o denunciar a aquesta en cas d'incompliment.

#### LA PROTECCIÓ DE DADES

Existeixen programes rastrejadors que permeten de localitzar adreces de correu electrònic als fòrums públics d'Internet: grups de notícies, xats, llistes de correu, etc.

L'arrova, com a element comú de totes les adreces, permet detectar i capturar automàticament gran quantitat d'adreces de correu electrònic, que després s'introdueixen en una base de dades en què els usuaris estan segmentats en funció del tema de debat o a la llista de distribució corresponent.

El xat permet que d'altres participants del xat introdueixin virus (o cavalls de Troia -troians-) a l'ordinador per tal de facilitar-hi un posterior accés. Per prevenir aquests casos cal emmascarar la nostra adreça de correu electrònic mitjançant l'addició d'un text que provoqui la devolució dels missatges enviats. Per exemple: usuariNOSPAM@domini.es

*Aquesta fitxa es informativa i no té cap valor jurídic vinculant*

Els operadors han de garantir la protecció de les dades personals en l'exercici de la seva activitat.

Els operadors podran tractar les dades amb finalitat de promoció comercial, sempre i quan l'abonat hagi donat el seu consentiment informat.

Ha de dirigir-se als abonats, almenys amb un mes d'antelació a l'inici de la promoció, informar-los del tipus de servei per al que s'efectuarà el tractament, els tipus de dades i la durada. Aquesta comunicació haurà d'efectuar-se a través d'un mitjà que garanteixi la recepció per part de l'abonat, podrà dur-se a terme de manera conjunta a la facturació del servei prestat. Ha de facilitar-se a l'interessat un mitjà senzill i que no impliqui cap cost, per tal de manifestar la seva negativa al tractament de les dades. En particular, és ajustat al reglament el procediment on la negativa pugui efectuar-se mitjançant un enviament prefranquejat o la trucada a un número telefònic gratuït o als serveis d'atenció al client.

Si en el termini d'un mes des que l'abonat rep la sol·licitud no s'hagués pronunciat al respecte, s'entendrà que consenteix el tractament de les dades, sempre que així s'hagués fet constar a la informació dirigida a l'abonat.

En tot cas, els abonats tindran la possibilitat de retirar en qualsevol moment el seu consentiment per al tractament de les seves dades.

#### LA PUBLICITAT PER INTERNET

Algunes empreses opten per l'enviament de publicitat no sol·licitada a través del correu electrònic a causa del seu baix cost. Aquest fet, però, perjudica la imatge de l'empresa i aquesta pràctica compta amb el rebuig generalitzat dels usuaris d'Internet.

L'enviament de publicitat o promocions mitjançant el correu electrònic o un altre mitjà equivalent està prohibida, llevat que el consumidor hagi prestat el seu consentiment o ja existeixi una relació comercial anterior i la publicitat es refereixi a productes o serveis similars als que inicialment va comprar o contractar el consumidor.

En tot cas, l'empresari ha d'oferir al consumidor la possibilitat d'oposar-se d'una manera ràpida i senzilla a l'enviament d'aquesta publicitat, inclòs el cas en què prèviament hagués prestat el seu consentiment.

És recomanable no obrir aquells correus dels que no en coneixem el remitent o no hi ha descripció del tema que contenen.

#### INTERNET I ELS MENORS

Internet s'ha convertit en una eina d'ús generalitzat tant entre els adults com entre els més joves amb un gran potencial educatiu i d'entreteniment. Però també ha comportat l'aparició de riscos per als menors i cal que pares i educadors estiguin prou informats per tal d'ajudar els menors a navegar per Internet de manera segura.

A l'Estat espanyol hi ha el Centre d'Internet Més Segura, que pertany a la xarxa europea Insafe, coordinada per Protégeles i el CUSICAT (Centre de Seguretat de la Informació de Catalunya). Aquest centre proveeix de recursos de sensibilització, línies de denúncia (Hotlines) i línies d'assessorament i ajuda (Helplines).

A l'apartat de publicacions del web Internet segura es recullen els diferents consells adreçats a ciutadania per tal d'ajudar els infants i els adolescents a navegar amb seguretat, usar les xarxes socials de forma segura i tenir un ús segur del dispositius mòbils:

- Familiaritzar-se amb Internet. Per poder ajudar els usuaris més joves cal que els adults coneguin també aquest mitjà.
- Parlar obertament amb els menors i adolescents sobre l'ús d'Internet i intentar crear un clima de confiança perquè ens informin sempre que vegin alguna cosa que no els agrada o que els fa sentir incòmodes.
- Navegar junts per la xarxa, així podrem ensenyar-los a navegar de manera segura i donar-los recursos, perquè sàpiguen utilitzar Internet responsablement. Per exemple, podem comentar amb ells la diferència entre publicitat i contingut educatiu o d'entreteniment i mostrar-los exemples de cada cosa.

*Aquesta fitxa es informativa i no té cap valor jurídic vinculant*



- Informar-se sobre els instruments de prevenció que són programes informàtics que permeten els adults prevenir l'ús que els menors fan d'Internet.
- Preguntar en els centres educatius quina política de seguretat segueixen.
- Establir regles bàsiques de seguretat a la llar i en el centre educatiu.
- Col·locar l'ordinador de casa a una sala comuna a la vista de tothom.
- Ensenyar els menors i adolescents a navegar amb seguretat per tal de distingir els continguts recomanables i comunicar-se de manera positiva.
- Cercar llocs web segurs adreçats a infants o adolescents.
- Davant un possible problema, reaccionar a temps, parlant amb el menor i trucar a la policia o algun altre organisme adient.

- Ordre IET/1090/2014, de 16 de juny, per la qual es regulen les condicions de qualitat del servei en la prestació dels serveis de comunicacions electròniques.
  - Llei 9/2014, de 9 de maig, general de telecomunicacions.
  - Llei 22/2010, del 20 de juliol, del Codi de consum de Catalunya (versió consolidada).
  - Resolució de 28 de juliol de 2009, de la Secretaria d'Estat de Telecomunicacions i per a la Societat de la Informació, pel qual es modifica l'annex I de la Ordre ITC/912/2006, de 29 de març, per la qual es regulen les condicions relatives a la qualitat en la presentació dels serveis de comunicacions electròniques.
  - Reial decret 899/2009, de 22 de maig, pel qual s'aprova la carta de drets de l'usuari dels serveis de comunicacions electròniques.
  - Llei 56/2007, de 28 de desembre, de mesures d'impuls de la societat de la informació
  - Reial decret legislatiu 1/2007, de 16 de novembre, pel qual s'aprova el Text refós de la Llei general per a la defensa dels consumidors i usuaris i altres lleis complementàries (versió consolidada).
  - Reial decret 1494/2007, de 12 de novembre, pel qual s'aprova el Reglament sobre les condicions bàsiques per a l'accés de les persones amb discapacitat a les tecnologies, productes i serveis relacionats amb la societat de la informació i mitjans de comunicació social. (Text consolidat)
  - Llei 22/2007, d'11 de juliol, sobre comercialització a distància de serveis financers destinats als consumidors.
  - Ordre ECF/215/2007, de 30 de maig, per la qual s'estableix el procediment d'atorgament i retirada del distintiu públic de confiança en línia, així com l'exercici de les funcions adreçades a vetllar pel manteniment dels requisits que en justifiquen l'atorgament.
  - Ordre ITC/1030/2007, de 12 d'abril, per la qual es regula el procediment de resolució de les reclamacions per controvèrsies entre usuaris finals i operadors de serveis de comunicacions electròniques i l'atenció al client pels operadors.
  - Ordre ITC/912/2006, de 29 de març, per la qual es regulen les condicions relatives a la qualitat de servei en la prestació dels serveis de comunicacions electròniques.
  - Reial Decret 424/2005, de 15 d'abril, pel qual s'aprova el Reglament sobre les condicions per a la prestació de serveis de comunicacions electròniques, el servei universal i la protecció dels usuaris. Modificat per Reial decret 329/2009, Reial decret 1768/2007 I Reial Decret 776/2006
  - Llei 59/2003, de 19 de desembre, de signatura electrònica.
  - Resolució de 3 de novembre de 2003, de la Secretaria d'Estat de Telecomunicacions i per a la Societat de la Informació, per la qual s'atribueix un rang de numeració específic per a la provisió de serveis de tarifació addicional sobre sistemes de dades.
  - Llei 32/2003, de 3 de novembre, General de Telecomunicacions.
  - Llei 34/2002, d'11 de juliol, de Serveis de la Societat de la Informació i el Comerç Electrònic.
  - Ordre de 21 de febrer de 2000 per la qual s'aprova el Reglament d'acreditació de prestadors de serveis de certificació i de certificació de determinats productes de signatura electrònica.
  - Reial Decret Llei 14/1999, de 17 de setembre, sobre signatura electrònica.
- DATA D'ACTUALITZACIÓ: 30/1/2015