Govern d'Andorra

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Navegació Segura

Conscienciació en ciberseguretat

Juny de 2022

ÍNDEX

Riscos en navegar per internet

Connectar-se a internet s'ha convertit en una situació més que quotidiana. Tant en l'àmbit personal com laboral, passem la major part del dia connectats, i això és una cosa que els ciberdelinqüents coneixen i aprofiten. Internet ens ofereix innumerables avantatges, però també exigeix una sèrie de precaucions per mitigar les ciberamenaces que ens aguaiten.

Llocs web falsos o il·legítims
Els ciberdelinqüents suplanten webs conegudes per enganyar-nos i aconseguir les nostres credencials, diners i informació de valor.

Spoofing
Conjunt de tècniques de hacking per suplantar la nostra identitat, la d'una web o entitat.

Captura de tràfic mentre naveguem
L'atacant es posiciona entre la comunicació del nostre dispositiu i el punt d'accés a la xarxa. Són atacs de tipus "man in the middle".

Descàrrega de contingut amb codi maliciós
Descàrrega del contingut en webs fraudulentes o llocs no oficials que continguin codi maliciós que infecta els nostres equips.

ÍNDEX

Ciberatacs en falses web o "fake web"

Un dels casos més comuns de ciberatacs en els últims temps és el "fake web", en el que l'atacant configura un lloc web sota el seu control per suplantar una web legítima, normalment de forma parcial (formularis d'accés o de pagament), per obtenir tant les credencials, com una transacció econòmica, com informació sensible de la víctima. És una de les tècniques utilitzades en els atacs de tipus phishing, i que poden ser molt difícil de detectar si estan molt ben elaborats i no prestem la deguda atenció.

L'atacant redirigeix a la víctima al lloc fals i si la víctima no se n'adona acabarà introduint la informació personal. Si la suplantació tècnica no és perfecta, normalment apareixerà un missatge d'error del tipus "la contrasenya introduïda no és correcta", "el correu electrònic o la contrasenya no són correctes"... En aquest moment la víctima es redirigeix a la pàgina original suposant un error en l'introduir les dades, i l'atacant ja haurà aconseguit les credencials de l'usuari.

L'atacant redirigeix a la web falsa

L' usuari introdueix la seva informació

La informació es enviada a l'atacant, que redirigeix a la web original

L' usuari continua amb les seves funcions

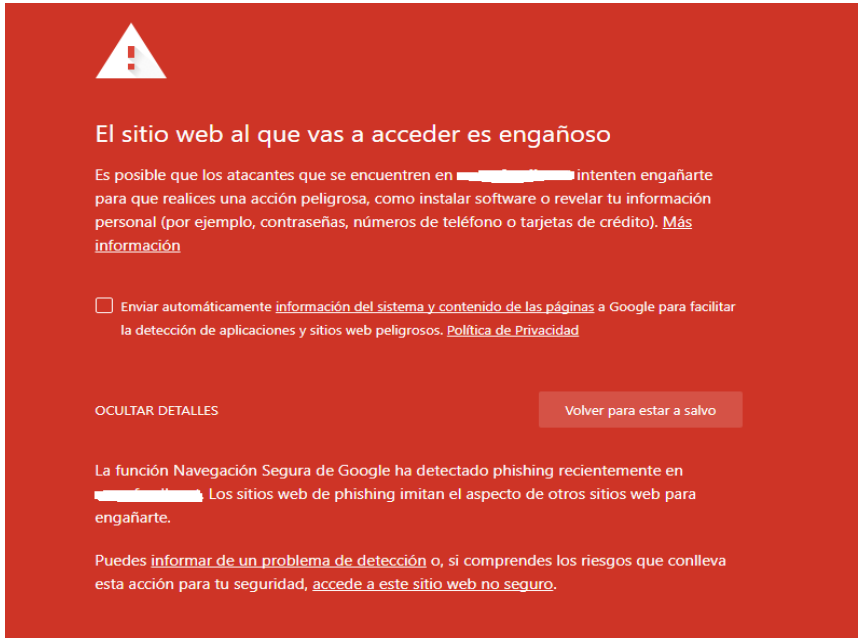
imagen: Flaticon es

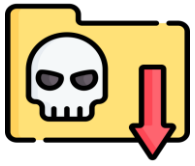
ÍNDEX

Eines de navegadors contra "fake web"

Actualment, alguns navegadors tenen configurat, de forma predeterminada, el bloqueig a llocs web de caràcter fraudulent. En el navegador de Google podem trobar les següents advertències:

- El lloc web al qual vas a accedir conté programari maliciós: el lloc que vas a visitar podria intentar instal·lar programari maliciós en el teu ordinador.
- El lloc web al qual vas a accedir és enganyós: és possible que el lloc que vas a visitar sigui de suplantació d'identitat (phishing).
- Lloc web sospitós: el lloc que vols visitar sembla sospitós i pot ser que no sigui segur.
- El lloc web al qual vas a accedir conté programes nocius: és possible que el lloc al qual vas a accedir intenti enganyar-te perquè t'instal·lis programes que podrien causar-te problemes quan navegues per Internet.
- Aquesta pàgina està intentant carregar scripts de fonts no autoritzades: el lloc que vas a visitar no és segur.





Important: Compte amb el que descarregues. Alguns llocs web intentaran enganyar-te perquè descarreguis programari nociu advertint-te que tens un virus. Ves amb compte i no descarreguis aquest tipus de programari.

imagen: Flaticon es

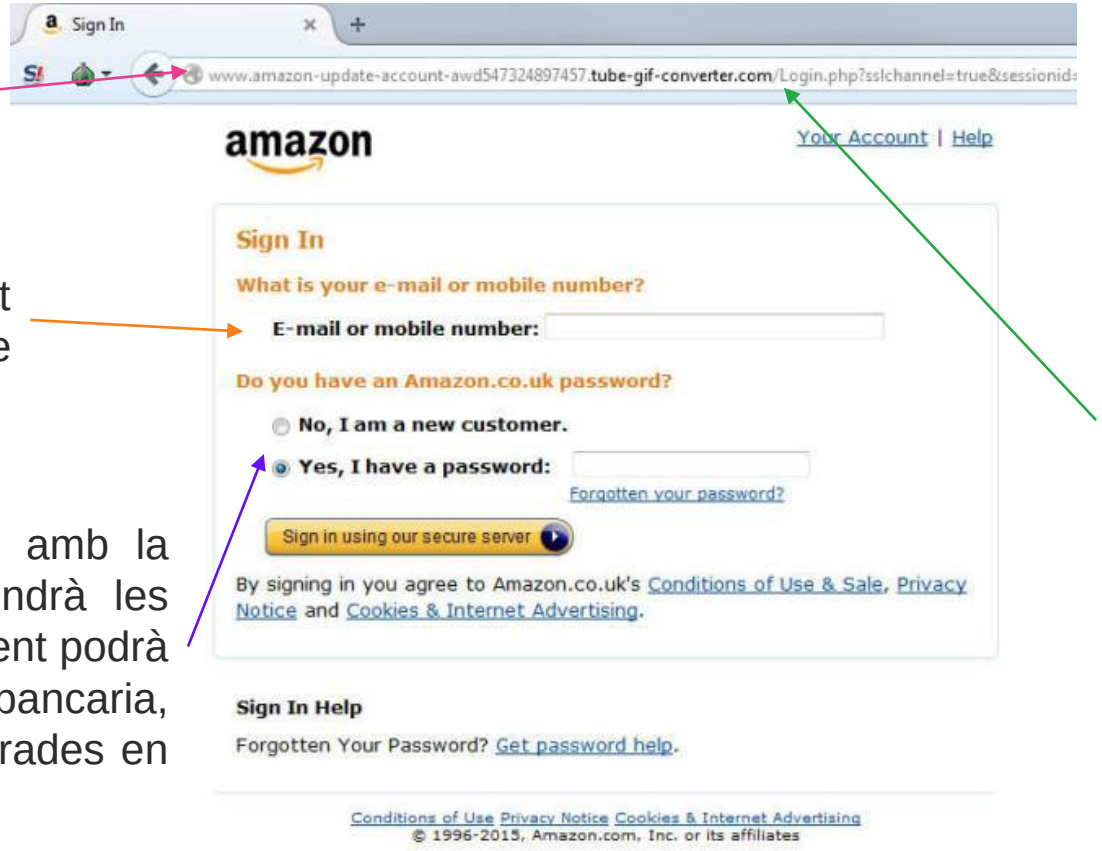
ÍNDEX

Ciberatacs a través de "fake web" - EXEMPLE

No utilitza el protocol https, no es una web segura.

L'atacant imita de manera molt fidel el formulari de accés de Amazon.

Quan l'usuari completi l' accés amb la seva informació. L'atacant, obtindrà les credencials d' accés, i possiblement podrà accedir a la seva informació bancaria, domicili i dades de targeta registrades en la web suplantada.



La URL no pertany a la web de Amazon, si no que hem estat redirigits a la web del atacant.

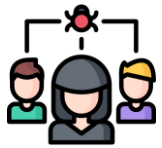
ÍNDEX

Captura de tràfic mentre naveguem

Un dels riscos als quals estem més exposats quan naveguem en la xarxa es la captura de tràfic o atacs del tipus "man in the middle". Aquest atac segueix la següent la metodologia: l'atacant es posiciona entre les comunicacions del nostre equip amb el punt d'accés wifi, capturant tot el tràfic d'informació que es doni entre els dos. Durant aquesta captura pot, no sol redirigir-nos a pàgines web falses o fraudulentes, sinó també infectar amb codi maliciós el mateix punt d'accés i obtenir informació sensible a partir d'aquesta captura.

Bàsicament, l'atacant té accés a la informació transitada a través del canal, i decideix si deixa passar aquesta informació o bé modificar-la perquè arribi a l'altre extrem informació falsa. En alguns casos, s'arriba inclús a suplantar la identitat d'un dels interlocutors.

Els punts d'accés wifi pública o els punts d'accés wifi amb baixa seguretat són escenaris molt probables per aquest tipus d'atacs, en els que el ciberdelinqüent utilitza el nom d'una xarxa de confiança perquè accedim i poder realitzar l'atac.

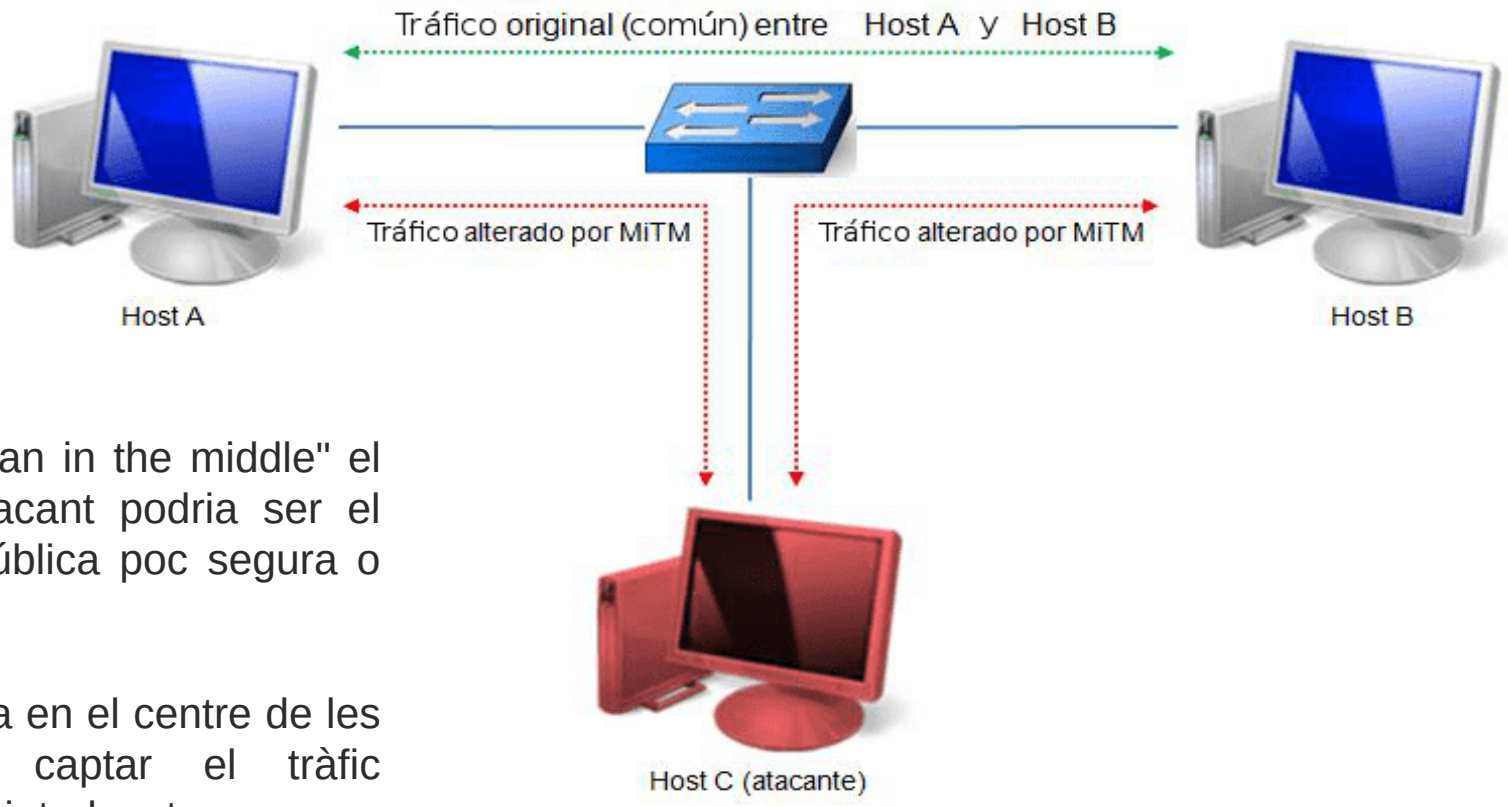


Les xarxes d'àrea local (LAN) corporatives són també vulnerables a aquest tipus d'atacs. L'atacant, una vegada tingui accés a la xarxa, llençarà un atac per passar desapercebut per als altres equips i poder, d'aquesta manera, capturar les comunicacions dintre de la xarxa empresarial.

imagen: Flaticon es

ÍNDEX

"Man in the middle" (MITM)



En un atac MITM "Man in the middle" el punt d'accés de l'atacant podria ser el router d'una xarxa pública poc segura o una xarxa il·legítima.

L'atacant es posiciona en el centre de les comunicacions per captar el tràfic d'informació entre els interlocutors.

imagen: insecuredata.blogspot.com

ÍNDEX

Enverinament de Cookies

Un altre exemple associat a la captura de tràfic d'informació en una connexió és l'enverinament de Cookies. Les Cookies són fitxers d'informació enviada per un lloc web i emmagatzemada pel navegador de l'usuari, amb finalitats tan diverses com establir la connexió, controlar la sessió (després d'un login), recordar preferències de l'usuari, o registrar l'activitat de l'usuari pela seva anàlisi.

En un atac del tipus MITM "Man in the middle", un atacant podria interceptar aquestes Cookies per fer-se amb la nostra informació o sessió, inclús modificar-les amb finalitats diverses. Aquest tipus d'atac podria afectar a llocs web que controlen les sessions dels usuaris amb altres tècniques (p. ex. amb tokens tramesos a través d'URL) però sense aplicar la deguda protecció.

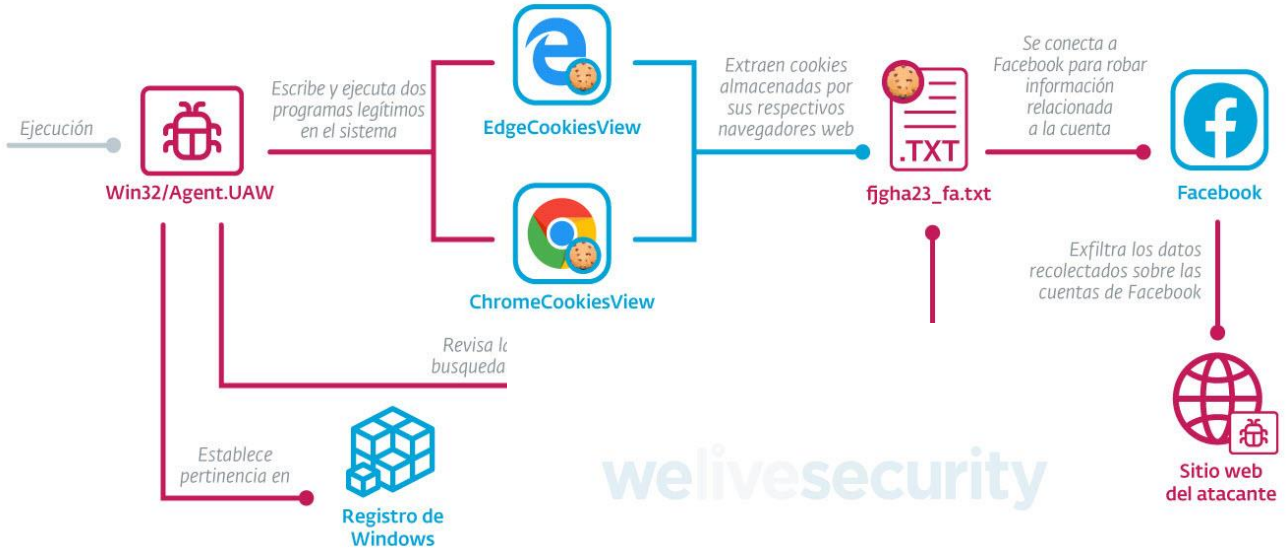


imagen: cert.gov.py

ÍNDEX

Descàrrega de contingut amb codi maliciós

Sovint sorgeix la necessitat de fer ús d'un nou programari o contingut específic que sense referències clares acabem buscant sense un criteri clar a través d'internet. En general, tota descàrrega d'internet és especialment perillosa, ja que els atacants solen penjar fitxers que continguin codi maliciós en llocs web molt diversos. De fet, a vegades han arribat a utilitzar repositoris de webs legítimes després de prendre el control. És interessant tenir present la varietat de programari maliciós o malware que ens podem trobar:

És molt important tenir present que el codi maliciós pot anar incrustat en diversos tipus de fitxers, com són executables però també en fitxers ofimàtics (Word, Excel, pdf).

A vegades va adjunt a un fitxer legítim i podria passar desapercebut inicialment.

- **Virus:** Malware dissenyat per copiar-se a si mateix i propagar-se en el màxim de dispositius.
- **Adware:** Software maliciós que ens mostra constantment anuncis no desitjats que redirigeixen a webs fraudulentes.
- **Spyware:** Malware que s'instal·la en l'equip i recopila informació de l'activitat per compartir-lo amb un usuari remot.
- **Trojan:** Malware que es camufla en l'equip fent-se passar per software legítim.
- **Backdoor:** S'instal.la en el sistema obrint una porta posterior per la que l'atacant pot prendre el control del equip de forma remota.
- **Keylogger:** Malware de seguiment que registra les tecles premudes per l'usuari per robatori de credencials.
- **Stealer:** Malware que accedeix a la informació privada emmagatzemada en un dispositiu.
- **Ransomware**: Malware que pren el control del dispositiu per xifrar l'accés a la informació del mateix i que sol demanar un "rescat" com desbloqueig d'aquesta informació.
- **Worm**: Malware que pot modificar les característiques del sistema.
- **Rogueware**: Malware que simula ser una eina antivirus i ens redirigeix a pàgines web fraudulentes amb el fi de "resoldre el problema".
- **Cryptojacking**: Utilitzen el control del nostre dispositiu per dur a terme extraccions de criptomonedes.

ÍNDEX

Guia de bones pràctiques

Assegurat de tenir l'antivirus actualitzat i amb totes les proteccions actives.

Mantingues actualitzat el sistema operatiu, navegador, plugins instal·lats en aquest i la resta d'aplicacions de l'equip.

Utilitza contrasenyes robustes i diferents. Diferència entre comptes personals i laborals.

Configura les regles del Firewall correctament per una major seguretat.

Ves amb compte per on navegues. Assegurat que és una web segura i evita els llocs no oficials.
Si la navegació la inicies des d'un enllaç extern, assegurat que és legítim.
Compte amb els URL escurçades.
Para atenció en la informació del navegador.

Descàrrega únicament software amb llicència i contingut de llocs oficials.
Escaneja tot fitxer descarregat.
Evita el contingut pirata i actualitzacions que solen tenir codi maliciós.

Restringeix la navegació des de xarxes wifi públiques o poc segures. Sobretot en accedir a llocs amb àrea privada per usuaris.
Fes ús de connexions VPN o xarxes mòbils.

ÍNDEX

1

Actualitzacions automàtiques: Garanteixen un nivell adequat de seguretat, ja que corregeixen les vulnerabilitats descobertes, solucionant errors o bugs i atorguen noves funcionalitats.

- Configurar el teu navegador de forma correcta es un gran pas per la seguretat de la teva navegació per internet. Tenint en compte les mesures i bones pràctiques de navegació segura, els següents passos seran de gran ajuda:

Chrome

En PC i MAC, Google Chrome és manté actualitzat automàticament. Per revisar l'estat d'actualització del navegador: Botó menú > Configuració > Informació de Chrome

Firefox

Botó menú > General > Actualitzacions de Firefox > Instal·lar actualitzacions automàticament (recomanat)

I seleccionar checkbox: Quant Firefox no s'estigui executant. Aquesta configuració mantindrà el navegador actualitzat inclús quan no s' estigui executant.

Safari

MAC: Es manté actualitzat juntament amb el propi sistema operatiu.
Menú apple > Preferències del Sistema > Actualització de software > Mantenir el Mac actualitzat automàticament
iPhone i iPad: Configuracions > Configuració > General > Actualització de software

Android: Play Store > Botó menú > Configuracions > Preferències de xarxa > Actualitzar aplicacions automàticament

iPhone i iPad: Configuracions > [nom] > iTunes Store i App Store> Actualitzacions de apps

ÍNDEX

2

Finestres emergents, plugins i llocs web fraudulents: Al navegar per internet ens exposem a varis riscos, i molts d'ells provenen de llocs web fraudulents o instal·lació d' extensions plugin amb codi maliciós o malware. Aquest llocs es difonen a través de finestres emergents pel que, bloquejar-les, es més que necessari.

Chrome

PC i MAC: Botó menú > Configuració > Seguretat i Privacitat > Configuració de llocs > Finestres emergents i redireccions > No permetre que els llocs enviïn finestres emergents ni utilitzin redireccions I per protecció front a malware: Botó menú > Configuració > Seguretat i Privacitat > Seguretat > Protecció millorada
Android: Botó menú > Configuració > Configuració de llocs > Finestres emergents i redireccions
iPhone i iPad: Botó menú > Configuració > Configuració de contingut > Bloquejar Finestres emergents

Firefox

Protecció enfront a finestres emergents: Menú > Configuracions > Privacitat i seguretat > Permisos > Bloquejar finestres emergents
Protecció enfront a malware: Menú > Configuracions > Seguretat > Permisos > Bloquejar contingut perillós i enganyós
Protecció enfront a instal·lació de extensions: Menú > Ajustes > Privacitat i seguretat > Permisos > Advertir quan els llocs web intenten instal·lar complements

Safari

MAC: Safari > Preferències > Seguretat i Activar la protecció contra la autoinstal.lació d' extensions.
iPhone i iPad: Per la protecció enfront a finestres emergents: Configuració > Safari > Bloquejar finestres.

ÍNDEX

4. Configuració segura del navegador

3

Emmagatzematge de contrasenyes: Els navegadors compten amb la funció d'auto completat de credencials per els formularis d' accés, el qual no es una opció molt segura, ja que fa als nostres equips susceptibles d'atacs a credencials. Es recomanable desactivar-lo.

Chrome

PC i MAC: Botó Menú > Configuració > Auto completar > Contrasenyes > Preguntar si vull guardar contrasenyes

Android, iPhone i iPad: Botó Menú > Configuració > Contrasenyes > Guardar contrasenyes (Desactivar)

Les contrasenyes guardades es podran eliminar des de la pàgina indicada en cada cas.

Firefox

Botó Menú > Configuració > Privacitat i seguretat > Usuaris i contrasenyes > Preguntar per guardar contrasenyes i inicis de sessió de llocs web

Les contrasenyes guardades es podran eliminar des de la mateixa pàgina.

Safari

MAC: Safari > Preferències > Omplir automàticament noms d'usuari i contrasenyes. Les contrasenyes guardades es podran eliminar des de la mateixa pàgina.

iPhone i iPAD: Les contrasenyes es gestionen a través del clauer de iCloud. Es considera un mètode segur.

ÍNDEX

4

JavaScript: Molts ciberdelinqüents aprofiten aquest llenguatge per explotar vulnerabilitats de robatori de sessió mitjançant atacs de "Cross-site scripting (XSS)", o "e-skimming", on modifiquen el codi d'una web comercial per obtenir dades personals i bancaries de l'usuari.

Chrome

PC i MAC: Botó Menú > Configuració > Seguretat i Privacitat > Configuració de llocs > No permetre que els llocs utilitzin Javascript

Android: Botó Menú > Configuració > Configuració de llocs > Javascript

iPhone i iPad: Javascript no pot deshabilitar-se.

Firefox

Escriu en la barra de recerca del navegador **about:config**, busca javascript.enabled i assigna el valor false.

Safari

MAC: Safari > Preferències > Seguridad > Permetre Javascript (desmarcar opció)

iPhone i iPad: Configuració > Safari > Avançat > Javascript (desmarcar opció)

***Aquesta configuració pot afectar al funcionament de pàgines que utilitzin continguts dinàmics.

ÍNDEX

4. Configuració segura del navegador

5

Cookies: Les cookies son fitxers que s'emmagatzemen en l'equip i que permeten realitzar un seguiment de la navegació del usuari. Es important restringir la seva configuració per garantir la privacitat del usuari.

Chrome

PC i MAC: Botó Menú > Configuració > Seguretat i Privacitat > Cookies i altres dades de llocs > Esborrar cookies i dades de llocs al tancar totes les finestres
Android: únicament permet esborrar cookies de forma manual: Botó Menú > Configuració > Privacitat i seguretat > Esborrar dades de navegació
iPhone i iPad: únicament permet esborrar cookies de forma manual: Botó menú > Opcions > Privacitat > Esborrar dades de navegació

Firefox

Configuracions > Privacitat i seguretat > Cookies i dades del lloc > Eliminar cookies i dades del lloc quan tanqui Firefox

Safari

MAC: Safari > Preferències > Seguretat > Eliminar cookies i dades emmagatzemades > Gestionar dades de llocs web > Eliminar tot
iPhone i iPad: Configuracions > Safari > Avançat > dades de llocs web > Eliminar totes les dades

ÍNDEX

4. Configuració segura del navegador

6

Descàrrega i execució automàtica: Si accedim a un lloc web fraudulent correm el risc de que en una finestra o pàgina emergent es realitzi la descàrrega i execució automàtica de contingut maliciós. Inclús no sent un lloc web fraudulent, hem d'anar en compte amb l' execució de contingut sense previ anàlisis.

Chrome

PC i MAC: Botó Menú > Configuració > Descàrregues > Preguntar on es guardarà cada arxiu abans de descarregar-lo
Android, iPhone i iPad únicament permet esborrar cookies de forma manual: Botó Menú > Configuració > Descàrregues > Preguntar quan guardar els arxius i Preguntar on guardar els arxius

Firefox

Configuracions > General > Preguntar sempre on guardar els arxius

Safari

MAC: Safari > Preferències > llocs web > Seleccionar preguntar (als llocs webs i al visitar altres llocs webs) > Eliminar cookies i dades emmagatzemades > Gestionar dades de llocs web > Eliminar tot
iPhone i iPad: Configuracions > Safari > Avançat > llocs web > Seleccionar preguntar (als llocs webs i al visitar altres llocs webs) > Eliminar cookies i dades emmagatzemades > Gestionar dades de llocs web > Eliminar tot

Govern d'Andorra

Agència Nacional de Ciberseguretat d'Andorra

ANDORRA DIGITAL

Entitats col·laboradores

andorra telecom

DIGITALAND by Ibermática | TIN