

GUÍA PER A PARES SOBRE SEGURETAT EN DISPOSITIUS



L'ENTORN DIGITAL



ESTABLIR LIMITS



CONTROL PARENTAL



PISHING



BON ÚS



COMUNICACIÓ



CIBERASSETJAMENT



TENDÈNCIES



OPEN DNS

GUIA PER A PARES SOBRE SEGURETAT EN DISPOSITIUS



Introducció

A l'era digital actual, els nostres fills utilitzen internet i les xarxes socials de manera quotidiana. Tot i que aquestes eines ofereixen moltes oportunitats, també presenten riscos que els pares han de comprendre. Aquest butlletí té com a objectiu proporcionar informació i consells per guiar els vostres fills en l'ús segur i responsable de la tecnologia.

Comprendre l'entorn digital

Informe-vos sobre les plataformes: Familiaritzeu-vos amb les xarxes socials i aplicacions que utilitzen els vostres fills, com Instagram, TikTok i Snapchat.

Cultura digital: Entengueu les tendències i desafiaments en línia que són populars entre els adolescents.

Educació sobre Seguretat a Línia

Phishing i estafes: Ensenyeu-los a reconèixer correus i missatges sospitosos.

Ciberassetjament: Parli sobre el ciberassetjament i com actuar si passa.

Contingut inapropiat: Ajudeu els vostres fills a identificar i evitar contingut nociu.



Phishing

El phishing és un tipus d'atac en línia que intenta enganyar les persones perquè revelin informació personal sensible, com ara contrasenyes, números de targetes de crèdit o dades bancàries. Aquests atacs es realitzen a través de mètodes de suplantació, on els delinqüents es fan passar per una entitat o persona fiable, com ara un banc, una botiga en línia o fins i tot un amic.

Com funciona el phishing?

1. **Correus electrònics o missatges falsos:** Els atacants envien un correu electrònic, missatge de text (SMS) o missatge a xarxes socials que sembla legítim. Sovint utilitzen el logotip i el nom d'empreses conegudes per semblar més convincents. Per exemple, podrien enviar-te un correu que sembla provenir d'un banc, dient que hi ha un problema amb el teu compte i que necessites fer clic a un enllaç per "solucionar-lo".

Attention! Your PayPal account will close soon!

Dear Member,

We have faced some problems with your account Please update the account .If you do not update will be Closed.

To Update your account, just confirm your informations.(It only takes a minute.)

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm that you're the owner of the account, and then follow the instructions.

[Relog in your account now](#)



Asunto: confirme sus datos,

Notamos que intento iniciar sesion en su area de cliente muchas veces.

Nuestro sistema de seguridad contra fraudes determino tus acciones como peligrosas.

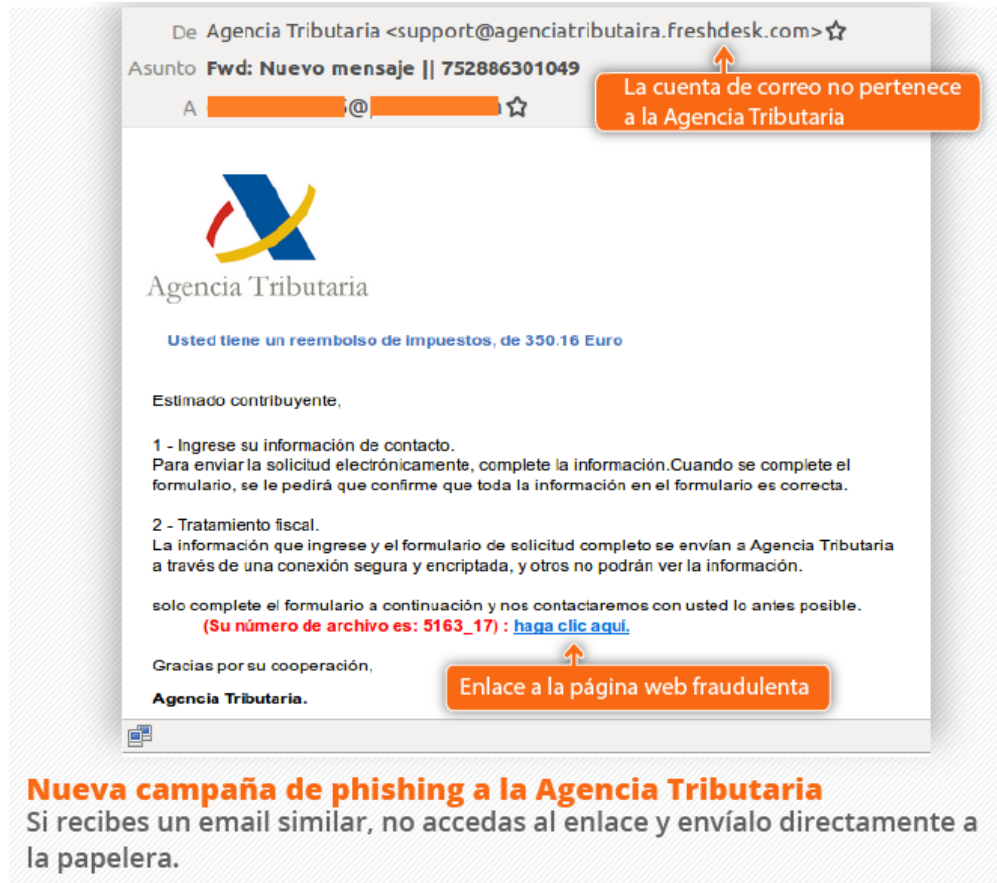
es necesario que confirme que es el titular de la cuenta original.

Su cuenta esta vinculada a su numero de telefono automaticamente despues de firmar el primer contrato.

Le enviaremos un codigo de 6 digitos.

[Completa el proceso](#)

2. **Enllaços fraudulents:** Els missatges contenen enllaços a llocs web falsos que semblen idèntics als llocs reals. Aquests llocs estan dissenyats perquè ingressis la teva informació personal, com ara contrasenyes o dades bancàries, sense que t'adonis que estàs sent estafat.



3. **Sol·licituds d'informació confidencial:** sovint, els atacants intenten crear un sentiment d'urgència perquè actuïs ràpidament. Per exemple, podrien dir-te que el teu compte està a punt de ser bloquejat o que has d'actualitzar la teva informació abans d'una data límit.

----- Mensaje reenviado -----
Asunto: [SPAM] Acción requerida: la contraseña del correo electrónico caducará pronto
Fecha: 2023 23:06:43 -0800
De: [Redacted]
Para: [Redacted]

La contraseña de su correo electrónico [Redacted] expira el [Redacted] /2023.

Para continuar usando este correo electrónico y retener la contraseña, use el botón mantener la misma contraseña debajo

[Mantenga la misma contraseña aquí](#)
Tenga en cuenta que solo puede descargar o leer el mensaje con el correo electrónico [-email-] Este mensaje fue enviado a Sin acceso de terceros

4. **Obtenció de dades personals:** Un cop l'usuari ingressa les seves dades al lloc fals, els atacants poden robar aquesta informació i utilitzar-la per cometre frau, com fer compres, robar diners o accedir a comptes personals.

Senyals d'un atac de phishing

Per protegir-vos, és important que els pares i estudiants coneguin els senyals més comuns d'un atac de phishing:

- **Errors gramaticals o d'ortografia:** Els correus de pesca sovint contenen errors de redacció, com faltes d'ortografia o frases mal estructurades.
- **Sol·licituds d'informació confidencial:** Cap entitat fiable demana informació personal sensible, com ara contrasenyes o números de targetes de crèdit, mitjançant un correu electrònic.
- **Enllaços sospitosos:** Si l'enllaç no coincideix amb el lloc web oficial (per exemple, un domini amb una lletra estranya o un URL curt), és un indicatiu de pesca.
- **Urgència o amenaces:** Els missatges que creen un sentit d'urgència ("Actua ara!" o "El teu compte serà bloquejat!") són comuns en els intents de pesca.
- **Remitent desconegut:** Si el correu prové d'una adreça estranya o sospitosa, és possible que sigui un intent de pesca.

Com prevenir el phishing?

- **No feu clic a enllaços sospitosos:** Abans de fer clic a qualsevol enllaç, és important verificar la URL i assegurar-se que es tracta d'un lloc legítim. Si tens dubtes, és millor escriure l'adreça del lloc directament al navegador.
- **Verificar la font:** Si rebeu un correu d'un banc, botiga o xarxa social demanant-vos que inicieu sessió o actualitzeu la vostra informació, és millor anar directament al lloc oficial en lloc de fer clic en un enllaç del missatge.
- **Habilitació d'autenticació en dos passos (2FA):** Molts serveis ofereixen una capa addicional de seguretat amb l'autenticació en dos passos, cosa que fa més difícil que els atacants accedeixin als comptes encara que tinguin la contrasenya.
- **Utilitzar programari antivirus i antiphishing:** Moltes eines de seguretat inclouen proteccions contra phishing, que et poden alertar si estàs intentant visitar un lloc web perillós.
- **Educar sobre els riscos del phishing:** És important que els pares ensenyin els seus fills a no confiar cegament en missatges que rebin al correu electrònic, xarxes socials o missatges de text.

Com prevenir el phishing als adolescents

- **Ser crítics amb els missatges rebuts:** Ensenya'ls a qüestionar els missatges que demanen informació personal, especialment si provenen de fonts no verificades.

- **Revisar la privadesa en xarxes socials:** Els atacants sovint recopilen informació de les xarxes socials per personalitzar els atacs. Configurar la privadesa adequadament pot reduir aquest risc.
- **Fomentar la comunicació:** Si els adolescents reben alguna cosa sospitosa, s'han de sentir còmodes comunicant-ho amb un adult de confiança abans de prendre qualsevol acció.

Conclusió

El phishing és una amenaça comuna però prevenible. Educar els joves sobre com identificar correus electrònics i missatges sospitosos, i com protegir la informació personal, és clau per evitar ser víctimes d'aquests atacs. Com a pares, és essencial estar atents i tenir converses obertes sobre els riscos en línia, ajudant els teus fills a reconèixer i evitar caure en paranys de phishing.



Ciberassetjament

El ciberassetjament (o cyberbullying en anglès) és una forma d'assetjament que passa a través de mitjans digitals, com ara xarxes socials, aplicacions de missatgeria, fòrums, videojocs en línia, correus electrònics o fins i tot plataformes de streaming. Consisteix en l'ús de la tecnologia per intimidar, fustigar, humiliar o amenaçar una altra persona. Atès que els adolescents passen una part important del seu temps en línia, el ciberassetjament ha esdevingut un problema seriós que afecta el seu benestar emocional i mental.

Què és el ciberassetjament?

El ciberassetjament passa quan una persona utilitza tecnologies digitals per assetjar, insultar o amenaçar-ne una altra, generalment de manera repetida. Podeu adoptar diverses formes, entre les quals s'inclouen:

- **Missatges abusius o intimidants:** Enviament de correus electrònics, missatges de text, xats o publicacions a xarxes socials amb insults, amenaces o comentaris cruels.

- **Exclusió social en línia:** Deixar algú fora d'un grup en línia, bloquejar-lo a xarxes socials o fer-li "shaming" en exposar informació privada sense el seu consentiment.
- **Difusió de rumors o mentides:** Publicació de rumors falsos, fotos o vídeos manipulats per fer malbé la reputació d'algú.
- **Imatges o vídeos humiliants:** Compartir contingut visual que ridiculitzi o avergonyeixi la persona, com fotos privades o vídeos gravats sense consentiment.
- **Suplantació d'identitat:** Crear perfils falsos a les xarxes socials per suplantar la identitat de la víctima i publicar contingut perjudicial en nom seu.

Conseqüències del ciberassetjament

L'impacte del ciberassetjament pot ser profund i afectar-lo a nivell emocional, social i físic. Entre les conseqüències més comunes es troben:

- **Aïllament social:** Les víctimes solen sentir-se excloses i soles, ja que l'assetjament en línia pot portar a l'aïllament tant al món digital com al real.
- **Problemes emocionals i psicològics:** El ciberassetjament pot causar ansietat, depressió, baixa autoestima i fins i tot pensaments suïcides. Les víctimes sovint s'enten que no poden escapar de l'assetjament, ja que les xarxes socials hi són sempre presents.
- **Baix rendiment acadèmic:** L'estrès i la preocupació causats pel ciberassetjament poden afectar el rendiment escolar dels adolescents, ja que no se senten segurs ni còmodes als seus entorns educatius.
- **Problemes físics:** L'angoixa emocional provocada per l'assetjament pot manifestar-se en símptomes físics, com ara mals de cap, insomni i altres trastorns de salut relacionats amb l'estrès.

Senyals que un adolescent pot estar sent víctima de ciberassetjament

És important que els pares sàpiguen identificar els senyals que el seu fill o filla podria estar sent assetjat en línia. Alguns dels senyals comuns inclouen:

- **Canvis en el comportament:** Si el teu fill es torna més reservat, irritable o ansiós sense raó aparent.
- **Canvis en l'ús de la tecnologia:** Si comença a evitar l'ús de certes xarxes socials, aplicacions o plataformes, o si es mostra preocupat/da per deixar el dispositiu a la vista.
- **Pors inexplicables o símptomes físics:** L'adolescent podria queixar-se de mals d'estómac, mals de cap, insomni o sentir-se més cansat del normal.
- **Depressió o pèrdua de confiança:** L'adolescent mostra signes de depressió, inseguretat o angoixa emocional.

Què poden fer els pares per prevenir el ciberassetjament?

Com a pares, és fonamental que juguin un paper actiu en la prevenció del ciberassetjament. Aquí et dono algunes recomanacions per ajudar el teu fill a navegar de manera segura al món digital:

- **Mantenir una comunicació oberta i honesta:**
 - Parleu amb el vostre fill sobre l'ús segur de les tecnologies. Pregunta-li com se sent en línia, si ha tingut problemes amb altres persones o si ha notat alguna cosa estranya.
 - Assegura't que el teu fill sàpiga que pot comptar amb tu si mai se sent assetjat o pressionat per altres.
- **Establir regles clares sobre l'ús de la tecnologia:**
 - Estableix normes clares sobre quines plataformes pot fer servir el teu fill, com comportar-se en línia i com protegir la seva privadesa.
 - Assegureu-vos que el vostre fill/a sàpiga com configurar la privadesa dels vostres comptes per evitar que persones no desitjades vegin la vostra informació.
- **Monitoritzar l'ús d'Internet:**
 - Encara que és important respectar la privadesa del teu fill, pots fer servir eines de monitorització que t'ajudin a supervisar les seves activitats en línia sense envair el seu espai personal.
 - Hi ha aplicacions de control parental que permeten establir límits de temps, bloquejar contingut inapropiat i monitoritzar les interaccions en línia.
- **Fomentar el respecte i l'empatia en línia:**
 - Ensenya'ls a ser respectuosos i empàtics amb els altres en línia, ja reflexionar sobre com les seves paraules o accions poden afectar els altres.
 - Ajuda'ls a comprendre que el que es diu en línia pot tenir un impacte real a la vida de les persones.
- **Reaccionar de manera adequada si passa un ciberassetjament:**
 - Si sospites que el teu fill està sent assetjat en línia, actua ràpidament. El primer és assegurar-te que se senti recolzat i comprès.
 - Pren captures de pantalla o guarda evidència dels missatges o continguts nocius.
 - Anima el teu fill a no respondre als missatges dels assetjadors, ja que això pot empitjorar la situació.
 - Si cal, contacta amb les plataformes en línia per denunciar l'assetjament o fins i tot amb les autoritats si la situació ho requereix.

- **Reforçar la importància de la privadesa:**

- Explica-li la importància de no compartir informació personal com adreces, números de telèfon, fotos íntimes o contrasenyes amb persones que no coneix bé.
- Assegureu-vos que el vostre fill/a tingui configurades les opcions de privadesa en xarxes socials i altres plataformes per limitar qui pot veure les seves publicacions.

Què fer si un fill és víctima de ciberassetjament?

Si descobreixes que el teu fill és víctima de ciberassetjament, aquí tens alguns passos a seguir:

- **Escoltar i recolzar:** El primer és oferir-li suport emocional. Escolta les preocupacions sense jutjar ni minimitzar la situació.
- **Denunciar l'assetjament:** Assegureu-vos que l'assetjament es reporti adequadament a les plataformes de xarxes socials o aplicacions on va passar. La majoria tenen opcions per denunciar contingut abusiu o assetjador.
- **Considerar la intervenció escolar:** Si l'assetjament té lloc dins l'àmbit escolar, és important involucrar l'escola perquè prenguin les mesures adequades.
- **Buscar ajuda professional:** Si el ciberassetjament està afectant greument la salut emocional del teu fill, podria ser útil cercar l'ajuda d'un terapeuta o conseller especialitzat.

Conclusió

El ciberassetjament és un problema seriós que afecta molts adolescents avui dia, però amb una comunicació oberta, educació sobre l'ús segur de la tecnologia i eines de monitoratge, els pares poden ajudar a protegir els seus fills. És important ensenyar-los a ser conscients dels riscos en línia i actuar de manera responsable i respectuosa al món digital.



Establir Normes i Límits

A l'era digital, l'ús d'internet forma part de la vida quotidiana dels nens i adolescents. Tot i els beneficis que ofereix, també és important establir unes pautes clares per garantir-ne un ús segur i equilibrat. Definir normes adequades ajuda a fomentar la responsabilitat i a protegir els menors dels possibles riscos en línia.

A continuació, es presenten tres aspectes clau a tenir en compte per gestionar l'ús d'internet a casa de manera efectiva:

- **Regles clares:** Definiu quant de temps poden passar en línia i quin tipus de contingut és acceptable.
- **Conseqüències:** Establiu què passarà si les regles no es compleixen.
- **Flexibilitat:** Adapteu les normes segons la maduresa i les circumstàncies del vostre fill.



Promoure un bon ús d'Internet

L'ús d'internet pot ser una eina poderosa per a l'aprenentatge i el desenvolupament personal si es gestiona de manera adequada. A més de fixar normes i límits, és fonamental promoure un ús conscient i enriquidor de les tecnologies digitals. Els pares i educadors poden jugar un paper clau en aquest procés, ajudant els nens i adolescents a aprofitar els beneficis d'internet mentre mantenen un equilibri saludable amb la seva vida quotidiana.

Per aconseguir-ho, cal tenir en compte tres aspectes essencials:

- **Activitats constructives:** Fomenteu l'ús d'internet per a projectes educatius i col·laboratius.
- **Balanç digital:** Animeu els vostres fills a equilibrar el temps en línia amb activitats a l'aire lliure.
- **Reflexió crítica:** Ensenyeu als vostres fills a analitzar la informació que troben en línia.



Estar al cas de les noves tendències

Comprendre les plataformes i tendències actuals permet establir millor les pautes d'ús i acompanyar els infants i adolescents en el seu entorn digital.

Per aconseguir-ho, és important tenir en compte dues estratègies clau:

- **Investigació contínua:** Dediqueu temps a investigar noves plataformes i tendències.
- **Participació activa:** Considereu unir-se a les xarxes que utilitzen els vostres fills per comprendre millor el seu entorn.



GUIA PER A PARES SOBRE SEGURETAT EN DISPOSITIUS



Ús d'Eines de Control Parental

Aplicacions de control: si no és Chrom Books, no disposem de la Family Link, l'opció que es fa servir als instituts on tenen Chrome Books.

Hi ha aplicacions gratuïtes com Microsoft Family Safety que intenten cobrir les mateixes funcionalitats, però limiten la seva gestió a les eines de microsoft i no cobreixen Chrome, Firefox o altres navegadors.

No obstant això, si el router d'accés a internet de què es disposa sí que ho permet, hi ha opcions com OpenDNS que permeten, canviant la configuració de DNS del router, evitar l'accés a llocs no aptes. Hi ha l'opció de fer això també en les configuracions del portàtil però no és possible en el nostre cas per no ser administradors d'aquest. Per explorar aquesta opció adjuntem informació addicional a Publicació Seguretat

Configuracions de privadesa: Ajudeu els vostres fills a establir opcions de privadesa als vostres comptes de xarxes socials.

Importància de la privadesa: Expliqueu als vostres fills per què és fonamental protegir la vostra informació personal.

Regles clares: Definiu quant de temps poden passar en línia i quin tipus de contingut és acceptable.



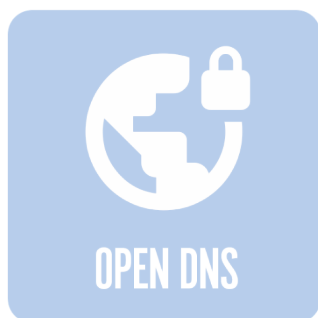
Fomentar la comunicació oberta

Acompanyar els infants i adolescents en el seu ús d'internet no es limita a establir normes i límits; també implica mantenir una comunicació oberta i fomentar una relació de confiança. Quan els joves se senten escoltats i compresos, són més propensos a compartir les seves experiències en línia i a demanar ajuda quan ho necessiten.

Per aconseguir-ho, cal tenir en compte tres aspectes fonamentals:

- **Converses regulars:** Mantenir un diàleg constant sobre el que fan en línia, els seus interessos i les seves amistats digitals.
- **Escoltar activament:** Mostrar interès genuí per les seves experiències, donant-los espai per expressar-se sense por a ser jutjats.
- **Modelar el comportament:** Ser un exemple positiu en l'ús de la tecnologia, demostrant hàbits digitals saludables i responsables.

Amb una comunicació basada en la confiança i el respecte, es pot ajudar els més joves a navegar pel món digital de manera segura i equilibrada.



Configuració d'Open DNS (control d'accés al router)

OpenDNS és un servei de DNS (Domain Name System) que et permet personalitzar i millorar la navegació dels teus dispositius, proporcionant característiques com a **filtratge de contingut, seguretat millorada i rendiment optimitzat**. A continuació us ofereixo una petita guia de configuració d'OpenDNS per utilitzar-lo com a **control parental** o per millorar la seguretat en una xarxa.

Passos per configurar OpenDNS

Crear un compte a OpenDNS

Primer, necessites crear un compte a OpenDNS per poder gestionar les configuracions.

- Aneu a <https://www.opendns.com> i seleccioneu Sign Up.
- Registra't amb el teu correu electrònic i crea una contrasenya pel teu compte.

Configuració d'OpenDNS al teu router o dispositiu

Perquè el filtratge de contingut i les configuracions de seguretat d'OpenDNS s'apliquin a tota la teva xarxa, has de canviar els servidors DNS a l'encaminador oa cada dispositiu individualment. Com hem comentat anteriorment, en no ser administradors del dispositiu, només tenim l'opció de configurar al router si aquest ho permet.

1. Accedeix a la configuració del teu router:

- Obre un navegador i entra a l'adreça IP del teu router (generalment és **192.168.1.1** o **192.168.0.1**).
- Introduïu el nom d'usuari i la contrasenya del router (si no els heu canviat, la configuració predeterminada hauria d'estar al manual del router o en una etiqueta al dispositiu).
-

2. Troba les opcions de DNS:

- Un cop dins de la configuració del router, cerca la secció que esmenta DNS (pot estar sota "Network", "Internet", "LAN Settings", etc.).

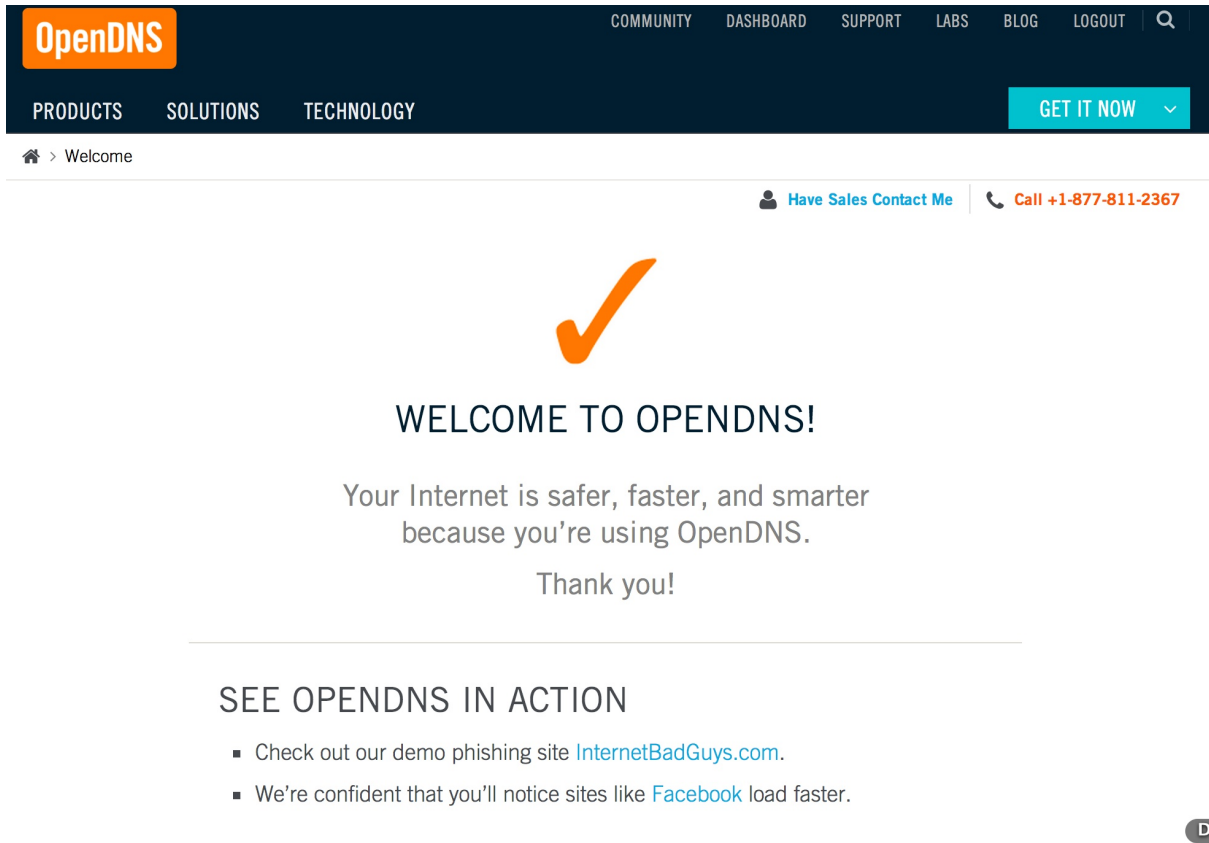
3. Configura els servidors DNS d'OpenDNS:

- Canvia els valors de DNS primari i secundari pels servidors d'OpenDNS següents:
 - DNS primari: 208.67.222.222

- DNS secundari: 208.67.220.220

4. Desa la configuració i reinicia el teu router.

Amb això, tot el trànsit de la vostra xarxa domèstica passarà a través dels servidors DNS d'OpenDNS, la qual cosa habilitarà el filtratge de contingut i les configuracions de seguretat.



The screenshot shows the OpenDNS website interface. At the top, there is a dark blue navigation bar with the OpenDNS logo on the left and links for COMMUNITY, DASHBOARD, SUPPORT, LABS, BLOG, LOGOUT, and a search icon on the right. Below this, a secondary navigation bar contains links for PRODUCTS, SOLUTIONS, TECHNOLOGY, and a prominent orange 'GET IT NOW' button. A breadcrumb trail below the navigation bar reads 'Home > Welcome'. On the right side of the page, there are two links: 'Have Sales Contact Me' with a person icon and 'Call +1-877-811-2367' with a phone icon. The main content area features a large orange checkmark, followed by the text 'WELCOME TO OPENDNS!', 'Your Internet is safer, faster, and smarter because you're using OpenDNS.', and 'Thank you!'. Below this, a section titled 'SEE OPENDNS IN ACTION' lists two bullet points: 'Check out our demo phishing site [InternetBadGuys.com](#).' and 'We're confident that you'll notice sites like [Facebook](#) load faster.'. A small 'D' icon is visible in the bottom right corner of the screenshot.

Recursos addicionals

1. Internet Segura for Kids (IS4K)

<https://www.incibe.es/menores/>

Iniciativa l'Institut Nacional de Ciberseguretat (INCIBE) que ofereix recursos educatius, consells i eines per ajudar els nens i els adolescents a navegar de manera segura a internet.

<https://www.youtube.com/watch?v=iW3oA4xOQ9E>

2. Fundació ANAR

<https://www.anar.org/>

Ofereix recursos sobre ciberassetjament i seguretat en línia, a més d'un servei d'orientació i suport per a nens i adolescents.

3. Agència de Seguretat de catalunya

<https://ciberseguretat.gencat.cat/ca/actualitat/mes-de-la-ciberseguretat/index.html>

Ofereix informació sobre els riscos d'Internet i també recursos per promoure un ús saludable de la tecnologia entre joves.

https://ciberseguretat.gencat.cat/web/.content/08_ciutadania/proteccio-menors/control-parental/tecnologiesDigitals_infanciaAdolescencia.pdf

4. Pantallas amigas

<https://www.pantallasamigas.net/>

5. Ciberseguretat per a tothom (Institut Nacional de Ciberseguretat)

<https://www.incibe.es/>

Ofereix recursos educatius i consells per a famílies sobre com gestionar la ciberseguretat a casa.

6. Consum i Seguretat (Organització de Consumidors i Usuaris - OCU)

<https://www.ocu.org/>

Proporciona consells sobre la seguretat en línia, així com recomanacions sobre aplicacions i eines de control parental.



CC BY-NC-SA 4.0

Reconeixement-NoComercial-CompartirIgual
4.0 Internacional

<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.ca>

