



Uso responsable e seguro das novas tecnoloxías

Guía para alumnado e familias



USO RESPONSABLE E SEGURO DAS NOVAS TECNOLOXÍAS

As novas tecnoloxías poden ser maravilosas, achégannos a nosa casa ou, con móbiles de última xeración, as nosas mans o coñecemento de calquera parte do mundo, permítenos viaxar sen saír da casa, falar cos que temos lonxe, compartir e desenvolver a nosa creatividade, facer esa receita de torta de chocolate ou arranxar esa persiana que se estragou. Pero se non se ten cabeza, poden ser moi perigosas. Podémonos meter nun lío moi gordo case sen darnos conta. Para evitalo: A nosa guía!

DE QUE TRATA ESTA GUÍA?

Esta guía ten como obxectivo facilitar o acceso a información sobre os **riscos** das novas **tecnoloxías** como as redes sociais, os teléfonos intelixentes, etc. facendo fincapé nos delitos ou riscos dos que poden ser vítimas, os delitos ou faltas que poden cometer por descoñecemento e a sensibilización sobre esta nova problemática.

A QUEN VAI DIRIXIDA ESTA GUÍA?

Esta guía vai dirixida principalmente o **alumnado** do noso centro e as súas **familias**, pero tamén pode ser útil para outros membros da comunidade con interese nesta materia.



Puntos a tratar

Delitos que os rapaces e rapazas corren o risco de cometer

Delitos relacionados coa difusión de imaxes e segredos

Delitos contra a propiedade intelectual e Plaxio

Apostas on line

Cyberbullying, cyberacoso

Difusión de información falsa

Sexting e Grooming

Oversharing, trashing, phishing

Stalking e Xeolocalización

Violencia de xénero e violencia sexual dixitais

Permisos no móvil

WIFI abertas e instrucción WIFI

Fraude online e Roubo de identidade

Fake News e filtros de burbulla

Radicalización online

Outras cuestións a ter en conta

Para ter en conta

Asociación as que podes acudir

Para atopar creacións libres de dereitos

Antivirus, cortalumes e seguridades

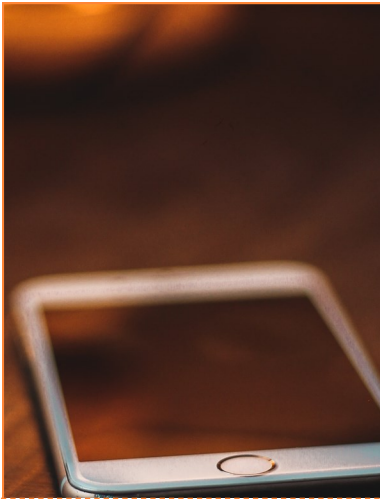
Contrasinais e seguridade

Cookies

Identidade dixital

Problemas sociais e a adicción a internet

Para máis información



DELITOS QUE OS RAPACES E RAPAZAS CORREREN O RISCO DE COMETER

Os principais delitos que os menores adoitan cometer a través de novas tecnoloxías son os relacionados co dereito a propia imaxe, o dereito a intimidade ou a propiedade intelectual.

E de grande importancia lembrar que o descoñecemento dunha lei non nos exime da obriga do seu cumprimento.

+

ASOCIACIÓN ÁS QUE PODES ACUDIR SE TE

3.3S DÚBIDAS

Moitas asociacións e organismos públicos teñen programas de apoio as vítimas de delitos na rede.

Ante calquera delito unha das túas opcións e acudir a Policía Nacional o a Guarda Civil.

Tamén podes atopar información ao respecto en [“INCIBE Instituto Nacional de Ciberseguridad”](#) ou en [“Internet Segura for Kids \(IS4K\)”](#)

DELITOS RELACIONADOS COA DIFUSIÓN DE IMAXES E SEGREDOS

A divulgación de imaxes dunha persoa na Internet sen o seu consentimento pode ser constitutiva de delito. Subir a Imstagram ou a Facebook imaxes dos nosos amigos ou coñecidos sen o seu permiso, supón un delito. Se ademais esas imaxes son especialmente privadas ou vergoñentas, pode verse agravado o dano e polo tanto a responsabilidade. Do mesmo modo, facer públicos os segredos ou datos íntimos dos nosos coñecidos ou amigos tamén está nesta categoría. No Título X, Capítulo I, artigos del 197 ao 201 del Código Penal di que a difusión de imaxes sen consentimento da vítima, e a difusión de segredos vulnera o seu dereito a intimidade e pode supor condenas de entre 1 e 7 anos de cárcere ademais de multas de 12 a 24 meses.

Se nas imaxes aparecen rapaces ou rapazas menores de idade espidos ou con contido sexual, pódese estar incorrendo nun delito de difusión de pornografía infantil. Con este delito as penas de cárcere poden aumentar considerablemente, ademais de supor una inhabilitación para calquera traballo onde se teña contacto con menores de idade, como ser profesor ou adestrador de fútbol. ([ver Sexting](#))



DELITOS RELACIONADOS COA PROPIEDAD

Moitas das creacións artísticas (imáxenes, videos, textos e música), científicas ou programas informáticos que atopamos na Internet están protexidos polas regulacións de dereitos de autor. Estas leis están deseñadas para asegurar os dereitos do creador sobre a súa obra. Divídense en dous dereitos; morais e patrimoniais. Se o autor reservase todos os dereitos sobre unha produción, esta protección esténdese durante toda a vida do creador máis os 70 anos posteriores a súa morte. De todas as maneiras, non nos temos que resignar a non atopar na Internet material que si poidaos usar, algúns autores poñen o seu traballo a disposición dos internautas con diversas reservas de dereitos, dende a libre difusión, uso e modificación da súa obra con códigos de recoñecemento da autoría como “Creative Commons” ou “Copyleft” ata outros que soamente permiten a difusión acreditada o uso acreditado sen modificación ou o uso para fins non comerciais. A propiedade intelectual queda recollida e protexida pola Lei de Propiedade Intelectual [BOE 22-04-1996] e o seu incumprimento pode derivar en multas ou en penas de cárcere.

FERRAMENTAS PARA ATOPAR CREACIÓNS LIBRES DE DEREITOS

Se necesitas imaxes, música ou outros contidos creativos de terceiros para un proxecto de clase, non podes usar o que che dea a gana. Tes que respetar os dereitos de autor ou incorrerías nun delito contra a propiedade intelectual.

Eso non quere dicir que non podas usar ningún material. Na rede atoparás páxinas web especializadas na distribución de contidos libres de dereitos ou con licencias que permiten a súa reutilización. Algunhas están especializadas en música, outras en imaxes. Do mesmo xeito, podes atopar programas de outras ferramentas do que se chama Software Libre e Software de Código Aberto.

Usando estes recursos poderás atopar aquilo que precisas sen te arriscar a cometer unha ilegalidade. Podes estar seguro, legal e de maneira gratuita.

ANTIVIRUS, CORTALUMES E SEGURIDADES

Ter os nosos dispositivos protexidos de ameazas mediante antivirus e cortalumes podenos aforrar moitos disgustos. Aínda así os sistemas de protección non son 100% fiables porque cada día aparecen ameazas novas na Internet.

A meirande parte dos virus entran nos nosos dispositivos a través dunha serie de vías. Por un lado, as páxinas web que teñen contidos de descargas ilegais ou pornográficas moitas veces son unha vía de acceso o noso ordenador. Os correos electrónicos procedentes de remitentes descoñecidos tamén poden ser sospeitosos. Non e aconsellable descargar arquivos adxuntos de emails descoñecidos ou facilitar vía email datos de especial perigo como números de conta ou contrasinais.

Se o noso banco, plataforma de pago, etc. quere contactar con nos adoitará a mandarnos un correo onde nos pide que entremos na súa páxina web e ademais incluírá información que non e visible a outros usuarios. Se o correo electrónico intenta redirixirnos directamente mediante un enlace debemos de sospeitar que poiderá ser una páxina ilícita que copio á orixinal para cometer Phishing.

PLAXIO

Ademais dun delito contra a propiedade intelectual por descargar ou compartir producións creativas alleas sen consentemento do autor, outro delito referido a [propiedade intelectual](#) é o de plaxio. Un plaxio é o uso da obra de outro autor facéndoa pasar como propia, aínda que este autor teña dado permiso para a súa reutilización.

APOSTAS ON LINE

Os xogos de azar son posible causa de un problema de ludopatía (adicción o xogo) polo tanto, o igual que os casinos físicos, os casinos en liña e as apostas online están prohibidas a todos os menores de idades. Pese a esta prohibición, cada vez máis rapaces/as fanse adictos as apostas ou o poker en liña.

CYBERBULLYING E CYBERACOSO

O cyberbullying e o cyberacoso son tecnicamente dos cousas distintas, as dúas supoñen un tipo de acoso a través de medios telemáticos, como as redes sociais ou os programas de mensaxería instantánea, a diferenza está nas características do abusador. No caso do cyberacoso o acosador é unha persoa adulta e, no do cyberbullying, o acosador é un menor. Se desta forma de violencia resultara un suicidio da vítima, o código penal prevé no artigo 143 penas de cadea de 4 a 8 anos por inducción o suicidio.

As consecuencias de ser vítima deste acoso cibernético poden ser de diversa índole, poden ir dende a perda de autoestima ata o Síndrome de Estrés Postraumático pasando por cambios na personalidade, insomnio, delirios ou medo xeneralizado entre outros.

DIFUSIÓN DE INFORMACIÓN FALSA

Publicar información falsa na Internet que xera alarma social como, por exemplo, dicir que hai una bomba nunha estación de tren cando non e verdade, pode supor un delito contra a orde pública segundo o artigo 561 del Código Penal e pode implicar de 6 a 12 meses de cárcere.

As consecuencias das diversas formas de violencia en liña poden ser devastadoras para a vítima e o seu entorno, pero tamén para o acosador/a e o entorno deste/a

SEXTING

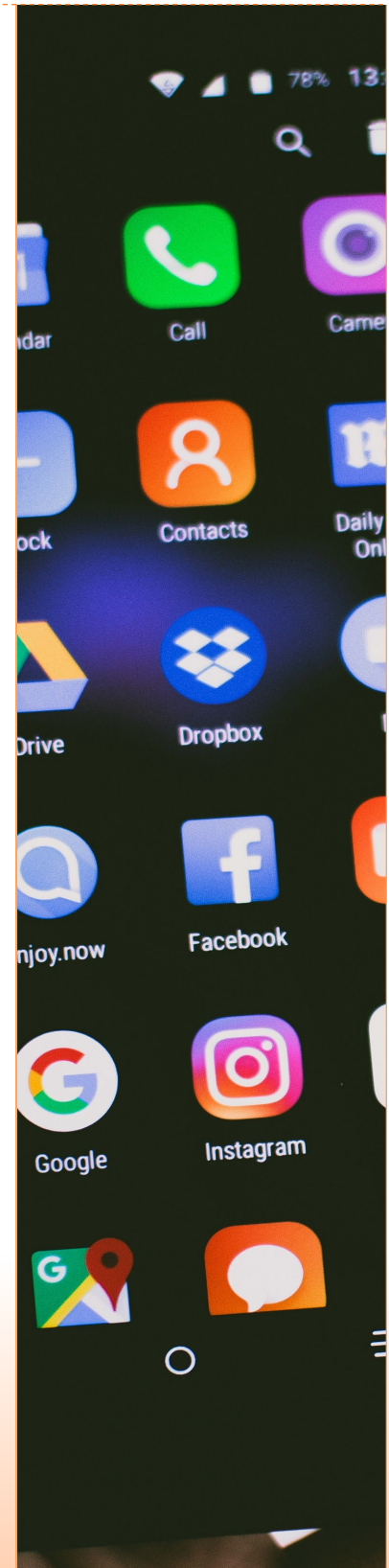
O sexting é unha práctica cada vez máis común entre os mozos e mozas, consiste principalmente en enviar fotografías de contido sexual a través das novas tecnoloxías. Moitas veces estes contenidos son despois compartidos pola outra parte sen consentimento do ou da fotografiado/a. Se a vítima é maior de idade, as penas van dende 3 meses a 1 ano, que poderíanse ampliar ata 5 anos se as fotografías se fixesen sen consentimento da vítima. Se o ou a fotografiado/a fose menor poderíase incorrer nun delito de difusión de pornografía infantil con penas de ata 12 anos.

Ainda que a fotografía moitas veces é feita pola vítima ou co seu consentimento, os máis novos poucas veces reparan nas consecuencias que pode ter a difusión deste material. Tenden a confiar que as persoas coas que comparten orixinalmente a imaxe (normalmente os seus intereses románticos)

non as van a difundir pero isto non sempre é así. A difusión a modo de vinganza e control pode ser parte dunha forma de violencia de xénero.

O sexting ten dúas modalidades principais; activo, que é o feito de enviar contido sexual a outra persoa, ou pasivo, que consiste en recibir imaxes, videos e outros materias de contido sexual. Cabe destacar que se cremos ou sabemos que as imaxes son dun o dunha menor, débense eliminar porque supoñen un delito de posesión de pornografía infantil. Nas mans dun groomer poden ser usadas para practicas child grooming (ver grooming)

Como no caso do acoso telemático, as consecuencias psicolóxicas do sexting poden ser devastadoras para a persoa afectada e o seu entorno, podendo dificultar as relacións sociais e de parella, xerar Estrés Posttraumático, perda da autoestima...



CONTRASINAIS E SEGURIDADE

Os contrasinais son o método que temos de demostrar que somos nos na rede, polo tanto conservar a privacidade dos nosos contrasinais é importante.

Para que un contrasinal sexa seguro convén que inclúa letras maiúsculas e minúsculas, números e signos coma o interrogante (?) ou ampersand (&).

Por seguridade é bo cambiar as contrasinais con certa asiduidade e non usar o mesmo contrasinal para sitios web con medidas de seguridade media como unha tenda online ou para sitios máis comprometidos como a banca en liña.

Outro feito a ter en conta é que, si temos a necesidade de tomar nota do contrasinal ata que o sepamos de memoria, non debe estar anotado no móbil ou noutro lugar onde nolo poidan roubar ou ver outras persoas.

Nunca debemos facilitar o noso contrasinal a través dun correo electrónico. Se a empresa necesita que cambiemos o noso despois de ter un fallo de seguridade, pedirannos que vaíamos a súa páxina para cámbialo.

GROOMING

O grooming é unha forma de acoso dun adulto a un menor con intención de índole claramente sexual. Un adulto interactúa cun menor a través dun chat, mensaxería instantánea ou rede social e conversa co rapaz ou rapaza facéndose pasar por outro menor. Usa unha linguaxe e fala duns temas que fan pensar que é outro rapaz/a. Mediante estas conversas vai obtendo a confianza do menor así como material que lle serve

para extorsionar a vítima, (como información que o menor non quere que se faga pública, fotografías, etc.) unha vez dispón de material dabondo, extorsiona o menor pedíndolle imaxes, vídeos ou outras esixencias de contido sexual. Se por medo o menor non busca axuda adulta, o groomer irá aumentando as súas esixencias ata intentar, nalguns casos, ter encontros sexuais físicos ca vítima e consumir un abuso ou violación.

OVERSHARING, TRASHING E PHISHING

O termo de Oversharing fai referencia o exceso de información de carácter privado que moitas veces se publica nas redes sociais ou na Internet que, no caso dos menores é moi habitual, pode facilitar outras actividades criminais como o grooming ou o [roubo de identidade](#). O trashing e o phishing fan referencia a obtención ilícita desa información persoal mediante manipulación, no primeiro caso dos dispositivos vellos co disco duro ser borrar, no segundo mediante software ou xaqueos informáticos. Deste xeito os cyberdelinquentes poden acadar contrasinais, números de conta bancaria ou outra información a que sacarlle rédito económico.

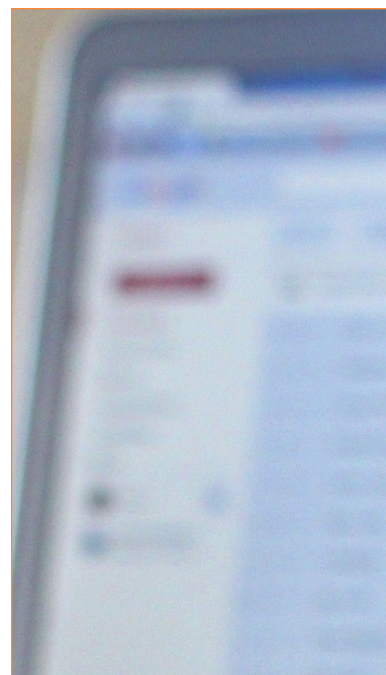
STALKING

É a vixilancia e acoso extremo a unha vítima contactando ou intentando contactar con ela por medios dixitais. Xenera unha sensación constante de acechamento e ansiedade na vítima que se sabe constantemente vixilada. Para este delito recollido no artigo 172 do código penal, se prevé condeas de 3 meses a 2 anos. Moitas veces este delito dase xunto cun delito de violencia de xénero dixital.

XEOLOCALIZACIÓN

Esta funcionalidade do móbil pode salvarnos a vida, pero tamén supor un gran risco. Permite saber cal é a ubicación do dispositivo en calquera momento e, polo tanto, do seu dono/a. Se nos rompemos unha perna no bosque pode ser de utilidade pero, cando quen controla a nosa posición é un acosador, secuestrador, etc. permítelle saber como acceder a nos en calquera momento.

Moitas Apps solicitan a xeolocalización cando para as súas funcionalidades non lles fai falta. Polo tanto convén ser coidadosos o darlles acceso a aplicación a xeolocalización. Para controlar o acceso das Apps a función do dispositivo e importante coñecer os permisos ([ver permisos](#))



Conven ser moi prudente a hora de facilitar información persoal nas RRSS ou noutros foros en liña.

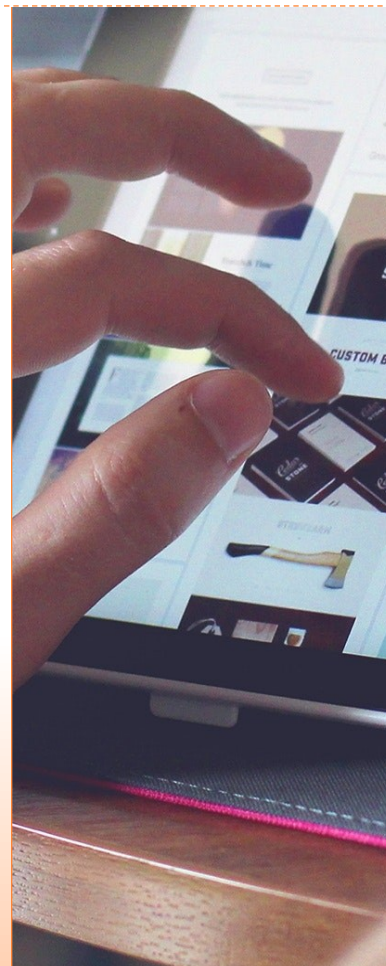
VIOLENCIA DE XÉNERO DIXITAL E

VIOLENCIA SEXUAL DIXITAL

Os delitos de violencia de xénero dixitais poden comprender moitos outros delitos nas redes. As vítimas de violencia de xénero nas redes poden sufrir cyberacoso, con insultos, rumores falsos, etc., tamén poden ser vítimas de distribución de imáxenes de sexting sen consentimento, coñecido popularmente como “Revenge porn” ou pornovenganza, do mesmo xeito poden sufrir stalking ou control das súas parellas ou exparellas por medio da

xeolocalización.

Como en toda forma de violencia de xénero preséntase normalmente actitudes machistas e sexistas, de control ou menoscabo da autoestima de vítima. Pero neste caso o vitimario aproveita a sensación de impunidade que lle dan as redes sociais para cometer o abuso. A “sextorsión” tamén é unha forma de violencia de xénero e sexual na rede.





PERMISOS NO MÓBIL

Os smartphones de hoxe en día permítenos controlar o acceso das aplicacións as funcionalidades do dispositivo. Co cal, aínda que o descargar a App aceptásemos que accedera as funcións de cámara, micrófono, contactos..., se por motivos de seguridade queremos cambiar estes permisos o noso teléfono permítenos ir a Axustes e premendo en permisos. Dende aquí podemos ver que aplica-

cións están accedendo a que función do dispositivo e denegarlle o permiso se o consideramos oportuno, como por exemplo, que unha aplicación dunha tenda en liña acceda a nosa cámara e poida facer fotografías cando ningunha das funcións de dita aplicación require de facer fotos, ou que un videoxogo de preguntas nos [xeoposicione](#) sen necesidade.

É fundamental ler os permisos que aceptamos cando descargamos unha App para saber que información van a recoller e en que condicións.

COOKIES

As cookies son pequenos anacos de información que recopila o noso navegador web, se lle damos permiso para facelo, e que serven para que as páxinas nas que estivemos navegando poidan ver a nosa actividade.

As cookies serven para que a web recoñeza ao usuario e poida gardar información sobre el para próximas visitas, personalizar a navegación e para facer un uso publicitario da información recopilada.

ROUBO DE IDENTIDADE E FRAUDE ONLINE

O roubo de identidade é un delito recoñecido no Código Penal con penas de cadea de 6 meses a 3 anos. Se non queremos ser vítima deste delito convén que sexamos coidadosos cos datos que facemos públicos na Internet.

Sen darnos conta, moitas veces publicamos nas redes sociais datos de carácter privado coma o noso nome completo, a nosa data de nacemento, fotografías xeolocalizadas da nosa casa, imaxes de documentos nos que aparece o noso número de DNI ou da Seguridade Social.

O uso de redes WIFI abertas tamén pode provocar que, mediante o [Phishing](#), consigan os nosos datos.

Tamén debemos asegurarnos de que non queden datos de carácter privado nos dispositivos que retiramos do uso.

Os nosos datos pódense usar para practicar fraudes, sustraer cartos das nosas contas bancarias ou [cyberacosar](#) a alguén deixando o “noso rastro” de datos e facendo que parezamos culpables dos delitos cometidos.

Otros fraudes na rede poden ser os de compras en liña que nunca recibes, especialmente se a páxina web non ten ningún dos selo de confianza o certificado dixital das tendas en liña, non nos dan opcións de pago e só admiten a tarxeta de crédito. Usar unha plataforma de pago segura ou pagos contra-reembolso poden resultar máis fiable a hora de facer un pago dunha tenda online.

Tamén poden ser falsas ofertas de emprego onde se lle reclaman cartos o futuro empregado ou no aluguer de vivendas. Se piden que adelantemos cartos, compremos o material, demos datos a través de vías non convencionais ou non atopamos máis información sobre a empresa que a da propia páxina web, debemos sospeitar.

OS RISCOS DAS REDES WIFI ABERTAS E AS INTRUSIÓNS NA REDE WIFI

Cando usamos una rede WIFI aberta ou gratuita debemos ser moi coidadosos porque é moito máis sinxelo para un delincuente poder entrar no noso dispositivo. Sempre será máis seguro usar a nosa tarifa de datos. Se nos decidimos a usar unha rede aberta non debemos enviar dende esa conexión datos espacialmente sensibles como inciar sesión con contrasinal, dar datos persoais ou usar a banca en liña.

Tamén debemos protexer a nosa rede WIFI da casa de posibles intrusións mediante distintas medida de seguridade. Como facer a nosa red invisible para os dispositivos que busquen redes e que soamente se poida atopar sabendo o nome exacto da rede. Outra opción é engadindo as direccións MAC dos dispositivos da familia para que só lle permita acceder a estes. As autoridades adoitan poñer a disposición dos usuarios [manuais](#) sobre como realizar estas tarefas.

IDENTIDADE DIXITAL

A identidade dixital é a imaxe que damos de nos a través das redes sociais ou outros medios cibernéticos.

Como eliminar información que está na rede é casi imposible, convén non subir a esta aquilo que non desexemos que se faga público ou que non da a imaxe de nós que queremos mostrar.

Isto é cada vez máis importante porque moitas universidades privadas, fundacións que dan becas ou empresas en procesos de selección de novo persoal ou do persoal que xa teñen en plantilla, etc. revisan as redes sociais dos seus alumnos, empregados ou candidatos como maneira de coñecelos mellor e toman decisións en función do que alí atopan.

As cousas que agora parecen divertidas, sen importancia ou normais, quizais dentro de 5 ou 10 anos non queramos que sexan coñecidas por calquera e, se están nas redes, están accesibles para quen as busque incluso despois de que as teñamos borradas das nosas contas das redes sociais.

PROBLEMAS SOCIAIS E A ADICCIÓN A INTERNET

A adición os videoxogos xa está recoñecida pola Organización Mundial da Saude. E a preocupación pola adición as novas tecnoloxías e internet creceu enormemente nos últimos anos.

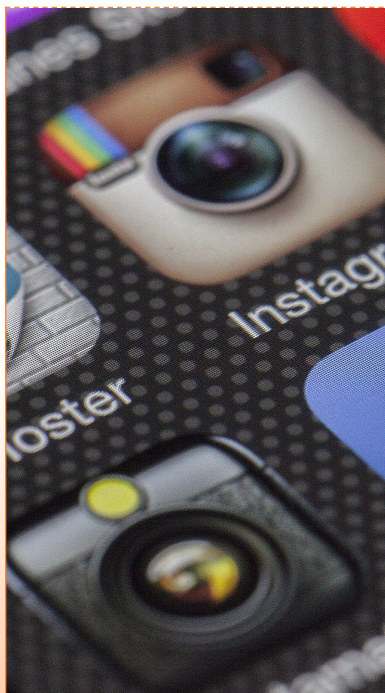
“Actualmente pódese definir a Adicción a Internet (AI) como a incapacidade do suxeito para limitar o uso desta ferramenta provocando un malestar significativo no individuo” (Kilic et al., 2016, citado por Jara et al. 2018)

FAKE NEWS E FILTROS DE BURBULLA

As Fake News ou noticias falsas son una lacra da sociedade actual. Unha sociedade que vive con acceso a información permanente pero na que as veces é difícil diferenciar o que é certo do que non. O impacto destas noticias falsas ou nas que se terxiversa a realidade é evidente en determinadas cuestións que xeran alarma social. Os bulos non só se repiten nas redes senon que a prensa tradicional moitas veces faise eco destas noticias falsas.

Ademáis, cada vez máis xente se informa das novas do día a través das redes sociais e os filtros de burbulla destas dificultannos ter unha versión global e obxectiva do mundo pois só nos ensinan as noticias que, segundo os seus algoritmos, son do noso interés. Non nos informan das cousas que consideren que non se corresponden cos nosos intereses co que é moi difícil facerse unha opinión propia ben informada dado que temos unha versión sesgada do que está a pasar.

"Se non reflexionamos de maneira crítica sobre o que lemos en liña nin acudimos a varias fontes de información, a nosa idea do mundo pode ser moi irreal."



RADICALIZACIÓN ONLINE

O uso de filtros de burbulla, a sensación de anonimato da rede e a globalización da información supoñen converter a Internet nun caldo de cultivo para a radicalización ideoloxica e, moitas veces violenta, dos usuarios. Estes grupos violentos captan os seus futuros membros a través das redes so-

ciais, foros, etc. e dándolle a súa propia visión do mundo, as veces moi afastada da realidade obxectiva, convencen os internautas das súas ideas extremas a través da propaganda e da interconexión con outros extremistas.



OUTRAS CUESTIÓNS A TER EN CONTA

Os perigos, riscos e novos feitos tipificados como delitos cambian moi rapidamente dado os esforzos que as autoridades nacionais e internacionais fan por intentar adaptarse os novos problemas e necesidades dos usuarios das tecnoloxías da información e a comunicación.

Convén intentar manterse informado sobre os cambios legislativos ou as ameazas que van surxindo polo progreso das tecnoloxías pero tamén dos avances encanto a ciberseguridade se refire. O uso responsable das TIC

pode achegar as nosas vida un mundo de coñecementos de gran valor, facilitando a aprendizaxe autónoma (self-learning) e permanente mediante o aprendizaxe electrónico (e-learning), aprendizaxe móbil (m-learning) e aprendizaxe combinado (b-learning).

Os cursos MOOC (cursos masivos en liña, en aberto), son cursos gratuitos a través da Internet que podennos facilitar o uso productivo das TIC , a aprendizaxe asequible dende a casa e a actualización de coñecementos de calquera disciplina.

PARA MÁIS INFORMACIÓN

Aquí aparecen unha serie de enlaces de interés:

[Instituto Nacional de Ciberseguridad](#)

[Oficina de Seguridad del Internauta](#)

[Internet Segura For Kids](#)

[Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado](#)

[Jamendo](#) (música libre de dereitos)

[Audionautix](#) (música libre de dereitos)

"As TIC abrenos as portas do coñecemento pero como toda aventura, ten os seus perigos e e mellor sabelo."



SOBRE ESTA GUÍA

As imaxes de esta guía proceden de Pexel unha fonte que permite o uso por parte de terceiros das súas imaxes sen ter que mencionar a autoría. De todas maneiras agradecemoslle aos seguintes autores o seu traballo desinteresado :

Imaxe de portada por rawpxel.com

Imaxe páxina 3 por Artem Bali.

Imaxe páxina 4 por Arun Thomas

Imaxe páxina 5 por Bruce Mars

Imaxe páxina 7 por Lisa Fotios

Imaxe páxina 9 por Pixabay

Imaxe páxina 10 por Burst

Imaxe páxina 12 por Pixabay

Imaxe páxina 13 por Bruce Mars

Imaxe páxina 14 por Junior Teixeira

Imaxe páxina 15 por Mohi Syed



BIBLIOGRAFÍA E WEBGRAFÍA

de España, C. G. (1995). Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Madrid: BOE del 24 de noviembre de 1995* . Recuperado de:

<https://www.boe.es/eli/es/lo/1995/11/23/10/con>

Internet segura for kids, IS4K. (2019). *Necesitas saber*. Recuperado de:

<https://www.is4k.es/necesitas-saber>

Jara, C. R., Vargas, F. H., Sanhueza, F., Núñez, P., Inostroza, E., López, J. A. S., & Contreras, D. (2018). Adicción a Internet y uso de redes sociales en adolescentes: una revisión. *Revista española de drogodependencias*, (43), 39-54. Recuperado de: <https://www.aesed.com/upload/files/v43n4-2-rrss.pdf>

Lebrero Baena, M. P., & Quicios García, M. D. P. (2011). *Pedagogía de la socialización*. Editorial UNED. Madrid

Oficina de Seguridad del Internauta, OSI. (2019). *Protégete*. Recuperado de:

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