Definición e explicación dos termos empregados na linguaxe de Internet e das Redes Sociais (RRSS)



PENSA

Conectarse a Internet é unha acción que realizamos case a diario. Internet é en realidade un conxunto descentralizado de redes de comunicación interconectadas, que funciona como unha rede única de alcance mundial.

As posibilidades que ofrece para acceder a información, para o entretemento, a comunicación e mesmo a compra de calquera produto son importantes, pero tamén encerra dificultades e desvantaxes. Por iso é necesario que coñezamos que vantaxes nos ofrece este sistema de comunicación, como utilizalas e como evitar os posibles perigos.

SABÍAS QUE...

Se Internet fose un país, sería o sexto máis contaminante do mundo. A pegada ecolóxica deste inmenso tráfico dixital equivale a un consumo aproximado do 7 % da electricidade mundial. Sé responsable co uso que fas, non abuses polo ben do planeta e mais polo ben da túa saúde física e mental.

Existen moitos servizos e protocolos na internet, á parte da web: o envío de correo electrónico, a transmisión e consulta de arquivos, as conversacións en liña, a mensaxería instantánea, a comunicación multimedia ou os xogos en liña.

ACCESO E CONEXIÓNS:

Son varios os criterios para clasificar as conexións a Internet, polo menos tantos como tipos de redes ás que podemos conectar o noso equipo. Ditas diferenzas poden atoparse no nivel físico e o tipo de tecnoloxía da que se serven.

a) **Líña telefónica**: Necesítase un módem, o cal converte os sinais dixitais do computador en impulsos de son que se transmiten pola liña telefónica. Este sistema de conexión caeu en desuso.

b) **Líña diXital**:

- **RDSI**: Trátase dunha liña telefónica, pero dixital (no canto de analóxica).
- **ADSL**: A ADSL (Asymmetric Dixital Subscriber Line) é unha tecnoloxía de acceso a Internet de banda ancha e é o tipo de conexión favorito en fogares e empresas.

c) **Cable**: Desde o punto de vista físico, a rede de fibra óptica precisa dunha infraestrutura nova e custosa, o que explica que aínda hoxe non estea dispoñible en todos os lugares.

d) **Satélite**: Este tipo de conexión segue sendo utilizada naqueles casos nos que non hai máis opcións, por exemplo en barcos, avións ou en zonas moi illadas onde non chega outro tipo de re



e) **Redes inalámbricas**: As redes inalámbricas ou Wireless difiren de todas as conexións anteriores, e a máis coñecida e utilizada é a WI- FI. WI-FI: É un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. As redes Wi- Fi posúen unha serie de vantaxes, entre as que destaca a comodidade. Pero, do mesmo xeito que a rede inalámbrica, a tecnoloxía Wi- Fi presenta os seus propios problemas intrínsecos. Algunhas destas desvantaxes son:

F**alta de seguridade**. Moitas destas redes convértense en redes abertas, sen protexer a información que por elas circulan.

Menor velocidade en comparación cunha conexión por cable, debido ás interferencias.

f) **Telefonía móbil**: A conexión a Internet, dentro da tecnoloxía móbil, utiliza distintos sistemas derivados do GSM (Global System Mobile).

INFORMACIÓN DE INTERESE

Para acceder a Internet temos que recorrer a provedores, é dicir, a compañías que crean unha conexión directa e permanente e ofrécennos a posibilidade de acceso contratando unha conta a cambio dun pago por este servizo. Convén, como en todos os contratos, ler atentamente as condicións.

En qué debemos fixarnos ao contratar unha conexión a Internet:

Cobertura do lugar da conexión: Ofertas hai moitas, pero é moi probable que, de non vivir en grandes cidades, non podamos acceder a todas elas.

Promocións e velocidade: o prezo final non adoita coincidir co anunciado, e moitas veces tampouco a velocidade, infórmate ben antes de o contratar. Non te fíes só da publicidade e contrata unicamente o que precises, non por ter posibilidade de contratar unha velocidade maior é obrigatorio contratala.

Pescuda se ten algunha cláusula de permanencia.

Servicio técnico: É recomendable que comprobes na medida do posible como funcionan os servizos de atención ao cliente.



Aspectos éticos, legales e de seguridade

Todos coñecemos as vantaxes da rede Internet, pero ao ser unha rede aberta e universal, está suxeita a distintos riscos relacionados co seu propio funcionamento e

co uso que dela facemos. Na internet debemos utilizar a lóxica e o sentido común, como o fariamos na vida real.

Do mesmo xeito que ocorre nas actividades que realizamos no mundo físico, todas as funcionalidades da internet poden comportar algún risco, entre os que podemos destacar:

- **Relacionados co seu funcionamento**: Problemas coaaccesibilidade, a conexión a determinadas webs ou servizos de Internet, virus, spams, etc.



- **Relacionados coa información**: Existe moita información pouco fiable xa que calquera pode subir contidos á rede.
- **Acceso a información inapropiada**: Información perigosa (violencia, inmoral ou ilícita) sobre todo para o colectivo menor de idade
- **Relacionados coa comunicación interpersoal**: Bloqueo do correo electrónico, mensaxes lixo e ofensivos, perda de intimidade persoal e de terceiros, accións ilegais como plaxios, difamacións, ameazas, etc.
- **Relacionados con actividades económicas**: Compras inducidas, publicidade, gasto telefónico desorbitado, estafas, roubos ou descargas ilegais.
- **Relacionadas coa propiedade industrial e intelectual**: pirateando unha marca ou os dereitos de autor, cando descargamos de maneira ilícita música, un xogo, un libro ou unha película.
- **Relacionados coas adiccións**: Existen riscos relacionados co abuso de determinadas prácticas como o xogo, compras compulsivas, adicción a contornas sociais como chats, videoxogos online...



INFORMACIÓNS DE INTERESE

O correo electrónico tamén pode causarnos moitosproblemas. Podemos vernos bombardeados por spam (publicidade non solicitada), ser enganados con falsas

cadeas de solidariedade ou diferentes métodos de estafa, así como recibir virus que afectan o noso computador. (Véxase ficha Correo electrónico)

QUE PODO FACER EU…?

- **Elixe un navegador segur**o: A maior parte das actividades que desenvolvemos por Internet céntranse no noso navegador. Deberemos ter en conta tamén o nivel de seguridade que este nos pode proporcionar.
- **Coida a protección do teu equipo**: Debemos ter instalado un antivirus no noso sistema operativo.
- **Comproba a configuración dos teus perfís**: É importante revisar o grao de privacidade que elixiches para o teu perfil nas redes sociais nas que participas. Se navegas desde un PC compartido, acórdate de pechar a sesión de todas as túas contas de email ou páxinas nas que esteas rexistrado cada vez que te conectas. E, por suposto, xamais compartas os teus contrasinais nin perfís. Se é preciso, cámbiaas con frecuencia para evitar que alguén poida utilizalas.
- **Se compartes imaxes ou información** doutras persoas a través de Internet, asegúrate de que eses datos ou fotografías non vaian prexudicar ou molestar ao seu protagonista, nin estean a invadir a súa privacidade ou violando a súa intimidade.
- **No renvíes cadeas**: Nunca reenvíes a todos os teus contactos as famosas cadeas, xa que con frecuencia conteñen virus, mesmo cando procede dun contacto de confianza.
- Lembra que Internet «no esquece» fácilmente a información, expresións ou imaxes que ti ou persoas da túa contorna, empresas e páxinas de todo tipo, colgan na web sobre ti. Só amigos verdadeiros. Antes de aceptar unha petición de amizade ou de agregar ti a alguén en calquera das redes sociais, pensa se de verdade se o coñeces e non hai ningún inconveniente en que acceda aos teus datos, á túa contorna e á túa vida íntima.
- **Publicar contido persoal**: este é un dos maiores erros que levan a cabo, sobre todo en redes sociais. Expoñer demasiado as actividades diarias e á túa familia é algo perigoso. Un exemplo de mal uso das redes sociais pode ser visto con moita frecuencia en Instagram. Esta rede ten unha ferramenta chamada Stories. Nela, podes publicar imaxes ou vídeos de 15 segundos que mostran o que estás a facer nese momento e queda a disposición dos usuarios da rede durante 24 horas.

- **Compartir información provinte doutras persoas**: Non debes divulgar imaxes, mensaxes ou testemuños de terceiros sen que eles o permitan. Ademais, non debes compartir contidos que poidan denigrar a imaxe de alguén. O cyberbullying é unha práctica considerada como acoso virtual.
- **Expoñer a seguridade**: Informacións como datos bancarios, localización e compras de bens non deben ser xamais compartidas nas redes sociais.
- **Facer clic en todo o que se ve:** Sabemos que para realizar varias accións na internet necesitamos facer clic en varias ligazóns, e iso non é un problema. O verdadeiro erro está en acceder a todas as ligazóns que se suxiren, sen sequera saber antes se son seguros. A pesar de que moitas persoas coñecidas suxiren que fagas clic en certos vínculos, non creas en todo o que les.
- **Protexe os teus datos persoais**: antes de aceptar ou rexeitar a proposta de utilización dos teus datos persoais para comunicacións comerciais, pensa o que supoñerá para ti a avalancha de información de terceiras empresas que vas recibir.

Redes sociais

Unha rede social é unha páxina web ou aplicación que serve como ferramenta de comunicación entre os usuarios que a utilizan. Principalmente compártese información en formato de texto, imaxes e vídeos, aínda que nos últimos anos se viu un auxe do formato en audio.

En España existen 29 millóns de persoas que empregan de maneira activa as súas redes sociais, segundo o estudo sobre o uso destas plataformas en España de The Social Media Family.

As redes sociais convertéronse nunha das principais vías de comunicación e interacción dos mozos. En ocasións, por mor disto, vense empobrecidas as relacións sociais do día a día, digamos que como consecuencia do uso excesivo destas redes sociais, as persoas interactúan menos no día a día. (Por exemplo: vas a un restaurante coa túa familia ou amigos e comprobas que cada persoa está a consultar o seu teléfono sen falar entre eles).

Co aumento do uso das redes sociais apareceron ameazas e riscos debidos á mala utilización destas. Como persoas consumidoras e usuarias das redes sociais débense adquirir hábitos para un uso responsable das mesmas. Hai aspectos que convén ter moi claros: débese respectar a todas as persoas, non se debe publicar información

persoal de interese (localización, residencia, o teu colexio ou instituto, as túas futuras viaxes, etc.).

En primeiro lugar, cando unha persoa decide entrar a formar parte dunha rede social, pode atoparse con diversas situacións conflitivas:



a) **Para poder acceder á rede**, é necesario aceptar as condicións de uso da páxina e a política de privacidade da mesma. Esta información non sempre é directamente visible e resulta necesario descargarla para poder acceder a ela. Con todo, é posible aceptala sinalando a opción de «acepto» sen necesidade de lela. Isto é algo moi frecuente e pode supoñer un risco xa que, ao aceptar esas condicións, estamos a dar o noso consentimento ao administrador da páxina para que dispoña dos nosos datos e as nosas imaxes.

b) **En moitos formularios de rexistro** solicítanse excesivos datos de carácter persoal, como, por exemplo, as crenzas relixiosas, a ideoloxía política, a orientación sexual, etc. Habitualmente estes datos non se solicitan como «imprescindibles», e **NON debemos facilitalos**.

c) A persoa usuaria decide quen pode acceder ao seu perfil e ver os seus datos persoais. É necesario, por seguridade, que só aceptes nas túas redes sociais a persoas que coñezas e sexan da túa contorna próxima. Debemos utilizar SEMPRE un perfil privado para relacionarnos nunha rede social que só permita aos teus amigos/seguidores/ subscriptores ver a información e publicacións que fas.

Despois de entrar a formar parte da rede, podémonos atopar con novas situacións:

a) **As persoas usuarias das redes sociais utilizan estes espazos** para compartir información: comentarios de experiencias persoais, fotografías, vídeos... En moitas ocasións toda esa información pode ser excesiva. NON debemos facilitar datos persoais que permitan a nosa localización ou obter información sobre a nosa familia, amigos, colexio, etc.

b) **Moitos motores de procura indagan nos contidos**.

c) **Un gran número de páxinas requiren a instalación de cookies para poder funcionar.**



Estes dispositivos, instalados no disco duro do usuario, recollen información sobre os sitios web que se visitan e poden obter información sobre os gustos e preferencias do usuario para personalizar o contido da súa páxina e amosalo acorde a estes, con fins publicitarios cada vez que se accede a ela.

d) **Se, por exemplo, decidimos subir unha foto persoal ao noso perfil nunha rede**, é posible que esa foto deixe de pertencernos só a nós e a partir dese momento os dereitos sexan compartidos coa entidade que a aloxa, que pode empregala para diversos fins.

Despois de participar nunha rede social, cando a persoa usuaria se expón deixar de pertencer a ela, pode xurdir unha nova dificultade. O risco principal nese momento é a imposibilidade de levar a cabo unha baixa efectiva. Aínda que o perfil estea pechado e non se poida acceder a el, os datos de rexistro seguen estando a disposición dos responsables da rede social. A persoa interesada debe saber que ten dereito a obter, sen dilación por parte do responsable do tratamento, a supresión dos datos persoais que lle concernan.

Unha das maiores preocupacións que tamén xorden respecto ao uso que os menores fan das redes sociais, é a posibilidade de que sexan vítimas dalgún tipo de acoso. Actualmente, cando falamos de acoso a través da rede, en función dos protagonistas da situación, podemos diferenciar dous tipos de acoso: cyberbullying y grooming.



O **cyberbullying**, ou acoso escolar a través de Internet, é un problema que se produce entre iguais ou, en ocasións, de alumnos cara a profesores.

Os grupos de WhatsApp empréganse en moitas ocasións, como medio para insultar e desvalorizar a un dos membros. Sempre existiu o bullying nos centros escolares, pero non ter que dar a cara para desvalorizar e facer sufrir a unha persoa é moito máis sinxelo.

O **grooming**, ou acoso sexual a través de Internet, vén dado por parte dun adulto, que actúa contra unha persoa menor cun fin sexual. A facilidade e inmediatez coa que, a día de hoxe se comparten imaxes do noso día a día, pode ser un punto moi importante a ter en conta neste tema.

Ambos os problemas non son novos e non xorden coas redes sociais, pero o anonimato, a rapidez e a sensación de inmunidade que proporcionan as comunicacións a través das redes sociais, contribuíron ao agravamento deste tipo de problemas.

TIPOS DE REDES SOCIALES

Hai redes sociais que reúnen os usuarios sen ter en conta unha temática concreta, redes sociais xeneralistas, e outras que están especializadas nun interese ou tema en común, redes sociais especializadas:

Redes sociais xeneralistas máis coñecidas e utilizadas: WhatsApp, Facebook, Twitter, Instagram, TikTok, Snapchat e VKontakte.

Redes sociais especializadas: LinkedIn, InfoJobs, 21Buttons, Spotify, Pinterest e Flickr.

Abonamento dunha contraprestación para os datos persoais

Trátase dun contrato como o resto, pero neste caso en lugar de diñeiro como contraprestación, págase con datos. A Directiva 2019/770 foi a primeira norma en recoñecer a posibilidade de que exista un contrato no que o consumidor poida explotar os seus datos persoais e utilizalos como moeda de cambio no mercado dixital [1].

Supón un importante avance para a protección dos consumidores, xa que se estenden os mecanismos de protección legalmente previstos a aqueles supostos nos que o consumidor non ha de pagar un prezo, pero ha de ceder os seus datos persoais.

Por iso, ao existir unha relación de consumo, o consumidor ten a obriga de reclamar os seus dereitos.

EN INTERNET, NON CREAS TODO O QUE VES

Un uso responsable de Internet nun contorno escolar, familiar e social implica ter presentes as seguintes cuestións:

Publicidade encuberta

Youtubers ou influencers fan publicidade de artigos ou servizos nos seus medios dixitais e redes sociais a cambio dunha contraprestación económica ou en forma de produtos (estratexia chamada product placement). Por iso, cómpre ter en conta que moitas das súas mensaxes son simplemente reclamos publicitarios para os seus seguidores.

Publicidade enganosa en Internet

Ver ficha Compras seguras en Internet.

Correos electrónicos fraudulentos

Con eles intentan vendernos produtos.

Con eles intentan acceder aos nosos datos persoais.

Ver ficha Compras seguras en Internet.

Smishing e Vishing

Dúas das novas estafas que se detectaron nos últimos tempos, alén das sinaladas na ficha Compras seguras en Internet, son smishing e vishing.

Smishing é unha técnica que consiste no envío dunha mensaxe SMS por parte dun ciberdelincuente a un usuario facéndose pasar por unha entidade lexítima (rede social, banco, institución pública, etc.) co obxectivo de lle roubar información privada ou de lle realizar un cargo económico. Polo xeral, a mensaxe invita a chamar a un número de tarificación especial ou a acceder a unha ligazón dunha web falsa baixo un pretexto [2].

Vishing é un tipo de fraude baseada na enxeñaría social e na suplantación de identidade. Realízase a través de chamadas telefónicas nas que o atacante suplanta a identidade dunha empresa, dunha organización ou mesmo dunha persoa de confianza, co fin de obter información persoal das súas vítimas. Primeiro, o atacante debe obter información confidencial sobre a súa vítima, como o seu nome e apelidos, correo, domicilio, parte dos datos da súa tarxeta de crédito, etc. Isto obteno grazas a outros ataques realizados sobre as súas vítimas, como o phishing (ver ficha Compras seguras en Internet). Ao que obtén esta información chega o momento de realizar unha chamada telefónica ao cliente facéndose pasar polo seu banco, por unha empresa de mensaxería ou por un servizo técnico para utilizar a información anterior e que a súa vítima confíe nel. Despois disto, tratará de obter máis información, tentará conseguir que o usuario instale algún malware (software hostil e intrusivo, como un virus, etc.) no seu equipo ou procurará que realice algún tipo de pagamento.

[1] INDRET

[2] INCIBE

PARA SABER MÁIS...

- INCIBE (Instituto Nacional de Ciberseguridade)
- OSI (Oficina de Seguridade do Internauta)
- AEPD (Axencia Española de Protección de Datos)
- Brigada de Investigación Tecnolóxica da Policía
- Grupo de Delitos Telemáticos da Garda Civil
- Educlic
- Instituto Nacional de Tecnoloxías Educativas e Formación do Profesorado:
- MSCBS

Materiales didácticos:

- Guía de uso seguro e responsable de Internet para profesionais de servizos de protección á infancia
- Guía para a comunidade educativa de prevención e apoio ás vítimas de ciberacoso no contexto escolar
- Educacion y FP
- Guía S.O.S. contra o ciberbullying

- Guía S.O.S. contra el Ciberbullying. Padres
- EDUCA TOLERANCIA
- INCIBE

Guía de actuación contra o ciberacoso:

- INJUVE
- Internet segura
- AEPD
- Compra segura en INTERNET GUÍA PRÁCTICA
- Xoguetes conectados

Guías para un bo uso do móbil e as redes sociais:

- Aprender a convivir co móbil
- Guía para pais e educadores sobre o uso seguro de Internet, móbiles e videoxogos
- Guía para mozos e adolescentes sobre o bo uso das tecnoloxías
- Guía de seguridade nas redes sociais
- Servizo de atención ás adiccións tecnolóxicas (Madrid)
- Axencia Española de Protección de Datos
- Brigada Central de Investigación Tecnolóxica da Policía
- Observatorio de la infancia
- Ejerce tus derechos
- Tu decides en internet