Guía de uso seguro de Internet e as redes sociais

para alumnado
de centros educativos

XUNTA
DE GALICIA

XUNTA
DE GALICIA

TÁBOA DE CONTIDOS

XUNTA DE GALICIA

1. PEGADA DIXITAL

1.1. Que é a pegada dixital?

Todo o que fas en Internet pode deixar un rastro. Esa curiosa pegada que queda asociada a ti ao navegar, ao crear un perfil nunha rede social, ao publicar contido ou ao xogar en liña con outras persoas chámase **«pegada dixital»**.

A pegada dixital é como o teu selo no mundo en liña. Cada vez que usas un ordenador, unha tableta ou un teléfono deixas un rastro de información. Desde as aplicacións que utilizas ata as fotos que compartes, todo deixa pegada. Pero, por que é importante?

Imaxina que con cada acción que realizas estás a construír unha imaxe sobre ti na rede. Esa presenza en liña é a túa pegada dixital: se alguén busca información sobre ti, será o que atope para facerse unha idea de como es.

O interesante é que podes decidir como desexas que sexa esa imaxe. Podes compartir momentos divertidos e positivos, como os teus logros ou as túas afeccións. Pero, coidado! Tamén podes caer no erro de compartir demasiada información persoal sobre ti ou comportarte de maneira inadecuada na rede.

1.2. Como se constrúe?

A túa pegada dixital constrúese principalmente grazas á combinación de varios elementos:

» **Os datos que proporcionas**

Por exemplo, cando abres un perfil nunha rede social proporcionas unha serie de datos persoais como a túa idade, o correo electrónico, o teu número de teléfono, unha foto de perfil, etc. Todos eles comezarán a crear unha imaxe sobre ti.

» A información que compartes

A través das túas redes sociais podes consumir moito contido doutras persoas, pero tamén podes interactuar con el comentándoo ou compartíndoo. Por outra banda, é posible que tamén compartas a través das túas redes contido propio que poderá do mesmo xeito afectar positiva ou negativamente á túa pegada dixital. Seguir un reto viral como saltar desde un lugar elevado pode parecer emocionante, pero tamén pode ser arriscado e comprometer ao mesmo tempo a túa seguridade e a túa reputación en liña.

» O que a rede di de ti

Á marxe do contido que compartas na rede, tamén afectará á túa reputación aquilo que outras persoas compartisen sobre ti. Pode ser contido inofensivo, pero en ocasións podes quedar etiquetado ou etiquetada sen a túa autorización en fotografías ou vídeos comprometidos. Este contido pode prexudicarte, polo que tamén é importante que o teñas en conta.

1.3. Riscos dunha pegada dixital negativa

Así como podes ter unha pegada dixital fantástica, tamén corres o risco de que exista contido que estea a ensuciar a túa reputación. Ten en conta que o contido negativo que circule sobre ti implica unha serie de riscos importantes:

» Deixa pegada

Todo o que se comparte na rede deixa pegada e non se esquece. Pode quedar alí para sempre. Fotos, comentarios ou publicacións desaxeitadas poden perseguirte no futuro. Lembra que aínda que despois te arrepintas e elimines a publicación, outra persoa puido ter feito unha captura da pantalla, polo que perderás o control sobre ese contido. Pensa dúas veces antes de pulsar en «Publicar».

» Dana a túa reputación

A túa imaxe en Internet é moi valiosa e construír unha boa reputación é clave. Unha pegada dixital negativa pode afectar a como te ven os demais (amizades, familia ou mesmo as empresas cando esteas na procura de emprego no futuro) e ofrecer unha versión de ti que non se axuste á realidade. Ás veces pódeste deixar levar por un impulso e deixar un comentario desafortunado. Seguramente non te represente, pero pode falar de ti negativamente.

» **Compromete a túa privacidade**

Compartir demasiada información persoal sobre ti na rede pode afectar non só á túa imaxe, senón que pode ocasionar que sexas máis vulnerable e que te expoñas a outros riscos. Nunca pensaches que se compartes publicamente cando te vas de vacacións coa túa familia estás informando tamén a persoas descoñecidas sobre cando a túa casa estará baleira? Ou se compartes moitas fotografías sobre ti, outra persoa podería utilizalas para suplantarte e, incluso, para manipulalas a través de intelixencia artificial (*deepfake*) ou doutros medios. A información pode ser unha ferramenta moi poderosa que depende en gran medida de quen a teña e como a use. Cando a información cae en mans equivocadas pode ser moi prexudicial.

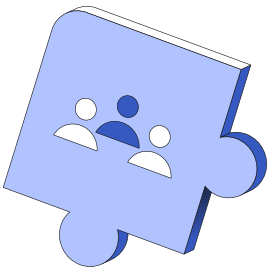
1.4. Como construír unha pegada dixital positiva?

Crear unha imaxe positiva sobre ti está nas túas mans. Para manter unha pegada dixital segura e axeitada é necesario que sigas as seguintes recomendacións:

1. **Pensa antes de publicar calquera contido**. É algo que che gustaría que permanecese na rede?

2. **Protexe a túa información persoal e non a compartas con descoñecidos.** Publicar fotos da túa casa podería permitir que unha persoa descoñecida saiba onde vives.

3. **Elixe coidadosamente os avatares e as imaxes asociadas aos teus perfís.** Evita compartir con persoas que non coñeces o teu rostro, xa que poderían utilizar a túa foto de perfil para outros fins (suplantación de identidade, *deepfakes*, etc.).



4. **Utiliza pseudónimos** para os nomes de usuario ou de rexistro. Desta maneira, protexerás en maior medida a túa privacidade. Se buscan por ti na rede será máis difícil atoparte porque non aparecerás tan facilmente nos resultados do buscador.

5. **Participa de maneira respectuosa na rede.** Trata aos demais como che gustaría que che tratasen.

6. **Respecta a privacidade doutras persoas** evitando compartir imaxes, vídeos ou outra información sen a súa autorización.

7. **Practica regularmente o *egosurfing*.** Consiste en realizar unha procura desde o teu navegador engadindo o teu nome e apelidos entre comiñas coa intención de coñecer que contido circula sobre ti na rede. Tamén é recomendable que busques polo teu número de teléfono ou polo teu correo electrónico porque, por exemplo, poden ser datos que se estean compartindo publicamente sen o teu consentimento. Grazas a estas procuras, poderás coñecer que información hai de ti na rede permitíndoche xestionar a túa imaxe.

https://ciberseguridadegalicia.gal/

Se queres máis información, visita ***https://ciberseguridadegalicia.gal/*** onde atoparás entre os recursos, na sección de «Divulgación e concienciación», recomendacións e moitos recursos á túa disposición.

Protexe e constrúe unha boa pegada dixital que te represente agora e no futuro!

XUNTA DE GALICIA

2. AS REDES SOCIAIS

2.1. O poder dos teus datos

Existen cada vez máis redes sociais no mercado e todas elas almacenan unha gran cantidade de información persoal sobre ti que debes protexer.

Cando publicas calquera tipo de contido a través dos teus perfís estás a expoñer parte da túa vida a Internet. É necesario que controles o que compartes, como o fas e quen pode acceder ao teu contido para protexer a túa privacidade e a túa pegada dixital.

Para evitar riscos innecesarios, é recomendable que non publiques o teu correo electrónico, o teu número de teléfono, a túa dirección ou localización, ou mesmo fotografías ou vídeos que te poidan comprometer.

Tamén é importante que respectes a privacidade doutras persoas de maneira que deberás evitar publicar conversacións privadas ou material audiovisual (fotos, vídeos ou audios) onde aparezan outras persoas sen o seu consentimento.

2.1. Protéxete nas redes

As redes sociais permitiranche acceder a un mundo conectado, pero para asegurar a túa experiencia, tamén é necesario que saibas como enfrontarte a algúns dos retos que presentan:

» **Adicción ás redes:** establece límites de tempo e equilibra o teu tempo en liña con outras actividades fóra das pantallas.

» **Roubo de contas:** os ciberdelincuentes pretenden facerse coas túas contas. Podes aseguralas protexendo as túas credenciais e evitando compartilas con outras persoas.

» **Suplantación de identidade:** compartir demasiada información persoal con descoñecidos facilita que outra persoa poida facerse pasar por ti. Crea contas privadas e practica o *egosurfing* tamén nas redes sociais para localizar posibles contas falsas que utilicen o teu nome de usuario.

- **Contactos descoñecidos e *bots*:** contar con moitos seguidores non sempre é algo bo. Limpa a túa rede de contactos que non coñezas na vida real porque poderían ter intencións maliciosas (facerse cos teus datos, difundir *spam*, infectar os teus dispositivos con malware ou estafarte). Moitas veces os atacantes usan *bots* (perfís falsos automatizados) para realizar estas tarefas. Non te deixes enganar! Repórtaos e bloquéaos nas túas redes.

- **Sorteos e concursos fraudulentos:** algunha vez fuches etiquetado nun suposto sorteo nas redes sociais? Evita esas promocións que son demasiado boas para ser verdade e que pretenden enganarte. A trampa está en que pulses nunha suposta ligazón para trocar o teu premio. Coidado! Poden infectar o teu dispositivo ou solicitarche información persoal para preparar enganos máis persoalizados.

- **Trolas e noticias falsas:** non te deixes levar por publicacións virais e verifica a información antes de compartila para facer da Internet un espazo máis seguro e fiable.

- **Retos virais:** os retos virais en redes sociais poden ser divertidos e inofensivos, pero tamén poden volverse arriscados e perigosos. Avalía os seus posibles riscos antes de unirte a un desafío: pode supoñer un perigo para ti ou para as persoas que te rodean? Lembra que podes reportalo desde as opcións das túas redes sociais.

- **Ciberacoso:** o acoso nas redes aliméntase da participación dos demais. Non o apoies e frea a súa difusión apoiando ás vítimas para denunciar o caso. Por exemplo, se ves que unha persoa comparte nun *chat* de *WhatsApp* un *sticker* coa cara doutra persoa para facer mofa dela, non participes na súa divulgación.

- ***Sexting*:** evita compartir imaxes que te poidan incomodar. Lembra que almacenar imaxes ou vídeos íntimos en calquera dispositivo é moi arriscado. Asegura a túa intimidade e, se te enfrontas a presións, non dubides en pedir axuda.

- ***Grooming*:** é cando alguén maior faise pasar por un amigo ou amiga en liña para gañar a túa confianza. Poden parecer amables e querer falar moito contigo, pero en realidade están a tratar de manipularte para que lles envíes fotos ou vídeos persoais, a miúdo de carácter sexual. Evita confiar en persoas que non coñezas fóra de Internet e lembra que se alguén está sendo molesto ou che pide que fagas algo que non queres facer, non fagas caso e busca axuda dunha persoa adulta de confianza.

2.3. Configuración de privacidade e seguridade

É probable que utilices e contes con varios perfís en distintas redes sociais. En cada unha delas é necesario que antes de utilizala configures as súas opcións de privacidade e seguridade para evitar os riscos aos que te podes enfrontar.

WhatsApp

Entra en **«Axustes > Privacidade > Revisión de privacidade»** para configurar todas as súas opcións, especialmente as seguintes:

- A través da sección **«Quen pode contactarte»** poderás definir quen poden ser os teus contactos, silenciar números descoñecidos e bloquear a outros usuarios.
- En **«Controla a túa información persoal»** definirás quen pode ver a túa foto de perfil e a última vez que te conectaches. Tamén poderás desactivar as confirmacións de lectura para que non quede rastro de cando liches unha mensaxe. Comproba nesta pantalla se estás ou non compartindo a túa localización en tempo real, e na sección **«Estados»** poderás definir quen pode ver as túas actualizacións.
- **«Engade máis privacidade aos teus *chats*»** permitirache limitar o acceso ás túas mensaxes e arquivos activando a opción **«Duración predeterminada das mensaxes»**, así como realizar copias de seguridade dos teus datos.
- A través de **«Engade máis protección á túa conta»** poderás elixir unha capa de seguridade extra da túa conta a través dun bloqueo de pantalla e activar a verificación en dous pasos, que che permitirá definir un código PIN que será necesario coñecer no caso de que necesites volver rexistrar o teu número de teléfono en *WhatsApp*.

Instagram

Esta rede social ofrece moitas opcións para protexer a túa conta. Pulsando sobre a imaxe do teu perfil e posteriormente sobre a icona con tres guións, accederás á sección **«Configuración e privacidade»**:

- No **«Centro de contas»** dispoñerás da información xeral de todas as túas contas de *Meta* (propietaria de *WhatsApp*, *Instagram* e *Facebook*).
- En **«Privacidade da conta»** deberás activar a opción «Conta privada» para que só te poidan ver as persoas que te seguen.
- Na sección **«Como poden interactuar contigo os demais»**:
  - En **«Mensaxes e respostas a historias»** poderás configurar que os teus contactos sexan os únicos que poidan enviarte mensaxes e responder ás túas historias.
  - En **«Etiquetas e mencións»** poderás seleccionar quen pode etiquetarte e mencionarte en vídeos ou imaxes.

- En **«Comentarios»** filtra quen pode comentar nas túas publicacións.
- En **«Compartindo»** poderás impedir que outros usuarios compartan as túas publicacións.
- En **«Interaccións limitadas»** limitarás temporalmente os comentarios e mensaxes non desexadas de usuarios ou de grupos.

TikTok

Esta rede social tivo unha gran acollida por millóns de persoas en todo o mundo grazas a súa gran capacidade para crear, compartir e difundir masivamente vídeos curtos.

TikTok tamén dispón de moitas opcións para protexer a túa privacidade. Para configuralas deberás dirixirte á icona con tres guións desde o teu perfil e posteriormente deberás pulsar en «Axustes e privacidade»:

» Na sección **«Privacidade»** poderás:

- Activar a túa conta privada e configurar outras opcións de visibilidade do teu perfil.
- Administrar as opcións para seleccionar quen pode comentar nas túas publicacións, mencionarte ou etiquetarte.

» Na sección **«Seguridade > Verificación en dous pasos»** poderás activar unha capa extra de seguridade identificando varios métodos para confirmar a túa identidade (un número de teléfono, un correo electrónico, unha aplicación de autenticación ou un contrasinal).

Twitch

É unha plataforma que permite o acceso a retransmisións en directo e a contido gravado. Inicialmente deuse a coñecer como unha gran comunidade relacionada co mundo dos videoxogos, aínda que actualmente a rede social tamén abarca outra gran variedade de temáticas.

Para protexer a túa conta deberás pulsar sobre a icona do teu perfil e dirixirte á sección **«Configuración > Seguridade e privacidade»** dende o teu navegador (as opcións dispoñibles a través da *app* móbil son máis limitadas):

- En **«Permitir a creación de contas adicionais»** desactivando esta opción poderás evitar que se creen outras contas nesta rede social utilizando o teu correo electrónico.

- No apartado **«Autenticación en dous pasos»** poderás activar unha capa adicional de protección para a túa conta. Neste caso, deberás incluír o teu número de teléfono móbil para que sempre teñas que introducir o código de seguridade que te chegará a través dunha mensaxe de texto cada vez que vincules a túa conta nun novo dispositivo.

- Na sección de **«Privacidade»** terás dispoñibles as seguintes opcións:

  - En «Usuarios bloqueados» poderás engadir e visualizar as contas que desexas bloquear.

  - En «Mencións en historias» e no apartado «Compartir *clips* en historias» poderás configurar quen pode mencionarte ou compartir os teus *clips* nas súas historias.

  - En «Bloquear murmurios de descoñecidos» poderás bloquear a recepción de mensaxes de persoas que non coñezas. Os murmurios permiten enviar mensaxes privadas a outras contas. Se non queres recibilos, activa esta opción.

  - Nesta sección tamén podes bloquear a recepción de agasallos en canles que non segues; ocultar emblemas e o número de subscricións regaladas, o estado da túa subscrición e o emblema de fundador nas distintas canles.

No caso de que retransmitas en directo dende a túa canle de *Twitch* e desexes configurar a súa protección, deberás pulsar sobre a icona do teu perfil e dirixirte á sección **«Configuración > Canle e vídeos».**

- Accedendo ó apartado **«Moderación»** poderás establecer controis avanzados sobre termos e frases non permitidos, controis sobre usuarios sospeitosos e vetados e proteccións adicionais para protexer a túa canle, por exemplo, de posibles *bots* que fagan *spam* ou de contas maliciosas.

Discord

Esta plataforma está baseada en servidores de *chat* onde as persoas pódense conectar e unir para falar sobre unha ampla variedade de temas á parte dos videoxogos e as películas.

Pulsando sobre o teu perfil e posteriormente sobre a icona de **«Axustes»** dende a zona superior dereita, poderás configurar as principais funcionalidades deste servizo.

Dende o apartado **«Conta»** terás a posibilidade de:

» Protexer o teu perfil a través da opción **«Autenticación de varios factores»**. Pulsando sobre a opción **«Habilitar aplicación de autenticación»** poderás vincular a túa conta con *Google Authenticator* ou con *Authy*. Ámbalas dúas son *apps* que xerarán códigos de seguridade para confirmar a túa identidade e protexer o teu perfil.

» Visualizar e xestionar os usuarios bloqueados a través do apartado **«Usuarios»**.

Accedendo ao apartado de **«Privacidade e seguridade»** contarás coas seguintes opcións:

» Na sección **«Filtro de Imaxes Explícitas (*Explicit Image Filter*)»** poderás escoller entre as seguintes funcións de filtrado:

- Filtrar todas as mensaxes directas (opción recomendada).
- Filtrar mensaxes directas de persoas que non estean na túa lista de amigos.
- Non filtrar mensaxes directas.

» Na sección **«Filtro de Spam nas Mensaxes Directas (*DM Spam Filter*)»** tamén poderás escoller entre as mesmas opcións de filtrado do apartado anterior coa intención de evitar a recepción de publicidade non desexada.

» No apartado **«Permisos de descubrimento»** poderás permitir ou bloquear que te atopen nesta rede outras persoas que dispoñan do teu número de teléfono ou do teu correo electrónico.

Consulta a canle de *YouTube* da Axencia Española de Protección de Datos (***https://www.youtube.com/@AEPD_es***) e as vídeo pílulas do portal ciberseguridadegalicia.gal (***https://ciberseguridadegalicia.gal/gl/tipoloxias-de-multimedia/video-pilulas***). En ambos sitios atoparás vídeos explicativos sobre como configurar a privacidade das túas redes sociais.

https://www.youtube.com/@AEPD_es

https://ciberseguridadegalicia.gal/

XUNTA DE GALICIA

3. OS DISPOSITIVOS MÓBILES

3.1. A seguridade dos dispositivos móbiles

Un dispositivo móbil é unha ferramenta moi potente que brinda acceso a un universo onde atoparás gran cantidade de información, relacións e contidos. Con todo, é necesario que teñas en conta que, como dispositivos intelixentes, tamén supoñen riscos aos que deberás enfrontarte:

» **Conéctanse a Internet:** un dispositivo conectado á rede está exposto a ameazas como ataques de ciberdelincuentes.

» **Conéctanse contigo:** gardan información sobre os teus intereses, por onde navegas e tamén poden coñecer a túa localización. Estes datos, dependendo das mans nas que caian, poden ser perigosos.

» **Conéctanse entre eles:** como dispositivos intelixentes poden interconectarse con outros equipos xerando novos riscos e vulnerabilidades. Por exemplo, pensa nun arquivo infectado cun *malware* que se descargou no teu dispositivo e logo sincronizouse automaticamente con outro dispositivo da túa casa a través dun servizo de almacenamento na nube.

3.2. Primeiros pasos para protexelos

Configurar adecuadamente o teu dispositivo móbil é esencial para garantir a súa seguridade e protexer a túa información persoal. Segue estas recomendacións antes de comezar a utilizar os teus dispositivos:

» **Establece un código de bloqueo no teu SIM e no teu dispositivo** para evitar que calquera persoa poida acceder a el. Patróns, PIN, contrasinais ou, mesmo, a túa pegada dactilar son as opcións máis habituais. Os datos biométricos (o teu rostro ou a túa pegada dactilar) son irrepetibles e, por tanto, máis seguros.

» **Configura un bloqueo de pantalla automático** para que, no caso de que non esteas a utilizar o teu dispositivo continúes protexéndoo.

» **Actualiza o sistema operativo e todas as túas aplicacións** para manter a protección dos teus dispositivos fronte aos ciberdelincuentes.

» **Evita a instalación de aplicacións que non proveñan das tendas oficiais** (*Google Play* no caso de sistemas *Android* ou *Apple Store* en *iOS*). As *apps* pirata poderían conter *malware* e poderían facerse co control dos teus datos.

» **Analiza a letra pequena dos servizos e *apps* que utilizas.** Aínda que moitos servizos en liña preséntanse como gratuítos, é fundamental que lembres que nada é completamente gratis. A través das políticas de privacidade poderás comprobar o que pretenden facer cos teus datos persoais. Ás veces podes estar autorizando que, por exemplo, utilicen as túas fotos para campañas publicitarias sen ti sabelo.

» **Revisa e deshabilita os permisos de aplicacións que non sexan necesarios** para o seu funcionamento. En ocasións poden solicitarche permiso para acceder a máis información da que realmente necesitan. Por exemplo, unha *app* que che permite usar o teu dispositivo móbil coma unha lanterna non debería solicitarche permiso para acceder a túa xeolocalización. Pero, no caso de aplicacións como *WhatsApp* que solicitan permiso para acceder a túa galería de imaxes, tería sentido se queres utilizar a funcionalidade de compartir fotos cos teus contactos.

» **Desactiva a xeolocalización e as conexións *Wifi* ou *Bluetooth* por defecto.** Actívaas só no caso de que as vaias a utilizar para evitar posibles perigos, xa que unha persoa podería tomar o control do teu dispositivo e acceder á túa información.

» **Conéctate só a redes *Wifi* seguras e confiables.** Evita as redes gratuítas como a que podes atopar nunha cafetería ou nun hotel que poden supoñer un alto risco para a túa información.

Adopta estas medidas nos teus dispositivos para construír unha sólida barreira de seguridade que protexa os teus datos e a túa privacidade.

Visita o sitio web do Instituto Nacional de Ciberseguridade (INCIBE) se desexas máis recomendacións e consellos sobre como configurar e protexer os teus dispositivos móbiles. Na sección dedicada á cidadanía atoparás o apartado «Temáticas» con información sobre os aspectos máis relevantes actualmente sobre ciberseguridade.

XUNTA DE GALICIA

4. PASOS PARA UNHA CONTORNA MÁIS SEGURA

4.1. O contrasinal, a chave ao teu mundo dixital

Os teus contrasinais son como chaves que protexen a túa información. Protexelos e fortalecelos son tarefas cruciais para manter baixo control a posibles intrusos. Como podes facelo?

» **Crea contrasinais únicos para cada servizo** que utilizas. Lembra que se utilizas o mesmo contrasinal para todas as túas contas, se se compromete un servizo, comprométense todos.

» **Deseña contrasinais robustos e difíciles de adiviñar.** Evita utilizar información persoal como nomes ou datas de nacemento. Son datos que podes compartir facilmente a través das túas redes e facilitarán o labor dos ciberdelincuentes para conseguir acceder ás túas contas.

» **Canto máis complexo e especialmente canto máis longo sexa, máis seguro será.** Como mínimo é recomendable que estean compostos por 12 caracteres combinando letras maiúsculas, minúsculas, números e caracteres especiais.

» **Cámbiaos regularmente** para engadir unha capa extra de seguridade.

» **Evita compartilos con outras persoas, gardalos en papel ou a través do teu navegador.**

» **Usa xestores de contrasinais para almacenar, organizar e xestionar dunha maneira máis segura os teus contrasinais.** Estes programas instalables nos teus dispositivos mellorarán a seguridade das túas claves almacenándoas nunha bóveda cifrada e axudaranche tanto na xestión como na súa definición.

» **Habilita a autenticación de dobre factor para protexer as túas contas.** As túas redes sociais e o teu correo dispoñen desta funcionalidade entre as súas opcións de seguridade. Actívaa en todos os servizos que conten con ela. Desta maneira, se alguén descubriu o teu contrasinal terás unha capa de seguridade adicional para protexer as túas contas.

Exemplo de contrasinal NON seguro	Exemplo de contrasinal SEGURO
✗ @Ana2015	✓ 3Nubes#de#Chuvia!

Descobre como crear e protexer as túas credenciais a través dos recursos que atoparás en ***https://ciberseguridadegalicia.gal/***. Contarás con píldoras informativas e infografías que te axudarán a crear e xestionar os teus contrasinais dunha maneira segura.

4.2. Navegando con conciencia

A rede está repleta de posibilidades para ti, pero tamén de oportunidades para un ciberatacante. Adopta estes hábitos ciberseguros e converte a túa experiencia en liña nunha viaxe segura:

» **Navega con prudencia.** Non todos os sitios web son iguais e existen algúns que poden ser inseguros. Revisa se no teu navegador aparece a icona con forma de cadeado que confirme que esa páxina que estás a visitar é segura.

» **Evita facer clic en ligazóns sospeitosas** (por SMS, correo electrónico, nunha web ou mesmo en redes sociais) que poderían buscar infectar os teus dispositivos ou facerse cos teus datos persoais.

» **Elimina as *cookies* do teu navegador de forma regular.** Estas «galletas» rastrexan a túa actividade na rede e é recomendable borrar as túas pegadas para salvagardar a túa privacidade. Busca entre as opcións do apartado de «Historial» ou «Privacidade» do teu navegador para eliminalas.

» **Lembra pechar sesión cada vez que deixes de usar as túas contas en liña.** Sobre todo, cando navegues en dispositivos utilizados por máis persoas. Calquera podería aproveitar a túa sesión aberta, ver o teu contido persoal e, incluso, actuar baixo o teu nome.

» **Cobre a túa cámara e confirma que o teu micrófono estea desactivado** cando non estean en uso a través dos teus dispositivos ou equipos (videoconsolas, portátiles, móbiles...) Revisa a configuración de privacidade para confirmar que programas e aplicacións poden acceder a eles.

» **Utiliza unicamente programas fiables e con licenza.** Non instalando *software* pirata diminuirás as probabilidades de que se infecten os teus dispositivos. Evita, por tanto, instalar *apps* que son de pago dende páxinas que as ofrecen de balde.

» **Actualiza os teus programas e aplicacións.** As actualizacións a miúdo conteñen parches de seguridade que fortalecerán as túas defensas ante posibles ameazas.

» **Protexe os teus dispositivos cunha solución antivirus.** Contar cun *software* de seguridade será de gran axuda para protexerte das principais ameazas en liña (*phishing*, *malware*, sitios webs fraudulentos, etc.).

» **Fai copias de seguridade da túa información máis importante.** É probable que poidas sufrir unha perda de datos en calquera momento. As túas fotos, os teus documentos, os teus traballos... E se non podes recuperalos?

XUNTA DE GALICIA

5. GLOSARIO

5.1. Que é iso?

Preguntácheste algunha vez que significan todas esas palabras estrañas que escoitas cando se fala sobre Internet e tecnoloxía? A rede está chea de palabras e conceptos novos que ás veces poden parecer confusos. Pero non te preocupes, estamos aquí para axudarte a descifralos.

Neste glosario, imos explorar algúns dos termos máis habituais para entender os principais conceptos e os novos retos aos que te podes enfrontar a través de Internet.

» ***APK:*** provén do termo «*Android Package Kit*» e fai referencia ós paquetes de instalación das aplicacións nos dispositivos *Android*. Podes obter arquivos APK de varias fontes, como a tenda oficial de aplicacións de *Google* (*Play Store*) ou mesmo de sitios web de terceiros. Con todo, é importante ser coidadoso ao descargar APKs de sitios web externos, xa que poderían conter *software* malicioso que pode danar ou roubar información do teu dispositivo.

» ***Bot:*** é a abreviatura de robot e fai referencia a un programa informático deseñado para realizar automaticamente accións específicas na rede. Os *bots* poden ser útiles e facilitar certas tarefas, pero tamén poden ser utilizados de maneira maliciosa para difundir *spam*, propagar desinformación ou realizar actividades fraudulentas en liña simulando, por exemplo, ser persoas reais nas redes sociais.

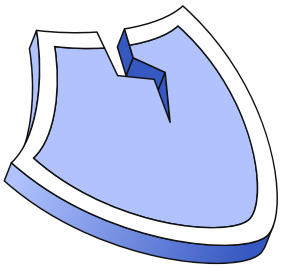
» ***Cyberbullying:*** consiste no acoso ou intimidación intencionada e repetida que se produce en liña a través de medios dixitais como as redes sociais.

» ***Cookies:*** son pequenos arquivos de texto que os sitios web almacenan no teu dispositivo para rastrexar a túa actividade en liña.

» ***Deepfake:*** é contido audiovisual (vídeos ou imaxes) creado xeralmente por intelixencia artificial que pretende enganar ás persoas ou difamar a alguén simulando que está a dicir ou facendo algo que realmente non fixo.

» ***Egosurfing:*** é cando buscas o teu propio nome e apelidos na rede para ver que información aparece sobre ti. Podes facelo utilizando un motor de procura como *Google*. É unha forma de ver o que outros poden atopar sobre ti en liña.

» ***Grooming:*** é cando unha persoa adulta utiliza a rede para finxir ser menor e establecer unha relación de confianza con menores. Unha vez que gañou a confianza das súas vítimas, pode tentar manipulalas para chantaxealas co obxectivo de obter favores sexuais ou explotalas doutras maneiras.



» ***Jailbreak:*** é un proceso que permite esquivar as restricións de seguridade impostas por *Apple* en dispositivos con sistema operativo *iOS*, como *iPhones* e *iPads*. Unha vez que se realiza o *jailbreak* nun dispositivo, elimínanse as limitacións do fabricante permitindo instalar aplicacións que non están dispoñibles na *App Store* oficial de *Apple*. Lembra que esta acción pode ser prexudicial para a túa privacidade e a seguridade do teu dispositivo.

» ***Malware:*** este concepto nace da unión dos termos en inglés «*malicious*» e «*software*». É, por tanto, un programa deseñado para danar ou infiltrarse nos teus dispositivos ou equipos sen o teu consentimento.

» ***Phishing:*** é unha técnica utilizada para obter información confidencial (como contrasinais ou detalles de tarxetas de crédito) ou infectar o teu dispositivo facéndose pasar xeralmente por unha entidade ou servizo de confianza. Un *SMS* simulando ser o teu banco alertándote de que a túa tarxeta bloqueouse por motivos de seguridade é un claro exemplo de *phishing*. Pretenden que te deixes levar polo engano e pulses nunha ligazón maliciosa que pode incluír *malware* ou que pode redirixir a un sitio web onde se solicitan os teus datos persoais.

» ***Sexting:*** esta práctica consiste en enviar fotografías ou vídeos que unha persoa toma de si mesma con contido sexual a través de dispositivos como teléfonos móbiles ou calquera outro dispositivo conectado a Internet. Aínda que non é ilegal, a práctica pode ser perigosa xa que as imaxes ou vídeos compartidos poden ser difundidos sen consentimento, o que pode ter consecuencias negativas para a privacidade e a reputación das persoas involucradas. Lembra que se neste caso existise unha chantaxe onde se ameaza con publicar ese contido íntimo estaríamos a falar de «*sextorsión*».

» ***Spam:*** denomínase *spam* a toda comunicación non solicitada realizada por vía electrónica. A miúdo utilízase para distribuír publicidade non desexada ou contido malicioso.

» ***Stalkear:*** fai referencia a unha forma de acoso ou espionaxe nas redes sociais onde se pretende seguir as actividades dunha persoa ou enviarlle mensaxes non desexadas. Para este cometido, xeralmente a persoa que actúa coma «*stalker*» usa contas falsas para ocultar a súa identidade.

» ***Troll / hater:*** son persoas que provocan deliberadamente na rede, sementando discordia ou molestando.

XUNTA DE GALICIA

6. REFERENCIAS

PEGADA DIXITAL

» **Internet segura for Kids:**

https://www.incibe.es/sites/default/files/contenidos/materiales/Campanas/is4k-guia-rrss.pdf

» **Pantallas amigas:**

https://www.pantallasamigas.net/privacidad-y-proteccion-de-datos/

» **Instituto Nacional de Ciberseguridade:**

https://www.incibe.es/ciudadania/tematicas/privacidad

» **Portal de Ciberseguridade de Galicia:**

https://ciberseguridadegalicia.gal/gl/recursos/multimedia/sesion-formativa-iniciacion-segura-pegada-dixital-e-redes-sociais

AS REDES SOCIAIS

» **AEPD (Axencia Española de Protección de Datos):**

https://www.aepd.es/areas-de-actuacion/internet-y-redes-sociales/protege-tu-privacidad

» **Internet segura for Kids:**

https://www.incibe.es/sites/default/files/contenidos/materiales/Campanas/is4k-guia-rrss.pdf

» **Portal de Ciberseguridade de Galicia:**

https://ciberseguridadegalicia.gal/gl/recursos/multimedia/sesion-formativa-iniciacion-segura-pegada-dixital-e-redes-sociais

https://ciberseguridadegalicia.gal/gl/tipoloxias-de-multimedia/video-pilulas

XUNTA DE GALICIA

OS DISPOSITIVOS MÓBILES

» **Instituto Nacional de Ciberseguridade:**

https://www.incibe.es/ciudadania/tematicas/dispositivos-moviles

» **Portal de Ciberseguridade de Galicia:**

https://ciberseguridadegalicia.gal/gl/recursos/multimedia/dispositivos-conectados

https://ciberseguridadegalicia.gal/gl/recursos/multimedia/colega-onde-esta-o-meu-mobil

https://ciberseguridadegalicia.gal/gl/tipoloxias-de-multimedia/video-pilulas

PASOS PARA UNHA CONTORNA MÁIS SEGURA

» **Instituto Nacional de Ciberseguridade:**

https://www.incibe.es/menores/educadores/ciberseguridad

» **Navega con rumbo (CPEIG en colaboración coa Xunta de Galicia):**

https://navegaconrumbo.cpeig.gal/

XUNTA DE GALICIA

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES

programa bienestar emocional
ámbito educativo