PREVENCIÓN = SAÚDE

Boletín para nais e pais

A prevención na casa

a mellor axuda

Boletín da Unidade Asistencial de Drogodependencias de Monforte

Equipo de Prevención

Uso e configuración segura de dispositivos móbiles de menores

Os nosos fillos utilizan habitualmente unha gran variedade de dispositivos tecnolóxicos para acceder a Internet: móbiles (tanto seus como dos seus pais), tablets, computadores, videoconsolas... E non quedan só en navegar por páxinas web, pois participan activamente en redes sociais, utilizan aplicacións de mensaxería instantánea, xogos, etc.

Nestes dispositivos está almacenada unha gran cantidade de información persoal, mensaxes, fotografías, contrasinais de acceso a distintas páxinas e servizos etc. Se alguén se fixese con esa información tería moitas ferramentas para facerlles dano.

Así pois, para que estean máis seguros en liña, habemos de axudarlles a facer un bo uso da internet, pero tamén protexer os seus dispositivos e as súas contas de usuario tanto nas redes sociais como noutros servizos en liña.

A que riscos enfróntanse se non protexen os seus dispositivos?

Calquera dos nosos dispositivos (conectados a Internet), ou contas en redes sociais ou outros servizos en liña poden poñer en risco a nosa seguridade, especialmente se non os protexemos da maneira adecuada:

Virus, tamén chamados malware. Poden afectarnos de diversas maneiras:

- **Danos no sistema e as súas aplicacións**. Poden cambiar a configuración do sistema (por exemplo cambiar a páxina de inicio do navegador, redirixirnos a páxinas maliciosas ou fraudulentas en lugar das oficiais, ofrecernos publicidade) e instalar aplicacións maliciosas (por exemplo para ver os nosos contrasinais, secuestrar e inutilizar o dispositivo a cambio dun rescate, utilizar o noso dispositivo para danar a outras persoas e organizacións).

- **Danos á nosa información**. Poden impedirnos acceder aos nosos documentos, fotos, vídeos etc. (por exemplo borrándoos, cifrándoos a cambio dun rescate, estragándoos ao engadir ou borrar algunha parte).

- **Perdas económicas**. Axudando a que caiamos, sen darnos conta, en páxinas web maliciosas (por exemplo suplantando as nosas redes sociais, bancos e tendas en liña), pedíndonos diñeiro a cambio dun "servizo" (por exemplo devolvernos o control do dispositivo, instalarnos un falso antivirus).

- E tamén **"acceso indebido a información privada"** como se detalla a continuación…

Persoas que acceden indebidamente á nosa información privada:

- **Danos á privacidade e intimidade**. O mero coñecemento da nosa información por parte doutra persoa sen desexalo. Ademais pódese agravar se esta información difúndese a outras persoas ou se se trata de mensaxes ou imaxes de carácter íntimo.

- **Danos na imaxe e reputación en liña**. Se alguén accede á nosa información privada, e difunde sen o noso permiso unha parte dela que nos pode resultar prexudicial (por exemplo imaxes íntimas). Tamén se pode producir pola publicación de mensaxes inapropiadas, tanto en nosas propias contas de redes sociais como en perfís falsos que se fan pasar por nós (ridiculizándonos, danando no noso nome a otras persoas).

- **Ciberbullying**.

- **Grooming, extorsión e chantaxe**. Se persoas malintencionadas conseguen mensaxes e imaxes íntimos, poden chantaxearlles e extorsionarlles tanto economicamente, como con fins sexuais (para conseguir máis imaxes e vídeos, ou para abusar sexualmente deles)/delas).

PREVENCIÓN

A prevención pasa por tomar diversas pautas de seguridade, tanto dirixidas a reducir as posibilidades de que os riscos se convertan en problemas reais, como para limitar as consecuencias negativas no caso de que así sexa.

En xeral trátase de **construír contrasinais robustas** e distintas en cada páxina. Polo menos con 8 caracteres, combinando maiúsculas, minúsculas, números e símbolos. Sen incluír palabras reais, nin información persoal (nomes, DNI, teléfono, data de nacemento…), nin letras ou números consecutivos (abc, 123).

Ademais, débense coidar, non compartilas con ninguén, nin teclearlas diante doutras persoas ou en equipos públicos. Cambialas de cando en vez, gardalas en xestores de contrasinais, usar teclados virtuais e verificación en dous pasos (se é posible). Configurar as opcións de recuperación (sen respostas sinxelas ás preguntas de seguridade, cun número de teléfono de recuperación).

Nos teus dispositivos móbiles, tablets, computadores:

- **Utiliza usuarios limitados**. Crea para os teus fillos unha conta de usuario estándar (en lugar de utilizar a de administrador).

- **Bloquea o equipo**, **pecha sesión**. Ao afastarse do computador, aínda que sexa un momento, bloquéalo (Win+L) para que ninguén poida acceder á túa información ou se faga pasar por ti no correo electrónico ou as redes sociais. Se é un equipo de uso público acórdache de pechar sesión. En móbiles e tablets configura un patrón de desbloqueo, ou mellor un pin ou un contrasinal.

- **Mantén actualizado o sistema** e todos os seus programas, aplicacións, plugins e complementos. Constantemente aparecen novas ameazas á seguridade dos dispositivos e aplicacións, polo que se deben instalar as actualizacións en canto están dispoñibles.

- **Instala un antivirus**. Tamén en móbiles e tablets. Mantenlo actualizado. Analiza o sistema de cando en vez. Analiza os arquivos que recibas por correo, ou descargues da internet, dunha memoria USB ou unha tarxeta de memoria (como as dos móbiles e cámaras dixitais).

- **Pensa antes de instalar**. Descarga aplicacións só desde fontes oficiais (Google Play en Android, App Store en iOS). Comproba que o que vas instalar é o que necesitas, que non é unha copia falsa ou pirata (pode levar virus). Comproba o desarrollador (é un destacado?), cantas descargas e comentarios ten, os permisos que pide. Durante a instalación, le as opcións para evitar instalar outros programas ou complementos que non desexas.

- **Realiza copias de seguridade periodicamente**. Tanto do sistema, como da túa información (contactos, arquivos, imaxes etc.)/ etc.).

- **Controla as túas conexións**. Protexe a túa Wifi con cifrado WPA2 e cambia as claves por defecto do router. Evita conectarche a redes Wifi públicas. Desactiva Wifi, Bluetooth e NFC cando non os necesites.

Nas túas contas de redes sociais e outros servizos en liña:

- **Determina as opcións de seguridade**. Contrasinais, verificación en dous pasos, as opcións de recuperación de contrasinais, notificacións de inicio de sesión e revísaas para detectar posibles accesos non autorizados.
- **Configura as opcións de privacidade**. Utiliza contas privadas só para os teus amigos en lugar de públicas. Decide se queres mostrar determinada información (localización, hora de última conexión, lista de amigos etc.)/ etc.). Restrinxe as procuras (por exemplo por nome, correo electrónico, ou en buscadores externos como Google ou Bing).
- **Controla a túa lista de amigos**. Pensa antes de aceptar solicitudes de amizade, se de verdade coñécesllle ou é un amigo dun amigo, un contacto virtual... Exponche se queres que esa persoa teña acceso á túa información. De pouco serve ter contas privadas se agregamos a descoñecidos.
- **Ten coidado tanto cos xogos e aplicacións das redes sociais** como con utilizar as túas contas de redes sociais para acceder a outros sitios web. Configura as súas opcións para limitar a difusión da túa información e evitar publicacións automáticas no teu nome.
- **Xestiona as publicacións dos demais**. Acepta ou rexeita as mensaxes ou fotos nos que che haxan etiquetaxe, ou que publicasen no teu perfil.

REACCIÓN

- **Se sospeitamos dun virus**. O dispositivo compórtase de forma estraña, vai moi lento, carga páxinas e publicidade que non desexamos, o sistema cólgase, non arrinca ben.

→ Analízao co teu **antivirus** e/o un antivirus en liña. Se non é capaz de resolvelo automaticamente, pide axuda a un profesional.

- **Se perdemos información**.

→ Recupera os datos da **copia de seguridade**. Se che piden diñeiro a cambio, non cedas á chantaxe, non pagues un rescate e contacta cos corpos policiais.

- **Se nos enganaron para acceder a páxinas maliciosas** que parecían ser as das nosas redes sociais, bancos ou tendas en liña.

→ **Contacta coa entidade para alertala**, bloquear os posibles pagos, solicitar a devolución do roubado. **Cambia os teus contrasinais**, tanto nas devanditas webs, como no resto (especialmente se son contrasinais similares).

- **Se alguén comparte as nosas mensaxes ou imaxes privadas.** Faise pasar por nós en redes sociais, publica no noso nome. Ameázanos ou chantaxea por Internet.

→ **Pídelle que borre as mensaxes** e devólvache a conta. **Repórtao** na rede social para que os eliminen, devólvanche o acceso á conta e bloquéenlle. **Cambia os teus contrasinais** de acceso ás redes sociais e ao resto de servizos. Garda **capturas de pantalla** como evidencia. **Denuncia** nos corpos de seguridade e/o fiscalía de menores.

- Se non o tes claro, o teu problema é distinto, ou simplemente non sabes por onde empezar.

→ **Consulta a nosa liña de axuda** (INCIBE)

Tes dúbidas ou necesitas axuda de maneira máis personalizada en relación co uso seguro e responsable dos menores na internet? Contacta connosco na **Liña de Axuda en Ciberseguridade de INCIBE, 017**. É un servizo gratuíto e confidencial.

A túa Axuda en Ciberseguridade é o servizo nacional, gratuíto e confidencial que INCIBE pon ao dispor dos usuarios da internet e a tecnoloxía co obxectivo de axudarlles a resolver os problemas de ciberseguridade que poidan xurdir no seu día a día. Está dirixido aos cidadáns (usuarios da internet en xeral); empresas e profesionais que utilizan Internet e as novas tecnoloxías no desempeño da súa actividade e deben protexer os seus activos e o seu negocio; e menores e a súa contorna (pais, educadores e profesionais que traballen no ámbito do menor ou a protección en liña ligada a este público).

O servizo é atendido por un equipo multidisciplinar de expertos, a través das diferentes opcións de contacto, que ofrecen asesoramento técnico, psicosocial e legal, en horario de 8 da mañá a 11 da noite, os 365 días do ano.

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

TU AYUDA EN CIBERSEGURIDAD

Teléfono 017

WhatsApp 900 116 117

Telegram @INCIBE017

Formulario web

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

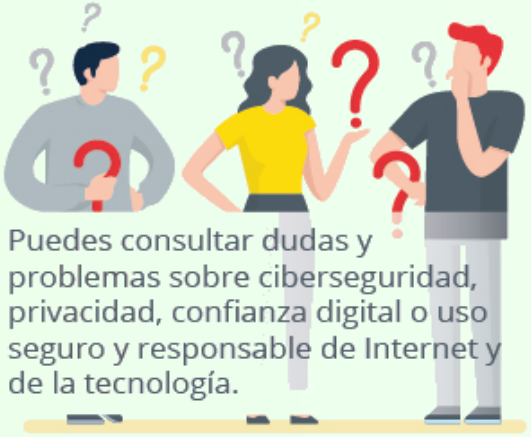
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

TU AYUDA EN
CIBERSEGURIDAD

DESCUBRE EL 017

¡Fácil de usar!

El nuevo número corto de ayuda en ciberseguridad.



Puedes consultar dudas y problemas sobre ciberseguridad, privacidad, confianza digital o uso seguro y responsable de Internet y de la tecnología.

¿En qué podemos ayudarte?

Acude al 017 si tienes dudas, has sufrido un problema etc.

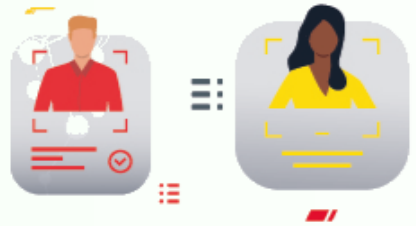
- ¿Quieres configurar la seguridad de un smartphone?
- ¿Necesitas ayuda para proteger tu dispositivo o una red wifi?
- ¿Has recibido un email de origen sospechoso?

- ¿Tu equipo informático ha sido infectado?
- ¿Han suplantado tu cuenta en una red social?

¿Cómo funciona?

365 días
De 9.00 a 21.00 h

Atendido por expertos en ciberseguridad, psicólogos, y asesoramiento legal.



¡Estamos para ayudarte! Llámanos.

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

UAD
Unidade Asistencial de Drogodependencias Monforte de Lemos

WhatsApp

CONCELLO DE MONFORTE DE LEMOS

604 059 719

DÚBIDAS ? *Pregunta e infórmate*

Tabaco, alcol, outras drogas, condutas adictivas

Facebook: UNIDAD ASISTENCIAL DE DROGODEPENDENCIAS DE MONFORTE

Suxerencias e comentarios:
uad@concellodemonforte.com

Se queredes poñervos en contacto connosco, estamos en:

UNIDADE ASISTENCIAL DE DROGODEPENDENCIAS
SERVIZO DE PREVENCIÓN
Plaza da Estación - 17
27400—Monforte de Lemos (Lugo)
Rex. C-27-000100

Facebook:
Unidad Asistencial de Drogodependencias Monforte de Lemos

TLF. 982 40 04 95

CONCELLO DE MONFORTE DE LEMOS
XUNTA DE GALICIA
CONSELLERÍA DE SANIDADE
SERVIZO GALEGO DE SAÚDE
UAD
UNIDADE ASISTENCIAL DE DROGODEPENDENCIAS MONFORTE DE LEMOS

Lembrade que no verán hai moitas outras actividades divertidas sen necesidade de utilizar as pantallas e as redes sociais.

No noso Facebook tamén poderedes ver algunhas ideas para este verán. E se non é verán tamén serven...

Feliz verán