Seguridad en Internet

Ayudemos a navegar a chicos y chicas
con los menores riesgos

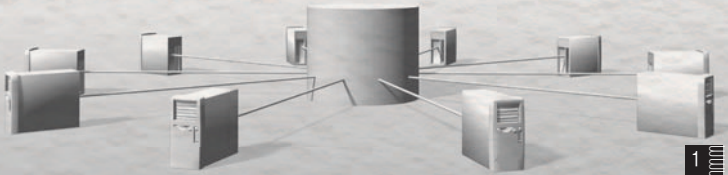
ERREABILITAZIOAN DIREN ARABAKO JOKALARIEN ELKARTEA
ASOCIACIÓN ALAVESA DE JUGADORES/AS EN REHABILITACIÓN

EUSKO JAURLARITZA
GOBERNO VASCO

¿Qué es Internet?

En informática, una red es un conjunto de ordenadores conectados entre sí. Si conectamos todas las redes que hay en el mundo, eso sería Internet.

Por lo tanto, INTERNET ES UNA RED DE REDES. Todos los ordenadores conectados pueden compartir información, archivos, mensajes, fotos... y muchas cosas más.



Para qué sirve Internet

Para mandar y recibir mensajes. Estar en contacto con otras personas.

Para buscar cualquier tipo de información. Temas de interés, contenidos para trabajos escolares, preparación de viajes y excursiones, conocer más nuestro entorno.

Para "conversar" con otras personas (chatear).

Para realizar gestiones desde casa: banco, citas sanidad (médico general, pediatra).

Para jugar: juegos de azar y de dinero, juegos de rol, videojuegos en red...

Algunas palabras

ACCESO.- cada una de las veces que alguien entra en una página web.

ANTIVIRUS.- programa que busca, y si así está indicado, elimina los virus informáticos que pueden haber infectado un disco rígido o disquete.

BUSCADOR.- un servicio que permite a un/a usuario/a localizar páginas web que tienen determinadas condiciones (parámetros búsqueda).

CHAT.- función que permite el diálogo, en tiempo real, entre personas usuarias de diferentes ordenadores. Se comunican a través del teclado.

PASSWORD.- conjunto de letras y números que identifican a los/as usuarios/as.

SPAM.- correo no solicitado, generalmente de tipo comercial.

CIBERBULLYING.- acoso a través de internet.

BLOG O BITÁCORA.- no es más que un espacio personal de escritura en Internet en el que su autor publica artículos o noticias. Están pensados para utilizarlos como una especie de diario on line que una persona usa para informar, compartir, debatir periódicamente sobre las cosas que le gustan e interesan.

Nombres de los buscadores más importantes*.

FORO.- Lugar de Internet donde la gente comparte su opinión, experiencias o dudas sobre cualquier tema. Un foro te permite empezar un tema al que otros/as podrán responder y expresar sus opiniones o contestar a un tema que haya planteado otra persona.

PHISHING.- Correos de entidades bancarias ficticias pidiendo que se proporcionen claves o números de cuenta a los/as usuarios/as para realizar una serie de comprobaciones. Son correos falsos.

Beneficios de Internet

Acceder de forma inmediata a multitud y gran variedad de conocimientos: recursos educativos, actualidad informativa, fotos, documentos, información sobre diferentes temas...

Acceder a toda una serie de información relativa a sus aficiones, cantantes, grupos favoritos, etc.

La dimensión interactiva de Internet les permite intercambiar ideas con interlocutores de cualquier punto del planeta y gozar de una plataforma para expresarse u opinar, experiencias que les pueden resultar gratificantes y enriquecedoras.

Conseguir ayuda para hacer los deberes escolares, ya sea mediante las enciclopedias en línea y otras obras de referencia, o bien contactando con expertos.

Los Riesgos en Internet

VER.- contenidos (textos o imágenes) de carácter denigrante, racista, discriminatorio, sexual, violento...

CONOCER.- En la red hay pederastas que haciéndose pasar por niños o jóvenes se ganan la confianza de los más jóvenes y pueden mantener conversaciones no apropiadas, de contenido sexual, e incluso concertar citas.

HACER.- A través de mensajes, foros, chats, los chicos y chicas pueden entrar en un mundo en el cual se les puede inducir a cometer determinados actos, que en ocasiones pueden ser delictivos.

COMPRAR.- Los chicos y chicas, pudiendo acceder a los datos bancarios del adulto/a o a su tarjeta de crédito podrían acceder a un mundo en el cual se puede comprar de todo, cueste lo que cueste, e incluso llegar a jugar a juegos de azar.

DESCARGAR.- Hay muchas páginas desde las que se pueden bajar al ordenador juegos, música, ficheros, que en ocasiones pueden estar infectados por virus e incluso pueden abrir las puertas a hackers que podrían acceder a nuestros datos más confidenciales.

Reglas básicas para preservar la seguridad de sus hijos e hijas en Internet

✖ Poner el ordenador con acceso a Internet en un lugar común de la casa, para uso común de todos y todas.

El ordenador ha de estar en un espacio común y siempre que sea posible, que la pantalla pueda ser visionada sin dificultad alguna por los padres y madres. Esto permitirá controlar el tiempo de utilización y también los contenidos a los que están accediendo los chicos y chicas. También permitiría observar su comportamiento y en el caso de darse alguna situación problemática (problemas con personas conocidas, situaciones de acoso, acceso a páginas no adecuadas), poder actuar en el momento.

✖ Decidir conjuntamente con los chicos y chicas el tiempo de conexión y los lugares a los que pueden acceder.

Aunque hay autores que sí que determinan una duración de conexión concreta, hay que valorar la edad del chico/a, para qué se está utilizando en ese momento la conexión a internet... Si se está utilizando como ayuda a un trabajo escolar dependerá de la necesidad en la búsqueda de información. Si quiere información sobre su grupo de música o solista favorito, o sobre temas relacionados con el deporte, también se puede negociar un tiempo que

consideremos oportuno teniendo en cuenta, por ejemplo, cuánto tiempo les permitiríamos oír música o leer una revista específica sobre el deporte que le gusta. En cuanto a la mensajería instantánea, o el Messenger, podría tenerse en cuenta el tiempo que permitirían hablar por teléfono a los chicos y chicas con una tarifa reducida.

✖ Ayudar a los chicos y chicas a entender que nunca han de citarse con una persona que hayan "conocido" a través de Internet (ni solos ni sin el conocimiento de sus padres).

Hay que enseñar a los chicos y chicas que la gente desconocida con la que se habla en la red puede no ser la persona que dice ser. No se ha de dar información sobre uno/a: dónde vive, su teléfono, otros datos personales. Y han de aprender una norma fundamental de la navegación segura: NUNCA ENCONTRARSE CON UN PERSONA DESCONOCIDA DE INTERNET SIN UNA PERSONA ADULTA O SIN OTROS/AS AMIGO/AS PRESENTES.

✖ No dar ni mostrar sus contraseñas a nadie (incluso a sus mejores amigos/as).

El hecho de hacerlo puede permitir el acceso de cualquier persona al contenido del ordenador: datos, ficheros privados, contenidos personales... que pueden ser utilizados por otras personas de formas no adecuadas o que pueden sustraer contenidos que son absolutamente privados. También sería conveniente que no dejaran grabada su contraseña en otros ordenadores (p.e., en los cybers). Se podrían dar casos de suplantación.

✖ Nunca enviar fotos a personas desconocidas ni a personas conocidas si no se sabe el uso que se va a hacer de las mismas y siempre con el conocimiento de los padres, tanto del contenido como del destino.

Cuando se remiten fotos a personas desconocidas no se sabe realmente el uso que se va a hacer de las mismas. En ocasiones, éstas solicitan a los chicos y chicas que se hagan fotos en determinadas situaciones, a veces no muy adecuadas, que luego pueden aparecer en ficheros que pueden ser abiertos por multitud de personas. En el caso de las personas conocidas, estaría bien tener claro el uso que se va a hacer de las mismas antes de remitirlas.

✖ No acceder a material enviado por desconocidos/as y no ejecutar ningún archivo de procedencia dudosa.

En ocasiones, los archivos que se pueden remitir contienen virus, troyanos, gusanos... que son programas cuyo objetivo es dañar, de una forma u otra, el equipo infectado. Por otro lado, están los programas espía que pueden instalarse en un ordenador mediante un virus, un troyano, o bien, como generalmente ocurre, estar ocultos en la instalación de un programa gratuito (freeware o adware). Su objetivo es recopilar valiosa información de nuestros hábitos de navegación, sin que nosotros tengamos conocimiento de ello. La información que recopilan los programas espías suele tener un uso estadístico y comercial, valioso para las empresas de publicidad. Pero estos programas pueden, y algunos lo hacen, acceder del mismo modo a información personal que tengamos almacenada (nombre, dirección de correo electrónico...) o incluso a datos vitales como cuentas de usuario y contraseñas.

✖ Enseñar a respetar a los/as demás también a través de la red.

No se ha de permitir que los chicos y chicas utilicen el anonimato que puede ofrecer Internet para hacer y decir cosas que no deberían. Lo mismo que se enseña a comportarse bien en la vida real, del mismo modo ha de ocurrir en la "vida virtual". Y han de tener claro que son responsables de lo que hagan y/o digan.

✖ No efectuar compras "online" sin consultar antes con los padres y madres.

Hay que tener en cuenta que hay timadores/as y especialistas del fraude que se dirigen a la gente más joven teniendo en cuenta que, si se les ofrece algo muy deseado por ellos/as, pueden tener menos cuidado que las personas adultas y ser engañados/as para conseguir los datos bancarios. Sería conveniente tener claro, si se va a comprar, qué y en qué página y estar presentes en el momento en el cual se desarrolle la misma.

Control de acceso a Internet

Es importante señalar que, aunque se opte por el control a través de diferentes programas de filtrado, es muy importante educar a los chicos y chicas sobre la importancia de la seguridad en Internet y cómo hay que aprender a ser responsable ante diferentes páginas y contenidos.

Hay diferentes métodos que permitirán a padres y madres el control del acceso a los chicos y chicas a ciertas páginas y contenidos de Internet. Sería importante que se tuviera en cuenta a cada niño/a a la hora de seleccionar uno u otro sistema.

FILTRO.- Es un programa (software) que permite controlar el acceso a algunos contenidos de internet. El programa bloquearía el acceso a las webs que contienen las palabras o categorías seleccionadas. Otras funcionalidades del mismo es que puede permitir restringir las descargas e incluso limitar el tiempo de navegación de los/as usuarios/as. También permite que se puedan establecer perfiles de configuración del filtro teniendo en cuenta la edad de cada uno de los/as usuarios/as. No obstante hay que tener en cuenta que el filtro es una herramienta que facilita la supervisión de los chicos y chicas pero nunca podrá reemplazar la labor de los padres y madres.

Canguronet (www.telefonicaonline.com)

Optenet (www.optenet.es)

Panda internet Security (www.pandasoftware.com)

Messenger (1)

Es un programa de mensajería instantánea. Los mensajeros instantáneos son un conjunto de programas que utilizan el protocolo TCP IP que sirven para enviar y recibir mensajes instantáneos con otros usuarios conectados a Internet u otras redes, además de saber cuando están disponibles para hablar. Las ventajas que los jóvenes ven en el messenger :

Les permite una comunicación continua, prolongada y económica.

Les permite elegir con quien se habla, mantenerse oculto hasta que interesa "aparecer", ampliar su red relacional.

Les permite estar "pasivamente disponible".

Posibilita para los jóvenes la creación de "otros yo" que pueden actuar como reales y que aspiran a "relacionarse y emocionarse de forma virtual". Para ello, el entorno en el que los jóvenes usan el messenger es en el hogar familiar, donde se sienten seguros y se desinhiben.

Messenger (2)

Es importante educar el uso del Messenger:

Se pueden pactar horarios, distinguiendo los tiempos de estudio y ocio.

Advertir a tus hijos/as del peligro de agregar a personas que no sean de confianza.

Mostrar interés por los nombres y las identidades de sus amigos/as del Messenger (tal como lo hace en la vida real).

Recordarles que no es prudente que den datos personales o familiares a conocidos de confianza que encuentren en el Messenger porque esa información puede ser utilizada por terceros malintencionados.

Tener conversaciones francas y abiertas con los /as hijos/as sobre los peligros que enfrentan y sobre las herramientas que tienen para protegerse. La primera regla de seguridad es: nunca envíe información confidencial por el Messenger: todo lo que se escribe y ve lo puede ver cualquier otra persona.

Enseñarles a cambiar su contraseña con frecuencia es otra medida de seguridad (alguien podría suplantar su identidad).

Coméntales que antes de hablar con una persona que tengan en el Messenger, deben cerciorarse de que realmente está en su PC o puede contestarle, muchas veces el ordenador está encendido pero la persona no se encuentra, y los datos que tu mandes los puede leer cualquiera que se encuentre cerca.

Una cosa es ser ingenuo y otra ignorante.

Los padres deben conocer el mundo en el que viven sus hijos/as.

Riesgos en relación con el uso de Internet

POSIBLES SIGNOS DE PELIGRO

.- Tiempo de permanencia en chats rooms.

.- Fotos de extraños/as descargadas en el ordenador.

.- Llamadas telefónicas, cartas o regalos de extraños/as.

.- Uso de cuentas de Internet de otras personas.

.- Cambios de actitud, deseo de ocultar la actividad que realiza el/la niño/a en la Red.

.- Que apague el ordenador al acercarse otra persona.

La adicción a Internet

.- Preocupación por la red.

.- Necesidad de usar Internet por periodos de tiempo cada vez mayores.

.- Esfuerzos, sin éxito, por controlar, reducir o frenar el uso de Internet.

.- Intranquilidad, malhumor, depresión, irritabilidad, al intentar reducir su uso.

.- No respetar el límite de tiempo de conexión.

.- Pérdida o abandono de alguna relación importante, trabajo o estudios.

.- Mentir a las personas del entorno con el fin de ocultar la afición a la red.

.- Utilizar Internet como una forma de escapar de problemas o aliviar estados de ánimo negativos.

En definitiva

La mejor manera de ayudar a nuestros/as hijos/as a navegar con seguridad es:

.- Que conozcan cuáles son los riesgos y las ventajas de navegar por internet

.- Educarlos/as para que naveguen de manera responsable

.- Darles estrategias para que puedan protegerse

Para ello:

uno. Familiarizarse con internet

dos. Hablar sobre el uso de internet

tres. Navegar juntos/as

cuatro. Tener información sobre instrumentos de control

cinco. Conocer si en el centro donde estudian se sigue alguna política de seguridad

seis. Marcar reglas de seguridad en casa

siete. Poner el ordenador en un lugar donde todos/as lo podemos ver

ocho. Enseñar a los/as menores a navegar con seguridad

nueve. Buscar webs seguras

diez. Reaccionar a tiempo ante un posible problema.

Recursos

Informar, concienciar y formar a Profesores/as y Educadores/as, Orientadores/as, Padres y Madres, Familia en general y a los propios jóvenes sobre los juegos de azar, videojuegos, internet, su uso y los riesgos que puede conllevar el abuso de los mismos.

Ofertar Asesoramiento a los ámbitos escolar, familiar y social, así como al colectivo de jóvenes, ante posibles situaciones de abuso y ante las dudas que pueden surgir respecto al uso del juego y las nuevas tecnologías.

www.onlinezurekin.org

OnlineZurekin
Ludopatiari eta teknologia berriei buruzko aholkularitza
Asesoramiento en Ludopatía y Nuevas Tecnologías