Riesgos de internet en nuestros menores

PLAN DIRECTOR
Para la mejora de la Convivencia y la Seguridad Escolar

Las nuevas tecnologías ofrecen grandes posibilidades y recursos para la satisfacción de nuestras necesidades culturales, educativas, de información y ocio, facilita las relaciones personales y sociales… etc.
Sin embargo, también implican riesgos, especialmente para los niños, los adolescentes y las personas con tendencia al aislamiento.

Debido a que los niños y adolescentes son fácilmente seducibles, su curiosidad o afán de conocer puede llevarles a situaciones comprometidas.
Nos preguntamos, ¿Qué ven? y ¿Con quién se relacionan?

Consejos

Establecer un conjunto de normas sencillas de utilización de Internet, razonables y consensuadas entre padres e hijos, estableciendo una serie de compromisos a nivel familiar adaptados a las edades e inculcar progresivamente valores relacionados con el buen comportamiento, el espíritu crítico y la evaluación de los contenidos consultados.

Ciclo inicial: de 6 a 8 años:

- ✓ Preparar la opción de menú Favoritos (en navegador web Internet Explorer) Fomentar el acceso a Internet desde aquí.

Ciclo medio: de 8 a 12 años

- ✓ ES IMPRESCINDIBLE QUE LOS PADRES PERMANEZCAN CON LOS HIJOS MIENTRAS ESTÁN NAVEGANDO

Todos los ciclos:

- ✓ Los padres deben hacer un seguimiento de las actividades de sus hijos frente al ordenador. Con discreción hacer un seguimiento, sobre el histórico.
- ✓ Enseñar a diferenciar la visión de la realidad que ofrece Internet. Hacer hincapié de que no todo lo que ofrece Internet es fiable.

- ✓ Establecer horarios y límites de conexión a Internet.
- ✓ No comunicar a nadie (ni siquiera amigos y salvo a los padres) el nombre de usuario y contraseña personales explicando las posibles repercusiones.
- ✓ Transmitir la necesidad de autoprotegerse frente a Internet, indicándoles que no faciliten información personal y/o familiar (nombre real, dirección, número de teléfono familiar o móvil personal, centro de estudios, hábitos,...) incluidas

Jorge F.

fotografías o cualquier tipo de documento por correo electrónico con información privada.

- ✓ NO REGISTRARSE CON DATOS REALES y utilizar siempre un “nick”
- ✓ No acordar citas con nadie a través de Internet. Resaltar la peligrosidad que puede suponer concertar un encuentro con algún ‘ciberamigo’ o lo que es lo mismo: un desconocido.
- ✓ Comentar ‘in situ’ y con discreción sobre los contactos de su lista de mensajería instantánea, eliminado los no conocidos personalmente.
- ✓ Mantener la filosofía de que el ordenador es un elemento a compartir y todos los miembros tienen ‘derecho’ a acceder a él y a utilizar los servicios de Internet. Adecuar una zona de acceso abierto de la casa para ubicar el ordenador. **No conviene que el joven disponga de ordenador en su habitación con conexión a Internet.**
- ✓ Incorporar **Filtros de Contenidos**.
  Bloqueo del acceso a páginas con contenido inapropiados.
  Usuarios de Windows: Menores: invitado – adultos: admin con clave.
- ✓ Conocer los lugares que frecuentan y puedan tener acceso libre a Internet (cibercafés, locutorios, bibliotecas, zonas Wifi abiertas…)
- ✓ Incidencia en la necesidad de actuar con respeto y responsabilidad
- ✓ Llevar un control sobre el tipo de descargas y sus contenidos, sin violar las leyes relativas a la propiedad intelectual o que puedan provocar la descarga fortuita de virus
- ✓ Las compras y ventas a través de Internet deben ser conocidas y supervisadas por los padres
- ✓ Transmitir la necesidad de que informen a los padres de comentarios que les resulten incómodos, molestos, si alguien les hace ‘sentir mal’ o reciben amenazas, etc.

Conclusiones:

- La supervisión y consejo de los adultos son esenciales.
- Cuanto más conocen los padres Internet más efectivos son asesorando a sus hijos.
- Se aconseja compartir actividades para intercambiar puntos de vista.
- Converse y establezca reglas con sus hijos (contrato de compromiso padres/hijos)

Precauciones - Seguridad:

Correo electrónico:

- ✓Admitir mensajes sólo de contactos
- ✓Nunca abrir los archivos adjuntos o los enlaces de desconocidos.
- ✓Utilizad en el correo filtros antispam.

Actualizar sistema operativo, navegadores y programas

Firefox + Complementos (Adblock Plus, WOT, NoScript,).
Chrome + Extensiones (AdBlock, WOT)

Antivirus actualizado: Anti-Espías, Anti-Malware

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

oficina de seguridad del internauta (zona de descargas libre y segura)

Cortafuegos o Firewall Activado: Evita ataques externos

WI-FI:

- ✓ Mejor cable-modem del router al PC
- ✓ Cambiar la clave del router por defecto por una clave compleja con caracteres especiales como: +?*<+…
- ✓ ENCRIPTAR con WPA2, mucho más segura que WEP
- ✓ Apagar el router cuando no se usa
- ✓ Con los ordenadores apagados, observar luces router.
- ✓ Filtrado MAC

Protección contra el Phishing

- ✓ Nunca conectar a banca electrónica través de enlace externo (e-mail, mensajes)
- ✓ Asociar móvil a cuenta bancaria para recibir notificaciones de cargos y transferencias
- ✓ No comprar en ordenadores públicos o comprometidos
- ✓ No dar datos de tarjeta ante llamadas recibidas, ni dar datos personales o bancarios a nadie.
- ✓ Usar tarjeta virtual
- ✓ Elija contraseñas seguras y diferentes para cada servicio de Internet.
- ✓ No piense que es inmune al software malicioso porque utilice un determinado sistema operativo o un dispositivo portátil.
- ✓ No confíe ciegamente en las aplicaciones de seguridad instaladas, éstas no remplazan a la navegación responsable ni a la prudencia del usuario.
- ✓ Tapar código tarjeta en cajeros y comercios
- ✓ No perder de vista la tarjeta