Prevención del Delito Cibernético

Objetivo

Fomentar la cultura de prevención en niñas, niños y adolescentes para el uso responsable y seguro del Internet .

Objetivos específicos

- ✓ Capacitar a los maestros sobre las modalidades del Delito Cibernético.
- ✓ Informar y sensibilizar a la población estudiantil acerca de los riesgos que existen al proporcionar información personal en Internet.

Delito Cibernético

Actos realizados a través de las computadoras, sistemas informáticos u otros dispositivos electrónicos de comunicación vía Internet, con la finalidad de cometer un delito.

Actividades más comunes realizadas en internet

Correo electrónico - MSN

Juegos en línea

Redes sociales

Investigación

Bajar o subir videos / música

Programas maliciosos (Malware)

- Correo basura (Spam)
- Gusano (Worm)
- Virus
- Puerta trasera (Trojan)
- Registrador del teclado (Keylogger)
- Programa espía (Spyware)

http://support.kaspersky.com/sp/faq/?qid=193238745

Recomendaciones para navegar seguros en Internet

- ✓ Antes de publicar información personal verifica que la página sea de confianza y que cuente con medidas de seguridad,
- ✓ Instala un Antivirus y actualízalo con frecuencia,
- ✓ Pon especial atención en el tratamiento de tu correo electrónico,
- ✓ Escoge contraseñas seguras que contengan letras y números. Cámbialas frecuentemente.

Sitios que pueden ser peligrosos

Redes Sociales

Programas de Mensajería instantánea simultánea

Te contactan con engaños

Proporcionas datos personales

Intercambias fotografías

Puedes ser víctima de:

Pornografía Infantil

Comercio Sexual Infantil

Maltrato Infantil

Abuso Sexual

Narcomenudeo

Factores de riesgo

- Proporcionar datos personales a desconocidos.
- Entrar a páginas que no cuentan con medidas de seguridad.
- Abrir correos de personas desconocidas.
- Participar en cadenas electrónicas.
- No actualizar el programa de antivirus.
- No tener una buena comunicación con la familia.
- Baja supervisión parental al navegar en la Web.

Modalidades que pueden dañar tu integridad

Ciberbullying: Es el uso de los medios electrónicos (Internet, telefonía celular y videojuegos On-line) para ejercer el acoso entre iguales.

Grooming: Acciones de seducción, creación de empatía o manipulación por parte de un adulto, dirigidas a niñas, niños y adolescentes con el objetivo de obtener videos o fotografías de índole sexual, o incluso buscar el posible contacto físico.

Sexting, una conducta de riesgo

Sexting: El Sexting es un neologismo (Sex: sexo y Texting: mensajería) para referirse al envío de contenidos eróticos o pornográficos por medio de teléfonos celulares.

Recomendaciones para el uso seguro de las redes sociales y programas de mensajería instantánea

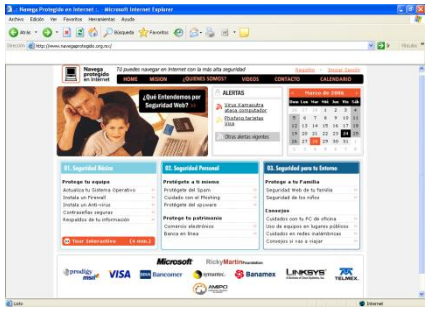
- Si publicas datos, que éstos no pongan en riesgo tu integridad o la de tu familia,
- En ningún momento te muestres con poca ropa o desnudo frente a la Web Cam,
- Configura la privacidad de tu perfil para que controles su acceso,
- No aceptes invitaciones de personas que no conoces,
- Bajo ninguna circunstancia aceptes una cita con personas desconocidos.

Recuerda: Cuando subes información o imágenes a la Web, ya no tienes el control de ellas ni las puedes borrar.

La escuela como factor de protección

Si quieres saber más.

http://asi-mexico.org/sitio/



www.navegaprotegido.org

www.cibercentinelas.org

www.enlaredprotege.org

www.internetsegura.cl

www.pantallasamigas.net

www.pegionline.eu

www.protegeles.com

www.segukid.es