

USO SEGURO Y RESPONSABLE DE TIC



IDENTIDAD DIGITAL



Es el rastro que cada usuario de Internet deja como resultado de su interrelación con otros usuarios o con la generación de contenidos

Actividad: Busca en Internet tu nombre y apellidos. Tras esta búsqueda cuéntanos que pueden ver los demás de ti en la red

GESTIÓN DE LA PRIVACIDAD

"control de la información personal que posee un determinado usuario que se conecta a Internet, interactuando por medio de diversos servicios en línea con los que intercambia datos durante la navegación"

Llevar a cabo una buena gestión de la misma es muy importante para evitar cualquier tipo de problema o estafas.



PROTEGER LA PRIVACIDAD DE LOS MENORES

CIRCULAR PARA LAS FAMILIAS DEL CENTRO EDUCATIVO:

<http://lasreflexionesdeedu.blogspot.com.es/2016/04/datos-personales.html>

Legislación:

<http://www.madrid.es/UnidadesDescentralizadas/InfanciayFamilia/Destacamos/Legislacion%20Infancia%20y%20Familia/Ley%20Derechos%20Infancia.pdf>



SUPLANTACIÓN DE LA IDENTIDAD



SUPLANTACIÓN DE IDENTIDAD EN INTERNET

Suplantación de identidad: consiste en la apropiación de derechos y facultades propias de la persona suplantada (por ejemplo, acceder a la cuenta de una red social).

Usurpación de la identidad: consiste en que una vez suplantada la identidad se empieza a interactuar como si realmente fuera propietario de esos derechos y facultades (por ejemplo, realizar comentarios o subir fotografías).

Ambos constituyen una apropiación de derechos y facultades que proceden de la persona perjudicada siendo éstos de uso exclusivo de la misma, como pueden ser sus datos personales, su imagen o su propio nombre y apellidos.

¿CUÁLES SON LAS PRINCIPALES FORMAS DE SUPLANTACIÓN DE IDENTIDAD ENTRE MENORES?

- a) Entrar sin consentimiento en la cuenta de otro menor para acceder a información sensible.
- b) Entrar sin consentimiento en la cuenta de otro menor para acosar o desprestigiar
- c) Hacerse pasar por otra persona
- d) Ganarse la amistad para cometer grooming
- e) Todas son correctas

TÉCNICAS MÁS USADAS PARA LA SUPLANTACIÓN DE IDENTIDAD

Phishing: fraude por suplantación de identidad, una técnica de ingeniería social.

Pharming: el ciberdelincuente infecta el ordenador del usuario de forma que se acaba redireccionando el tráfico web de una página legítima, utilizada habitualmente por el usuario, hacia otra página falsa creada por el ciberatacante.

SMiShing: por medio de mensajes SMS, se solicitan datos o se pide que se llame a un número de teléfono o que se entre a una web.



MEDIDAS A TOMAR EN CASO DE DETECTAR UNA SUPLANTACIÓN DE IDENTIDAD

Denunciarlo ante la plataforma o el servicio a través del cual haya tenido lugar

Denunciarlo a las Fuerzas y Cuerpos de Seguridad del Estado con pruebas y evidencias <https://www.osi.es/es/actualidad/blog/>

Informar a los buscadores que están enlazando

Cambiar todas las contraseñas



PAUTAS DE PREVENCIÓN

- Limitar la difusión de datos personales y privados
- Configurar opciones de privacidad
- Ser discretos publicando fotos
- Pensar antes de publicar
- Valorar las posibles consecuencias
- Mantener un equipo seguro (actualizar software y antivirus)
- Contar con cuentas de usuario limitadas
- Bloquear ventanas emergentes.
- Hacer uso de filtros anti spam
- Gestión adecuada de contraseñas
- Precaución de enlaces sospechosos, descargas, ficheros, correos desconocidos...
- Descargas en páginas oficiales
- Segundos factores de autenticación o verificación
- Bloquear el ordenador y cerrar sesiones
- Precaución con ordenadores y redes wi-fi públicas
- Contraseñas de bloqueo

<https://www.youtube.com/watch?v=2TferQprZ0g>



Actividad 1: JUEGO Y ANIMACIONES PARA TRABAJAR EN GRUPO COOPERATIVO Y GRUPO GRANDE <http://www.cuidatuimagenonline.com/>

Actividad 2: Se puede utilizar una plantilla en la que haya que completar información personal tal como nombre, apellidos, cumpleaños, dónde vivo y con quién, colegio, nombre del mejor amigo/a, comida favorita, libros interesantes y hobbies. Para ello los niños reflexionaran sobre lo que quieren y no quieren compartir con sus compañeros de clase. Además pueden pegar una foto o un dibujo de ellos mismos.



BÚSQUEDA, CREACIÓN Y USO DE CONTENIDOS DIGITALES EN INTERNET



BRAINSTORM

Riesgos de los juegos

Modelos corporales que promueven la salud

Ser crítico con la información

Estilos de vida y hábitos saludables

Preguntar y dialogar con los adultos



PROTECCIÓN ANTE VIRUS Y FRAUDES



RIESGOS DE LOS VIRUS EN INTERNET

Corromper o borrar información

Impedir el uso de programas o del PC

Obtener información:

- datos bancarios y TC
- información personal y contraseñas
- fotografías
- uso webcam
- suplantación de identidad...



MÉTODOS DE INFECCIÓN

Infección por archivo/programa malicioso

Infección por visitar una web

Infección por pulsar un enlace

Infección por conectar dispositivos externo

Ingeniería social (*estrategias de engaño*: ver una foto, problemas de mantenimiento, ver quién visita tu perfil...)



TIPOS DE FRAUDE ONLINE:

Rogues : falsos antivirus

Phishing: robo de contraseñas personales y credenciales bancarias

Redes Zombie: red de ordenadores que llevan a cabo una acción de forma conjunta

SMS Premium: envío de mensajes *SMSPremium*

¿QUÉ HACER SI EL DISPOSITIVO SE HA INFECTADO?

1. Dejar de utilizar el dispositivo.
2. No realizar ninguna actividad que pueda suponer riesgo de pérdida de información.
3. No realizar compras por Internet con el dispositivo infectado.
4. No acceder al correo electrónico, redes sociales u otro servicio que requiera introducir datos de usuario y contraseña.
5. Eliminar de los navegadores los certificados digitales instalados
6. Hacer una copia de seguridad de todos los datos críticos a una unidad externa analizadas con un antivirus
7. Escanear el dispositivo con un antivirus online.
8. Escanear el dispositivo con herramientas *Anti Malware* y *AntiSpyWare*.
9. En caso de duda, es recomendable llevar el ordenador o dispositivo a un servicio técnico.

MEDIDAS PREVENTIVAS

Verifica los enlaces cortos antes de acceder a ellos

Verifica los programas antes de instalarlos

Ten cuidado con las preguntas de seguridad

No abrir mensajes provenientes de una dirección electrónica desconocida.

Evitar la navegación por páginas webs sospechosas

Configurar adecuadamente la privacidad en las redes sociales

Utilizar navegadores seguros como Google Chrome, Mozilla Firefox, Opera o Safari.



Netiqueta 



DEFINICIÓN

Código social de Internet basado en un principio fundamental:

“Nunca obres con los demás lo que no
quieras que obren contigo” Confucio.

Este término surge para establecer unas normas de buenas maneras a tener en cuenta en el uso de Internet.

Estas normas se pueden comparar con las reglas de etiqueta del mundo real.

<http://lasreflexionesdeedu.blogspot.com.es/2016/04/buenas-tardes-estainfografia-sobre-la.html>



TECNOADICCIONES



TECNOADICCIONES

¿QUÉ SON?

“Las tecnoadicciones se describen como una inclinación desmedida respecto al uso de las tecnologías, las cuáles limitan la libertad del ser humano por la gran dependencia que provocan”.



DESCUIDO INTERESES Y RELACIONES

PÉRDIDA ACTIVIDADES HABITUALES

DESCONTROL CONDUCTA



DEPENDENCIA

ABSTINENCIA

TOLERANCIA.

ACTITUD DEFENSIVA

NEGACIÓN DEL PROBLEMA...

RECOMENDACIONES PARA LOS MENORES

- 1. Durante el fin de semana puedes conectarte más tiempo, pero no más de una hora seguida.**
- 2. Ponte un horario de uso, como lo haces para cualquier otra actividad.**
- 3. No debes conectarte todos los días. Dos días como máximo entre lunes y viernes.**
- 4. Controla el tiempo que estás conectado. No más de una hora seguida. Respeta los horarios de dormir, comer y obligaciones domésticas.**
- 5. Antes de conectarte, piensa qué vas a hacer en Internet.**
- 6. Busca actividades alternativas a Internet para ocupar el tiempo libre.**
- 7. No debes conectar los programas de mensajería instantánea ni redes sociales mientras utilizas el ordenador para los trabajos del cole.**
- 8. Confecciona un registro donde anotes todas tus actividades y también la conexión a Internet (día, hora y tiempo de la conexión).**

COMUNIDADES PELIGROSAS EN INTERNET



<https://youtu.be/jJvPLhc1rTg>

¿QUÉ SON?

Las comunidades en línea son un grupo de personas que carecen de un lugar físico, cuyas interacciones están marcadas por intereses comunes y que tienen una identidad dentro de un espacio de Internet y éstas se convierten en un riesgo en el momento en el que el contenido es inapropiado para los menores o se trata de comunidades peligrosas.



PRINCIPALES TIPOS DE COMUNIDADES PELIGROSAS

Comunidades pro-anorexia y pro-bulimia

Comunidades que fomentan la autolesión "self-harm"

Comunidades que fomentan el odio "*hate-speech*"

Comunidades que promueven hábitos de vida no saludables

Comunidades que realizan apología del suicidio

Comunidades que realizan apología de la pedofilia

Comunidades relacionadas con juegos online.



¿DÓNDE ESTÁN?

Webs propias

Foros

Blogs

Redes sociales

Canales YouTube

Mensajería instantánea...



REDES SOCIALES Y DISPOSITIVOS MÓVILES

¿Por qué accedemos?

¿Cuándo lo hacemos?

¿Cuánto tiempo le dedicamos?

¿Saber proteger tu privacidad y la de otros?

¿Pides ayuda a un adulto cercano?

¿Conoces los peligros?



CIBERACOSO



<https://youtu.be/tX4WjDr5XcM>

¿QUÉ ES EL CIBERACOSO?

«el daño intencional y repetido infligido por parte de un menor o grupo de menores hacia otro menor mediante el uso de medios digitales».



10 CONSEJOS BÁSICOS CONTRA EL CIBERBULLYING

No contestes a las provocaciones, ignóralas. Cuenta hasta cien y piensa en otra cosa.

Compórtate con educación en la Red. Usa la Netiqueta.

Si te molestan, abandona la conexión y pide ayuda.

No facilites datos personales. Te sentirás más protegido/a.

No hagas en la Red lo que no harías a la cara.

Si te acosan, guarda las pruebas.

Cuando te molesten al usar un servicio online, pide ayuda a su gestor/a.

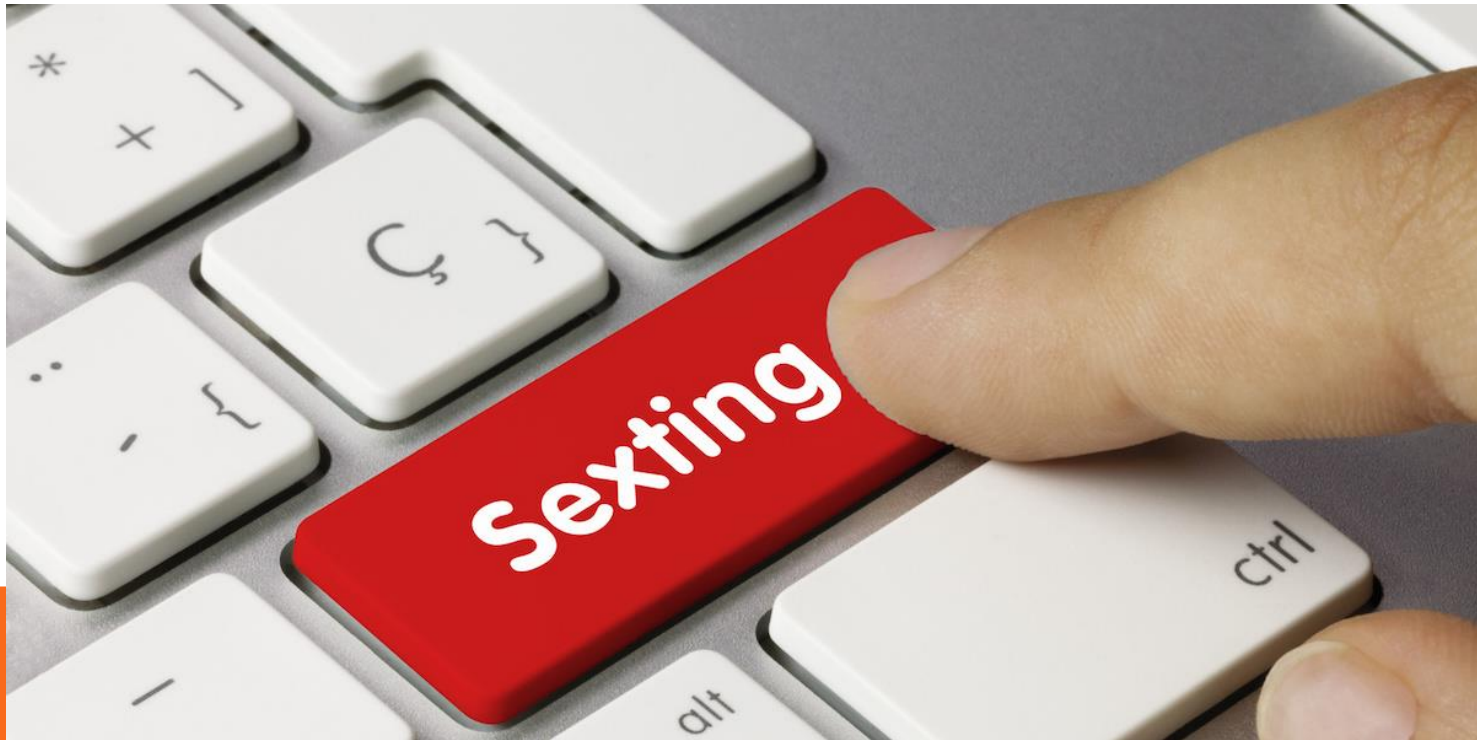
No pienses que estás del todo seguro/a al otro lado de la pantalla.

Advierte a quien abusa de que está cometiendo un delito.

Si hay amenazas graves pide ayuda con urgencia.



SEXTING



¿QUÉ ES?

«difusión o publicación de imágenes o vídeos de tipo sexual, producidos por el propio remitente, principalmente a través del teléfono móvil o por otros»

Sexting Activo

El protagonista de dichas imágenes aparece en fotos o vídeos en posturas sexys, provocativas o inapropiadas.

Sexting Pasivo

Acto de recibir las imágenes sin que seamos el protagonista de las mismas.



RIESGOS

Humillación y linchamiento social

Exposición al insulto público

Indefensión y culpa

Efectos psicológicos (tristeza, depresión, suicidio...)

Efectos en el entorno próximo

Ciberacoso y/o grooming

Geolocalización y riesgos físicos

Riesgo para la protección del honor, la intimidad y la imagen

Consecuencias legales



CONSEJOS PARA EL BUEN USO DE LA WEB CAM: <https://youtu.be/FLKR5aq3Zbw>

PAUTAS PARA LOS MENORES

- Conocer el nivel de seguridad y privacidad de los dispositivos y aplicarlo de manera responsable.
- No ceder ante la presión ni el chantaje.
- No ser partícipe del sexting: ni creándolo, ni reenviándolo, ni fomentándolo.



¿QUÉ HACER ANTE UN CASO DE SEXTING?

¡ NUNCA DUDES EN HABLARLO CON UN ADULTO PRÓXIMO! ÉL O ELLA TE AYUDARÁN
PARA DENUNCIARLO Y PONERLE FIN

http://www.policia.es/org_central/judicial/udef/bit_alertas.html

https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

¡ ELLOS PUEDEN AYUDARTE!



GROOMING



¿QUÉ ES EL GROOMING?

El grooming, es un tipo de ciberacoso ejercido deliberadamente por un adulto para establecer una relación y un control emocional sobre un menor con el fin de conseguir un beneficio sexual

<https://youtu.be/Pa2ttVRA-xU>



MODOS MÁS UTILIZADOS POR EL *GROOMER* PARA CONTACTAR Y ACOSAR AL MENOR

Redes sociales

Foros y chat

Plataformas de juegos en línea

Teléfono móvil

Webcam

