

**Solucionario. Actividad 3****Normas para prevenir los virus**

- No conectar a tu ordenador un pendrive o memoria USB que consideres infectados con algún virus.
- No utilizar software "pirata" de dudosa procedencia.
- No abrir emails ni archivos adjuntos que procedan de una persona desconocida.
- Revisar con atención los documentos descargados y no permitir la ejecución de macros internas al abrirlos.
- Mantener al día las actualizaciones del sistema operativo.
- Asegurarse de que está activo el firewall del sistema operativo para filtrar el tráfico del equipo con Internet.
- Instalar en el equipo un buen programa antivirus y mantenerlo siempre actualizado.
- Cuando se sospeche de la existencia de una infección, actualizar el programa antivirus y escanear todas las unidades de disco.

**¿Cómo defenderse del ciberbullying?**

- Trata de ignorar las provocaciones.
- Lo que se hace en Internet también tiene consecuencias.
- Quien abusa está cometiendo un delito.
- Si consideras que te acosan, conserva las pruebas: emails, capturas de pantalla, etc.
- Si te molestan de forma intencionada y reiterada, pide ayuda a tus mayores o al profesorado.
- Si recibes amenazas graves, solicita esa ayuda con urgencia.

**¿Cómo prevenir el grooming?**

- No proporcionar imágenes, vídeos o informaciones personales a personas desconocidas.
- No dar las contraseñas del equipo a nadie para evitar el robo de información.
- Mantener la privacidad de las imágenes e informaciones personales.

**¿Qué hacer ante un caso de grooming?**

- No ceder al chantaje en ningún caso.
- Pedir siempre ayuda a tus mayores o al profesorado.
- Revisar el equipo con un programa anti-malware.
- Modificar todas las contraseñas de acceso.
- Aumentar las opciones de privacidad de tu perfil en las redes sociales.
- Buscar y guardar las pruebas del chantaje: capturas de pantalla, conversaciones, mensajes, etc.

**¿Cómo evitar la sextorsión?**

- Evita el envío de fotos comprometidas a tu pareja. El afecto se puede demostrar de otras formas. Piensa que puede utilizarla de forma no adecuada cuando vuestra relación haya terminado.
- Reflexiona sobre las posibles consecuencias derivadas del envío de una foto personal comprometida a cualquier otra persona, sea conocida o no.

**¿Cómo evitar la usurpación de identidad?**

- Nunca comuniques a nadie tus contraseñas.
- Evita que nadie te mire cuando introduzcas la contraseña.
- Utiliza contraseñas seguras evitando aquellas cortas o triviales.
- En los ordenadores de uso público o del centro recuerda cerrar la sesión. No almacenes las contraseñas.

**¿Qué debes hacer cuando detectes una usurpación de tu identidad?**

- Cambia rápidamente la contraseña de acceso, si sospechas que está siendo utilizada.
- Si ya no puedes entrar porque te han cambiado la contraseña, denúncialo a tus mayores o al profesorado.

- Trata de reparar y explicar a las personas afectadas lo que han realizado en tu nombre.
- Si alguien se hace pasar por ti creando una cuenta similar a la tuya, denúncialo.

#### ¿Cómo evitar el phishing?

- Nunca responder a ninguna solicitud de datos personales usando el correo electrónico, los sms o las llamadas telefónicas. Las entidades u organismos nunca solicitan esta información por estos medios.  
Ellos ya tienen tus datos y en todo caso es la persona usuaria quien puede llamar para solicitarlos en caso de olvido o pérdida. Pero no al revés. Es cuestión de sentido común.
- Desconfiar de la dirección de sitio web o página contenida en un mensaje sospechoso. Normalmente se parecen a la dirección original del banco o entidad que dicen ser, pero no es igual.
- Asegurarse de que el acceso a la gestión de bancos por Internet se hace en una página de navegación segura HTTPS://. Este sistema exige que la entidad bancaria disponga de un certificado de seguridad y cifrado seguro que garantiza su autenticidad al cliente.

#### Síntomas de la ciberadicción

- Dispersión de la atención: se plantean varias tareas a la vez sin centrar la atención ni terminar ninguna de ellas.
- Búsqueda de satisfacción: se buscan constantemente contenidos relacionados con ciertos gustos o adicciones: juegos, temáticas, etc.
- Adaptación al estímulo: con el tiempo se buscan cada vez contenidos más estimulantes para alcanzar el mismo efecto.
- Creación de distintas identidades: se accede a un foro o chat con distintas identidades o personalidades.
- Del mundo real al virtual: se va sustituyendo el mundo real por el virtual abandonando las amistades reales y buscando solamente amistades a través de la red.
- Pérdida de la noción del tiempo: se conecta para una tarea determinada pero se termina dedicándole mucho más tiempo.
- Conexión compulsiva: se siente la necesidad de conectarse muchas veces al día, aunque sea durante un corto periodo de tiempo. Esto se suele traducir en no dedicarle tiempo suficiente a otras tareas: deberes, aseo personal, cuidado, comida, vida familiar, etc.
- Síndrome de abstinencia: muestra malhumor y nerviosismo cuando no se puede conectar como consecuencia de un "castigo" o una avería.
- Menos horas de sueño y comida: se prolonga la conexión a Internet por las noches en lugar de dedicarlas a dormir o incluso comer un bocadillo delante de la pantalla para no perder tiempo.

#### ¿Cómo resolver la ciberadicción?

- Acordar un horario concreto y moderado de conexión a Internet
- Concretar las tareas a realizar en Internet antes de conectarse y tratar de mantener la atención en ellas hasta su terminación.
- Moderar el uso de videojuegos en la red. Utilizar Internet para otras tareas más interesantes.
- Es importante hablar con los mayores y el profesorado. Te pueden ayudar a organizar tu tiempo.
- Diversificar tus actividades cotidianas tratando de dedicarle a cada una el tiempo necesario.
- Cultivar a diario las relaciones personales y familiares.
- Respetar las horas de sueño y descanso, así como las comidas acompañado en familia.
- Dedicar el tiempo necesario al estudio y tareas escolares.