GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

red.es

"Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad"

[Red.es]

JUEGOS EN FAMILIA SECUNDARIA (13-17 AÑOS)

PROTECCIÓN ANTE VIRUS Y FRAUDES

JUEGO Nº 1. CAZAVIRUS

Ficha de consulta de la actividad

Recomendado para:	• Jóvenes de entre 13 y 17 años.
¿Cuáles son los objetivos?	• Proporcionar a los jóvenes información sobre los distintos tipos de virus. • Desarrollar conductas que conduzcan a la prevención de infección por virus informático.
¿Qué habilidades se desarrollan?	• Estrategia. • Reflexión. • Valoración de posibilidades. • Razonamiento. • Deducción.
¿En qué consiste la actividad/juego?	• Cada equipo debe adivinar los lugares de la cuadrícula del equipo contrario en la que se encuentran los virus.
¿Cómo trabajamos el conocimiento sobre virus?	• Detectando el conocimiento previo que nuestro hijo/a tiene sobre los tipos de virus existentes. • Proporcionando al menor información sobre el riesgo de los virus. • Motivando al menor a través del juego a conocer los distintos tipos de virus.
¿Qué material necesito?	• Guía para padres sobre tipos de virus. • Anexo 1: Tabla de juego. • Papel y lápiz.
Otros	• Resultados esperados: Concienciar a los jóvenes de los riesgos de los virus y ayudarles a conocer los distintos tipos de virus existentes, así como mejorar su forma de pensar de forma estratégica. • Más información.

Desarrollo de la actividad

Comenzaremos la actividad preguntándole a nuestro/a hijo/a qué tipos de virus conoce y los riesgos que entrañan en cuanto a robo de información, robo de identidad, y daños que pueden causar en los dispositivos. Para poder explicarle mejor los riesgos de los virus, podremos apoyarnos en la guía para padres, madres y tutores sobre tipos de virus y cómo prevenir la infección, así como en los siguientes vídeos:

¿Qué sabemos sobre los virus informáticos?

https://www.youtube.com/watch?v=J0O3D-6kxLI

Cómo saber si tu teléfono móvil tiene un virus

https://es.finance.yahoo.com/video/sabes-si-tu-tel%C3%A9fono-m%C3%B3vil-085818811.html

A través del vídeo podremos establecer un primer contacto con la temática para después explicarle al menor los distintos tipos de virus existentes. Además, por el notable uso que los menores dan de Internet a través del móvil, consideramos interesante ofrecer información sobre cómo podemos detectar si nuestro teléfono ha sido infectado por uno de ellos. Así, nos aseguraremos de contar con la información necesaria para poder comenzar el juego.

Guía para padres, madres y tutores

Entendemos ***virus*** como **"programas informáticos que buscan alterar el funcionamiento de los dispositivos (ordenadores, tabletas, teléfonos móviles, etc.) y en muchos casos, robar información del usuario"**.

Objetivos de los virus:

La mayor parte de los virus actuales tienen un objetivo común: obtener información de los usuarios infectados:

- Datos bancarios.
- Números de tarjetas de crédito.
- Información personal.
- Fotografías.
- Contraseñas de acceso a correo electrónico y redes sociales.
- Uso de la webcam del usuario sin que éste sea consciente de que está siendo grabado**.**

Ataques a terceros

Muchos programas maliciosos permiten tomar el control absoluto del ordenador y realizar cualquier tipo de acción sin conocimiento del usuario, como por ejemplo:

- Suplantación de identidad y envío de correos electrónicos en nombre de la víctima.
- Utilizar el ordenador de la víctima para realizar ataques a otros ordenadores.
- Infectar a otros ordenadores para obtener información de sus usuarios.
- Realizar estafas en las que figurará el ordenador de la víctima (y su IP) como origen del delito.
- Enviar publicidad.

Virus en dispositivos móviles

El riesgo es aún mayor en los dispositivos móviles, ya que estos virus pueden:

- Escuchar y grabar llamadas realizadas y recibidas en los teléfonos móviles.
- Enviar mensajes SMS Premium que incrementarán el coste de la factura.
- Obtener información de la posición geográfica del dispositivo mediante GPS.
- Hacer grabaciones con la cámara y tomar fotos sin conocimiento del usuario.

Y también están a la orden del día otros complementos como las barras de navegación que se instalan por defecto al instalar un programa, y que sin ser virus, obtienen información no autorizada del usuario sobre sus hábitos de navegación, con el objetivo de mostrar publicidad relacionada.

Métodos de infección

Mientras que los primeros virus requerían la acción humana para su propagación (por ejemplo, ejecutando un programa infectado con imágenes), hoy día existen virus que no requieren de esta intervención. En algunos casos, la infección puede llevarse a cabo sin que el usuario sea consciente de ello, simplemente conectándose a una página web infectada, introduciendo un pen-drive USB, o abriendo un correo electrónico que contiene una imagen (aparentemente inocua), pero que realmente contiene código que se ejecuta de forma automática en el momento en que se visualiza dicha imagen.

Los virus informáticos se propagan de ordenador a ordenador, en muchas ocasiones sin la ayuda de una persona, aprovechando una vulnerabilidad del sistema operativo o del navegador para propagarse. Actualmente, los ciberdelincuentes aprovechan fallos de seguridad en plugins y aplicaciones que los usuarios utilizan habitualmente (por

ejemplo, Adobe Flash Player, Java, Acrobat Reader, etc.). Otra estrategia muy habitual consiste en redirigir al usuario a páginas maliciosas a través de enlaces de chats y redes sociales, "invitando a ver un vídeo gracioso" o "fotos de famosas". Lo más peligroso de los virus informáticos es su capacidad para replicarse, por lo que el ordenador de la víctima podría enviar cientos o miles de copias de sí mismo, creando un efecto devastador enorme. Un ejemplo sería el envío de una copia de sí mismo a cada uno de los contactos de la libreta de direcciones del programa de correo electrónico.

Ingeniería social

En los últimos tiempos ha tomado gran relevancia la Ingeniería Social, es decir, embaucar con engaños y manipulaciones a los usuarios para conseguir información que posteriormente será utilizada para llevar a cabo la infección y la sustracción de información (claves de acceso, contraseñas, etc.).

Hoy día son muy comunes las estrategias de engaño en las que se "invita" a la futura víctima a pulsar sobre un enlace que le llevará a una web fraudulenta en la que se intentará infectar su dispositivo (ordenador, tableta o teléfono), o se le solicitarán datos de acceso a sus cuentas bancarias a través de correo electrónico, o incluso se le pedirá que introduzca su clave de usuario y contraseña, alegando un falso mantenimiento del servicio.

Protección antivirus

Ningún antivirus es efectivo al 100%. El antivirus siempre va por detrás del código malicioso. Cada día surgen cientos de nuevos virus en Internet, y el tiempo que transcurre desde que el virus está activo hasta que un antivirus incorpora la información de cada nuevo virus en sus bases de datos, es un tiempo de riesgo y exposición al que todos los usuarios están expuestos.

Los laboratorios de los fabricantes de antivirus analizan cada día miles de patrones de código presuntamente malicioso. La detección de nuevos virus puede ser cuestión de horas o de días, y en ese periodo de tiempo se pueden infectar miles de ordenadores, tabletas y teléfonos.

Contextualizado el menor en la temática de los virus, comenzamos con la actividad, en primer lugar realizaremos la formación de equipos. En función del número de

participantes, pueden formarse equipos de 2-3 jugadores, o bien, se puede participar de forma individual.

Para poder jugar, cada equipo debe contar con dos cuadrículas de 10 filas y 10 columnas como ficha de juego, adjunta como anexo 1. Cada posición en la cuadrícula se identifica con un número para las columnas (del 1 al 10) y con una letra para las filas (de la A a la J). Cada cuadrícula representa un ordenador: el ordenador propio y el ordenador contrario. En una de las cuadrículas, el equipo coloca sus virus y registra los intentos de desinfección del oponente; en el otro, se registran los intentos propios, al tiempo que se deduce la posición de los virus del contrincante.

Cada equipo debe adivinar los lugares de la cuadrícula del equipo contrario en la que se encuentran los virus.

Virus

Al comenzar, cada equipo posiciona sus virus en la primera cuadrícula, de forma secreta, invisible al equipo oponente. Cada equipo ocupa, según sus preferencias, una misma cantidad de casillas, horizontal y/o verticalmente, las que representan sus virus. Ambos equipos deben ubicar igual el número de virus, por lo que es habitual, antes de comenzar, estipular de común acuerdo la cantidad y el tamaño de los virus que se posicionarán en la cuadrícula. El tamaño de los virus se establecerá en función de su peligrosidad. Así, por ejemplo, cinco casillas consecutivas conforman un troyano; tres, un gusano, y una casilla aislada, un *adware*, y los participantes podrían convenir, también a modo de ejemplo, en colocar, cada uno, un gusano, tres troyanos y cinco malware.

Desarrollo del juego

Una vez todos los virus han sido posicionados, se inicia una serie de rondas. En cada ronda, cada equipo en su turno «dispara» hacia la red de su oponente indicando una posición (las coordenadas de una casilla), la que registra en la segunda cuadrícula. Si esa posición es ocupada por parte de un virus contrario, el oponente cantará ¡**Detectado**! si todavía quedan partes del virus (casillas) sin dañar, o ¡**Desinfectado**! si con ese disparo el virus ha quedado totalmente destruido (esto es, si la acertada es la última de las casillas que conforman el virus que quedaba por acertar). Si la posición indicada no corresponde a una parte de virus alguno, cantará ¡**Limpio**!

Cada equipo referenciará en esa segunda cuadrícula, de diferente manera y a su conveniencia, los intentos de desinfección que han caído sobre un virus oponente y los que han no han detectado nada. En la implementación del juego con lápiz y papel, pueden señalarse con una cruz los tiros errados y con un círculo los acertados a una nave, o con cuadrados huecos y rellenos.

El juego puede terminar con un equipo ganador o en empate. Quien descubra y destruya primero todos los virus de su oponente será el vencedor. Como en tantos otros juegos en los que se participa por turnos, en caso de que el participante que comenzó la partida elimine en su última jugada el último virus de su oponente, el otro participante tiene derecho a una última posibilidad para alcanzar el empate, a un último disparo que también le permita terminar de eliminar el virus contrario, lo que supondría un empate. Si bien lo habitual es continuar el juego hasta que haya un ganador, el empate también puede alcanzarse si, tras haber disparado cada jugador una misma cantidad de tiros fija y predeterminada (como una variante permitida en el juego), ambos jugadores han acertado en igual número de casillas contrarias.

Una vez terminado el juego es importante que traslademos al menor la importancia d prevenir y actuar frente a infecciones informáticas. Para ello explicaremos al menor la siguiente guía sobre cómo actuar y prevenir virus informáticos.

Guía para padres, madres y tutores

Recomendaciones evitar infecciones de virus:

- **Mantener actualizado todo el software instalado, el sistema operativo, el navegador de Internet y antivirus**. Es fundamental contar con un antivirus actualizado en todos los dispositivos (ordenadores, tabletas y teléfonos móviles).
- **Utilizar cuentas de usuario limitadas.** Es aconsejable utilizar un usuario con permisos restringidos que no pueda instalar programas. De ese modo, si se cuela un virus, será más difícil que pueda instalarse. Las cuentas de usuario con permisos de administración sólo deben utilizarse para instalar aplicaciones, o para cambiar la configuración del equipo.
- **Verificar los enlaces cortos antes de acceder a ellos**. Los enlaces cortos, empleados especialmente en pantallas móviles para ahorrar en caracteres, se configuran como un caldo de cultivo perfecto para ataques de *phishing*, ya que el usuario no sabe hacia dónde apunta el enlace. Para poder prevenir este tipo de

riesgos, es interesante que conozcas algunos servicios que permiten previsualizar el enlace antes de acceder al mismo y saber así, previamente, si es el correcto.

- **Evitar la navegación por páginas web sospechosas**. (Programas gratis, juegos gratis, fotos de famosas, etc.).
- **Descargar los programas solo de las páginas oficiales.** Para evitar la instalación de programas manipulados maliciosamente se recomienda descargarlos únicamente de sus páginas oficiales.
- **Ten cuidado con las preguntas de seguridad:** Algunos servicios ofrecen la opción de utilizar preguntas de seguridad para que, en caso de olvido, sea posible recuperar la contraseña. No obstante, algunas respuestas a estas preguntas pueden ser conocidas por personas del entorno. Por ejemplo: ¿Cómo se llama tu mascota? Por esta razón, no es recomendable utilizar preguntas de seguridad con respuestas obvias. Es conveniente establecer respuestas complejas que no puedan ser averiguadas por personas cercanas.
- **Evitar introducir en los equipos medios de almacenamiento extraíbles de dudosa procedencia.** Estos dispositivos se conectan vía USB y pueden ser una puerta de entrada para los virus.

Prevención en el hogar

Las herramientas de Control Parental pueden suponer una gran ayuda para los padres a la hora de evitar que los menores puedan verse involucrados en fraudes electrónicos e infecciones de virus.

Configurar adecuadamente estas herramientas ayudará a prevenir la instalación de aplicaciones infectadas, ya que estableciendo las restricciones adecuadas, se impide que el menor pueda realizar acciones que puedan poner en riesgo la información del dispositivo. Por otro lado, también se podrá evitar el uso no autorizado de la cámara de fotos, el envío de mensajes, o la realización de llamadas.

Estas herramientas también ayudan a controlar y a filtrar la navegación por Internet de los menores, tanto en ordenadores como en tabletas, ya que se pueden establecer restricciones para que no se pueda navegar por sitios web potencialmente peligrosos que pueden contener virus y otros programas maliciosos.

Consejos sobre la instalación de aplicaciones en dispositivos móviles

- Descargar aplicaciones sólo desde fuentes confiables.
    - Play Store para Android.
    - Apple Store para IOS.
    - Marketplace para Windows Phone.
- Sospechar ante un número bajo de descargas.
- Desconfiar si los comentarios son excesivamente halagadores, pues pueden estar escritos por el propio desarrollador o personas de su entorno.
- Comprobar los permisos de acceso al teléfono que se solicitan antes de iniciar la instalación. Por ejemplo, una aplicación de linterna no tiene sentido que requiera permisos para acceder al registro de llamadas.
- Desactivar en los dispositivos móviles la opción Permitir Orígenes Desconocidos ubicada en Ajustes -> Seguridad -> Orígenes desconocidos.
- Instalar un antivirus para dispositivos móviles.
- No utilizar navegadores extraños, ya que pueden contener vulnerabilidades que permitan “a los malos” robar las contraseñas.

¿Cómo saber si un dispositivo está infectado?

- Se abren páginas web que no se han solicitado.
- El dispositivo funciona más lento de lo normal, deja de responder o se bloquea con frecuencia.
- El dispositivo se apaga solo (aun teniendo batería).
- El dispositivo se reinicia cada pocos minutos.
- El dispositivo no se puede iniciar.
- Las aplicaciones no funcionan correctamente.
- No se puede obtener acceso a los discos o a las unidades de disco.

- Aparecen mensajes de error poco usuales.
- Los menús y los cuadros de diálogo aparecen distorsionados.
- La factura refleja llamadas que no se han realizado, mensajes SMS que no se han enviado.
- Alguien responde a un correo electrónico que no se ha enviado.
- Aparecen mensajes de publicidad constantemente.
- Se muestran mensajes o imágenes inesperados.
- Se reproducen sonidos o música inusuales de forma aleatoria.
- El lector de CD-ROM se abre y se cierra de forma misteriosa.
- El antivirus se desactiva solo.
- Los programas se inician de forma espontánea.
- El cortafuegos informa de que algunas aplicaciones intentan conectarse a Internet, sin que el usuario las haya puesto en marcha. Los archivos y carpetas han sido borrados o su contenido ha cambiado.
- El disco duro muestra más actividad de lo normal, aun cuando no hay programas funcionando, (por ejemplo, si la luz en su unidad principal parpadea de forma rápida).

¿Qué hacer si se tiene la certeza de que un dispositivo está infectado?

Ante la evidencia de que un ordenador o teléfono ha sido infectado por un virus, se debe reaccionar rápidamente y llevar a cabo las siguientes medidas siguiendo el orden recomendado:

1. Dejar de utilizar el dispositivo.
2. No realizar ninguna actividad que pueda suponer riesgo de pérdida de información, por ejemplo:
    a. No realizar compras por Internet con el dispositivo infectado.

b. No acceder al correo electrónico, ni a redes sociales, ni a ningún otro servicio que requiera introducir datos de usuario y contraseña.

3. Desconectar el dispositivo de Internet, quitando el cable del router y desactivando la conexión WIFI.

4. Deshabilitar el envío de datos en tabletas y teléfonos.

5. Eliminar de los navegadores los certificados digitales instalados (por ejemplo, el certificado digital de la Fábrica Nacional de Moneda y Timbre que se utiliza para la declaración de la renta, y que identifica al usuario con la misma validez que el DNI).

6. Apagar el dispositivo. Si no es posible apagarlo (por ejemplo, porque es un teléfono y es necesario realizar llamadas) hay que asegurarse de que está desconectado de la red WIFI y del router.

7. Hacer una copia de seguridad de la información importante (fotos, documentos, archivos de trabajo, etc.) Se recomienda hacer la copia de seguridad con el dispositivo apagado, accediendo desde otro dispositivo, siempre que sea posible.

8. Verificar que los datos de la copia de seguridad no están infectados. Existe el riesgo de que al conectar una unidad externa (disco externo, pen drive) para guardar los datos de la copia, ésta también sea infectada.

9. En algunos casos existe la posibilidad de restaurar el dispositivo a los valores de fábrica. Esta opción borrará todos los datos personales y configuraciones, por lo que es altamente recomendable realizar previamente una copia de seguridad.

10. En caso de no poder restaurar el dispositivo a los valores de fábrica, llevarlo a un servicio técnico para que un experto haga una limpieza general, y si es necesario, formatear las unidades de almacenamiento (disco duro, tarjeta SD, etc.) y reinstalar el sistema operativo.

Cómo evaluamos los resultados

El desarrollo de este juego pretende fomentar el trabajo en equipo y reforzar el conocimiento de los distintos tipos de virus en los menores, cómo prevenirlos y cómo actuar frente a ellos.

Padre, madre e hijo/a leerán juntos las recomendaciones para prevenir y actuar en caso de infección de virus. Tras esa primera lectura para confirmar el conocimiento adquirido por ambos realizarán una pequeña ronda de preguntas. Para facilitar la tarea imprimirán las guías para padres, madres y tutores facilitadas. Por turnos los padres/madres e hijos/as se realizarán preguntas de contenido del tipo:

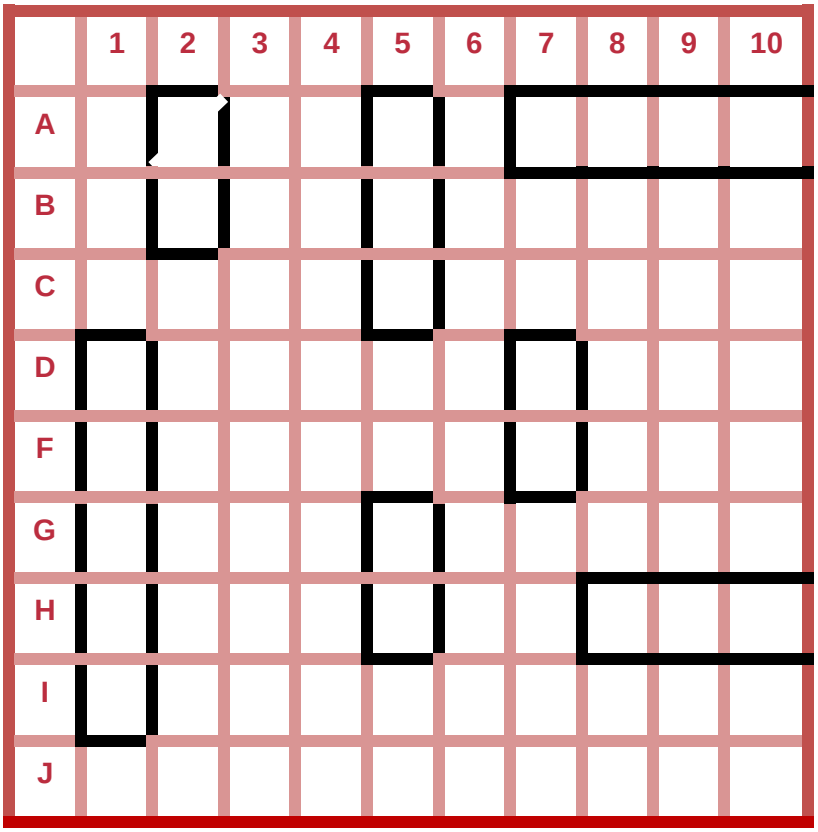
- ¿Qué harías si no puedes restaurar el dispositivo móvil a los valores de fábrica?
- ¿Qué precauciones deberías tener si crees que tu dispositivo ha sido infectado por un virus informático?
- Dime tres indicios que te alerten de que tu dispositivo ha sido infectado por un virus informático.

Según las respuestas de los menores nos indicará aquellos aspectos que será necesario reforzar.

Anexos

Anexo 1.

(Si lo deseas, puedes imprimirlo para utilizarlo como tablero)



Más información

Los siguientes recursos son de utilidad para ampliar el conocimiento sobre protección ante virus y fraudes:

Monográfico de protección ante virus y fraudes

Marco teórico de referencia para aprender herramientas, sistemas y pautas para proteger a los menores ante virus informáticos y situaciones de fraudes por Internet.

Disponible en: http://www.chaval.es

Curso en línea Seguridad TIC y Menores

Curso de 30 horas de duración bajo metodología MOOC (*Massive Online Open Course* - Curso en línea masivo y abierto-) dirigido a padres y educadores. Sensibiliza sobre los riesgos a los que se enfrentan los menores en el uso de Internet y las nuevas tecnologías, ofreciendo estrategias, pautas y recomendaciones para su prevención y respuesta en caso de producirse un incidente. Contiene un módulo exclusivo de protección ante virus y fraudes.

Disponible en: http://www.chaval.es

JUEGO Nº 2. CONTRASEÑAS

Ficha de consulta de la actividad

Recomendado para:	• Jóvenes de entre 13 y 17 años.
¿Cuáles son los objetivos?	• Enseñar a los jóvenes a crear contraseñas robustas con el objetivo de incrementar la seguridad informática de sus accesos a cuentas online.
¿Qué habilidades se desarrollan?	• Estrategia. • Reflexión. • Valoración de posibilidades. • Razonamiento. • Deducción.
¿En qué consiste la actividad/juego?	• El equipo 1 (el menor) debe crear contraseñas robustas que no sean descubiertas por el equipo contrario (padres, familiares o amigos).
¿Cómo trabajamos la construcción de contraseñas robustas?	• Detectando el conocimiento previo que nuestro hijo/a tiene sobre la necesidad de crear contraseñas robustas. • Proporcionando al menor información sobre el riesgo de las contraseñas débiles. • Motivando al menor a través del juego a crear contraseñas robustas que le sirvan en los servicios de Internet y aplicaciones.
¿Qué material necesito?	• Guía para padres, madres y tutores. • Papel y lápiz.
Otros	• Resultados esperados: Concienciar a los jóvenes de la necesidad de crear contraseñas robustas para los servicios que utilizan en Internet, así como ayudarles a mejorar su forma de pensar de forma estratégica. • Más información.

Desarrollo de la actividad

Comenzaremos la actividad preguntándole a nuestro/a hijo/a si sabe construir contraseñas robustas. Para poder explicarle mejor cómo crear contraseñas robustas, podremos apoyarnos en el siguiente material:

Guía para padres, madres y tutores

Gestión de contraseñas: las contraseñas deben ser secretas, robustas y no repetidas.

- **Secretas**. La fecha de nacimiento no es una contraseña secreta para las personas que del entorno (familiares, amigos, compañeros de clase). Es muy importante transmitir esta recomendación a los menores, acostumbrados a compartir las claves con amigos. Si se produce una enemistad, la otra persona tendrá acceso a toda su información.
- **Robustas**. "1234" o "qwerty" no son contraseñas robustas. Es conveniente utilizar combinaciones de mayúsculas, minúsculas, números y símbolos de puntuación, con una longitud mínima de 8 caracteres, y evitar palabras conocidas y nombres propios.
- **No repetidas**. Utilizar la misma contraseña para el correo electrónico, para acceder a las cuentas bancarias, y para acceder a las redes sociales, significa estar poniendo en riesgo toda la información en caso de que alguien descubra (o robe) la contraseña.

Uno de los problemas de utilizar claves demasiado simples, es que existen programas diseñados para probar millones de contraseñas por minuto.

Después de explicarle al menor los conceptos sobre la creación de contraseñas robustas, podremos comenzar el juego.

En esta actividad pueden participar grupos pequeños o grandes. Se deben crear 2 equipos. Un equipo puede estar formado por los adultos (padre, madre o cualquier adulto que desee unirse al juego) y otro por los menores.

Cada grupo debe crear una contraseña lo más robusta posible de no más de 12 caracteres. Para crear la contraseña robusta debemos tener en cuenta las siguientes normas:

- Debe incluir combinaciones de mayúsculas, minúsculas, números y símbolos de puntuación.
- Debe evitar palabras conocidas y nombres propios.
- Debe ser secreta, no repetida y fácil de recordar.

Una vez generada la contraseña por cada grupo se introducen en: https://blog.kaspersky.es/password-check/ para comprobar cuál es más robusta.

La que tarda más tiempo en ser descifrada sería la más robusta, por tanto gana el juego.

EJEMPLO DE CÓMO SE PUEDEN GENERAR CONTRASEÑAS

1. Elegimos una frase que nos resulta fácil de recordar y preferiblemente que contenga mayúsculas, minúsculas, números y símbolos de puntuación: “Mi deporte favorito es la Formula 1.”

2. De esa frase elegimos la primera letra de cada palabra, todos los números y símbolos. Nos quedaría: “MdfeIF1.”.

3. Si la frase que hemos elegido no contiene todas las combinaciones de letras siempre podemos:

- Sustituir una letra por un número. Ej: La letra “e” por un “3”, la “a” por un “4”.
- Sustituir una letra por un símbolo. Ej: La letra “a” o la “o” por “@”.

Cómo evaluamos los resultados

A medida que avance el juego, podremos comprobar si nuestro/a hijo/a es capaz de crear contraseñas robustas. Para comprobar que asimila los conocimientos, cada vez que se proponga una contraseña y se adivine se pueden hacer tres preguntas al menor:

- ¿Era una contraseña secreta? ¿Por qué?
- ¿Era una contraseña robusta? ¿Por qué?
- ¿Coincide con otra contraseña tuya? ¿Por qué?
- ¿Cómo podría haber sido más segura la contraseña propuesta?

Más información

Los siguientes recursos son de utilidad para ampliar el conocimiento sobre protección ante virus y fraudes:

Monográfico de protección ante virus y fraudes

Marco teórico de referencia para aprender herramientas, sistemas y pautas para proteger a los menores ante virus informáticos y situaciones de fraudes por Internet.

Disponible en: http://www.chaval.es

Curso en línea Seguridad TIC y Menores

Curso de 30 horas de duración bajo metodología MOOC (*Massive Online Open Course* - Curso en línea masivo y abierto-) dirigido a padres y educadores. Sensibiliza sobre los riesgos a los que se enfrentan los menores en el uso de Internet y las nuevas tecnologías, ofreciendo estrategias, pautas y recomendaciones para su prevención y respuesta en caso de producirse un incidente. Contiene un módulo exclusivo de protección ante virus y fraudes.

Disponible en: http://www.chaval.es