

CURSO DE SEGURIDAD EN DISPOSITIVOS.

**UNIDAD DIDÁCTICA
PROTECCIÓN
ANTE VIRUS**

Mariajo

M^a JOSÉ MARCOS GURRIONERO

27/01/2017

UNIDAD DIDÁCTICA

PROTECCIÓN ANTE VIRUS

1.- DESCRIPCIÓN.

Nuestros alumnos cada vez utilizan más pronto los móviles y sin conocer ni saber a los riesgos que se exponen en cuanto a los virus y fraudes.

Siendo esta la realidad, es necesario que el alumnado conozca aquellas pautas y herramientas que pueden protegerle de los distintos **virus y fraudes** que circulan por Internet.

2.- OBJETIVOS

El objetivo de esta Unidad Didáctica será orientar el aprendizaje de nuestros alumnos pautas básicas de mantenimiento, actualización y seguridad, introduciéndole en los conceptos de fraude y virus informático.

Informar y capacitar al alumnado para actuar frente a los a virus y fraudes a través de Internet, ofreciéndole recomendaciones, pautas y herramientas para su prevención y/o actuación en caso de verse afectados por ellos.

Conocer qué son y cómo funcionan los virus informáticos y los fraudes para poder prevenirnos ante ellos.

Aplicar medidas y pautas para la protección de ordenadores y dispositivos móviles ante los virus.

3.- CONTENIDOS

- ✓ Conocimiento del concepto de virus (malware)
- ✓ Tipos de virus
- ✓ Medidas de prevención
- ✓ Pautas y recomendaciones

4.- ACTIVIDADES

Actividad 1. Exposición de las diapositivas y diálogo.

Algunas Premisas.

- En España se roba un móvil cada dos minutos¹.
- 279.319 denuncias por sustracción de móviles en 2014.
- En España hay 50 millones de líneas móviles de los que el 81% de los dispositivos son smartphones².
- En España más del 80% de los usuarios de Internet se conecta a través de un dispositivo móvil.

1.- Cinco Días (4-3-2015).
2.- Observatorio nacional de las Telecomunicaciones y de la SI (Abril-2015).



Junta de Castilla y León

Plan de Seguridad y Confianza Digital en el ámbito educativo



Seguridad y dispositivos móviles.

CONDUCTAS DE RIESGO

- Dispositivos desprotegidos.
- Instalación de software de procedencia no certificada.
- Ficheros recibidos a través de redes sociales.
- Respuesta a correo electrónico malicioso.
- Clic en publicidad falsa o engañosa de las apps.
- Páginas web contaminadas.
- Actuaciones del usuario (fotos geolocalizadas,...).

CONSEJOS PARA USO DE MÓVILES Y/O TABLETAS

- Protección por contraseña de acceso.
- Instalar gestor que permita borrar datos.
- Uso de sistema de cifrado.
- Verificación en dos pasos en las cuentas que lo permitan.
- Instalación de Apps de confianza.
- Atención a los permisos solicitados por las Apps.
- Haz un backup de datos e imágenes sensibles periódicamente.

WIFI PÚBLICA

- Conecta la Wifi sólo cuando la utilices.
- No transfieras nunca información sensible con conexión a Wifis públicas o abiertas (correo, cuenta bancaria, compras en línea, redes sociales,...)

CONTRASEÑAS

- Longitud mínimo 8 caracteres.
- Números, letras y símbolos.
- Frase que sólo tú conozcas.
- No almacenar.

GEOLOCALIZACIÓN

- Ten cuidado con las imágenes o videos que publiques o en las que te etiqueten, pueden dar pistas del lugar en el que te encuentras.
- Destruye la información que ofreces de forma pública.

ACTUALIZACIÓN

- Utiliza siempre PIN y bloqueo automático.
- Apaga la pantalla y el dispositivo.
- Utiliza antivirus.
- Mantener el software actualizado.
- Actualiza tus aplicaciones sólo desde sitios oficiales.

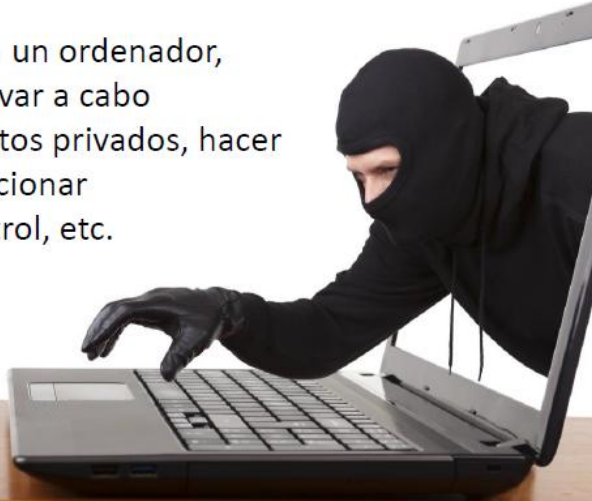
Junta de Castilla y León

Actividad 2. Conocimiento del concepto de virus (malware)

Definición

Malware (virus informático)

Programa capaz de colarse en un ordenador, smartphone o tableta para llevar a cabo **acciones maliciosas**: robar datos privados, hacer que el dispositivo deje de funcionar correctamente, tomar su control, etc.




Ver el video. [Con los dispositivos móviles, ¡mejor no correr riesgos!](#)

Ver el video. [Cuento, Virus Informáticos](#)

Actividad 3. Tipos de virus

Tipos de Virus



VIRUS

Información del perfil

Información Básica
Soy el más viejo de todos mis maltratos compañeros y he sido programado para molestar a los usuarios de ordenadores y demostrar la falta que son mis creadores. Además, sé ponerlos a hacer algo de dinero, ¡paga!

Aficiones


- Facilitar
- Destruir la información de los ordenadores
- Hacer que tu séquito vaya lento

Lugares de Residencia
Siento estar ubicado en los programas que tu ordenador cree que son de fin y así pasar desapercibido hasta que llegue el momento de hacer el mal.

Tiene una relación
Con todo el malware que existe. Pero eso soy su predilección...

No Me Gusta

- Las actualizaciones de seguridad
- Los antivirus
- Las caídas y las precauciones de los usuarios en internet



TROYANOS

Información del perfil

Información Básica
Soy un malware eficaz y muy usado. Mi gran arma es que no soy lo que parece ser.

Aficiones

- Me gusta la leyenda del caballo de Troya
- Darle el control de tu ordenador a mi amo
- Cada vez me gustan más los móviles. Puedo acceder a toda su información.
- Juntarme con otros troyanos y hacer fiestas en las botnets

Lugares de Residencia
Aplicaciones y archivos del sistema operativo.

Orígenes
Provenio de adjuntos de correos y programas que parecen inofensivos

Tiene una relación
Con puertas traseras (backdoors) y otros troyanos en botnets

No Me Gusta

- Los antivirus y anti-troyanos
- Que no se ven de adjuntos sospechosos
- El software legítimo. Yo prefiero programas piratas



Actividad 3.

Ver el video. [Trojanos: malware que abre la puerta a programas que afectan a la seguridad informática](#)



Ver el video. [Virus: malware que infecta y altera el normal funcionamiento de la computadora](#)

Mecanismos y vías de infección



EJEMPLOS

RANSOMWARE. Bloqueo de ficheros. Cifrado datos



Virus de la Policía

EJEMPLOS

Redes zombies



Servicio Antibotnet de la OSI



Actividad 4. Medidas de prevención

Video. [Usa un escudo e impide el avance de los virus](#)

Medidas de prevención

OSI Oficina de Seguridad del Internauta

¿Quieres saber? Encuesta de valoración Contacto Bienvenidos

Ponte al día ¿Qué deberías saber? ¿Cómo protegerte? ¿Necesitas ayuda?

Herramientas

Ponemos a tu disposición una serie de herramientas para que tu navegación por Internet sea más segura y protegida.

Las herramientas están clasificadas en cuatro grandes bloques: "Antivirus, seguridad y protección de acceso", "Privacidad y seguridad de datos", "Mantenimiento" y "Protección, análisis y desinfección". Dependiendo de cuál sea tu necesidad, deberás buscarla en un bloque u otro. Por ejemplo, si lo que necesitas es una herramienta antivirus, entonces deberás dirigirte al bloque "Protección, análisis y desinfección". En cualquier caso, si no encuentras lo que buscas y necesitas ayuda, no dudes en escribirnos a través de nuestro formulario de contacto; nuestros técnicos te guiarán.

ANTIVIRUS, SEGURIDAD Y PROTECCIÓN DE ACCESO

PRIVACIDAD Y SEGURIDAD DE DATOS

MANTENIMIENTO

PROTECCIÓN, ANÁLISIS Y DESINFECCIÓN

Recomendaciones genéricas

Instalaciones seguras

Descargas oficiales

Actualización antivirus

Instalación cortafuegos

Actualización de sistema, navegadores y demás programas

Copias de seguridad

Cifrado de información

Recomendaciones genéricas

Cuentas de uso limitado. Gestión desde el administrador

Buena gestión de contraseñas

Cambiar clave WiFi del router

Precaución al usar dispositivos y wifi públicos

Cuidado con las URL y los enlaces cortos

Evita navegar por webs sospechosas

Configura adecuadamente la privacidad en redes sociales

Evita dispositivos extraíbles de dudosa procedencia

CURSO DE SEGURIDAD EN DISPOSITIVOS.

ALUMNOS DE 4º, 5º Y 6º DE EL MADERAL CRA GUAREÑA ZAMORA

Bibliografía:

Licencia de contenidos



La presente publicación pertenece a **INCIBE (Instituto Nacional de Ciberseguridad)** y está bajo una licencia **Reconocimiento-No Comercial-Compartir Igual 4.0 Internacional de Creative Commons**. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- **Reconocimiento.** El contenido de esta publicación se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a **INCIBE** y su iniciativa **Menores OSI** como a sus sitios web: <https://www.incibe.es> y <https://menores.osi.es>. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- **Uso No Comercial.** El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.
- **Compartir Igual.** Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuirla bajo esta misma licencia.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE como titular de los derechos de autor.

Texto completo de la licencia: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es_ES

La presente publicación sólo refleja las opiniones del autor. La Comisión Europea no es responsable de ningún uso que pudiera hacerse de la información que contiene.

<https://www.osi.es/es>