Seguridad en el uso de las TIC

IES Miguel Hernández

2º ESO

1. Introducción

Como ya sabemos, Internet tiene muchísimas ventajas pero también está lleno de peligros y riesgos. Cuando salimos a la calle estamos atentos de que no nos quiten o se nos pierdan nuestras carteras o monederos donde llevamos toda nuestra documentación, todos esos datos que nos identifican, como el DNI, nuestras fotos, esa entrada de tu concierto favorito, en definitiva protegemos nuestra intimidad. ¿Por qué no hacemos lo mismo en Internet? En la tranquilidad de nuestras habitaciones nos creemos a salvo del mundo, pero en el momento en el que nuestro ordenador se conecta a la telaraña mundial, que es Internet, estamos totalmente desprotegidos, expuestos a millones de riesgos que nos traerán consecuencias graves si no tomamos las medidas oportunas.

2. Tu ordenador: “Un robot clasificador”

Tu ordenador lo apunta todo, guarda todas las páginas web que has visitado, las películas, o la música que has descargado, las búsquedas que has hecho en Google, tu correo electrónico, los datos que has rellenado en algún formulario de inscripción, tus contraseñas, tus conversaciones en las redes sociales..., todo. Nunca olvida nada a no ser que tú se lo digas y lo peor de todo: cualquiera que tenga unos conocimientos mínimos de informática podrá saberlo todo sobre ti y utilizar tus datos de forma inadecuada.

Veamos qué se guarda en cada sitio:

Historial:

Aquí se almacenan la gran mayoría de las páginas web que has visitado. Son algunas de las “huellas” que vas dejando por la Red, así que conviene borrarlas para que nadie las siga.

Cookies:

Son unos **archivos informáticos diminutos** enviados por los sitios web que se almacenan en nuestro navegador y que **obtienen datos sobre nosotros**.

El trabajo de las cookies es "contarles" a las marcas y empresas cómo nos comportamos en internet para colocar anuncios de acuerdo con nuestros gustos e intereses.

Entre otras cosas, pueden recabar este tipo de información:

- direcciones y contraseñas del correo electrónico
- nuestro número de teléfono y dirección
- nuestra dirección de IP
- el sistema operativo de nuestra computadora
- el navegador que utilizamos
- páginas que hemos visitado anteriormente

Archivos temporales:

Las imágenes y contenidos de las páginas web que has visitado se almacenan en nuestro ordenador para así acelerar la carga de la página cuando vuelvas a visitarla. Pero a partir de estos archivos se puede acceder a los datos que has escrito en las páginas web que has visitado.

Ejercicio 1

Abre el navegador Google Chrome, e investiga cómo se eliminan el Historial, las Cookies y los Archivos Temporales. Escribe detalladamente la secuencia de pasos a seguir para conseguirlo en una entrada de tu blog.

Realiza las mismas operaciones para el navegador Mozilla Firefox

3. El ataque de los VIRUS

Ahora ya sabes más sobre tu ordenador, pero todavía no estás a salvo y tienes una nueva misión: no dejar que se convierta en un zombi manejado por extraños y protegerle de todos los peligros que existen en Internet.

Los virus son programas maliciosos creados para manipular el normal funcionamiento de los sistemas, sin el conocimiento ni consentimiento de los usuarios.

Los virus son solo un tipo específico de este tipo de programas. Para referirse a todos ellos se suele utilizar el término **MALWARE** que procede de las palabras en inglés **MAL**icious soft**WARE.**

Los programas maliciosos pueden alterar tanto el funcionamiento del equipo como la información que contienen o se maneja en ella. Las acciones realizadas en la máquina pueden variar desde el robo de información sensible o el borrado de datos hasta el uso del equipo como plataforma para cometer otro tipo de actividades ilegales –como es el caso de las redes zombies-, pudiendo llegar incluso a tener sus respectivas consecuencias legales.

Los programas maliciosos afectan a cualquier dispositivo que tenga un Sistema Operativo que pueda entender el fichero malicioso, es decir:

- Ordenadores personales
- Servidores
- Teléfonos Móviles
- Tablets
- Videoconsolas

Ejercicio 2

Busca en Internet los tipos de malware que existen y crea una nueva entrada en tu blog llamada Ejercicio 2 en la que expliques qué hace cada uno de ellos.

¿Por qué hay gente que crea malware?

En sus comienzos la motivación principal para los creadores de virus era la del reconocimiento público. Cuanta más relevancia tuviera el virus, más reconocimiento obtenía su creador. Por este motivo las acciones a realizar por el virus debían ser visibles por el usuario y suficientemente dañinas como para tener relevancia, por ejemplo, eliminar ficheros importantes, modificar los caracteres de escritura, formatear el disco duro, etc.

Actualmente los programas maliciosos han evolucionado y suelen perseguir un fin lucrativo. Para lograr más fácilmente su cometido suelen pasar desapercibidos para el usuario, por lo que son más difíciles de detectar de forma sencilla. Hay varias formas en las que el creador del programa malicioso puede obtener un beneficio económico, las más comunes son:

- **Robar información** sensible del ordenador infectado, como datos personales, contraseñas, credenciales de acceso a diferentes entidades...
- **Crear una red de ordenadores infectados** -generalmente llamada red **zombie** o botnet- para que el atacante pueda manipularlos todos simultáneamente y vender estos servicios a entidades sin escrúpulos que puedan realizar acciones poco legítimas como el envío de SPAM, envío de mensajes de phishing, realizar ataques de denegación de servicio, etc.
- **Vender falsas soluciones de seguridad** que no realizan las acciones que afirman hacer, por ejemplo, falsos antivirus que muestran mensajes con publicidad informando de que el ordenador está infectado cuando en realidad no es así, la infección que tiene el usuario es el falso antivirus.
- **Cifrar el contenido de los ficheros del ordenador y solicitar un "rescate"** al usuario del equipo para recuperar la información, como hacen los criptovirus o **ramsonware**.

Ejercicio 3

Busca en Internet los virus más peligrosos de la historia y crea una nueva entrada en tu blog llamada Ejercicio 3 en la que expliques qué hacía cada uno de estos virus.

¿Cómo llegan a nuestro ordenador?

Existen gran variedad de formas por las que el malware llega a un ordenador; en la mayoría de los casos son las siguientes:

- **Explotando vulnerabilidades** de las aplicaciones instaladas o del sistema operativo.
- Mediante **ingeniería social.** El eslabón más débil de cualquier sistema siempre es el usuario.
    - En el siguiente vídeo se explica cada uno de los distintos tipos de ataque por Ingeniería Social
        - https://www.youtube.com/watch?v=UW73wlzfpoI
    - En el siguiente vídeo extraído de la serie Mr Robot puedes ver un ejemplo de IS
        - https://www.youtube.com/watch?v=GIlS5eJHYNI

- **Descargar el fichero** desde el correo o desde redes P2P como Torrent.
- **Dispositivos extraíble**s: muchos gusanos suelen dejar copias de sí mismos en dispositivos extraíbles para que automáticamente, cuando el dispositivo se conecte a un ordenador, ejecutarse e infectar el nuevo equipo

Ejercicio 4

Lee el artículo que encontrarás en el siguiente enlace "Ingenieria Social"

Crea una nueva entrada en tu blog llamada Ejercicio 4 en la que expliques qué es la Ingeniería Social. El texto debe tener entre 100 y 150 palabras.

Pon algún ejemplo de Ingeniería Social

4. ¿Cómo protegemos nuestro ordenador?

Las tres herramientas básicas para mantener protegido nuestro ordenador son : Antivirus, Antispyware (antiespías) y Firewall (cortafuegos).

Antivirus

El antivirus es un programa que **ayuda a proteger tu ordenador contra la mayoría de los virus, worms, troyanos y otros invasores indeseados**.

Los antivirus monitorizan actividades de virus en tiempo real y hacen verificaciones periódicas, o de acuerdo con la solicitud del usuario, buscando detectar y, entonces, anular o remover los virus del ordenador.

El antivirus debe ser actualizado frecuentemente, pues con tantos códigos maliciosos siendo descubiertos todos los días, los productos pueden hacerse obsoletos rápidamente.

Ejercicio 5

Busca en Internet los 3 mejores antivirus del 2020.

Crea una nueva entrada en tu blog llamada Ejercicio 5 en la que enumeres las principales características de estos antivirus.

Antispyware (antiespías)

Un spyware es un programa malicioso que se aloja en tu ordenador y envia, sin tu consentimiento, información a terceras personas.

Estos programas maliciosos buscan principalmente recopilar datos sobre tu comportamiento en Internet, qué has comprado online y hasta las teclas que pulsas en el teclado, sí: ¡pueden descubrir tus contraseñas!.

Hay una variante de Spyware llamada “Adware”, que nos sigue por la red para saber nuestras visitas, gustos e intereses, para de esta forma interactuar con nosotros por medio de anuncios de tipo banner.

Un antispyware es una aplicación diseñada para detectar los Spyware y ayudarte a tratar de eliminarlos. Funcionan de forma similar a los antivirus.

¿Cómo reconocer el spyware?

Pueden aparecer iconos nuevos o no identificados en la barra de tareas en la parte inferior de su pantalla, y las búsquedas pueden provocar que se le redirija a un buscador diferente.

El spyware puede bombardearte con publicidad hasta extremos insoportables, cambiar tus resultados de búsqueda de modo que veas más anuncios o saturarte a base de anuncios emergentes.

¿De dónde sale el spyware?

El spyware de móvil o de ordenador suele acabar en los dispositivos de los usuarios cuando descargan juegos o aplicaciones que contienen adware. Las aplicaciones gratuitas son especialmente propensas al adware.

En ocasiones, el spyware forma parte del paquete de instalación y si te limitas a aceptar la información tal cual, sin verificar lo que vas a instalar exactamente, puede que acabes introduciendo spyware en tu

ordenador. Además, cabe la posibilidad de que al hacer clic en un anuncio emergente se inicie una descarga de spyware.

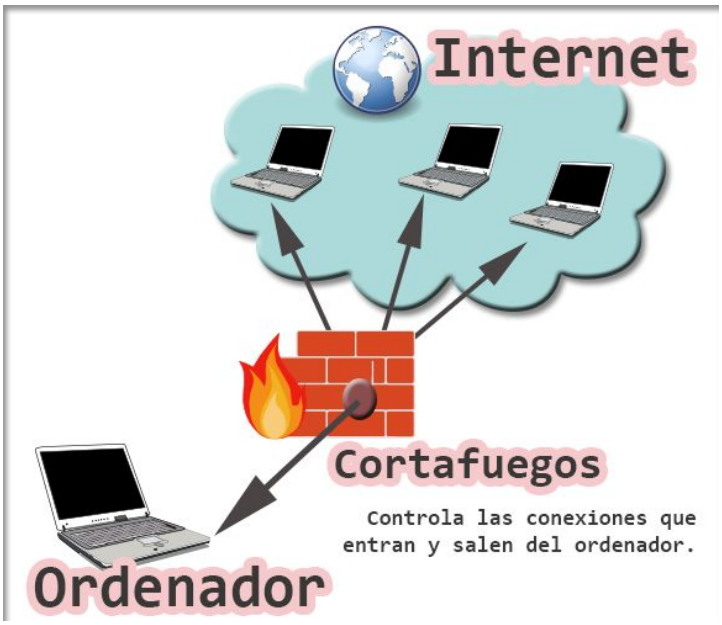
Firewall (cortafuegos)

Es un sistema de seguridad para **bloquear accesos no autorizados a un ordenador** mientras sigue permitiendo la comunicación de tu ordenador con otros servicios autorizados.

Para ello se utilizan una serie de reglas que establecen cómo deben ser tratados los elementos que se envían o reciben en tu ordenador y si estos elementos pueden continuar su camino hasta su destino o deben ser interceptados y devueltos a su origen.

Haciendo una analogía, el cortafuegos es como el portero de una discoteca. Él es quien decide quién entra y quién no.

Si el dueño de la discoteca (el usuario del ordenador en este caso) le ha ordenado expresamente que no puede entrar nadie con zapatillas deportivas, con la cabeza cubierta o con camisa azul, todo aquel cliente que cumpla con alguna de esas características se quedará irremediablemente fuera del local.



5. Seguridad en dispositivos móviles

¿Sabes qué pasa cuando das “Sí, acepto” en una app?

Ejercicio 6

Crea una nueva entrada en tu blog llamada Ejercicio 6 en el que hagas un resumen del vídeo **"¿Sabes qué pasa cuando das "Sí, acepto" en una app?"**

La extensión del resumen será de entre 300 y 350 palabras.

Ejercicio 7

Crea una nueva entrada en tu blog llamada Ejercicio 7 en la que respondas a las siguientes preguntas:

- ¿Qué es el phishing?
- ¿Qué tipos existen?
- ¿Qué riesgos tiene?
- Pon ejemplos reales de cada uno de los tipos de phising

6. Privacidad en Internet

La privacidad en Internet puede resumirse en la siguiente frase: **cuando un producto es gratis, el producto eres tú**.

Ejercicio 8

Visualiza los siguientes vídeos en Youtube:

- La verdad sobre la Privacidad en Internet y la GDPR de Gina Tost
- ¿Por qué me vigilan, si no soy nadie? de Marta Peirano

Crea una nueva entrada en tu blog llamada Ejercicio 8 en la que respondas a las siguientes preguntas:

- ¿Para qué quieren las empresas información sobre mi?
- ¿Qué riesgos tiene el hecho de que exista toda esa información sobre nosotros?

Nuestros datos personales no sólo dicen cómo nos llamamos y dónde vivimos, también hablan de nuestros gustos, aficiones, creencias, etc. Por eso, debemos saber cómo protegerlos.

¿Qué son los datos personales?

Datos que permiten identificar a una persona. Por ejemplo, nuestro nombre, la fecha y lugar de nacimiento, DNI, dirección postal y electrónica, sexo, religión, fotografías, vídeos... incluso nuestra dirección IP.

¿Por qué debemos protegerlos?

Porque si nuestros datos no están protegidos, pueden ser usados de forma fraudulenta. Una persona malintencionada podría suplantar nuestra identidad y hacer cosas como, utilizar nuestros datos bancarios para hacer compras o transferir nuestro dinero a otras cuentas, acceder nuestras cuentas de correo electrónico o hacerse pasar por nosotros en nuestros perfiles de redes sociales.

¿Por qué a las empresas les interesan nuestros datos?

Muchas compañías los utilizan para dirigir publicidad personalizada o para hacer estudios estadísticos sobre nuestros hábitos de consumo o gustos.

Ejercicio 9

Investiga en Internet acerca del proyecto “Sé dónde vive tu gato”.

Crea una nueva entrada en tu blog llamada Ejercicio 9 en la que expliques en qué consiste este proyecto y en los peligros del geoetiquetado.

La extensión de la entrada será entre 150 y 200 palabras

7. Identidad digital

Nuestra vida en Internet es un reflejo de nuestra vida real. Los pasos que damos en una pueden afectarnos en la otra, por eso es importante que conozcamos qué es la identidad digital y cómo podemos protegerla.

La identidad digital toda la información que existe en Internet acerca de nosotros. Es decir, nuestras publicaciones en redes sociales, webs y foros, las noticias y publicaciones oficiales relacionadas con nosotros (como por ejemplo, una multa publicada en el BOE o una beca recibida) así como los comentarios o fotografías donde otras personas nos etiqueten forman un conjunto de información que nos define en la red.

Ejercicio 10

Haz clic en los siguientes enlaces para ver los vídeos

- Tu identidad tiene una parte digital, ¿lo sabías?
- Huella digital. Construir una identidad digital

Después de ver los vídeos anteriores crea una nueva entrada en tu blog llamada Ejercicio 10 en la que respondas a las siguientes preguntas.

- ¿Cómo se crea nuestra Identidad Digital?
- ¿Cómo podemos conocer nuestra Identidad Digital?
- ¿Cómo podemos proteger nuestra Identidad Digital?
- Busca en Google tu nombre y apellidos entre comillas “Nombre Apellido1 Apellido2” y di qué información hay publicada sobre ti

8. Contraseñas seguras

No es buena idea usar tu fecha de nacimiento, de aniversario o el nombre de tu perro como contraseñas. Son fácilmente descifrables mediante un poco de ingeniería social.

Según informes recientes, un 80 % de los ataques debidos a ciberdelincuentes se han servido de contraseñas poco seguras o robadas. Para defenderse, es muy recomendable contar con claves seguras, a ser posible indescifrables. Estas contraseñas se crean combinando letras, números y símbolos y son todavía más seguras si son únicas, es decir, si no se emplean en más de un lugar.

Una forma de mejorar la seguridad de las contraseñas, además de emplear un generador de claves, es activar la **autenticación en dos pasos (2FA).** Si queremos todavía más seguridad podemos utilizar la **autenticación biométrica (huella dactilar, cara, iris, etc…)** aunque en el caso de la huella dactilar es posible hackearla mediante una foto.

En el siguiente vídeo Chema Alonso nos explica cómo pueden copiar nuestras huellas dactilares

https://www.youtube.com/watch?v=DB6UZcjPBCM&list=PLbIOfT2M0M1KszEgugr_y3xbcBa5qupRb&index=31&t=0s

Ejercicio 11

Entra en la web https://password.kaspersky.com/es/ y comprueba cúanto tardaría un ciberdelincuente en averiguar tu contraseña.

Accede ahora a la web https://www.pandasecurity.com/spain/mediacenter/seguridad/10-trucos-para-crear-contrasenas-seguras/

Después de leer los 10 trucos para crear contraseñas seguras de la anterior web crea una nueva entrada en tu blog llamada Ejercicio 11 en la que reflexiones sobre la fortaleza de tu contraseña y pongas un ejemplo de una contraseña segura según la web de Panda Security.

Ejercicio 12

Investiga en Internet sobre la autenticación OAUTH y sobre qué riesgos tiene. Crea una nueva entrada en tu blog llamada Ejercicio 12 con la información encontrada. La extensión de la entrada será de entre 150 y 200 palabras.

Ejercicio 13

Investiga en Internet sobre la autenticación en 2 pasos. Crea una nueva entrada en tu blog llamada Ejercicio 13 con la información encontrada. La extensión de la entrada será de entre 150 y 200 palabras.

Uso seguro de las TIC

Las oportunidades que nos brinda Internet para facilitar muchas de las actividades humanas y contribuir al desarrollo personal de los usuarios son indiscutibles. Entre las más destacadas tenemos:

- **Gran Biblioteca Mundial**. En la web podrás encontrar fácil y rápidamente información sobre los temas más variados.

- **Repositorio de música y películas**. También existen sitios donde se proporcionan archivos de audio (Ivoox, SoundCloud, etc) y de vídeo (Youtube, Vimeo, etc) que se pueden utilizar como fuente de información y de ocio. Además de plataformas donde ver series y películas (Netflix, HBO…).

- **Permite ver TV, leer prensa, escuchar radio, etc**.

- **Gestión de bancos, trámites administrativos, viajes, compras, etc**. Con Internet se ha desarrollado de forma considerable el comercio electrónico que consiste en realizar trámites comerciales usando el ordenador, a cualquier hora y sin salir de casa.

- **Comunicarse con los demás: email, mensajería, foros, etc**.

- **Crear y publicar contenidos: blog, web, red social, servicio de vídeo, etc**.

Pero aunque todas estas ventajas existen, Internet también lleva asociado una serie de riesgos que debemos conocer.

- **Acceso a contenido o imágenes inadecuadas**: Existen webs que pese a contener información científica, pueden resultar inapropiadas y hasta nocivas para niños y menores por el modo en el que se abordan los temas o la crudeza de las imágenes (sexo, violencia, drogas, determinados relatos históricos y obras literarias...). La multimedialidad de Internet puede hacer estos contenidos aún más explícitos e impactantes.

- **Acceso a información peligrosa, inmoral, ilícita.** Existe información poco recomendable(pornografía infantil, violencia, todo tipo de sectas...) y hasta con contenidos considerados delictivosque incitan a la violencia, el racismo, la xenofobia, el terrorismo, la pedofilia, el consumo dedrogas, participar en ritos satánicos y en sectas ilegales, realizar actos delictivos

- **Acceso a información poco fiable o falsa**: Existe mucha información errónea y poco actualizada en Internet, ya que cualquiera puede poner información en la red.

- Fake News:

- **Recepción de "mensajes basura".** Ante la carencia de una legislación adecuada, por e-mail se reciben muchos mensajes de propaganda no deseada (spam) que envían indiscriminadamente empresas de todo el mundo. En ocasiones su contenido es de naturaleza sexual o proponen oscuros negocios. Otras veces pueden contener archivos con virus.

- **Acciones ilegales.** Proporcionar datos de terceras personas, difundir determinadas opiniones o contenidos, plagiar información, insultar, difamar o amenazar a través de los canales comunicativos de Internet... puede acarrear responsabilidades judiciales (como también ocurre en el "mundo físico").

- **Robo de identidad:** Internet es un lugar donde prevalece el cruce desmedido de información, pero debemos ser muy cuidadosos con nuestros datos porque nuestra información personal puede ser fácilmente robada por criminales cibernéticos. Las consecuencias de ser víctima de suplantación de identidad incluyen: mostrar una imagen distorsionada de sí mismo en Internet; ser víctima de burlas, insultos o amenazas, tener un descrédito frente a otros; sufrir una pérdida económica, etc.

- **Adicción**: El uso de internet también puede causar adicción, pudiendo considerar que una persona la padece cuando ésta es incapaz de controlar el tiempo que está conectado. Además de que Internet puede ser usado para potenciar otras adicciones como juego, compras compulsivas, pornografía, etc.

- **Estafas**: El **phishing** es un tipo de estafa que intenta obtener de la víctima sus datos, contraseñas, cuentas bancarias, números de tarjetas de crédito o del documento nacional de identidad, etc. mediante engaño para utilizarlos en el robo de fondos de sus cuentas.

- **Ciberacoso**:

    - El acceso a chats en línea con otros usuarios puede poner a los niños y jóvenes en contacto con personas que buscan víctimas para llevar a cabo un **acoso sexual**, y que intenten entablar una relación de amistad para conseguir que el menor les envíe fotos de carácter erótico.

    - Hay que tener especial cuidado con lo que se conoce como **sextorsión**, chantajes que utilizan las imágenes y vídeos personales conseguidos fingiendo una amistad, para forzar a la víctima a que mande material pornográfico o entregue dinero, bajo la amenaza de difundir las imágenes íntimas entre sus conocidos.

    - Otro de los abusos que se pueden producir en Internet es el **grooming**, que consiste en que un pederasta o acosador sexual emplea un perfil falso para entrar en contacto con niños o adolescentes en las redes sociales y obtener datos, imágenes, o incluso las claves de acceso de las cuentas de los menores. Con ello consigue hacer un chantaje amenazando con hacer pública toda la información que ha ido consiguiendo si no se cumplen sus deseos.

- **Distorsión de la realidad:** Las redes sociales sobre todo, son un cúmulo de imágenes e información en la que muchas veces lo que vemos no es real, o no lo es del todo. Así, podemos sucumbir en la creencia que los cuerpos perfectos de Instagram o las historias que se comparten por Facebook son verdad cuando en realidad, corresponden a una creación de quien lo publica.

Ejercicio 14

Accede a los siguientes enlaces para ver lo que hay detrás de las fotos perfectas de Instagram.

- Instagram vs Realidad
- Instagram vs Realidad II
- Instagram vs Realidad III

Crea una nueva entrada en tu blog llamada Ejercicio 14 en la que hagas una reflexión de entre 150 y 200 palabras sobre lo que has visto y leído en estos artículos.

Ejercicio 15

Investiga en Internet sobre los consejos para hacer un uso seguro de Internet. Crea una nueva entrada en tu blog llamada Ejercicio 15 en la que elabores un decálogo o 10 consejos para hacer un uso seguro de Internet.

Bibliografía

https://tecnologia-informatica.com/que-es-un-antivirus-como-funciona/

https://einatec.com/que-es-un-antispyware-y-como-funciona/

https://www.xataka.com/basics/antispyware-que-mejores

https://www.avast.com/es-es/c-spyware

https://www.kaspersky.es/resource-center/preemptive-safety/how-anti-spyware-provides-the-best-defense-for-your-computer

https://www.xataka.com/basics/firewall-que-cortafuegos-sirve-como-funciona

https://computerhoy.com/noticias/internet/cortafuegos-informaticos-que-son-que-sirven-26747

https://www.osi.es/es/actualidad/blog/2014/07/14/tu-privacidad-es-importante-no-la-descuides

https://www.clavesegura.org/es/

http://canaltic.com/internetseguro/manual/index.html

https://ddd.uab.cat/pub/dim/16993748n2/16993748n2a4.pdf