CURSO DE SEGURIDAD BÁSICA DE INFORMÁTICA EN EL HOGAR

Formador: Fabio Quintero Pérez

NÚMERO DE HORAS (ESTIMADAS): 30 horas.

OBJETIVOS: Informar adecuadamente sobre la necesidad de la seguridad informática en nuestros dispositivos y privacidad de datos en el hogar.

RELACIÓN DE TEMAS:

*Aclaración: Siendo este un tema tan complejo y cuyas partes están muy desarrolladas entre si, será normal encontrarnos viendo una unidad y parate de otra, sin seguir una linealidad como podría hacerse en otros cursos, No obstante se va a intentar respetar lo mejor posible la "linealidad" en el contenido para que el alumno/a conozca en todo momento el contenido por el que nos movemos.

Introducción:

- Concepto de Seguridad.
- Concepto de Privacidad.

Seguridad en equipos informáticos:

- Permisos, cuentas y contraseñas.
- Usuario Administrador vs. Usuario Estándar.
- **Práctica: Anexo1.- Cómo crear usuario, poner contraseña y darle permisos.pdf.**

Seguridad en dispositivos móviles:

- Android: ROOT.
- Ios: Jailbreak y Unlock

Vulnerabilidades en la Seguridad:

- Actualizaciones de los equipos.
- **Práctica: Anexo2.- Actualizar manualmente tu sistema operativo Windows.pdf.**
- **Práctica: Anexo3.- Configuración de las actualizaciones de Windows.pdf.**
- **Práctica: Anexo5.- Controlar las actualizaciones en tu PC.pdf.**
- Seguridad en la red: Uso de Firewall.
- **Práctica: Anexo6. - Acceso al firewall y configuración de permisos.pdf.**
- Conexión a internet por WIFI.

- Práctica: Anexo7· - Hallar la mac en un PC·pdf·
- Navegación por internet (Seguridad y Privacidad): TOR y VPN Ópera·
- Práctica: Vídeos de instalación y configuración de TOR y VPN Ópera·
- Antimalware·
- Práctica: Anexo4·- Trabajando sobre un Phishing real·pdf·
- Antivirus·

El cifrado de la Información:

- Bitlocker y otros programas·
- Práctica: Anexo8·- Cifrar un archivo con compresión·pdf·
- Unidades virtuales cifradas·
- Práctica: Anexo9· - Encriptar una parte o todo nuestro disco duro o pendrive·pdf·
- Generadores y cajas de claves·

Seguridad en unidades USB y otros dispositivos removibles·

- Borrado de Seguridad·
- Práctica: Anexo10· - Borrado Seguro de documentos y archivos·pdf·

Encriptación del Correo Electrónico·

- Alternativa de encriptación al Texto Plano PGP·
- Práctica: Anexo11·- Alternativa de encriptación al texto plano de los correos electrónicos y otras aplicaciones·pdf·

Privacidad y Seguridad en las Redes Sociales:

- Principios a tener en cuenta·

1.- Introducción:

Debido a la gran tecnificación que se ha llevado en los últimos tiempos y mecanismos cibernéticos necesarios sobre todo para las telecomunicaciones y gestión de empresas, se ha hecho cada vez más palpable la necesidad de crear unos protocolos de seguridad que mantengan a salvo las infraestructuras informáticas y todos sus datos.

Concepto de Seguridad: Hablamos de Seguridad informática cuando se ha conseguido que las infraestructuras de un lugar estén reguladas de tal forma, por la que que no pueda ser transgredida por ningún medio físico y humano y carezca de vulnerabilidades en ese momento (Tanto datos como acceso a equipos informáticos están dispuestos para que sólo las personas autorizadas puedan acceder a ellos).
Las acciones realizadas para completar la seguridad informática debe ser proactiva, de forma que se anticipe a las posibles transgresiones o vulnerabilidades del presente y del futuro.

> "Como ejemplo podemos relatar el ataque informático sufrido por la empresa Telefónica por un virus malicioso (malware) del tipo ransonware por el que todos los equipos se quedaban bloqueados y "secuestrados" hasta que hicieran un pago en bitcoins a los hackers (a partir de ahora llamaremos hackers a toda persona que de forma ilicita quiera apropiarse de datos personales de otras personas) que realizaron esta acción." Los autores pedían monedas bitcoins para proporcionar un algoritmo (Código que desbloqueara los ordenadores infectados)

- **Resumen adaptado del Artículo periodístico de los ocurrido en el medio "cinco días" con fecha del 12/05/2017**

Cuando hablamos de seguridad para las personas, estamos hablando también del **concepto de su privacidad**.

Aunque antiguamente no se le daba un valor importante a la privacidad de las personas, en los últimos tiempos su importancia está creciendo exponencialmente, de tal manera, que se están creando cada vez más normas, reglas y leyes que deben ser cumplidas para no vulnerar los datos personales y privados de cada persona. Así en españa podemos estar hablando de la **Agencia Española de Protección de Datos: https://www.aepd.es/**, sistema regulador oficial encargado de la protección y privacidad de los datos de carácter personal. Cualquier problema relacionado con la creencia de que nuestros datos privados han sido vulnerados ilegalmente debemos hacerlo saber o comunicar debidamente a través de las áreas de actuación de esta agencia:

- **Internet y Redes Sociales: https://www.aepd.es/areas/internet/index.html.**
- **Reclamaciones de Telecomunicaciones: https://www.aepd.es/areas/telecomunicaciones/index.html.**
- **Publicidad no deseada: https://www.aepd.es/areas/publicidad/index.html.**
- **Protección de datos para niños y niñas: http://www.tudecideseninternet.es/agpd1/.**
- **Videovigilancia: https://www.aepd.es/areas/videovigilancia/index.html.**
- **Proyectos Avanzados Europeos: https://www.aepd.es/areas/ue/index.html.**

Así pues **hablamos de privacidad en el sentido humano**, los métodos y acciones por los cuales los datos personales del individuo se ven protegidos de ser obtenidos por terceras personas o empresas para un uso inadecuado o presumiblemente ilegal o con finalidades distintas a los deseos del propio individuo.

Invito a leer un artículo periodístico en el medio intereconomía titulado: "Caso Facebook: ¿Hasta dónde pueden llegar mis datos personales?" publicado el 27 de marzo de 2018.

Resumen adaptado del artículo:

"Como ejemplo podemos relatar en como el estudio a través de datos filtrados a través de la plataforma y red social FaceBook, se utilizaban y se transmitían a empresas privadas para hacer frente al modo en que se dirigían a las personas y poder de esta manera influir en su poder de decisión en alguna materia como por ejemplo la política."

Debemos comentar que en la gran mayoría de ocasiones, los conceptos de seguridad y privacidad van "cogidos de la mano" (unidos) para las personas en su hogar, de tal forma, que tienen que hacer un frente común ante ambas vulnerabilidades, para conseguir que sus datos personales y sus equipos informáticos estén a salvo.

2.- Seguridad en equipos informáticos:

Cuando nos referimos a la seguridad en el sentido amplio de la palabra de los equipos informáticos nos estamos refiriendo a las configuraciones que realizamos o debemos diseñar en el mismo, para mantenerlo seguro y a salvo de ataques y vulnerabilidades externas.

Muchas personas pensarán ***<<"Yo no soy una persona importante ¿para qué van a querer "hackear" mi equipo" y ver lo que tengo dentro de mi PC?>>****, pero nada más lejos de la realidad, cada uno de nosotros es un posible blanco para los "rastreadores" (Hackers) en internet y más aún cuando ven lo fácil que sería introducirse en tu ordenador y buscarte problemas que no deseas o pensaban que no podían ocurrirte como utilizar tu PC para cometer delitos (pornografía infantil, robo de identidad, ataque a cuentas bancarias, acoso de personas,...) Aunque al final logres demostrar que tu no has sido el causante de todos esos delitos, llegar a demostrar que todo fue por*

culpa de una brecha de seguridad en tu PC o red de Internet, el excesivo esfuerzo en dinero, tiempo, abogados,... puede ser realmente insoportable para tu persona, habiendo llevado a muchas personas a la ruina social, económica y sociológica (desgaste moral) por estas circunstancias·

Lo que mucha gente no sabe o no se da cuenta es que en el momento que dejamos "fáciles" las cosas para que cualquier persona extraña pueda acceder a nuestro equipo informático, tal vez no lo haga sólo para ver nuestros documentos o fotos, sino que rastree nuestras cuentas bancarias, que muy bien pudieran quedarse vacías por momentos o utilicen nuestro equipo para atacar a otros equipos, de manera que si investigan posteriormente, tu equipo ha estado "asaltando" otros ordenadores y tú aparecerás como el responsable y el culpable de esa situación en principio· Entonces ahí es en donde te darás cuenta lo importante que hubiera sido tener en cuenta algunas normas básicas para no ser "hackeado"·

> ***Invito a la lectura de una artículo en internet a través del medio de comunicación "El Tiempo" el 13 de marzo de 2017·***
> ***Resumen adaptado:*** *Una mujer como cualquier día pincha un enlace en Facebook que le parece interesante· Nada le parecía sospechoso, e incluso la publicación estaba realizada por un concocido de las redes, lo que les daba más confianza el ver lo que se decía en el mismo· A partir de ese momento todo fue una pesadilla· El hacker se hizo con el control del PC y de todo su contenido, chantajeando a esta mujer con enseñar ciertas fotografías pocos apropiadas a sus entornos sociales, seguidores y amigos... El ciberatacante uso una vulnerabilidad en el complemento Flash de Adobe (plugin que esta considerado en deshuso y al que se reconcoce ciertas vulnerabilidades por las que un hacker puede hacerse con el control de un PC·*
> *"Es importante desactivar o desinstalar aquellos programas o plugins que no utilicemos y que podrían ser un gran agujero de seguridad para nuestros equipos"·*

Como siempre hay que tener unos estándares y la primera premisa para cumplir con el estado de seguridad es ***usar el sentido común****: Anticipar y prevenir circunstancias que*

puedan poner en peligro nuestros equipos es la mayor herramienta para prevenir las vulnerabilidades de nuestro equipo.

> Por ejemplo, hay muchas personas que usan contraseñas muy sencillas para acceder a su PC, como la fecha de su cumpleaños, la digitación 123, su nombre o la de su mujer o de sus hijos, inclusive hay personas que no colocan ninguna contraseña sobre todo en equipos portátiles los cuales sacamos de casa y pueden terminar perdiéndose o ser robados y caer en malas manos.

Es muy importante tener en la cabeza los siguientes conceptos a la hora de configurar la seguridad de nuestro equipo y son:

Las Cuentas, los permisos y las contraseñas. Todo ello va ligado en conjunto y debe ser tenido en cuenta para apoyar la seguridad de nuestro equipo.

Las Cuentas son los espacios de trabajo que creamos en un ordenador para trabajar, jugar, guardar nuestros documentos, fotos música, navegar por internet, introducirnos en nuestras cuentas bancarias, ...

Cada cuenta tiene unos permisos o se los concedemos: Normalmente se habla de permisos de Administrador y permisos de Usuario, aunque en ocasiones podremos hablar también de permisos para Usuarios Invitados. Esto es importante tanto si tenemos nuestro PC para un uso personal o familiar (lo usan también nuestros hijos-as, nuestra mujer,...)

Aparte de aclarar de principio de la conveniencia de que todas y cada una de las cuentas deberían tener su propia contraseña, también es muy importante que todas las cuentas a utilizar diariamente, tengan sólo permiso de usuario.

Práctica: Anexo1.- Cómo crear usuario, poner contraseña y darle permisos.pdf.

Cómo se tendría que mantener configurado un PC respecto a seguridad:

1. **El PC debe tener una sola cuenta de administrador** cuya contraseña sólo deba saber la persona que se encargue de mantener a día el PC, como la instalación y desinstalación de programas,... Esto se debe a que con permisos de administrador se puede hacer todo lo que se quiera en el equipo, inclusive ver y manipular el resto de cuentas del PC. Las instalaciones de programas y juegos deben ser de origenes de confianza como juegos o programas comprados en una tienda.

2. El PC puede tener tantos usuarios como se quiera, pero todos deberán configurarse como **usuarios estándar (nunca como administradores)**. También cada usuario debe tener su propia contraseña. Teniendo usuarios estándar limitamos el uso de ciertas características del PC que podrían poner en peligro el mismo. Por ejemplo la instalación de programas malignos que vulnerarían completamente nuestro sistema, ya se porque lo instalásemos nosotros pensando que son de confianza como que se instalaran a través de la navegación por Internet.

3. **Las contraseñas puestas en cada cuenta deben de ser de difícil adivinación (**que no sea tu nombre, ni la fecha de tu cumpleaños,...) Lo más seguro es colocar palabras con mayúsculas y minúsculas, números y una longitud igual y superior a 8 dígitos. **Ejemplo: 3Ste3sMlpC**. Como véis la contraseña es difícil de acertar, pero para prevenir aún más deberíamos incluso utilizar palabras inventadas, ya que con programas de ataque de cifrados por diccionario (usan todas las palabras y sus combinaciones que se pueden encontrar en los diccionarios lingüísticos de diferentes países para averiguar la contraseña) podrían acceder al equipo.

   ***De forma anexa, dejo enlace a la página de Asociación del Internauta, donde puedes descargarte un "generador de claves y contraseñas" con su programa Claves.exe.**

4. **El PC debe de estar siempre actualizado a la última versión de su sistema operativo.** En este caso estamos tratando sobre Windows. Como es lógico, el uso de Windows XP es como poner una etiqueta a tu PC y que los hackers lean "puedes entrar aquí libremente, hay barra libre" por eso es necesario tener instalados sistemas operativos que todavía tengan soporte de Microsoft como Windows 7, 8.1 y 10.

Práctica: Anexo2.- Actualizar manualmente tu sistema operativo Windows.pdf.

3.- Seguridad en dispositivos móviles:

Cuando tenemos un teléfono móvil, asociamos a él casi toda nuestra vida, ya sea por comodidad o por el uso diario del mismo al usarlo para enviar o recibir llamadas.

Hacemos fotos y vídeos personales que guardamos en el mismo, asociamos redes sociales (Facebook, Twitter, Instagram, ...) usamos aplicaciones de mensajería instantánea como Whatsapp o Telegram, navegamos por Internet haciendo búsquedas, usamos el GPS y el programa incorporado correspondiente para buscar una calle o nos dirija a un lugar preseleccionado,...

Imaginaros por un momento que pierdes ese teléfono o te lo roban... Habrás perdido media vida y lo que es peor, alguien puede ver y usar esos datos para "hacer el mal" siendo tu el perjudicado en todos los sentidos.

Por ello, debemos tener una contraseña o pin colocado en nuestro móvil, para que nadie tenga acceso a él tan fácilmente. Por otro lado, empresas como Google permite en sus teléfonos android su localización y el borrado de todos los datos a distancia a través de tu PC u otro teléfono android, para que de esta forma nadie pueda tener acceso a todo tu contenido personal. Otro tanto pasa con Apple y sus teléfonos con los.

Aunque debería ser ya sabido hacer root a los teléfonos con SO Android o hacerles un Jailbreak y Unlock a los teléfonos con SO Ios, conlleva a una enorme pérdida de seguridad de tus datos.

Precauciones para "asegurar" tu teléfono móvil:

1. Llevarlo siempre contigo y no dejarlo en mesas, cajones, taquillas del trabajo,...
2. Mantener apagado el dispositivo Bluetooth y WIFI siempre que no lo utilices.
3. Usar un pin o patrón de bloqueo para que sólo tu tengas acceso a tus datos. Está demás decir que dicha contraseña no debemos decírsela a nadie y debemos teclear en pantalla los números del pin correspondiente alejado de miradas ajenas...
4. Cuidado dónde enchufas tu móvil a la hora de cargarlo fuera de tu casa, Precaución con las"Cargas de móviles gratis" en el aeropuerto, tiendas,... ya que no sabes de dónde provienen dichos cables, muy bien pudieran estar conectados a un equipo que te estuviera robando la información.
5. Muchísimo cuidado con las redes WIFI públicas (Normalmente de acceso gratuito) ya que alguien puede crear una red WIFI falsa y estar recogiendo todos tus datos, como contraseñas de redes sociales, o lo que podría ser peor, las contraseñas de tus cuentas bancarias. En todo momento usar tu red de datos móvil. Si no tenemos Internet en el móvil, deberemos esperar a conectar con una red WIFI de confianza como la de nuestra casa o en su defecto usar una VPN (Siendo usuarios más avanzados)
6. Hay que tener cuidado también con los juegos y programas que descargamos y lo haremos de tiendas genuinas y originales como la Play Store o Amazon. Descargar una aplicación de orígenes desconocidos, podría meternos en problemas como que nos "secuestren" y bloqueen nuestro móvil hasta que no paguemos una cantidad de dinero o bitcoins para desbloquearlos o perdamos nuestra información ya que esa aplicación se dedica constantemente a enviar todos nuestros datos a otro lugar y otro dispositivo de desconocida procedencia.
7. El uso de cargadores externos (cuando pudiéramos cargar nuestro dispositivo en la calle) son también en extremo sospechosos, ya que algunos de esos cables pueden terminar en un dispositivo que nos robe nuestros datos en vez de un enchufe de la pared que nos suministre electricidad.

8. Muy importante, mantener el dispositivo bluetooth apagado siempre y cuando no lo estemos utilizando, puesto que éste siempre ha sido y es el punto más vulnerable para acceder a un teléfono.
9. Existen otros métodos más bien enfocados a la "ingienería social" que corresponderían por ejemplo a que una persona extraña consiguiera instalar un programa en tu teléfono en un momento de descuido y no te dieras cuenta. Estos programas funcionan en segundo plano y son difíciles de detectar. Sospecha cuando pierdas o te roben un móvil y lo encuentres al poco tiempo.
10. Ante todo mantén siempre el sentido común y desconfía de todo lo que no te parezca normal o veas que le ocurren cosas raras a tu teléfono móvil.

Recordemos que si conectamos con frecuencia nuestro PC a nuestro móvil y no tenemos una auditoría de seguridad en alguno de los equipos, un equipo puede infectar a otro y viceversa.

4.- Vulnerabilidades en la seguridad de tus equipos informáticos:

Uno de los principales enemigos de los hackers, son las actualizaciones proporcionadas por los fabricantes de sistemas operativos y por las actualizaciones de componentes de tu equipo, ya que un ataque se puede producir a través de un sistema operativo o del firmware de un componente de hardware. Así pues, queda claro que actualizar nuestros dispositivos debe ser una de las prioridades más importantes para mantener la seguridad.

En cada paquete de seguridad lanzado, no sólo se solucionan los posibles problemas del propio software (un programa que no funciona, una pantalla que se queda en negro,...) sino las vulnerabilidades que se hayan encontrado hasta ese momento en ese software o firmware.

¿Cómo actualizamos nuestro equipo informático Windows?

Prácticas: Anexo3.- Configuración de las actualizaciones de Windows.pdf.
Anexo5.- Controlar las actualizaciones en tu PC.pdf.

Cuando navegamos por internet es cuando nos encontramos más expuestos y vulnerables ante ataques hacker, desde redirigirnos nuestra navegación a páginas clonadas falsas en donde nos hacen introducir nuestros datos, pensando nosotros que es la verdadera (Phishing)hasta hacernos descargar un archivo que cuando lo ejecutamos veremos como ha quedado arruinado nuestro PC.

Práctica: Anexo12.- Como evitar ser hackeado.pdf

Si has descargado el archivo y lo has abierto en el PC habrás visto lo fácil que es colar un virus en un PC. Sólo es una simulación, no pasa nada.

Para evitar caer en estas trampas, **usaremos el sentido común y la lógica** y nos fijaremos en detalles que nos pueden dar pistas de que alguien quiere "hackearnos":
Imagina que recibes supuestamente un correo electrónico de tu banco indicándote que debes introducir las claves de operaciones online porque ha habido un fallo en los sistemas y te marca un enlace específico para que lo hagas. Abres ese enlace y todo parece ir bien, el logo del banco y el resto de apartados son las mismas de siempre... Confiado introduces tus códigos de operaciones online de ese banco y ¡Pam! Tus datos han pasado a una persona desconocida para hacer un uso fraudulento con ellos.
Las Páginas más clonadas (copiadas) para conseguir tus claves, a este acto se llama **"phishing"** son por ejemplo las del Banco Santander y las del BBVA, aunque ya han ido circulando otras de bancos menos famosos. Esto no sólo puede pasar con los bancos, también pueden pasar con cuentas de Iphone y otras de empresas o servicios que puedan tener gran cantidad de nuestros datos como "bancos de fotografías" o empresas en la nube donde podamos guardar gran cantidad de documentos de trabajo y es que perder un archivo excel con 10.000 entradas no es nada bueno.

Ahora vamos a trabajar para que esto no pase y no nos ocurra, al menos en un 90% de veces, ya que este tipo de hacking se basa en el llamado **"hacking social"** y es en donde se busca a través de tu vida social (redes sociales, blogs,…) pistas con las que poder trabajar y sacarte contraseñas, emular emails de amigos o compañeros de

trabajo,... Por ejemplo si tienes un perro con el que sales mucho en fotos en tu perfil de Facebook y se pronuncia su nombre y has utilizado ese nombre para colocarlo como contraseñas en varias de tus cuestas, date por hackeado o hackeada en cualquier momento·

Práctica: Anexo4·- Trabajando sobre un Phishing real·pdf

Indiscutiblemente las actualizaciones del equipo son importantes y nos aportan un 80% de la seguridad de nuestro dispositivo·

Seguridad en la red: uso de Firewall·

El Firewall es un programa informático que controla el acceso de datos de red al equipo informático y de datos del equipo informático a la red, pudiendo configurarse para cortar tanto los datos entrantes y salientes y sus puertos determinados TPC y UPD· Por ejemplo, para las comunicaciones tradicionales de http (navegación en páginas web) utilizamos el puerto TCP 8080 de forma nativa y estandar·

Algunos otros protocolos y puertos de ejemplo y su uso:

Uso (Programa, juego, ···)	Protocolo (PUERTO)
BitTorrent	TCP 6881/6969
IRC	TCP 6667
Servidores de Minecraft (Juego)	TCP 25565
MySQL	TCP 3306
MSN Messenger	TCP 1863

SMTP (emails)	TCP 465
HTTPS/SSL (Páginas web seguras)	TCP 443
IMAP4 (emails)	TCP 143
POP3 (emails)	TCP 110
Time Protocol (Sincronización de hora)	TCP 37

Más tipos de puertos, listados según la
Asociación de internautas·org·

Teniendo acceso al firewall, tendremos acceso a introducir y enviar paquetes de datos de nuestro PC a la red y de ahí al punto que se quiera·

Por ejemplo, contando como vulnerabilidad de firewall, descargamos un programa poco seguro en la red, apenas pesa unos kbs, pero con el suficiente código que abra el acceso a un puerto de comunicaciones de entrada y salida de datos· Eso le daría al atacante (hacker) la posibilidad posterior de introducir e instalar un programa invisible a nuestros ojos, por ejemplo uno de los llamados "KeyLoggers" que recogería en un archivo de texto cada una de las pulsaciones de nuestras teclas para posteriormente enviarlas al hacker· En ese preciso momento y sin necesidad de calentarse la cabeza obtendría todos los códigos de nuestras redes sociales, la de nuestro banco y quizás de informes confidenciales y secretos de la empresa para la que trabajas·

Por otro lado es bueno conocer los puertos que tenemos abiertos y que programas los usan así como para poder cambiarlos por conflictos con otros programas que usan los mismos como el denegar a un programa o juego acceso a la red de nuestro PC·

Normalmente Windows y los programas de descarga segura se encargan de autoconfigurar el firewall, disponiendo que puertos usaran y en principio no debería existir mayor problema en su uso, pero si hemos notado un agujero de seguridad en nuestras comunicaciones de nuestro PC (Que el servicio del banco nos muestre horas y días de conexión que no hemos hecho) empezar por aquí sería el siguiente paso para desarmar una vulnerabilidad de sistema y ver que programas usan o no los puertos del

firewall e informarnos de los programas de los que no estemos seguros de instalación o uso, en deshabilitarlo del uso del firewall.

Práctica: Anexo6. - Acceso al firewall y configuración de permisos.pdf

Siempre es aconsejable tener un Firewall activado en el equipo, ya sea el que viene por defecto en Windows u otro que nos agrade más o nos brinde más características de seguridad y control de nuestro PC.

Conexión a Internet con WIFI:

Con las nuevas tecnologías y el paso del tiempo ha aumentado las personas que se deciden por el uso de una conexión inalámbrica para su PC, sin contar con otros dispositivos móviles como teléfonos, tabletas o impresoras que también usen esa tecnología de conexión. Pero a la vez que esta tecnología se ha vuelto más popular y más extendida se ha hecho objetivo de todo tipo de tretas "hackers" para obtener información y control sobre otros equipos informáticos, por este medio. Ya tan sólo no debe preocuparnos la seguridad de nuestro equipo (interno) sino de factores externos como WIFI, USB,... que necesitamos para nuestro trabajo.

Aunque hay muchos tipos de "hackeo" desde el acceso externo al WIFI, en este curso de seguridad básica vamos a ver los tipos de vulnerabilidades entre nuestro router y nuestro PC, que es en donde más problemas de seguridad podemos encontrarnos.

Recomendaciones generales:

1.- Colocar el router en la mejor posición de la casa o habitación que ofrezca señal dentro de nuestro hogar pero poca o nada fuera de ella.

2.- Aunque los técnicos nos hayan configurado el router con una contraseña (ellos la conocen y en el momento que una persona ajena a ti conozca una de tus contraseñas tu seguridad mengua al 50%) deberías cambiarlas todas a la que mejor te convenga. Si no sabes como hacerlo, lee el manual del router o busca en internet como se hace. Seguro que hay algún tutorial que te muestre como se hace.

3·- Las contraseñas deben estar bien diseñadas es decir, nada de fechas de cumpleaños, nombres de hijos, mascotas,... La longitud de la misma debe ser al menos de 8 a 16 dígitos, contener letras mayúsculas y minúsculas, números y algún carácter tipo %,+,-...
4·- En algunos casos es recomendable ocultar el nombre de la red WIFI o SSID, de forma que tras un escaneo normal de redes, tu red no se pueda ver· Esta característica la debes encontrar dentro de las opciones de tu router·
5·- Utilizar la última "protección WIFI" disponible o de la que disponga tu router para encriptar la contraseña y sea más difícil de descifrar· En este caso en la edición de manual se está utilizando el protocolo WPA2·

¿Quién está conectado a mi PC o Red Wifi?

Hay diferentes maneras de comprobarlo pero aquí veremos las más fáciles al ser un curso básico e introductorio:

Desde tu propio PC con el programa **Wireless Network Watcher (Gratuito)**·
Enlace: http://www·nirsoft·net/utils/wireless_network_watcher·html

Para tu móvil android podemos encontrar otra solución como **Fing-Escáner de red**·
Enlace: https://play·google·com/store/apps/details?id=com·overlook·android·fing&hl=es

Después de haber realizado las indagaciones correspondientes, podemos hacer las siguientes acciones para evitar que tengan acceso a nuestros datos y redes:

1·- Poner en conocimiento de tu compañía telefónica el acceso fraudulento a tu red y posiblemente tus equipos·

2·- En algunos paises, puedes poner una denuncia en la policía o en juzgados para que encuentren al autor y lo condenen legalmente según la ley vigente·

3·- Cambiar la contraseña tanto de acceso al Router como a su configuración y WIFI (Tendrás que cambiar la contraseña en todos tus dispositivos)

4·- Aún después de haber hecho todo esto, debes leerte bien el manual para hacer la configuración más restrictiva de tu router y que normalmente tiene el nombre de filtrado de MAC· En ese apartado tienes que poner todas las MACs de todos los equipos a los que permites la conexión· Cualquier otro aparato que no tenga listada la MAC en tu router, no podrá conectarse a el en principio (aunque habría otras formas que no se van a exponer aquí, en donde ya hablaríamos de una persona con conocimientos muy avanzados y con intenciones muy oscuras respecto a tu red y tus datos)

La MAC es un código único e *¿inigualable? Funcionando como una dirección física· Que poseen todas las tarjetas de red (cable o wifi) de un PC, tableta, móvil, impresora,...
*En hackeos muy avanzados podemos ver como se pueden clonar estos códigos de MAC y pasar como unos verdaderos· No obstante, en la seguridad de tu hogar no debas temer por este tipo de problemas a no ser que los documentos que manejes tengan relación con archivos de alto secreto de tu empresa, los cuales ya deberían estar protegidos debidamente por la misma·

¿Cómo consigo la dirección MAC de mis equipos?

En teléfonos móviles suele venir en las opciones de WIFI del propio teléfono y también en tabletas·

Con equipos más novedosos como impresoras debes leer el manual del equipo ya que hay muchas en el mercado y cada una tiene su forma de enseñarte la MAC·

Práctica: Anexo7· - Hallar la mac en un PC·pdf

También puedes hallarlo descartando la MAC en el programa que expusimos anteriormente Wireless Network Watcher·

Navegación por internet (Seguridad y Privacidad): Navegadores TOR y Ópera·

Vamos a incidir ahora en las formas seguras y de privacidad de navegación por internet·

Privacidad, por el hecho de dejar los menores rastros posibles de "tu identidad" (quien eres, cual es tu dirección IP,desde donde navegas, qué páginas visitas...) en Internet·
Seguridad en tanto que recordemos que el pensamiento lógico es la primera defensa para tu seguridad (navegar por páginas seguras, descargar programas y juegos de páginas web oficiales y seguras, comprobar las direcciones web de los enlaces que pinchamos...) usar un navegador que nos ayude en estas tareas también es muy importante·

Hay multitud de formas de conseguir privacidad y seguridad mientras navegamos, pero siendo este un curso básico de seguridad, vamos a recurrir a 2 programas que nos van a facilitar mucho las cosas aún siendo personas con un conocimiento limitado de informática·

Hablemos primero del navegador Ópera·
Este navegador lo puedes descargar desde la página: **https://www·opera·com/es·**
Ópera nos va a proporcionar sobre todo privacidad, ya que podremos aplicar en las opciones una VPN gratuita (Virtual Private Network - Red Privada Virtual) Expliquemos brevemente y de forma muy gráfica en que consiste esto:
Cuando nos conectamos a Internet y en este caso navegamos, nuestra red proporciona una numeración dentro de la red Internet, denominada IP (Internet Protocol - Protocolo de Internet) con la que somos identificados (**Puedes ver cual es tu IP en la siguiente dirección:http://www·cualesmiip·com/ y si quieres asombrarte más, puedes ver como a través de esa IP pueden reconocer desde dónde te conectas a Internet desde el país que nos conectamos desde aquí: https://geoiptool·com/es/· Hay herramientas que afinan más y te dan hasta la dirección de tu casa**)· Es como una dirección de una casa· Por ello, todo lo que hagamos dentro de Internet, páginas web que visitamos, programas o juegos que nos descargamos,... queda registrado a nuestra IP con lo cual, esos datos que deben ser privados, pueden pasar a dejar de serlo, ya

que ciertas compañías (Google, Facebook,...) utilizan esos datos entre otras cosas para mostrarnos publicidad personalizada. **Por ejemplo** si visitamos muchas páginas web de coches porque nos gusta saber y conocer acerca de ellos, muy probablemente Google, Facebook u otra compañía nos muestre anuncios de ventas de coches, y sus derivados como piezas, gasolineras, talleres,...

Si queremos aumentar nuestra privacidad, utilizamos por ejemplo lo que hemos descrito antes como VPN (Existen otros medios más avanzados de privacidad, pero este método básico es más que suficiente para el uso en el hogar)

Entendamos su funcionamiento (aunque no funciona así específicamente, te dará una idea de lo que hace)

UN PC SIN VPN:

- PC → IP → INTERNET.

UN PC CON VPN:

- PC → IP → VPN(FILTRO) → OTRA IP → INTERNET.

Ahora a través del siguiente vídeo aprenderemos a activar la VPN en el navegador Ópera.

Hay que aclarar que este método sólo es válido mientras naveguemos con Ópera. Si lo haces con otro navegador o utilizas otros servicios basados en Internet como Skype, Steam, ... no tienes ninguna VPN activa y por lo tanto se verá tu IP real.

El uso de TOR,Privacidad y Seguridad (Todo en uno):

Nuestro siguiente paso es el uso del navegador Tor, programa que "cambia nuestra IP real en varias veces" a través de distintos Proxys (servidores) - (creando un simil,

rastrear nuestra verdadera IP se hace más difícil) y su configuración por defecto desactiva varias vulnerabilidades como java, flash,...

Lo importante que hay que tener en cuenta usando este navegador es actualizarlo cada vez que se nos pida.

Lo puedes descargar desde el siguiente enlace: **https://www.torproject.org/**

Ver Vídeo de descarga, instalación y factores a tener en cuenta con TOR.

Debemos recordar que el uso de estos programas no ustituyen el uso de un antivirus. El uso de un antivirus es imprescindible siempre.

Antimalware y Antivirus.

En el mercado existen multitud de programas con funciones de antivirus, antimalware o ambos tanto de forma comercial como de forma gratuita.

Estos programas una vez instalados se dedican a escanear nuestro PC, para ver si hemos sido infectados por algún archivo "maligno" y en su caso siempre que sea posible, localizarlo y eliminarlo de nuestro PC.

Digo en cuanto sea posible, porque la cantidad de virus que se crean a diario y circulan por la red por diferentes medios es masiva, por lo que mientras los laboratorios detectan el archivo (virus, malware) lo aíslan, conocen su funcionamiento y crean una "vacuna" que vaya incluida en la siguiente actualización del antivirus, puede pasar algún tiempo en el cual si eres infectado, tendrás que esperar a que saquen un remedio contra ese virus o malware que repare tu equipo y lo "desinfecte" o tendrás que "formatearlo" (Borrar todos tus discos duros conectados al PC e instalar nuevamente el sistema operativo y tus programas y juegos preferidos) perdiendo información y datos que no tuvieras guardados (Teniendo una copia de seguridad siempre fuera de tu PC) y mucho tiempo en volver a restablecer el PC como lo tenías anteriormente. En

cualquier forma esta situación sería un completo desastre, por eso comento siempre que ***el sentido común es la primera defensa ante la seguridad de nuestro PC.***

Existen infinidad de Virus, Malware y vulnerabilidades, de forma que aparte de poder quedar infectado tu PC, puedes infectar automáticamente los equipos informáticos de amigos con el que compartas archivos o los de tu propia empresa usando un simple pendrive que compartas entre el trabajo y la casa o usando tu propio PC para realizar alguna actividad laboral (Nada decir de las consecuencias para tu situación laboral como un despido si el daño empresarial es grande y se descubre que el foco de la infección proviene de tu PC o pendrive).

Personalmente recomiendo el uso del propio antivirus que viene incorporado con Windows "Windows Defender" por varias razones:

1.- Viene incorporado con el propio sistema. No hace falta adquirirlo aparte. Por ello el rendimiento del PC puede ser más óptimo ya que algunos antivirus de otras compañías, pueden ralentizar el PC durante el análisis y escaneo del mismo.

2.- Contiene componentes de antivirus y antimalware, siendo éste muy completo para mantener la seguridad de nuestro PC.
Se actualiza automáticamente.

3.- Tiene todas las funciones avanzadas que puedas encontrar en otro antivirus de la competencia.

No obstante si este antivirus no te convence, te indico los siguientes antivirus gratuitos a continuación:

1. ***Avast Antivirus:*** *https://www.avast.com/es-es/index#pc*
2. ***AVG Free:****https://www.avg.com/es-es/free-antivirus-download*
3. ***Karsperky Free:****https://www.kaspersky.es/free-antivirus*

También podéis ver una comparativa de antivirus realizada por la OCU (Organización de Consumidores y Usuarios):

El cifrado y borrado seguro de la información de tu PC: Seguridad en dispositivos removibles (Pendrives, HDD portátiles, ...)

Hemos estado viendo las amenazas en seguridad que nos podemos encontrar en la red e Internet que pueden perjudicarnos en gran medida.
La información que tenemos guardada es privada y para muchos es muy importante que siga siéndola, puesto que seguro que tienes algún documento que deseas que no vea nadie.

Para esto tenemos 2 opciones de mantener seguro nuestros datos, aparte de bloquear el acceso a nuestro PC y es que en ocasiones también debemos transportar cierta información en dispositivos portátiles como pendrives, discos duros portátiles,... (Por ejemplo podemos perderlos o compartirlos con alguien, sin recordar a ciencia cierta que "información sensible" se haya guardada en ese dispositivo)

Cifrar la información: A través de un programa o aplicación encapsulamos los datos entre una contraseña maestra (que nosotros pongamos) y una serie de algoritmos matemáticos que cambian la forma y apariencia de nuestros archivos, por lo que éstos no pueden ser visualizados tal y como los teníamos antes de cifrarlos. La acción de cifrado es reversible de forma que cuando queramos (con la contraseña que usamos) podremos volver a tener los archivos exactamente como estaban, pudiendo visualizarlos.

Práctica: Anexo8.- Cifrar un archivo con compresión.pdf.
Práctica: Anexo9. - Encriptar una parte o todo nuestro disco duro o pendrive.pdf

Borrado de la información: El borrado de archivo es muy importante. Imagínate que quieres vender tu equipo informático, el cual tiene un disco duro con el que estuviste

trabajando durante 3 años y contenía fotos y documentos personales, cuentas bancarias,... que no te gustaría que viera nadie. Pero entonces tu piensas que si borras los datos e inclusive formateas el disco duro (Eres un usuario avanzado en informática y sabes hacerlo), mis datos estarán a salvo y nadie podrá verlos. **FALSO: Tus datos podrían ser recuperables** en un alto porcentaje. **Windows no borra los datos cuando tu pulsas en la opción eliminar, simplemente los hace desaparecer de tu vista** para que tu no puedas verlos insertando un símbolo delante del archivo o documento borrado, incluso si hubieras vaciado la papelera de reciclaje. Con el formateo pasa algo parecido, escribiendo sólo en las primeras pistas del dispositivo que tu disco esta formateado y listo para ser usado, pero el resto de información sigue ahí escondida, esperando a que un buen "hacker" recupere esa información y te fastidie de por vida... Para ello usaremos un programa que borra definitivamente los datos de tu PC haciéndolos prácticamente irrecuperables, salvo que la CIA o la NSA estén interesados en ellos ;).

Práctica: Anexo10. - Borrado Seguro de documentos y archivos

Cifrado de comunicaciones: Correo electrónico y otros.

El Cifrado de las comunicaciones es muy importante sobre todo si queremos que nadie tenga acceso a nuestras conversaciones privadas como en el correo electrónico, en el cual todo lo que se envía y se recibe se hace a través de lo denominado texto plano. Cualquier persona que interceptara esos correos electrónicos, no le sería difícil ver su contenido, porque para el "hacker" le equivaldría ver todo el contenido del texto como si estuviera leyendo un documento TXT.

Para evitar este tipo de problemas se creó la **OpenPGP: https://www.openpgp.org/**

Desde esta página puedes encontrar el modo de encriptar todas tus conversaciones, emails, chats,... desde distintas plataformas o sistema operativos, de ahí que haya dejado el enlace para que cada uno dependiendo de sus circunstancias (Navegador, cliente de correo, sistema operativo,...) utilice un método u otro.

Yo voy a dejar un anexo con un tutorial donde instalando un simple programa y configurándolo ya tendremos nuestra propia red segura para enviar emails, chatear o enviar archivos.

Práctica: Anexo10. - Borrado Seguro de documentos y archivos.pdf

Privacidad y Seguridad en las Redes Sociales:

Cada vez que nos conectamos a las redes sociales, podemos estar dando infinidad de datos personales, nuestros o de nuestros amigos, que pueden ser "Explotadas" por "hackers" y otro tipo de "gente mala", los cuales pueden hacer muy mal uso de la información.
Tener una identidad o perfil social en cualquiera de las plataformas existentes (Facebook, Twitter, Instagram, ...) requiere de ciertas responsabilidades a la hora de publicar cierta información o fotos en las que cualquiera puede tener acceso, sino has configurado correctamente en las opciones de esa red social el grado de privacidad que quieres manejar (Por ejemplo que ciertas publicaciones la vean sólo amigos...) Hasta hace poco la aplicación Twitter y Facebook mostraba en tiempo real tu ubicación. O sea que aquella persona que entrara en tu perfil podía ver dónde estabas en ese momento.

Y entonces tu dirás "¿Y a mi qué? Me da igual que sepan dónde estoy…"
Pero ¿Y si una persona dedicada a desvalijar casas (un caco o ladrón) ve que estás fuera de tu provincia porque estás de viaje y aprovecha el tirón sabiendo que no estás en casa para "limpiarte el piso"? Esto sólo es un ejemplo gráfico de lo que puede pasar y sin que tu hayas escrito nada en la aplicación...

Por otro lado puedes estar muy contento porque estás en un concierto y publicas una foto diciendo que van a ser las 3 mejores horas de tu vida (que también se geocalizan, o sea que se puede conocer a través de un programa que lee metadatos las coordenadas dónde se ha realizado la foto) Pasamos a que la mala persona puede obrar en contra tuya con esos datos también.

Dar excesivos datos personales (DNI, teléfono, dirección, lugar dónde trabajas,…) también puede crear un perfil muy completo de ti, de forma que "te roben la identidad" y alguien se haga pasar por ti. Esa persona que se hace pasar por ti puede hacer cosas como crear cuentas de bancos a tu nombre, pedir créditos, crear tarjetas de crédito, comprar pisos o coches,... disfrutarlos y dejar de pagarlos y luego, la policía va a por ti, siendo muy difícil de demostrar que tu no has hecho nada de eso y que simplemente has sido un "pardillo" que ha caído en una trampa.

Si has caído en esa trampa, tan sólo queda ponerte en manos de un buen jurista de robo de identidades donde se deberá demostrar de todas las formas posibles que ciertas compras y actividades no fueron realizadas por ti, sino que las hizo una persona suplantando tu identidad. Identificar que han duplicado tu identidad y alguien se está aprovechando de ella es de difícil detección. Normalmente nos venimos a dar cuenta cuando el delincuente ha "quemado" esa identidad y no la necesita usar más y es entonces cuando puedes empezar a recibir cartas de bancos, de tarjetas de créditos, de compañías hipotecarias, exigiéndote el pago de compras que se realizaron con tu falsa identidad. El camino es largo y difícil de llevar psicológica y fisiológicamente, pero al final conseguirás demostrar que tu no fuiste el culpable, sino que al contrario fuiste igual o mayor víctima de bancos y compañías que timaron.

Práctica Anexo 12: Datos de Fotografías y como nos pueden seguir el rastro.

*Ojo, las fotografías no son los únicos documentos que dejan rastros de nuestras acciones, otros documentos como hojas de cálculo, documentos de word o el historial de nuestro navegador web, pueden ofrecer pistas y datos importantes a nuestros hackers atacantes…

Los datos que se deben de dar a través de redes sociales deben ser los más escuetos e imprescindibles. Inhabilitar el uso del GPS en las redes sociales (que muestran dónde estáis en todo momento) y lo mismo con las fotografías. Existen cientos de programas que permiten el borrado de los metadatos de las fotografías como las coordenadas GPS de las mismas. Deberéis buscar algo así como "borrado de datos EXIF" en vuestra tienda de aplicaciones. Una vez tratadas las imágenes con éxito y habiendo borrado las coordenadas GPS, ya es más seguro publicar una foto en internet siempre que dicha foto no muestre lugares muy conocidos, donde se os pueda localizar. Guardar esas fotos para vuestro album privado y publicad aquellas cuyos fondos sean poco o nada relevantes para las personas que las vean.

También debemos tener cuidado de lo que publicamos, decimos públicamente y fotos que colgamos en nuestra plataforma de red social, siendo consecuentes y responsables en última instancia de todo lo que publicamos. Por ejemplo, Insultar o acusar a otra persona de algo que no ha hecho o tu no tienes pruebas de ello, se puede convertir en un delito de "calumnia" tipificada en el código penal. Poner una fotografía dónde aparecen menores de edad y no tienes la autorización paterna para ello, también es un delito de protección de datos y va contra la ley del menor.
Antes de publicar algo, debemos tener mucho cuidado y luego no sirve el decir que tu no sabías que eso era delito, ***porque el desconocimiento de las leyes no eximen de su cumplimiento*** *y las condenas se pagan igual...*

Como siempre, ***usad el sentido común (No hagas o digas lo que no te gustaría que te hicieran o dijeran de ti)*** *y si tenéis dudas antes de hacer algo consultadlo, que Internet es muy grande y hay mucha información en ella, que si tienes tiempo para publicar un Twitt y tienes alguna duda, también tendrás tiempo de asegurarte de lo que vas a decir no entraña ningún peligro para ti o para nadie judicialmente y socialmente hablando...*

¿Qué nos queda en internet, después de todo, la Seguridad y la Privacidad y si la vendemos o dejamos que nos la quiten, que nos quedará por poseer o que nos diferenciaran los unos de los otros?

PIÉNSALO BIEN. SÓLO TIENES UNA VIDA. ÚSALA CON GARANTÍAS.