DIGITAL ACCESS

DIGITAL SKILLS FOR PEOPLE LIVING IN THE 3RD AGE
Effective Digital Access to Public Services

Erasmus+

PROYECTO DIGITAL ACCESS

MÓDULO DIDÁCTICO

Conocimientos intermedios de seguridad online

Preparado por: AKLUB
Septiembre 2018

Este proyecto ha sido financiado con el apoyo de la Comisión Europea. Esta publicación refleja únicamente los puntos de vista de los autores, y la Comisión no puede ser responsable de cualquier uso que pueda hacerse de la información contenida en el mismo.

Contenido

CARGA DE TRABAJO: [TODAS LAS UNIDADES HORAS DE APRENDIZAJE + TIEMPO TOTAL PARA LOS EJERCICIOS]

Resumen

Este módulo diseñado para ampliar el conocimiento básico de los usuarios no iniciados o principiantes en internet sobre la seguridad online. Los objetivos principales de la unidad es capacitar al usuario para protegerse contra los ciber-delincuentes y mantener la información personal a salvo, asegurando que sus datos y activos online no se vean comprometidos.

Palabras clave

Red inalámbrica doméstica, programa antivirus, virus, malware, programa antispyware, spyware

OBJETIVOS DEL MÓDULO

Acciones/logros		
Adquirir una comprensión de las actividades delictivas basadas en Internet dirigidas a los individuos y la adquisición de las habilidades para identificar y evitar estas actividades.		
Conocimiento	**Habilidades**	**Competencias**
Asegurar las conexiones a Internet	Entender lo que es una red inalámbrica doméstica Aprender a configurarla Conocer las reglas para su seguridad	Ser capaz de configurar y administrar la seguridad de su red inalámbrica doméstica
Los programas antivirus	Entender que son los virus y las necesidades de los programas antivirus Ser capaz de elegir el programa antivirus adecuado Saber cómo evitar los virus en su ordenador	Saber cómo proteger su equipo contra la infección por virus.

Malware	Entender que es el malware y la necesidad de programas antimalware Ser capaz de elegir el programa antimalware adecuado Saber cómo evitar el malware en su ordenador	Saber cómo proteger su equipo contra el malware.

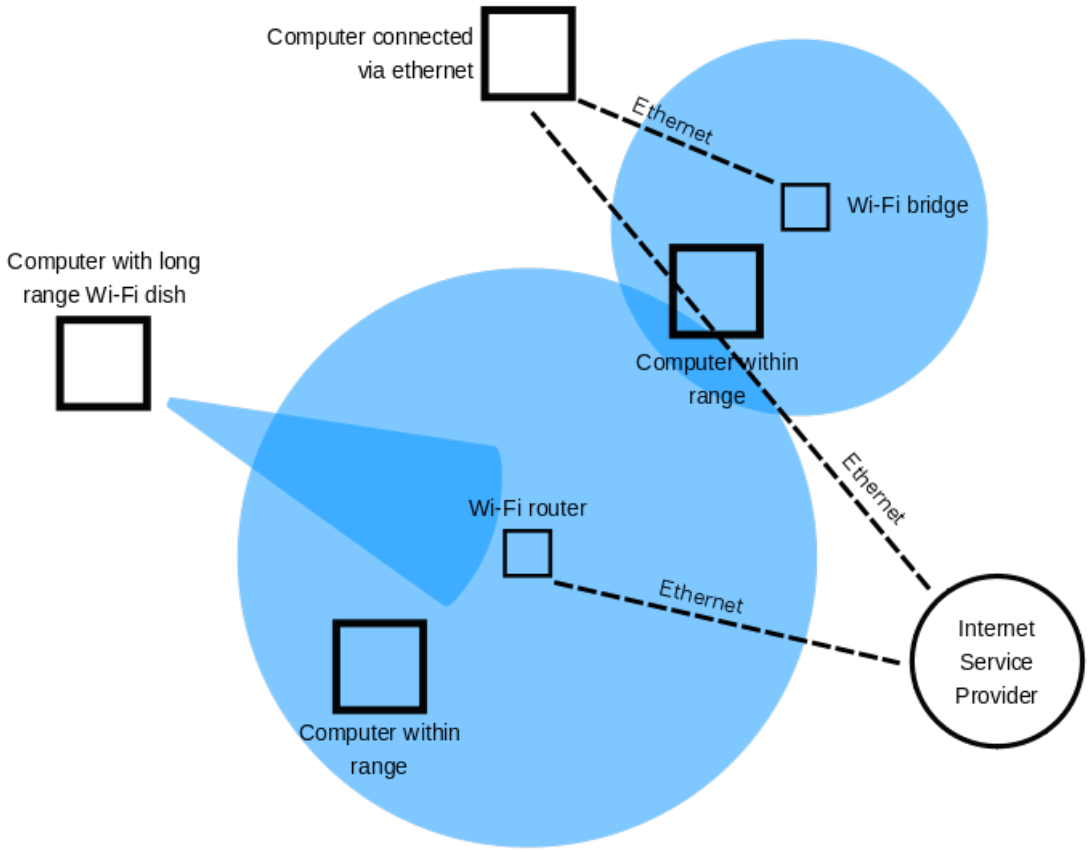
UNIDAD 1Protección de la conexión a Internet

La red inalámbrica doméstica

En pocas y simples palabras, una red inalámbrica doméstica básica significa conectar un punto de acceso a Internet, como un cable de su proveedor de servicios de Internet, a un enrutador (inalámbrico) para permitir que varios dispositivos se conecten a la red muy rápidamente.

En muchos casos, una vez que se ha instalado un router inalámbrico, buscamos una ubicación un lugar en nuestra casa para ello y luego lo olvidamos. Mientras todos nuestros dispositivos estén configurados y conectados a través de la red Wi-Fi, eso es todo lo que importa, ¿verdad? ¡Incorrecto!

.



Probablemente muchos de ustedes no se dan cuenta, pero el enrutador de Internet es uno de los dispositivos más importantes en nuestro hogar. Es la puerta de entrada a nuestro acceso a Internet y también propensos a expolios por los ciber-delincuentes que pueden colarse en nuestros dispositivos y obtener acceso a nuestro sistema.

La única medida que la mayoría de la gente usa para proteger su red doméstica es establecer una contraseña y evitar que los vecinos y otras personas controlen sus datos. Pero tenemos que ser más serios acerca de la seguridad y hacer algo más que simplemente establecer una contraseña simple. Un riesgo grave es que un criminal online podría romper sus pobres medidas de seguridad Wi-Fi y "escuchar" su tráfico de internet, con el fin de recuperar información sensible, o aprovecharse de su red para lanzar ataques malintencionados, tales como ataques de intermediario, rastreo de redes o robo de datos.

Aunque son relativamente fáciles de usar y acceder, las redes Wi-Fi no siempre son redes seguras**.** Wi-Fi viene con un montón de problemas de seguridad, y vale la pena recordar la vulnerabilidad (krack) encontrada en el protocolo de acceso inalámbrico protegido II (WPA2), que afectó a todos los dispositivos conectados a través de Wi-Fi.

Por esta razón, aprender a proteger su red doméstica inalámbrica contra los ciber-delincuentes es una jugada sabia e inteligente. Teniendo en cuenta el número de dispositivos de “Internet de las cosas (IoT)” que puede poseer, asegurarse de que su red es extra segura es aún más importante, y a pesar de que a veces cuidar de su ciberseguridad puede ser una tarea tediosa, es necesaria.

En esta unidad, usted aprenderá cómo puede asegurar mejor su red doméstica y disminuir las posibilidades de ver sus valiosos datos comprometidos.

Paso 1. Cambie el nombre de la red doméstica predeterminada

Si desea proteger mejor su red doméstica, lo primero que debe hacer es cambiar el nombre de su red Wi-Fi, también conocida como SSID (Service Set IDentifier).

Mientras que dar su Wi-Fi un nombre algo provocativo como "no se puede hackear esto" puede a veces ser contraproducente, otros nombres como "esto no es un WiFi" o "demasiado vuelo para una WiFi" son perfectamente aceptables.

Cambiar el nombre predeterminado de su Wi-Fi dificulta que los atacantes malintencionados sepan qué tipo de enrutador tiene. Si un ciber-delincuente conoce el nombre del fabricante de su enrutador, sabrá qué vulnerabilidades tiene ese modelo y luego intentará explotarlas.

Le aconsejamos encarecidamente que no llame a su red doméstica algo como "john's Wi-Fi". Usted no quiere que sepan a primera vista qué esa red inalámbrica es suya, cuando hay probablemente tres o cuatro otras Wi-FIS vecinas.

Además, recuerde que revelar demasiada información personal en un nombre de red inalámbrica puede exponerlo a una operación de robo de identidad.

Aquí tiene una Guía paso a paso y sencilla que explica cómo puede cambiar fácilmente el nombre de su red inalámbrica.

Paso 2. Asegúrese de establecer una contraseña fuerte y única para proteger su red inalámbrica.

Usted probablemente sabe que cada router inalámbrico viene pre-configurado con un nombre de usuario y una contraseña por defecto**,** que se necesita en primer lugar para instalar y conectar su router. La peor parte: es fácil de adivinar para los hackers, especialmente si conocen el fabricante.

Por lo tanto, asegúrese de cambiar ambos inmediatamente.

Una buena contraseña inalámbrica debe tener al menos 20 caracteres de longitud e incluir números, letras y varios símbolos**.**

Utilice esta Guía para configurar una contraseña segura. Los amigos que vienen de visita pueden quejarse de la longitud inusual de su contraseña, pero esto podría disuadirlos de consumir innecesariamente sus datos con mensajes aburridos de Facebook o Instagram.

Paso 3. Aumente su seguridad Wi-Fi activando el cifrado de red

Las redes inalámbricas vienen con múltiples lenguajes de encriptación, tales como WEP, WPA o WPA2.

Para entender mejor esta terminología, WPA2 significa acceso Wi-Fi Protected 2 y es un Protocolo de seguridad y un estándar actual en la industria que encripta el tráfico en las redes Wi-Fi (las redes WPA2 están casi en todas partes). También reemplaza el protocolo WEP, más antiguo y menos seguro (Wired Equivalent Privacy), y es una actualización de la tecnología WPA original. Desde 2006, todos los productos certificados por Wi-Fi deben usar la seguridad WPA2.

WPA2 AES también es ahora un sistema de seguridad estándar, por lo que todas las redes inalámbricas son compatibles con ella. Si desea habilitar el cifrado WPA2 en su enrutador inalámbrico, utilice estos seis pasos. Si está utilizando un router inalámbrico TP-Link, aquí le decimos cómo proteger su red inalámbrica.

La buena noticia es que el WPA3 ya está aquí y reemplazará a WPA2. La Alianza Wi-Fi anunció recientemente su estándar de seguridad de red inalámbrica de próxima generación que tiene como objetivo resolver un problema de seguridad común: las redes Wi-Fi abiertas. Además, viene con mejoras de seguridad e incluye un conjunto de características para simplificar la configuración de seguridad Wi-Fi para los usuarios y los proveedores de servicios.

Paso 4. Apague la red doméstica inalámbrica cuando no esté en casa

Con el fin de asegurar su red, le recomendamos encarecidamente que deshabilite la red doméstica inalámbrica**,** en caso de períodos prolongados de no uso. Usted debe hacer lo mismo con todos los dispositivos que están utilizando cables Ethernet, cuando no va a estar en en casa.

Al hacer esto, usted está cerrando cualquier ventana de oportunidad a los piratas informáticos malintencionados, que podrían intentar obtener acceso a ella mientras estás ausente.

Estas son algunas de las ventajas de deshabilitar la red inalámbrica:

- **Razones** de seguridad – apagar los dispositivos de red, minimiza las posibilidades de convertirse en un objetivo para los hackers.
- **Protección contra sobretensiones** – cuando apaga su dispositivo de red, también disminuye la posibilidad de ser dañado por picos de energía eléctrica;
- **Reducción de ruido**: aunque las redes domésticas modernas son mucho más tranquilas en estos días, deshabilitar su red doméstica inalámbrica puede añadir tranquilidad a su hogar.

Paso 5. ¿Dónde se encuentra el enrutador en su casa?

Probablemente no ha pensado en esto inicialmente, pero donde ubique su lugar Wi-Fi en su casa también puede tener un impacto en su seguridad.

Coloque el router inalámbrico lo más cerca posible del centro de su casa**. ¿**Por qué? En primer lugar, proporcionará el mismo acceso a Internet a todas las habitaciones de su hogar. En segundo lugar, usted no quiere que su rango de señal inalámbrica alcance demasiado fuera de su casa, donde puede ser fácilmente interceptado por personas malintencionadas.

Por esta razón, recomendamos no colocar su enrutador inalámbrico cerca de una ventana, ya que no hay nada que bloquee la señal que va fuera de su casa.

Paso 6. Utilice una contraseña de administrador de red fuerte para aumentar la seguridad Wi-Fi

Para configurar su enrutador inalámbrico, generalmente necesita acceder a una plataforma o sitio online, donde puede realizar varios cambios en la configuración de su red.

La mayoría de los routers Wi-Fi vienen con credenciales predeterminadas como "admin" y "Password" que son tan fáciles de romper para los hackers malintencionados.

¿Sabías que el número de redes inalámbricas ha aumentado drásticamente en los últimos 8 años? En 2010 había 20 millones redes Wi-Fi en todo el mundo, y en 8 años, ese número aumentó a 400 millones.

Paso 7. Cambie su dirección IP predeterminada en el router inalámbrico

Cambiar la dirección IP predeterminada a una menos común es otra cosa que debería considerar a hacer para asegurar mejor su red doméstica, y hacer que sea más difícil para los hackers rastrearlo.

Para cambiar la dirección IP de un router, debe seguir estos pasos:

1. Inicie sesión en la consola de su enrutador como administrador. Estos pasos básicos le enseñarán cómo conectarse fácilmente a su red doméstica como administrador. Normalmente, el tipo de barra de direcciones se ve como http://192.168.1.1 o http://192.168.0.1
2. Una vez que esté allí, inserte el nombre de usuario y contraseña en la página de inicio de sesión;
3. A continuación, seleccione Red > LAN que se encuentra en el menú del lado izquierdo;
4. Cambie la dirección IP a la preferida y, a continuación, haga clic en Guardar.

Nota: después de haber cambiado la dirección IP, deberá escribir la nueva dirección IP en la barra del navegador web.

También puede cambiar el servidor DNS que utiliza su enrutador inalámbrico para filtrar el tráfico de Internet y esta lección le mostrará cómo hacerlo.

Paso 8. Apague la funcionalidad DHCP en el router

Para mejorar la seguridad de la red inalámbrica, debe desactivar el servidor del protocolo de configuración dinámica de host (DHCP) en su enrutador, que es lo que las direcciones IP se asignan a cada dispositivo en una red. En su lugar, debe hacer uso de una dirección estática e introducir la configuración de red.

Esto significa que usted debe entrar en su dispositivo y asignarle una dirección IP que sea apropiada para a su router.

Paso 9. Deshabilite el acceso remoto

La mayoría de los routers le permiten acceder a su interfaz sólo desde un dispositivo conectado. Sin embargo, algunos de ellos permiten el acceso incluso desde sistemas remotos.

Una vez que hayas desactivado el acceso remoto, los actores malintencionados no podrán acceder a la configuración de privacidad de tu router desde un dispositivo que no esté conectado a tu red inalámbrica.

Para realizar este cambio, acceda a la interfaz web y busque "acceso remoto" o "administración remota**".**

Paso 10. Mantenga siempre el software de su router actualizado

El software es una parte esencial de la seguridad de su red inalámbrica. El firmware del router inalámbrico, al igual que cualquier otro software, contiene fallas que pueden convertirse en vulnerabilidades importantes y ser explotadas despiadadamente por los hackers, ya que éstos la encontrarían.

Desafortunadamente, muchos routers inalámbricos no vienen con la opción de actualizar automáticamente su software, por lo que tiene que pasar por la molestia de hacer esto manualmente.

Incluso para aquellas redes Wi-Fi que pueden actualizarse automáticamente, todavía requiere que usted ejecute esta configuración. Pero, le recordamos la importancia de la aplicación de parches de software y cómo descuidar hacer esto puede dejar puertas abiertas para los ciber-delincuentes para explotar diversas vulnerabilidades. Lea lo que los expertos en seguridad tienen que decir acerca de la actualización de su software y por qué es una clave para la seguridad online.

Paso 11. Un cortafuegos puede ayudar a proteger su red Wi-Fi

Los firewalls no son sólo programas de software utilizados en su PC, también existen en la variedad de hardware.

Un firewall de hardware hace prácticamente lo mismo que uno de software, pero su mayor ventaja es que agrega una capa adicional de seguridad.

La mejor parte de los firewalls de hardware es que la mayoría de los mejores routers inalámbricos tienen un cortafuegos integrado que debe proteger su red de posibles ciberataques. Esta lección puede ayudarle a averiguar si su enrutador tiene un cortafuegos integrado y cómo puede activarlo. Y sugerimos encarecidamente que lo active, si no es por defecto, como una capa adicional de protección.

Si su router no tiene uno, puede instalar un buen dispositivo de cortafuegos a su router con el fin de proteger su sistema de intentos malintencionados de piratería contra su red doméstica.

Paso 12. Mejore la protección de los dispositivos conectados con mayor frecuencia a su red doméstica

Importante: ¡no deje ninguna vulnerabilidad expuesta para que puedan aprovecharla los criminales online!

A pesar de que ha aumentado la protección de su router y de la red doméstica, es necesario asegurarse de que no tiene ningún agujero de seguridad que puede ser explotado por los delincuentes online**.**

Esto es lo que le recomendamos que haga:

1. Recuerde mantener siempre sus dispositivos actualizados con el software más reciente disponible**;**
2. Siempre aplique los últimos parches de seguridad para asegurarse de que no se deja ningún agujero de seguridad abierto a los actores malintencionados.
3. Compruebe qué dispositivos se conectan más a menudo a su red doméstica y asegúrese de que tienen antivirus y/o un software de seguridad anti-malware instalado. Si usted no sabe cuál debe elegir, esta guía será muy útil.
4. Asegúrese de proteger sus dispositivos utilizando múltiples capas de seguridad que consisten en software de seguridad especializado, tales como programas antivirus actualizados y software de filtrado de tráfico. Puede considerar el uso de un programa de software antimalware.

Conclusión

Asegurar la red doméstica debe ser una prioridad para cada uno de nosotros interesados en mantener los datos seguros. Estos pasos pueden ser realmente útiles incluso para la persona que no es experto en tecnología.

Además, no olvide que la seguridad de su red inalámbrica puede ser a veces débil, y propenso a brechas. Casi no importa cuán fuerte sea su contraseña o si su software está actualizado, si los ciber-delincuentes pueden simplemente secuestrar sus datos de Wi-Fi.

UNIDAD 2: los programas antivirus

Resultado

La mayoría de los sistemas necesitan software antivirus. Esto es lo que hay que elegir, cómo instalarlo, y cómo utilizarlo para mantenerse a salvo.

Virus

Es algo que todos esperamos evitar, pero la verdad del asunto es que no podemos esquivarlo para siempre. Algunos de nosotros somos los desafortunados adquirentes de virus informáticos. Las siguientes reglas le ayudan a controlar y minimizar los riesgos.

Instale un programa antivirus

Ya sea que se conecte a Internet o no, tener una protección confiable es el camino a seguir. Los programas anti-virus son una inversión mínima y valen el dinero que cuestan, así que tan pronto como encienda ese ordenador, ¡asegúrese de que está protegido! En esta lección puede encontrar un enlace a las reseñas de software antivirus. Usted puede elegir entre ofertas gratuitas y pagadas, elegir el más adecuado para usted y instalarlo fácilmente desde el sitio web original.

Evitar sitios Web sospechosos

Muchas veces los sitios web le notificarán si está a punto de entrar en un sitio web que intenta instalar o ejecutar un programa en su ordenador, pero no siempre. Evite sitios web como esos.

Nunca abra archivos adjuntos de correo electrónico sin revisarlos

La forma más común de propagación de virus sigue siendo a través del correo electrónico. Asegúrate de usar un proveedor de correo electrónico que requiera que se escaneen todos los archivos adjuntos antes de abrirlo, para asegurarte de que el equipo no recibe ningún virus.

Configure exploraciones automáticas

Configurar escaneos para que se ejecuten en su ordenador, diariamente o semanalmente, es una buena idea para deshacerse de cualquier virus. Esto mantiene su ordenador actualizado y libre de problemas.

Mira tus descargas

Entendemos que la descarga de archivos de Internet como la música y las películas es lo que muchos de nosotros hacemos, pero también nos expone a muchos en problemas. Los archivos grandes como esos son fáciles de infectarse, así que ten en cuenta lo que estás descargando.

¡Actualización, actualización, actualización!

La “Actualización Crítica” de Microsoft Windows es un ejemplo de mantenerse por delante de todos los hackers. La actualización crítica es una rama completa de Microsoft que se dedica a mantener los ordenadores libres de virus. Mantenga siempre su sistema actualizado

Siempre estar al tanto

Tanto si usted es un fanático del ordenador, como si simplemente usa el suyo de modo esporádico, siempre debe saber cuáles son los últimos virus y cómo afectarán a su ordenador. Esto le preparará si algo sucede para que pueda solucionar el problema antes.

Evite el software pirata

Todo el mundo sabe que se puede descargar software ilegal o 'pirata' online que parece ser más fácil para la cartera, pero en realidad la descarga de esos programas le perjudica. Someten a su equipo a errores difíciles de detectar y terminará causándole más problemas.

Instale un cortafuegos

Un cortafuegos es un programa que se ocupa de controlar las pantallas entrantes de Internet y tráfico de red. Junto con su programa de virus, que puede ayudar a prevenir el acceso no autorizado a su ordenador.

Prepárese

Si usted recibe noticias de un virus que está extendiéndose como fuego descontrolado, debe de estar seguro de estar en alerta máxima. No acepte descargas y tenga cuidado al abrir correos electrónicos y archivos.

Esta unidad debe ayudarle a prepararse para cualquier virus informático que pueda venir a su manera. ¡Recuerde siempre ser cauteloso e inteligente cuando se utiliza el ordenador!

UNIDAD 3: malware

Resultado

Identificar y lidiar con el ciberacoso y las vías para reportarlo.

Malware

El malware, abreviatura de "software malicioso", se refiere a un tipo de programa informático diseñado para infectar el ordenador de un usuario legítimo e infligir daño en él de múltiples maneras. El malware puede infectar ordenadores y dispositivos de varias maneras y viene en un número de formas, sólo algunos de los cuales incluyen virus, gusanos, troyanos, spyware y más. Es vital que todos los usuarios sepan reconocer y protegerse del malware en todas sus formas.

Entonces, ¿qué es el malware? Viene en una variedad desconcertante de formas. Los virus informáticos son probablemente el tipo más conocido de malware, llamado así porque se propagan haciendo copias de sí mismos. Los gusanos tienen unas características similares. Otros tipos de malware, como el spyware, reciben el nombre de lo que hacen: en el caso de spyware, transmite información personal, como números de tarjetas de crédito.

La protección de su ordenador y dispositivos personales del malware, requiere tanto la vigilancia personal continua y la ayuda de las empresas de seguridad profesional. Hoy en día, el malware no sólo apunta a sus ordenadores domésticos, sino también a los dispositivos móviles que usted y su familia están utilizando. Y el problema es más grande de lo que usted podría pensar.

Usted puede ser víctima de un ataque de malware a través de sus navegadores web, correo electrónico, las redes sociales que utiliza, mensajería instantánea, y archivos descargados.

Su dispositivo puede infectarse a través de casi cualquier proceso online o incluso de la memoria USB de un amigo, por lo que es importante utilizar un programa de seguridad que puede proporcionar una protección proactiva completa, ayudándole antes de infectarse.

Así que después de preguntar "¿Qué es el malware?", las siguientes preguntas lógicas son, "¿quién lo está creando, y por qué?" Los días en que la mayoría de malware se creaba por los bromistas adolescentes hace mucho tiempo que pasó. El malware hoy en día está diseñado en gran medida por y para los criminales profesionales.

Estos criminales pueden emplear una variedad de tácticas sofisticadas. En algunos casos, como webs de tecnología, los ciber-delincuentes incluso han "bloqueado" los datos de un ordenador-haciendo la información inaccesible y entonces exigiendo rescate a los usuarios para obtener acceso a esos datos de nuevo.

Pero el principal riesgo que los ciber-delincuentes plantean a los usuarios frecuentes de ordenadores es robar información de banca online, tales como cuentas bancarias y tarjetas de crédito y contraseñas. Los hackers criminales que roban esta información pueden utilizarla para vaciar su cuenta o ejecutar fraudulentamente saldos de tarjetas de crédito en su nombre. O pueden vender la información de su cuenta en el mercado negro, donde esta información confidencial obtiene un buen precio.

Protección contra malware

Así que ahora estamos en la pregunta más importante de todas: "¿Cómo me aseguro de que mi equipo o red está libre de malware?"

La respuesta tiene dos partes: vigilancia personal y herramientas protectoras. Una de las formas más populares para propagar el malware es por correo electrónico, que puede ser disfrazado para parecer como si fuera de una empresa que nos resulta familiar, como un banco, o un correo electrónico personal de un amigo.

Tenga cuidado con los correos electrónicos que le piden que proporcione contraseñas. También con correos electrónicos que parecen ser de amigos, pero tienen sólo un mensaje como "¡Echa un vistazo a este nuevo sitio web!" seguido de un enlace. La vigilancia personal es la primera capa de protección contra el malware, pero no basta simplemente con tener cuidado. Debido a que la seguridad empresarial no es perfecta, incluso las descargas de sitios legítimos a veces pueden tener el malware adjunto. Lo que significa que incluso el usuario más prudente está en riesgo, a menos que tome medidas adicionales.

Instalar software anti-spyware:

Spyware es un programa de software que recopila información personal o información sobre una organización sin su aprobación. Esta información se redirige a un sitio web de terceros. Los programas espía están diseñados de tal manera que no son fáciles de eliminar. El software anti-spyware se dedica exclusivamente a combatir el spyware. Al igual que el software antivirus, el software anti-spyware ofrece protección en tiempo real, analiza toda la información entrante y ayuda a bloquear la amenaza una vez detectada.

Se recomienda el software anti spyware que puede encontrar al final de la lección. Usted puede ir a través y elegir el más adecuado para usted.

Ninguna protección es absoluta. Pero una combinación de conciencia personal y herramientas protectoras bien diseñadas hará que su ordenador sea tan seguro como pueda ser.

Ejercicios

Ejercicio 1: Tome el control de su router a través de una contraseña única:

Paso 1: inicie sesión en su enrutador inalámbrico.

Abra Internet Explorer y teclee en la dirección http://192.168.0.1 o http://192.168.1.1 (por abandono, la mayoría del router tendrá **192,168**. 0.1 o **192,168**.**1,1**como la dirección IP del router predeterminado. Esta es la dirección que ingresaría en la barra de direcciones de su navegador para acceder a la página de configuración de router.)

Ahora inicie sesión en su router. ¿¿Qué??. ¿No tiene ID de usuario y contraseña??. No te preocupes. Tengo sus credenciales (siempre que no haya cambiado antes)

Su ID de usuario y contraseña deben ser:

Cinco Caracteres. Todo minúsculas. 1º alfabeto, despues 4º alfabeto, después, 13 alfabeto después 12 alfabeto y después 14 alfabeto

Hágalo simple para usted:

User ID: admin

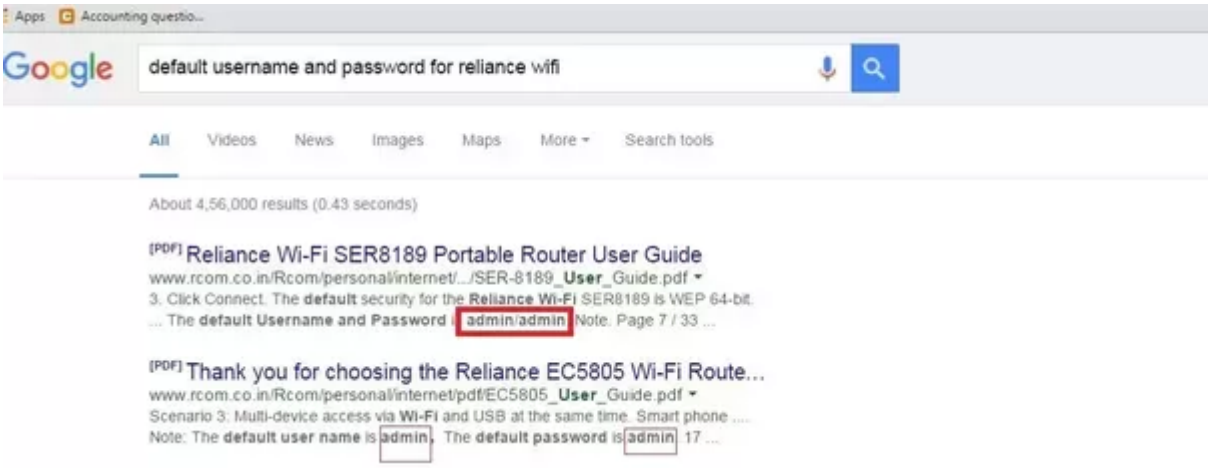
Contraseña: admin

O

User ID: admin

Contraseña (en blanco):

Si no funciona para usted, por favor, busque e Google la identificación de usuario/contraseña por defecto para su router/proveedor de servicios.

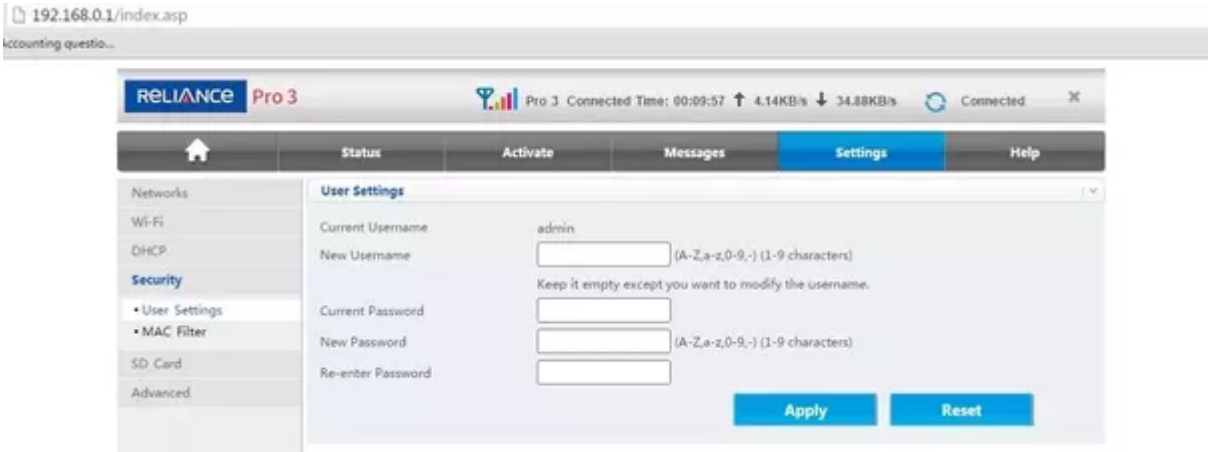


Paso 2: cambie su ID de usuario y contraseña inmediatamente.

- Ir a la configuración

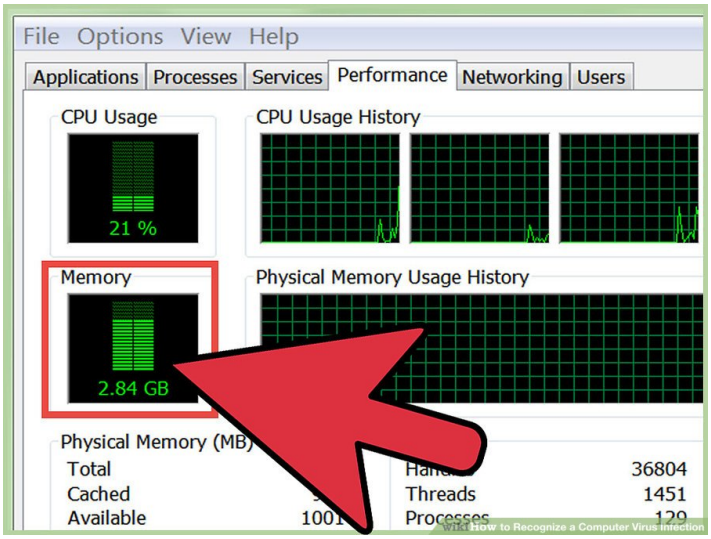
- Configuración de usuario

- Actualice sus nuevas credenciales



Ejercicio 2: Reconocer el virus en el ordenador

1. Compruebe la actividad de su disco duro. Si no está ejecutando ningún programa y la luz de su disco duro se enciende y se apaga constantemente, o puede escuchar el trabajo del disco duro, puede tener un virus que está trabajando en segundo plano



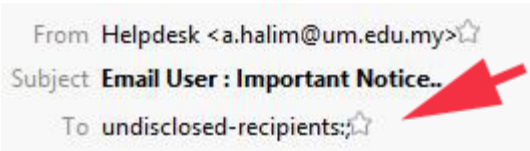
2. Tiempo ¿cuánto tiempo tarda su ordenador en arrancar? Si empiezas a notar que el ordenador tarda mucho más tiempo de lo habitual para arrancar, un virus puede estar ralentizando el proceso de inicio.

Si no puede iniciar sesión en Windows, incluso con la información de inicio de sesión correcta, es muy probable que un virus se haya apoderado del proceso de inicio de sesión.

3. Mire las luces del módem. Si no tiene ningún programa en ejecución y las luces de transferencia del módem parpadean constantemente, es posible que tenga un virus que transmita datos a través de la red.

Ejercicio 3: Reconocimiento de un correo electrónico de malware

1. **Dirección de correo electrónico del remitente**. Si la dirección del remitente no es familiar o no coincide con una dirección esperada para una empresa, es probable que sea un correo electrónico de malware. La mayoría de los correos electrónicos de malware parecen ser avisos de entrega de paquetes, facturas, fax/escaneos o avisos judiciales. Estos correos electrónicos raramente parecen venir de una dirección apropiada, por ejemplo, los correos electrónicos que afirman ser de DHL o UPS son propensos a ser malware si son de la dirección no coincide con UPS.com o DHL.com.
2. **El asunto o adjunto del correo electrónico contiene su nombre de usuario.** Un correo electrónico de malware puede contener su nombre de usuario en el asunto o el archivo adjunto, o el campo Asunto puede estar en blanco. Compare esto con los correos electrónicos normales, que casi siempre tienen un tema y rara vez mencionan su nombre de usuario de correo electrónico.
3. **Sea reticente a abrir un adjunto.** Muchos correos electrónicos que contienen malware le alentarán a abrir un archivo adjunto. Muchos archivos adjuntos pueden seguir siendo dañinos incluso si se está ejecutando el antivirus. Los correos electrónicos sobre los problemas de entrega de paquetes no tienen motivo para exigir que abra un archivo adjunto; si estuvieran enviando un correo electrónico sobre un problema de entrega legítimo podrían simplemente informarle en el cuerpo de texto del correo electrónico.
4. **Sea reticente a seguir un enlace.** Algunos correos electrónicos de malware son similares a los correos electrónicos de phishing donde te animan a seguir un enlace Web. Este enlace Web podría conducir a malware, así que por favor considere todos los consejos anteriores.
5. **Verificación de la información.** Si un correo electrónico le está pidiendo que confirme, revise o proporcione información usando un archivo adjunto, puede ser un archivo adjunto de malware. Reconsidere si esto parece seguro y póngase en contacto con soporte si tiene dudas. Es posible que no sea seguro abrir el adjunto.
6. **Advertencia de problema, amenaza o urgencia**. Los correos electrónicos de malware a menudo incitan al miedo, preocupación, o a una sensación de urgencia. Si un correo electrónico le anima a resolver un problema abriendo un archivo adjunto, debe ser muy cauteloso. Algunos correos electrónicos parecen ser una segunda respuesta a la que le piden un seguimiento. Los ejemplos incluyen lidiar con problemas de entrega de paquetes, información sobre apariencias falsas en los tribunales, o facturas falsas de entidades con las que no puede estar haciendo negocios.
7. **Destinatarios no revelados/no listados.** Si la lista de destinatarios de correo electrónico muestra destinatario no revelado/no enumerado, o una dirección de correo electrónico que no sea el suyo, entonces puede ser malware.



8. **Adjunto sospechoso.** Si el correo electrónico tiene un adjunto inesperado, como un archivo con las extensiones. doc,. zip,. xls,. js,. pdf,. ACE,. ARJ,. WSH,. SCR,. exe,. com,. bat u otros

tipos de archivo de Microsoft Office, entonces puede ser malware. Tenga en cuenta que a veces la extensión de archivo está oculta o el contenido es diferente de lo indicado.

9. **Texto sin formato/ausencia de logotipos.** Los mensajes de correo electrónico más legítimos tienden a escribirse con HTML y pueden tener una mezcla de texto e imágenes. Los correos electrónicos de malware raramente tienen imágenes y tienden a tener un formato sencillo.
10. **Saludo genérico**. Si el correo electrónico se dirige con una frase genérica como "*Estimado cliente*" entonces puede ser un malware o un intento de phishing.
11. **Contenido de datos adjuntos inesperados.** Si finalmente abre un archivo adjunto y el contenido está vacío o es muy diferente de lo que esperaba, puede ser malware. Por favor, ¡póngase en contacto con soporte para ayuda inmediatamente! El soporte puede ser capaz de limitar el daño o ayudar a recuperarlo.

¿Cómo se ven los correos electrónicos de malware reales?

Aquí hay una captura de pantalla real de un buzón que contiene 19 correos electrónicos de malware:

Subject	Correspondents	Date
URGENT RFQ	AL WALEED EQUIPMENTS	03/13/2017 06:55
	starsescorts@gmail.com	03/15/2017 01:27
New Order Attached **KINDLY SEND INVOICE	Amr Hassan	03/15/2017 19:30
We're sad to let you know that our delivery was unusuccessful....	FedEx Expedited Express	03/16/2017 02:53
47929 username2	pkeith@gejlaw.com	03/16/2017 05:29
Delivery Status Notification	webmaster@stroy-exp...	03/16/2017 05:47
	vowsbyjudy@shaw.ca	03/16/2017 14:38
Formal Inquiry	"Anaïs VANACKER"<Va...	03/16/2017 21:16
We have delivery problems with your parcel #7104543	webmaster@whfarm2....	03/17/2017 00:57
INQUIRY	Saigon Offshore	03/17/2017 03:47
	dava@ac-lyon.fr	03/17/2017 14:25
54343 username	juanro5554@hotmail.c...	03/17/2017 14:48
Item Delivery Notification	alifeof8@server.alifeofj...	00:34
UPS courier can not deliver parcel #004287245 to you	webmaster@stroy-exp...	06:23
Parcel Delivery Notification	abidjanbateau@vps286...	06:52
Visa Card Award	info@visa.com	07:21
Problems with item delivery, n.4930349	Apache	09:54
Package Delivery Notification	Apache	10:06
Delivery Status Notification	contrav8@box980.blue...	17:05

Ejercicio 4: cuestionario de seguridad online

Cumplimente este cuestionario online y vea que nota obtiene.

https://www.proprofs.com/quiz-School/Story.php?title=eSafety-quiz

MÁS LECTURAS Y RECURSOS

Los términos que debe conocer

https://www.lifewire.com/top-internet-terms-for-beginners-2483381

Planificación de seguridad en Internet para personas mayores

(descarga en PDF)

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=18&cad=rja&uact = 8 & ved = 2ahUKEwiz8LGAjNjdAhVSGsAKHbISB8QQFjARegQIBxAC & URL = https% 3A% 2F% 2Fvict imserviceslanark. CA% 2Fphotos% 2Fcustom % 2FVSLG% 2FResources% 2FSafetyPlanningForSe niors_English. pdf & USG = AOvVaw3WNu9papw-5PbHbhKSxVFi

Los mejores consejos de seguridad en Internet (descarga en PDF)

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=12&ved=2ahUKEwiz8LGAjNjdAhVSGsAKHbISB8QQFjALegQIBRAC & URL = https% 3 A% 2 F% 2 F Query. Prod. cms. RT. MIC Rosoft. com% 2Fcms% 2Fapi% 2Fam% 2Fbinary% 2FRE1ImTu & USG = AOvVaw0QyXRMv5RLg-kAS0tIaUvz

Cómo protegerse de malware – YouTube video

https://www.youtube.com/watch?v=uJRqZTNMCMo

Los mejores servicios antivirus de 2018

https://www.itproportal.com/guides/best-antivirus-services-for-2018/ ***el***

El mejor software antimalware de 2018

https://www.TechRadar.com/news/Best-Free-anti-malware-software

La protección de sus datos

https://youtu.be/BL7WJM342Uc

Seguridad online para personas mayores

https://www.connectsafely.org/seniors/

Más información de seguridad online

https://www.protectseniorsonline.com/resources/

¿Cómo comprobar si el equipo tiene un virus

https://www.youtube.com/watch?v=4i_cCPhewu4