Sé proactivo con la seguridad

Emily aprendió cómo proteger su computadora del malware, pero por qué se contagió con malware?

Así como usted puede protegerse de los carteristas en una ciudad manteniendo su cartera vigilada y no contando su dinero en público, usted puede aprender hábitos de seguridad para usar su computadora.

Vamos a seguir a Emily mientras aprende cómo usar su computadora para navegar por internet de manera segura.

#1: Siempre verifique la dirección URL del sitio web

Una característica de un sitio seguro es una dirección confiable; siempre debe tener un nombre razonable y relevante para el tipo de página que espera visitar. Por ejemplo, si usted está navegando Facebook, el URL debe contener “facebook.com”

Usted puede poner el cursor del ratón sobre una liga en internet sin hacer clic para ver a dónde lo llevará cuando pulse la liga.

La “S” en “HTTPS” al principio de una dirección web significa que los datos enviados están seguros. Muchas páginas también muestran un icono de un candado para mostrar que el sitio es seguro. Si un sitio web es confiable y verdadero, usualmente tendrá una dirección física o un teléfono que puede ser verificado con facilidad.

Como una regla general, si un sitio web ofrece algo demasiado bueno, normalmente es una trampa. Si usted recibe un correo electrónico o una ventana se abre diciendo que debe responder inmediatamente para reclamar un premio o para recuperar algo, tenga cuidado.

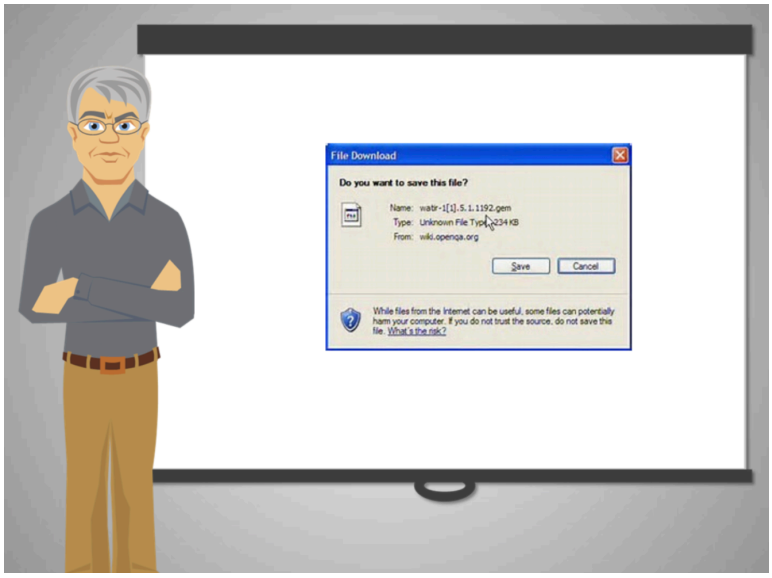
Cuando esté iniciando sesión en algún sitio o enviando información personal o financiera, asegúrese de poner atención y verificar que la dirección del sitio sea segura.

 # 2: Manténgase alejado de las ventanas emergentes

Los sitios web confiables usualmente no le dan información usando ventanas emergentes que aparecen de pronto; estas ventanas deben tratarse con extremo cuidado y cerrarlas sin hacer clic en el contenido.

Tenga cuidado de cualquier ventana que aparezca de repente. Estas ventanas típicamente ofrecen cosas “demasiado buenas para ser ciertas.” ¡Póngase listo cuando navegue por sitios web!

Para más información sobre cómo evitar los sitios inseguros, vea el curso “Las estafas en línea”



 # 3: Evite descargar archivos extraños

Descargar archivos es una de las maneras más comunes para infectar una computadora con malware. Piense primero si de verdad necesita descargar ese archivo antes de hacer clic.

Muchas páginas muestran botones atractivos, pero en realidad son ligas a archivos que tienen malware. Si ve que de pronto algo empieza a descargarse sin que usted lo haya iniciado, cancele de inmediato y salga de ese sitio.

No debe abrir ningún archivo que haya descargado si no está seguro de qué es.

Siempre verifique con alguien antes de instalar un programa que le parezca sospechoso.

 # 4: Tenga cuidado cuando use redes Wi-Fi públicas

Una conexión pública inalámbrica puede usarse sin ingresar una clave. Algunos lugares con redes públicas son librerías, cafeterías, restaurantes, parques, aeropuertos y tiendas departamentales.

Si va a usar su tarjeta del banco en internet, evite las redes públicas; para eso, es más seguro usar una computadora conectada a la red alámbrica o privada.

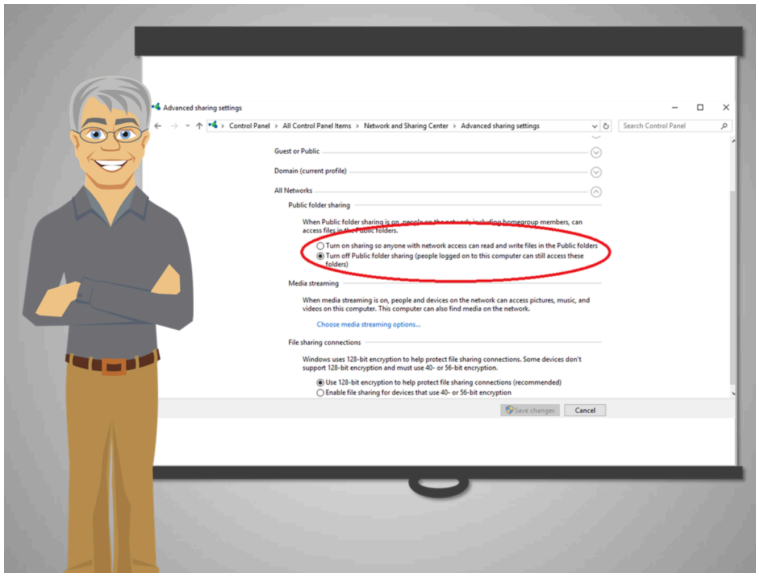
Cuando se conecta a una red pública, sin usar una clave, es posible que alguien en la red pueda ver lo que usted hace.

Por supuesto eso no pasa siempre, pero, así como sus cosas pueden ser robadas en los lugares públicos si usted no las cuida, la gente puede obtener su información si usted está usando una red pública sin precaución.

Es mejor ser cuidadoso y acostumbrarse a usar medidas de precaución siempre que use internet en lugares públicos.

Estos son unos consejos para cuando use una Wi-Fi pública:

Seleccione una red confiable. No se conecte automáticamente a cualquier Wi-Fi que vea, especialmente si tiene un nombre sospechoso. Por ejemplo, si está en una biblioteca, seleccione la red que parezca oficial. Algunas personas pueden crear redes con nombres muy similares a los reales para atraer a la gente. Si tiene duda, pregunte a un encargado cuál es el nombre de la red que ofrece el lugar.



Verifique que su computadora tenga la opción de *compartir archivos* deshabilitada – Muchos dispositivos tienen esta opción por comodidad, pero con esta opción habilitada, usted les permite a otros visitar y tomar archivos de su dispositivo.

Verifique que las páginas que visita tengan HTTPS en la dirección; esto evita que sus datos sean interceptados por otros en el mismo sitio. Esto es especialmente importante cuando usted usa su clave para visitar sitios que tienen información personal.

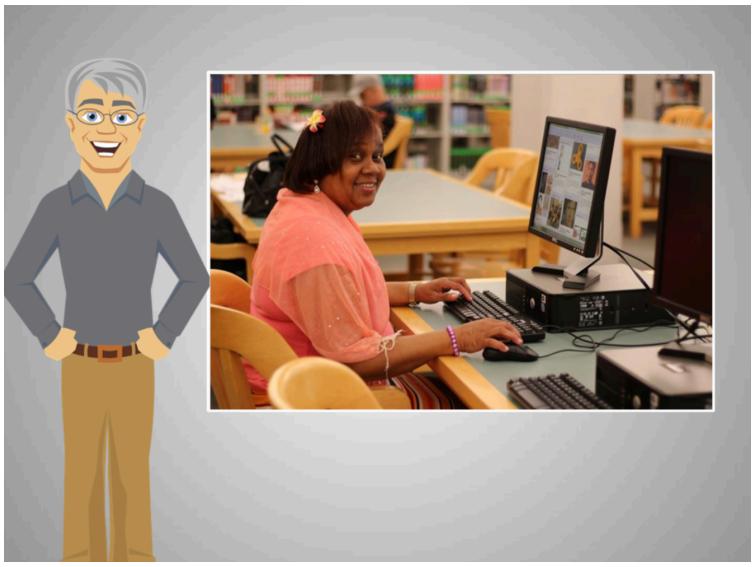
Las redes públicas son buenas para navegar internet y buscar cosas, pero nunca envíe información personal en una red Wi-Fi pública. Si usted planea ver su cuenta de banco o accesar información confidencial es mejor que use una red privada.

 # 5: Proteja su computadora personal con una clave de acceso.

En caso de que alguien tenga acceso a su computadora sin su consentimiento, una clave de acceso puede evitar que la persona haga uso de ella y así su información estará protegida.

Para ponerle clave o cambiar la clave de su computadora, abra el Panel de Control desde el menú de inicio, escoja la opción de *User Accounts*. Después escoja Crear o Cambiar su/mi clave. Siga las instrucciones en la pantalla para agregar o remover su clave.

Este proceso puede parecer difícil la primera vez que lo haga. Pida ayuda a una persona de su confianza si las instrucciones son confusas. Escriba su clave y manténgala en un lugar seguro por si se le olvida.



La computadora de Emily estaba muy lenta a consecuencia de no actualizar el software, no usar un programa de protección, y por navegar sitios web inseguros.

Emily aprendió cómo proteger su computadora y usted también. ¡Tenga cuidado de mensajes que le piden que proporcione información confidencial – siempre revise!

Manténgase atento a los mensajes de correo electrónico no solicitados, a las ventanas emergentes y a los sitios web sospechosos. Actualice sus programas, verifique las direcciones de las páginas que visita y lea con cuidado.

Aprenda a identificar los signos de alarma.

Ahora que su computadora funciona correctamente, Emily está lista para regresar a navegar por internet y hacer su vida más fácil y entretenida.

Built by Microsoft

Microsoft