Tech Savvy Seniors

Introducción a la Seguridad Cibernética: Como estar a salvo en línea.

El internet se ha vuelto una parte indispensable en nuestras vidas y podemos hacer muchas cosas en línea. Sin embargo, queremos decirle como usar internet de una manera segura y contarle las precauciones generales para así proteger su privacidad.

1. ¿Necesito protegerme en internet?

En internet, cualquiera puede falsificar su identidad, asi que Ud. necesita saber de quién debe aceptar correos, donde es seguro hacer compras y a quien debe darle su información personal.

El software de seguridad de internet juega un rol muy importante para mantenerlo seguro ante los crímenes cibernéticos.

Algunos pasos de sentido común le harán difícil una estafa:

- Tenga sus computadoras y todas las contraseñas de redes inalámbricas protegidas.
- Nunca le de detalles privados o comprometedores en línea a extraños.
- Instale un software de seguridad.

2. Las amenazas que puede recibir:

1. Malware (software malicioso):

Es creado con la intención de acceder a su computdora y obtener información, usualmente con el propósito de vender a otras partes interesadas. El tipo más común de malware conocido es un virus. Ud. Necesita tener cuidado que programas baja y abre en su computadora. Si baja un programa desde una fuente de mala fama, puede estar infectado.

Aun si Ud. navega seguramente, no puede prevenir que maliciosos códigos estén 100%infectados por el último código malicioso o el descuido de un usuario. Consiguientemente, debe instalar en su computadora un software de antivirus y habilitar la protección en tiempo real. La vacuna puede ser esencial para la seguridad de la PC porque efectúa inspecciones cuando no solo Internet, pero otros aparatos externos como el USB y CD son detectados.

2. Piratas informáticos (hackers)

Tratan de aprovecharse de la vulnerabilidad en la seguridad de su computadora para acceder a sus archivos personales.

Como ejemplo, ¿conoce el sistema de compartición de archivos Windows? Este permite a una computadora enviar documentos a otra computadora sobre un sistema de red. Pero si no esta protegido por una contraseña, el pirata informático puede detectar eso y usarlo para acceder a sus archivos o implantar un virus u otro tipo de malware en su PC.

3. Robo de identidad, hurgo y estafadores.

No hay reglas para decir quien es Ud. en internet por eso hay personas que pretenden ser algo o alguien que no son para que les de dinero o les revele información personal como el número de su tarjeta de crédito y accesos bancarios en línea. Esencialmente, los timadores han lanzado su negocio en línea y están intentando aprovecharse de Ud. Una estafa común es el intento de hurgo en donde el estafador pretende ser una persona u organización con la cual Ud. tiene una conexión y así consigue sacarle información personal como los datos de su cuenta bancaria.

Existen algunas maneras muy sencillas para ayudarle a identificar estafas de correo basura y hurgo y evitar meterse en problemas en internet. Aquí hay algunas cosas para estar pendiente:

- Revise el tema del correo electrónico y quien se lo envía. ¿Es de alguien que Ud. conoce o describe algo a lo que Ud. recuerda haberse suscrito Si no, es probablemente una estafa.
- ¿Hay una oferta de dinero a cambio de su información personal? ¿Promete consecuencias negativas si Ud. no responde con su información personal o clicando o conectándose? ¿Tiene su nombre en el campo PARA? Estas son todas indicaciones que se trata de una estafa.
- ¿El correo contiene errores de gramática y deletreo y esta presentado de una manera muy pobre? Es de una cuenta de correo gratis (Outlook.com, yahoo.com, Gmail.com). Si lo es y el emisario es desconocido para Ud. véalo sospechosamente.

Los correos electrónicos de “Estafa de vanidad” pueden ser muy llamativos y parecer auténticos. Si esta tentado, asegúrese de preguntarse por qué Ud. recibiría este tipo de correo, esos nombres, direcciones y sitios de web.

4. ¿Qué hace el software de seguridad?

Tipos de softwares de seguridad

La buena noticia es que Ud. puede protegerse de la mayoría de los ataques usando un software de seguridad. Su computadora ya viene con algún software construido, pero Ud. debe añadir uno adicional sobre ese. Hay diferentes tipos que puede conseguir:

1. **Antivirus:** protege su computadora de la mayoría de los malwares (y se basa en las defensas construidas de su computadora para el resto) Puede conseguirlo gratis o a un precio muy bajo.

2. **Paquete de seguridad en internet:** : Un paquete de software que protege su computadora de un gran rango de amenazas, incluyendo malwares, fraudes, correo no deseado, sitios de web tramposos, piratas informáticos y mucho más. Los paquetes de seguridad de internet tienen un precio anual (usualmente entre $60 y $130).

Protegiendo su computadora

1. Un Firewall actúa como un punto de seguridad para el tráfico de internet. Solamente permite pasar tráfico autorizado.
2. Un software antivirus rastrea y remueve cualquier malware, incluyendo virus, un programa espía y un adware, eso viene en su computadora. Es común que su computadora no venga con un software de antivirus y deba instalarlo.

5. Eligiendo un software de seguridad

Se recomienda que cualquier aparato al que Ud. conecte a internet, su PC, tableta o smartphone, este protegido por un software de antivirus o, idealmente, un traje de seguridad de internet. Si no puede abonar la tarifa anual puede conseguir una aplicación gratuita. Esto no lo protegerá tan bien como el traje de seguridad, pero le ofrecerá una protección básica.

Microsoft: www.microsoft.com/securityessentials

AVG: www.avgfree.com.au

Avast!: www.avast.com

Comodo: www.antivirus.comodo.com

6. Manteniendose Seguro (un software de seguridad no es suficiente)

Instalar un sistema de software de seguridad en su computadora es una gran e importante paso para protegerse en línea. Pero esa no es toda la solución: estos softwares no pueden protegerlo de timadores y criminales cibernéticos. Muchas de las cosas que hacemos en línea incluyen información que es importante, personal y privada. Su información personal es información que lo identifica. Para protegerla debe ser muy cuidadoso con lo que comparte públicamente
en línea.

¡Sentido común y una saludable dosis de sospecha hará que Ud. sea muy difícil de estafar!

Estas son algunas simples cosa que puede hacer para mantenerse a salvo:

1. Use una contraseña fuerte y única y cámbiela regularmente.
2. No publique información personal en sitios públicos.
3. No abra correos adjuntos a menos que este muy seguro.
4. Tenga cuidado con los correos que responde.
5. Tenga cuidado a quien le da los datos de su tarjeta de crédito.
6. No instale programas de fuentes no fiables.