Proteja su Privacidad en Línea

Cada vez más las actividades en línea se han convertido en parte fundamental de la vida diaria de las personas. De forma cotidiana, seguramente usted envía correos electrónicos, revisa su cuenta de redes sociales o el estado del clima, reproduce videos en tiempo real, envía *tweets*, comparte fotos, descarga música, crea documentos o hace copias de respaldo de archivos utilizando servicios en línea tales como OneDrive o Dropbox, entre otras actividades.

Cuando usted utiliza un navegador de red (como Internet Explorer o Firefox) o una aplicación, toda esta información que usted publica, envía, o crea en línea, va de su computadora, teléfono u otro dispositivo conectado a Internet hacia la nube. Y desde allí, tal información es enviada a los servicios y personas con las que usted interactúa.

Con toda esa información guardada en la nube usted puede no estar consciente sobre el impacto que la Internet puede tener respecto de su privacidad y la seguridad de sus datos, así que es importante que aprenda algunas medidas básicas para ayudar a protegerla.

No todos los servicios de nube son iguales. Tal y como lo hace en el mundo real, utilice servicios de empresas bien establecidas y de reconocida prestancia, ya sea que ofrezcan redes sociales, servicios de correo electrónico, servicios para compartir fotos o servicios de almacenaje de información, etc., verificando en todo caso que sus políticas de privacidad sean confiables y ofrezcan una adecuada administración de los datos. Esto, sin duda alguna, ayudará a minimizar sus riesgos de pérdida o uso no autorizado de sus datos.

Usted también puede contribuir a fortalecer su privacidad en línea siguiendo estos consejos prácticos los cuales le ayudarán a controlar lo que usted revela acerca de sí mismo y a determinar quién tiene acceso a esa información.

Proteja su información

Aumente la seguridad de su computadora. (Microsoft le puede ayudar a hacerlo: aka.ms/proteja-su-pc)

- Mantenga todo su software (incluyendo su navegador de red y aplicaciones) al día con actualizaciones automáticas. Instale anti-virus y software anti-spyware de compañías en las que confíe. Proteja su *router* inalámbrico con una contraseña segura y use unidades de memoria externa (*flash drives)* con precaución.
- Ignore cualquier mensaje de correo electrónico, advertencias emergentes u otros avisos que digan que protegerán su dispositivo o que ofrezcan remover virus. Es altamente probable que hagan justo lo contrario.

Cree contraseñas fuertes. Utilice frases largas u oraciones que mezclen mayúsculas y minúsculas, números y símbolos. Mantenga sus contraseñas privadas y únicas para cada sitio. (Aprenda cómo hacerlo: aka.ms/contrasena-segura)

¡Su información ya está en la nube!

La nube es una red de computadoras en Internet – una "nube" de computadoras – en la cual datos, incluyendo los suyos, pueden ser almacenados. Cuando usted revisa su correo electrónico o las noticias, paga facturas o juega en línea, usted está accediendo a la nube. Su información también se encuentra en la nube si sus archivos están almacenados ahí.

Dado que los datos están en la nube, usted puede accederlos desde – y compartirlos con – su teléfono o computadora o cualquier otro dispositivo conectado a Internet.

Reporte el robo de identidad

Si usted ha sido víctima del robo de identidad, repórtelo inmediatamente a las autoridades competentes en su país y obtenga de ellos recomendaciones de los siguientes pasos que puede tomar.

Más ayuda

- Obtenga más información sobre cómo proteger su privacidad en Internet: aka.ms/tu-privacidad
- Aprenda cómo protegerse del robo de identidad en línea: aka.ms/robo-de-identidad
- Descubra cómo Microsoft le ayuda a proteger su privacidad: aka.ms/consejos-seguridad-en-linea
- Aprenda a reconocer mensajes, vínculos o llamadas telefónicas de *phishing*: aka.ms/estafa-en-linea
- Obtenga consejos en general sobre cómo utilizar Internet en forma más segura: http://www.alertaenlinea.gov/temas/evite-estafas

Deje la actividad sensible para una red segura en el hogar. No realice transacciones bancarias, compras, revise correos electrónicos o haga otro tipo de negocios que expongan sus nombres de usuario o contraseñas sobre un Wi-Fi "prestado" o público (tales como *hotspots*). Puede ser que otras personas que estén utilizando la red puedan ver lo que usted está enviando. (Aprenda cómo utilizar el Wi-Fi en forma más segura: aka.ms/wifi-seguridad)

De respuestas sin sentido a las preguntas de seguridad – respuestas que no se puedan encontrar buscándolas en Facebook, por ejemplo, pero que usted pueda recordar. Por ejemplo, si la pregunta es "¿En dónde nació?", la respuesta puede ser "verde".

Piense antes de compartir

- No ponga nada en línea que usted no quisiera ver en una cartelera. Proteja sus números de cuenta, nombres de usuario y contraseñas con especial cuidado.
- Adopte controles de privacidad fuertes para manejar quién puede acceder a su perfil o fotos, cómo puede ser encontrado por otros en Internet, quién puede hacer comentarios, y cómo bloquear el acceso no deseado.
- Lea la política de privacidad del sitio web o aplicación. La misma debe explicar qué datos recolecta acerca de usted, cómo los comparte y protege, y cómo puede usted accederlos y actualizarlos.

Protéjase contra el fraude

Detecte los signos de una estafa. Los más peligrosos son aquellos que parecen ser genuinos. Tenga cuidado con las solicitudes de su "banco" preguntando por contraseñas, notificaciones de que se ha ganado la lotería, solicitudes para que ayude a un extraño lejano a realizar una "transferencia de fondos", ofertas para mejorar su crédito o protección contra virus, y provocaciones similares. (Aprenda a reconocer y evitar las estafas: aka.ms/estafa-en-linea).

Tenga cuidado *antes* de abrir archivos adjuntos o de dar clic en vínculos en mensajes extraños o inesperados, aún si son de amigos o compañías en las que confía. Podría ser víctima de una estafa en línea – tal como *phishing* – o descargar software que le permita a hackers controlar remotamente su computadora o grabar datos personales sensibles – tales como contraseñas o números de cuenta – a medida que usted los digita. Verifique antes con el remitente para asegurarse de que el mensaje sea genuino en lugar de hacer clic en Contestar.

Busque evidencia de que un sitio web es seguro y legítimo antes de ingresar datos sensibles, y asegúrese de entrar al sitio utilizando un camino en el que usted confíe, tales como un marca páginas *bookmark* o un favorito que usted haya creado.

*Los signos positivos de una conexión segura incluyen una dirección web que comience con http**s** ("**s**" significa segura) y un candado cerrado. Una indicación aún mejor (para aquellos sitios web que la soportan) es una barra de dirección verde.*