OUCH! | Febrero, 2020

El Boletín Mensual de Concientización en Seguridad para ti

Privacidad en redes sociales

Resumen

La mayoría de las personas nunca considerarían entrar a una habitación llena de gente y compartir en voz alta los detalles de su vida privada (desde aspectos de salud hasta nombres, edades, trabajos o ubicación de escuela de familiares y amigos) con un total de extraños. Pero a menudo estas mismas personas no pensarán dos veces antes de publicar la misma información en redes sociales. Las consecuencias de compartir demasiada información puede afectar no solo tu vida personal y profesional, sino también la vida de tus familiares y amigos.

Las redes sociales son un excelente lugar para reconectarse, compartir y aprender. Sin embargo, solo asegurar que las configuraciones de privacidad de tus redes sociales son robustas no es la única manera de protegerte a ti mismo. Una vez que publiques cualquier cosa en línea, perderás el control sobre ella. Necesitas entender qué es lo que se recopila y cuál es el uso que se le da. Aquí encontrarás algunas consideraciones de privacidad que debes tomar en cuenta cuando utilizas redes sociales:

Configuraciones de privacidad: Crea cuidadosamente y revisa frecuentemente las configuraciones de privacidad de todas tus cuentas de redes sociales, especialmente cuando haya cambios en los términos del servicio y políticas de privacidad. Recuerda que si has definido las configuraciones de quién puede ver tus publicaciones, toda tu información está siendo recopilada, minada y almacenada en los servidores de las plataformas de redes sociales—quizás para siempre.

Árbol de privacidad: Las configuraciones de tus redes sociales no pueden protegerte de tus amigos, parientes y compañeros de trabajo que pueden ver tus publicaciones y luego tengan la capacidad de compartir esas mismas publicaciones con otras personas de su círculo de amigos, etc.

Publicaciones sobre tu familia: A todos nos encanta hablar de nuestros amigos y familia. Pero publicar fotos tontas de pasteles de cumpleaños, problemas de salud o de comportamiento pueden provocar acoso, especialmente para aquellos que son jóvenes y podría afectar sus vidas personales.

Intercambio de información: Si un servicio es "gratuito", entonces tú eres el producto. Investigaciones han encontrado que lo que haces en línea se puede vender a otros.

Servicios de localización: Tus datos de registro de llegada a algún lugar pueden agregarse a otros datos personales para crear un perfil de tu vida y tus hábitos, que pueden provocar acoso u otro tipo de reacciones similares. Adicionalmente, ten en cuenta la información de localización incluida en cualquier foto o video que publiques.

Inteligencia Artificial: Esta junto con las redes sociales y la mercadotecnia son la combinación perfecta. Los mercadólogos ahora utilizan información recabada de tus hábitos en línea para llenarte de anuncios centrados en tus últimas búsquedas o compras, y así seguir aprendiendo más sobre ti.

Muerte digital: Cuando una persona muere, su presencia digital llega a ser más vulnerable a personas mal intencionadas, si los que le sobreviven no mantienen o eliminan sus cuentas. La privacidad de un individuo no se trata solo de esa persona, puede afectar también a su familia extendida y amigos.

Divulgación involuntaria: La información que publicas sobre ti mismo puede revelar mucho de tu historia personal, y por lo tanto las respuestas de tus preguntas de seguridad secretas en línea.

La privacidad es más que solo configurar las opciones de privacidad en tus cuentas de redes sociales. Cuanta más información compartas, y cuanto más compartan otros sobre ti, mayor será la información recabada y utilizada por corporaciones, gobiernos u otros. Una de las mejores formas de protegerte a ti mismo es evaluar y limitar lo que compartes y lo que otros comparten sobre ti, independiente de las opciones de privacidad que utilices.

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.
Sitio web: http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Editor invitado

Cathy Click *cuenta con casi 14 años de experiencia en el desarrollo del programa de concientización en seguridad de la información para una empresa de la lista Global 500 de Fortune. A Cathy le encanta abordar temas técnicos complicados y traducirlos a un lenguaje fácil de entender para ayudar a las personas a aumentar su seguridad en línea .*

Recursos

Herencia digital:	http://www.sans.org/u/Z2G
Estafas a través de redes sociales:	http://www.sans.org/u/Z2L
¿Realizo respaldos?:	http://www.sans.org/u/Z2Q