CONSEJOS

Privacidad y seguridad en redes sociales

hiperderecho

Introducción

Las redes sociales permiten conectarse rápido y fácil con amigos, conocidos y familiares, pero también abren la puerta a que personas que no invitaríamos a nuestro ambiente de confianza intenten entrar en él.

Debido a la gran popularidad de las redes sociales como una herramienta de interacción, entretenimiento, e incluso trabajo, es imposible aislarse por completo de ellas. Sin embargo, sí es posible hacer un uso más informado y seguro de las herramientas que las redes sociales nos dan.

Hiperderecho ha preparado esta ayuda memoria para resaltar algunos de estos conceptos generales, y detallar algunas consideraciones para las redes que actualmente son más relevantes para adolescentes y jóvenes.

Creemos que las redes sociales, como cualquier tecnología, tienen gran potencial para el empoderamiento social, pero solo si son usadas de manera crítica e informada.

Considera los consejos en esta guía para hacer más privada y segura tu experiencia usando redes sociales.

Usar tecnología no es lo mismo que entenderla

Recuerda que aunque una persona sea usuaria de tecnología a tiempo completo, puede igual estar poco informada sobre cómo realmente funcionan los servicios que usa.

Piensa, por ejemplo, en un automóvil: casi todos usamos un auto, bus, o taxi a diario. Sin embargo, ¿qué tanto sabemos de cómo funciona un auto? ¿Sabemos identificar un auto "seguro"? ¿Sabemos qué sucede bajo el capót del auto?

De la misma forma, usar un servicio no nos hace especialistas en él, ni conocedores de los entretelones del mismo. Quizá pasamos muchas horas al día en Facebook, o usamos Instagram hace muchos años, pero eso no nos hace inmunes a errores comunes que ponen en peligro nuestra privacidad y seguridad.

Lección

No confundas estar familiarizado y acostumbrado a un servicio, con entenderlo a la perfección.

Es mejor empezar con una cuenta privada

La manera más sencilla de estar más seguros en internet es evitando compartir información de forma innecesaria, es decir, haciendo nuestras cuentas privadas como primera opción.

Mantener nuestro perfil personal, fotos y publicaciones como elementos privados, aun si no entendemos del todo una red social, es siempre mejor a escoger un perfil público que pueda ser explotado por desconocidos.

Todas las redes sociales mencionadas en esta guía permiten crear perfiles casi perfectamente privados. Así que nuestra recomendación es considerar siempre esta opción como punto de partida.

Si escoges recordar una cosa de esta guía, que sea lo siguiente: mientras menos información reveles, menos expuesto a amenazas estarás.

Lección

No te dejes llevar por la emoción de compartir contenido, piensa bien si una cuenta privada no es una mejor opción para ti.

Si parece muy bueno para ser verdad...

Otra buena idea es desconfiar de ofertas, eventos y grupos en donde lo que se ofrece es "demasiado bueno para ser verdad".

Un clásico ejemplo son los eventos de "sorteo de iPhone directo de Apple", o "venta de computadoras de exceso de stock, a mitad de precio". Estas son tácticas para captar nuestra atención y recolectar nuestros datos para posibles estafas.

En algunos de estos engaños se pidan datos como correos electrónicos, nombres completos, números de documento, teléfono. El objetivo de los estafadores es identificar posibles víctimas para robar su identidad, o engañarlos para que les entreguen dinero, como "cuotas iniciales" para entrar a sorteos, o grupos privados.

Te recomendamos no tomar en cuenta mensajes o “datos” que suenan demasiado buenos para ser verdad, ¡lo más probable es que sean una gran estafa!

Lección

Si algo suena demasiado bueno para ser verdad, o a un precio demasiado bueno, es muy probable que no solo sea falso, si no también una estafa.

Datos extra: etiquetar ubicación, amigos

La mayoría de redes sociales te permiten "etiquetar" tus publicaciones con datos como el lugar, o las personas con las que estás. La idea, para la red social, es hacer más fácil que otros usuarios puedan encontrar tus publicaciones.

Estas opciones, a veces indiscretas, suelen ser inofensivas si se usan de manera cuidadosa. Sin embargo, no ignores que sí existe un peligro real al compartir demasiados detalles y dejar un “rastro digital”.

Por ejemplo, si frecuentemente compartes fotos etiquetando a tusamigos cercanos o lugares favoritos, es fácil luego analizar estos datos y crearnos una idea muy completa de tu círculo social y costumbres.

Te recomendamos ser selectivo con estas etiquetas. Asegúrate de que tienes el consentimiento de tus amigos para etiquetarlos, y sé respetuosos de no etiquetar lugares como casas u oficinas privadas.

Lección

Sé selectivo para no dejar un “rastro digital” de tus amigos, rutina, y de tus espacios privados.

Tu cuenta, usuario y contraseña

Tu usuario y contraseña de una red social no son datos que debas compartir con nadie, bajo ninguna circunstancia, ni siquiera con la red social misma.

Aunque a veces piensas que la persona con quien quieres compartir estos datos tiene toda tu confianza, es posible que esa relación cambie con el tiempo, o incluso de un día al otro. Sin saberlo, podrías haber dejado tus mensajes y fotos en manos de alguien que por descuido o por mala onda puede compartirlos con otros.

También te recomendamos no confiar en personas que te exigen o presionan para entregar tu contraseña de redes sociales. Estos intentos de manipulación, aludiendo a "confianza", son malas señales. Lo mejor es negarnos firmemente.

Del mismo modo, no te recomendamos usar cuentas "compartidas" por familia o amigos, pues estas cuentas crean un falso sentido de seguridad y desvirtúan lo que significa la privacidad en línea.

Lección

No compartas tu contraseña con nadie. Podrías acabar compartiendo más datos personales de los que crees. Desconfía si te presionan.

Consejos para Facebook, Instagram y WhatsApp

Facebook

Para proteger: Quién puede ver nuestro perfil personal, nuestras publicaciones. Quién puede escribirnos a la bandeja de entrada (inbox).

Para evitar: Incluir demasiada información sobre lugares ("check-ins"), personas, o actividades.

Para considerar: No ingresar datos de perfil innecesarios como relaciones familiares, o centro de estudios. A pesar de la insistencia de Facebook, estos datos no son necesarios.

Tip clave: Visitar la sección de "Privacidad" en Configuración, y asegurarnos que estamos de acuerdo con todas las opciones .

Herramienta: La opción "Chequeo de privacidad" (Privacy Check-up) en el menú de Ayuda. La herramienta explica paso por paso varias de las opciones de Facebook sobre privacidad.

Instagram

Para proteger: Quiénes pueden ver nuestras publicaciones, enviarnos mensajes, y quiénes nos siguen.

Para evitar: Incluir demasiados detalles de nuestros amigos, lugares. Cuidar los Instastories, para evitar dar datos en tiempo real de nuestra actividad.

Para considerar: Qué revelamos en Instastories, si realmente queremos una cuenta pública, y qué datos personales se pueden ver en nuestras fotos.

Tip clave: Revisar las opciones en "Privacidad y Seguridad" en Configuración para escoger si nuestra cuenta es privada, revisar cuentas bloqueadas y quiénes pueden enviarnos mensajes.

Herramienta: La sección de Configuración en Instagram es de las más completas y permite tener una cuenta muy privada, nuestra sugerencia es considerar cada una de las opciones.

WhatsApp

Para proteger: Nuestra foto de perfil, nombre, estados, y (opcionalmente) nuestros indicadores de lectura y actividad.

Para evitar: Compartir estados de WhatsApp (stories) porque son visibles a cualquier persona que tenemos en los contactos del teléfono. Responder a números desconocidos. Reenviar o creer mensajes "cadena" sobre oportunidades, ofertas, sorteos, desastres.

A considerar: Si estamos de acuerdo con hacer pública nuestra foto de perfil y nuestro nombre. La configuración por defecto hace que cualquier persona con nuestro número de teléfono pueda ver nuestra foto de perfil y nombre.

Tip clave: Confirmar en persona el número de teléfono de cada contacto nuevo, para saber que estamos hablando con quien creemos.

Herramienta: La sección "Privacidad" en "Cuenta" en Configuración permite escoger quiénes queremos que puedan ver nuestros datos como foto, última conexión, estados.

Elaborado por
hiperderecho

Otra buena idea de
hiperderecho.org

Fotos
Erik Lucatero, freestocks.org, Priscilla Du Preez, Tim Bennettvva