El País (Cali)

Publicación	El País General, 6	Fecha	12/06/2022
Soporte	Prensa Escrita	País	Colombia
Circulación	69 610	V. Comunicación	580 854 943 COP (138,848 USD)
Difusión	159 001	Tamaño	1456,72 cm² (98,1%)
Audiencia	159 001	V.Publicitario	73 293 999 COP (17 520 USD)

Siglo Data + HALLON INTELIGENCIA DE MEDIOS

INFORME EXCLUSIVO

LOS PELIGROS DE EXHIBIR LA VIDA PRIVADA EN REDES

Según la OMS el uso excesivo de las tecnologías tiene la misma consecuencia que una droga. De esta forma ha determinado que la adicción a Internet como smartphones o tablets entre otros, se califica ya como enfermedad.

Algunos autores, ven en el abuso de las publicaciones en las redes, la necesidad de recibir cariño y la valoración social. También está la necesidad de aprobación y aceptación de los demás, y la intención de paliar la soledad.

Al fiscal paraguayo Marcelo Pecci, asesinado en Colombia, los sicarios lo ubicaron rastreando las publicaciones de las redes sociales de su esposa. Autoridades advierten que no es la única víctima cuya información en la web fue clave para los delincuentes. Claves para blindarse.

El detalle lo reveló esta semana el Fiscal de Colombia, Francisco Barbosa, en una rueda de prensa: los asesinos de Marcelo Pecci, el fiscal antimafia de Paraguay, rastrearon su ubicación gracias a las publicaciones que hacía su esposa en Instagram y otras redes sociales. "Los delincuentes manifestaron que en muchas ocasiones estuvieron perdidos, pero gracias a esas publicaciones ubicaron al fiscal en un hotel de Barú, Cartagena", dijo Barbosa.

En su Instagram, efectivamente la periodista Claudia Aguilera, esposa de Pecci, compartió las fotos tanto de su reciente boda, como de la luna de miel en Cartagena: las caminatas por el centro histórico, las visitas a las playas y una de las imágenes más conmovedoras: un primer plano de sus manos entrelazadas, sosteniendo unos diminutos zapatos rojos. El fiscal Pecci y Claudia esperaban un bebé. A los sicarios, por supuesto, no les importó.

Los encargados de hacerle seguimiento a la pareja, según la Fiscalía de Colombia, fueron identificados como Cristian González y Marisol Londoño, ya capturados. Se mantuvieron agazapados en las redes, siguiendo pistas que los condujera al fiscal. El resto de la estructura criminal estaba liderada por un hombre llamado Francisco Correa. Fue quien contactó al sicario que le disparó a Pecci desde un jet ski en Barú.

Las autoridades insisten: dejar los perfiles de las redes sociales abiertos, sin ninguna barrera de privacidad, es igual a dejar la puerta de la casa abierta de par en par e irse de paseo. El fiscal Pecci no es la única víctima de la información personal que se publica en la web que en ocasiones es usada en contra de sus autores.

En 2021 asesinaron en Cali a Carolina Zúñiga Hernández. Tenía apenas 22 años. La encontraron amarrada de pies y manos. También la torturaron. La Policía ofreció una recompensa de $10 millones para encontrar al asesino, quien la citó a través de Facebook.

Un investigador de la Unidad de Delitos Informáticos de la Policía asegura que no son tan escasos los casos de personas que anuncian en sus redes sociales que están en vacaciones y que han encontrado al regreso sus casas desocupadas justo por revelar ese dato al parecer tan inocente: "salimos de viaje", luego la casa está disponible para los ladrones.

Según la Fiscalía colombiana, los asesinos del fiscal paraguayo Marcelo Pecci lo siguieron gracias a estas publicaciones en redes sociales de su esposa, durante su viaje de luna de miel.

Sol González, especialista en seguridad informática de la compañía Eset Latinoamérica, recuerda la historia de un hombre que anunció en Facebook su destino en las próximas vacaciones junto con la foto de los pasajes, y en la fila para ingresar al avión un par de días después le informaron que el tiquete ya había sido usado.

En México, en 2021, Daniel Moreno publicó en una red social que había conseguido las escasas boletas para el estreno mundial de la película 'Spiderman, sin regreso a casa', y subió la foto de la compra en línea con el respectivo código QR. Alguien le hizo un 'pantallazo' al código y le robó las boletas.

"El lema de las redes sociales siempre ha sido compartir, compartir y compartir. Sin embargo, es supremamente importante determinar, en primera instancia, el nivel de acceso a nuestro perfil. La primera barrera es que los perfiles sean privados, para que no los pueda ver cualquier persona. En teoría el manejo de las redes debería ser muy dirigido a la gente que es cercana, amigos, familia y gente de absoluta confianza", dice el profesor Pedro Wightman, director del programa de Matemáticas Aplicadas y Ciencias de la Computación de la Universidad del Rosario.

El profesor Wightman, así como Nazly Borrero Vásquez, ingeniera en ciberinteligencia de la compañía Cyber – Risk Intelligence, coinciden también en que un error muy común a la hora de usar las redes sociales es activar la geolocalización, que permite determinar en tiempo real los lugares donde nos encontramos. También etiqueta el contenido multimedia que publicamos con el lugar exacto donde se tomó la foto o el video.

"Se debe desactivar esta geolocalización, naturalmente. Y a la hora de publicar se debería hacer con retraso de tiempo. Es decir, si sale de vacaciones y desea compartir las fotos del viaje, hágalo cuando regrese, no durante el viaje. O si está en un restaurante que le gustó, publíquelo al día siguiente, no en tiempo real", agrega el profesor Wightman.

Por cierto: para desactivar la localización se debe abrir la configuración del teléfono. En 'Personal', o 'herramientas', hacer clic en 'Acceso a la ubicación', donde se activa o desactiva el uso del GPS en el dispositivo.

Hace unos años se hizo, a propósito, un experimento social en Estados Unidos, que trataba de mostrar los vulnerables que somos al publicar tanta información personal en las redes sociales. La página donde se hizo el experimento se llamaba 'Please Rob me' (por favor róbame).

Allí revisaban redes sociales, identificaban las publicaciones de la gente que anunciaba que estaba en un res-

El País (Cali)

Publicación	El País General, 7	Fecha	12/06/2022
Soporte	Prensa Escrita	País	Colombia
Circulación	69 610	V. Comunicación	580 854 943 COP (138,848 USD)
Difusión	159 001	Tamaño	1456,72 cm² (98,1%)
Audiencia	159 001	V.Publicitario	73 293 999 COP (17 520 USD)

Siglo Data + HALLON INTELIGENCIA DE MEDIOS

taurante, o en un paseo, y publicaban la lista de quienes estaban fuera de su casa según, también, la geolocalización de las redes.

El portal generó polémica y cerró, pero sus creadores argumentaron que lo que pretendían era crear conciencia sobre el inminente peligro que implica revelar en la web la información de donde nos movemos, así como los horarios, las rutinas.

"En general la recomendación es publicar lo menos posible. La sociedad debe recobrar el sentido de la privacidad. Saber que publicar en estas redes no nos va a hacer más felices o a convertirnos en mejores personas. Entender que detrás hay una explotación del hedonismo y del narcisismo. No podemos olvidar además que toda la información que publicamos se nos devuelve. Es decir: es cierto que las redes nunca nos cobran un peso por estar allí, pero la información que subimos les sirve de insumo para que la vendan a terceros, que son los que nos van a enviar publicidad de acuerdo a nuestras preferencias", agrega el profesor Wightman.

De hecho Facebook ya ofrece un portafolio para monitorear nuestras emociones: 'me encanta', 'me importa', 'me entristece', 'me gusta', y mandarnos a nuestro perfiles contenidos que se parezcan a eso a lo que reaccionamos. El fin de las redes es mantenernos conectados.

La ingeniera en ciberinteligencia, Nazly Borrero Vásquez, recuerda que hay que poner atención al contexto de las fotos que subimos, los detalles. A veces, en una selfie, aparece también el carnet de la empresa donde trabajamos, o la dirección de la casa, o la placa del carro, o la tarjeta de crédito cerca a la mesa del restaurante, o el uniforme con el nombre del colegio donde estudian los hijos, datos que son vistos por los delincuentes como un botín.

También es importante no hacer públicos datos íntimos como la fecha de nacimiento, el teléfono o el correo personal, pues les permite a los hackers hacer ingeniería social para descifrar las contraseñas, que, por cierto, no deben ser palabras, sino juegos de letras mayúsculas y minúsculas con números y caracteres especiales. Para no crear contraseñas distintas que sean difíciles de memorizar, se sugiere concebir una sola contraseña pero con juegos de las letras distintos, es decir que se cambien las letras que van con mayúsculas, por ejemplo.

Y otro error muy común en redes es aceptar contactos desconocidos por el simple hecho de que tienen "amigos en común", lo que genera cierta confianza. El problema es que no sabemos si en realidad son personas o un bot: una especie de robot creado por un software para hacerse pasar por personas y llenar información en páginas web o detectar en redes correos electrónicos, números de teléfono o cédulas.

"En la web debemos cuidar nuestros datos personales, igual que en el mundo analógico. Por ejemplo, cuando nos piden documentación para sacar una tarjeta de crédito o un plan de celular, sacamos las fotocopias de la cédula y se la entregamos al asesor, lo que no está bien. Cuando la persona tiene un buen historial crediticio puede pasar que saquen más fotocopias para abrir créditos de manera fraudulenta. Sucede con frecuencia. Se debe advertir en la fotocopia que se entrega que es exclusivamente para X proceso, no dejarla abierta. Ráyela. Hay una cultura en Colombia de creer que los fraudes le pasan al otro, o al que tiene plata o es famoso, y no es así. Todos los días se cometen fraudes con la información que suben a sus redes ciudadanos del común", añade Nazly.

El profesor Pedro Wightman concluye, por su parte, que se debe limitar la información que subimos a las redes, porque en ocasiones cierto afán por figurar, nos hace cometer tonterías que pueden resultar costosas sobre todo por un asunto: todavía no percibimos el peligro que hay en la web al dejar por ahí nuestra cédula, la fecha de cumpleaños, el restaurante donde nos encontramos. No percibimos el peligro porque fisiológicamente no estamos diseñados para sentir miedo de un computador, dice el profesor. Pero el peligro está. Mientras posteamos la caminata por la playa le podemos estar abriendo la puerta a los delincuentes para que nos hagan daño.

"No olvidemos que publicar en una red social sin precauciones es igual a pararse en la Plaza de San Francisco de Cali y darle nuestras fotos y datos personales a cualquier extraño que pase. A la mayoría tal vez no le interese, pero a otros sí, y no necesariamente por buenas razones", dice Pedro Wightman.

Una de las recomendaciones de expertos en seguridad informática es mantener privados los perfiles de las redes sociales. También recomiendan no aceptar contactos desconocidos, ni publicar en tiempo real los lugares que visitamos.

Cuidarse en las redes sociales

1. No divulgar demasiada información personal, no es necesario contarlo todo. No revelar fecha de nacimiento, números de teléfono personales, correos personales, direcciones, pues es información que puede ser usada en nuestra contra a través de fraudes.

2. Mantener los perfiles privados. Las redes sociales permiten modificar la configuración de privacidad. En el caso de Facebook, se debe hacer clic en account, en la parte superior derecha. Allí se selecciona configuración y después privacidad, para garantizar que solo los contactos y amigos puedan ver nuestra información y no cualquier persona.

3. Desactivar la localización. El GPS de los teléfonos inteligentes permite subir información de ubicación a cualquier contenido multimedia enviado o recibido. Redes sociales como Twitter, Facebook e Instagram lo usan para facilitar el marcado de las fotos, pero se sugiere no usarlo para prevenir que los delincuentes sepan cuándo y dónde estamos. También recopilan información sobre estilo de vida, lugares frecuentes, rutinas, etc.

4. Contraseñas seguras. Combine mayúsculas, números y caracteres especiales.

5. Tenga cuidado con mensajes de texto en los le informan que ganó algo, pues pueden contener virus que secuestran la información de los dispositivos.

> Si se es una persona pública, actores y gente del espectáculo que requieren que su perfil sea público, se debería tratar de hacer publicaciones con un retraso del tiempo. Es decir, si van a vacaciones, publique las fotos después de las vacaciones".

> Detrás de la necesidad de publicar en redes de manera constante la vida privada hay una explotación del hedonismo y del narcisismo".

PEDRO WIGHTMAN
Universidad del Rosario