

Operación 3: Sin rastro

FÁTIMA RODRÍGUEZ COYA

Sí, no, en parte, disociado...
Llevamos muchas horas de debate y líneas de análisis en torno al derecho de acceso a la información y la protección de datos de personales (y las que nos quedarán) pero, ¿qué tal lo llevamos a nivel doméstico? Como siempre, la diferencia en lo personal estriba en que todo es menos protocolizado, o al menos eso parece.



Del mismo modo que no dejamos medicamentos ni tóxicos al alcance de los niños, quiero pensar que tampoco dejamos notas pegadas a la pantalla del ordenador con nuestras claves o documentos en el escritorio titulados *Contraseñas*. Seguro, ¿no? Si aún no es así: busca una solución ya, porque esta es la parte fácil.



[Propuesta: utiliza denominaciones que no sean obvias, ni contengan la palabra contraseña; crea un contacto ficticio en tu agenda y guarda en él las cifras de tus claves como si fuesen números de teléfono; utiliza truncamientos XXXXXX56 o desgloses por módulos tipo PINmvl+pueblo+56].

información técnica de la toma y ya no digamos si el teléfono tiene activada la geolocalización. Por mera curiosidad, os invito a investigar un poco sobre 'Sé dónde vive tu gato' (*I know where your cat lives*) la iniciativa de un profesor americano que mapeó cerca de un millón de gatos explotando los

acceder a las propiedades del fichero y desde ahí, seleccionar la opción que nos permita editar o quitar propiedades [puede variar en función del sistema operativo y programas que utilicemos, en Windows la ruta sería: seleccionar el fichero > Propiedades > Detalles > Quitar propiedades e información



En un momento en el que realizamos la mayor parte de nuestras gestiones por medios electrónicos y nuestras manos ya no se desprenden de ese apéndice llamado teléfono con el que intercambiamos todo tipo de información, la cantidad de datos que generamos y recibimos es ingente, en una medida muy superior a la que a veces somos capaces de calibrar.

Nos reímos de esos casos en los que el ladrón entra a robar y deja olvidado su currículum en la casa que atraca. Nos parece una falta de todo: atención, inteligencia, profesionalidad, pero ¿cuántas veces estamos haciendo lo mismo en entornos electrónicos? Sacamos una foto con el móvil y la compartimos o publicamos. Inocuo, ¿verdad? Pero esa foto es mucho más que una imagen: los datos Exif aportan mucha

metadatos de las imágenes que sus dueños colgaban en las redes sociales (21.015 de esos gatos se encuentran en España).

Son pequeños detalles aparentemente sin importancia, migajas de información que sumadas e interrelacionadas pueden retratarnos más aún que al ladrón que dejó olvidado su currículum. Obviamente el consejo no pasa por dejar de utilizar estos medios, sino por ser conscientes y minimizar los riesgos de la sobreexposición informativa.

¿Qué podemos hacer? En el caso de la foto, si no queremos que las imágenes se geolocalicen, puede bastar con desactivar los servicios de ubicación tipo GPS de la cámara o teléfono. Si queremos anular más información o hacerlo de un modo selectivo, podemos

personal, donde incluso nos da la opción de generar un duplicado anonimizado sin perder el original]. También existen aplicaciones específicas para ello, como MAT (Metadata Anonymisation Toolkit).

Sin embargo, la desprotección de datos personales no se da en exclusiva por esa circunstancia, sino que muchas veces *entran* a por ellos con múltiples artes, gracias a la configuración de aplicaciones (ya sean estas de móvil o de ordenador) o en las redes de comunicación. Por eso, para frenarlo hará falta conocer las condiciones del servicio, habilitar sistemas de seguridad o configurar correctamente dichas aplicaciones. Aunque las combinaciones son múltiples, vamos a destacar a continuación algunas medidas de fácil acceso e instalación:



Navegación

- Utilizar redes de comunicación distribuidas tipo Tor (Orbot para móviles), similares en apariencia a cualquier navegador, pero que mantienen la integridad y el secreto de la información sin desvelar las IP.
- Evitar las cookies de terceros: mediante configuraciones, borrándolas al terminar la sesión e instalando complementos en el navegador como Adblock Plus, que bloquea la publicidad intrusiva y de seguimiento del usuario.

Comunicaciones

- Cifrar las llamadas con aplicaciones tipo Signal o RedPhone y la mensajería instantánea, por ejemplo, con Telegram, que en su opción de chat secreto cifra los mensajes. Cryptochat puede ser otra alternativa.
- Encriptar los correos electrónicos que consideremos pertinentes con extensiones como Mailvelope, compatible con Gmail, Yahoo y Outlook.
- Enviar documentos con Snapchat para que, una vez

vistos por el destinatario, se autodestruyan en su dispositivo a los pocos minutos.

Seguridad

- Gestionar de forma responsable nuestras contraseñas.
- Disponer de algún detector de malware que, con un funcionamiento similar al de un antivirus, destruya ese software malicioso que se instala en nuestros dispositivos para la obtención de información, hacer publicidad o secuestrar su uso. Una buena opción gratuita es AdwCleaner, que además funciona como un potente herbicida cuando el malware echa raíces y se resiste a abandonar nuestro equipo.
- Limpiar de forma recurrente las cookies que puedan quedar alojadas tras la navegación, utilizando por ejemplo el CCleaner (CleanMaster sería su asimilado para móviles).
- Detekt: una herramienta de acceso público que permite detectar en ordenadores los programas espía de vigilancia más conocidos (incluso algunos utilizados por gobiernos).

No se trata de que ahora nos pasemos a la navegación en la web profunda pero sí que conozcamos a qué nos exponemos para poder trazar algunas barreras de protección, porque con frecuencia focalizamos en lo particular y perdemos la visión de conjunto. ¿Acaso alguien había reparado en el desfase de los títulos de esta serie? ¿Operación 3? Es probable que el salto del dos al cuatro haya pasado desapercibido para muchos, pero ha sido un modo de ejemplificar la necesidad de tener una visión general para poder identificar inconsistencias que de otro modo, pasarían tan inadvertidas como los metadatos de las fotografías gatunas.

A diario bajamos las persianas de nuestra casa para guardar con celo nuestra intimidad de miradas indiscretas, al mismo tiempo que abrimos de par en par las puertas de nuestra vida digital a anónimos desconocidos, que entran y salen sin que nos enteremos. Seamos pues prudentes, y aprendamos también nosotros a movernos sin rastro. ■