Palabras clave:
privacidad online, brechas de seguridad, Internet seguro, contraseñas, protección de datos

SEIS ESTRATEGIAS PARA (PRE)OCUPARNOS DE NUESTRA PRIVACIDAD EN INTERNET

El alto precio de lo gratuito

El mundo digital no tiene misterios para las nuevas generaciones. Pero la facilidad con la que se manejan es engañosa; es importante entender cómo la tecnología nos hace vulnerables para aprender a proteger nuestros datos y privacidad.

TEXTO: **DAVID ARROYO GUARDEÑO**
ILUSTRACIÓN: **DANIEL MONTERO GALÁN**

El ecosistema digital ha convertido la inmediatez en la seña de nuestro tiempo[1]. Asumimos que para cada deseo existe un producto o un servicio que lo sacia de forma rápida, directa y con bajo o nulo coste. Sin embargo, pese a que esa respuesta casi instantánea a nuestras necesidades puede parecer algo positivo y muy conveniente, la gratuidad de los servicios tiene contrapartidas que el usuario no siempre conoce.

Incluso los niños, adolescentes y jóvenes que han crecido con acceso a internet y se manejan con las pantallas como peces en el agua[2], a menudo no saben o no dan importancia a aprender a navegar por esas aguas de forma segura. He aquí seis situaciones cotidianas en las que nuestra seguridad se ve comprometida, y de las que podemos protegernos mejor con un poco de esfuerzo y atención.

1. Aplicaciones invasivas instaladas "por defecto"

Según datos de 2025, Android[3] es el principal sistema operativo que emplean quienes acceden a internet desde un dispositivo móvil. Como otros sistemas operativos, proporciona acceso a un buen volumen de aplicaciones gratuitas preinstaladas[4] con prácticas de recopilación de datos potencialmente invasivas, a menudo, sin el conocimiento del usuario. Porque lo cierto es que rara vez, por no decir nunca, leemos con detenimiento los términos de uso que aparecen en pantalla al empezar a usar un dispositivo o al instalar una aplicación, incluso dando nuestro consentimiento.

Frente a esta tendencia mayoritaria, la opción más segura es instalar y usar solamente aquellas aplicaciones o servicios estrictamente necesarios, leyendo antes detenidamente la letra pequeña. Si los términos de uso de Android (o cualquier otro sistema operativo) o de un fabricante nos obligan a tener disponibles aplicaciones que consideramos invasivas, conviene explorar otras opciones.

2. Higiene en el uso del correo electrónico

Prácticamente todos los usuarios de telefonía móvil disponen de —al menos— una cuenta de correo electrónico. Además, en el contexto laboral casi cualquier trabajador está obligado a disponer de una dirección de *email*, normalmente vinculada a un servidor de correo corporativo. Si hablamos de los estudiantes, en muchas comunidades autónomas es la propia consejería de educación la que proporciona a los alumnos una dirección de correo electrónico. Al final, no solemos decidir si tener o no tener una cuenta: nuestro margen de elección se limita a escoger entre consultarla vía web (de forma que la seguridad dependerá del proveedor del servicio y del navegador web que empleemos) o mediante un gestor de correo electrónico (que es una aplicación que nos permite descargar los mensajes y conservar una copia de ellos en nuestro ordenador).

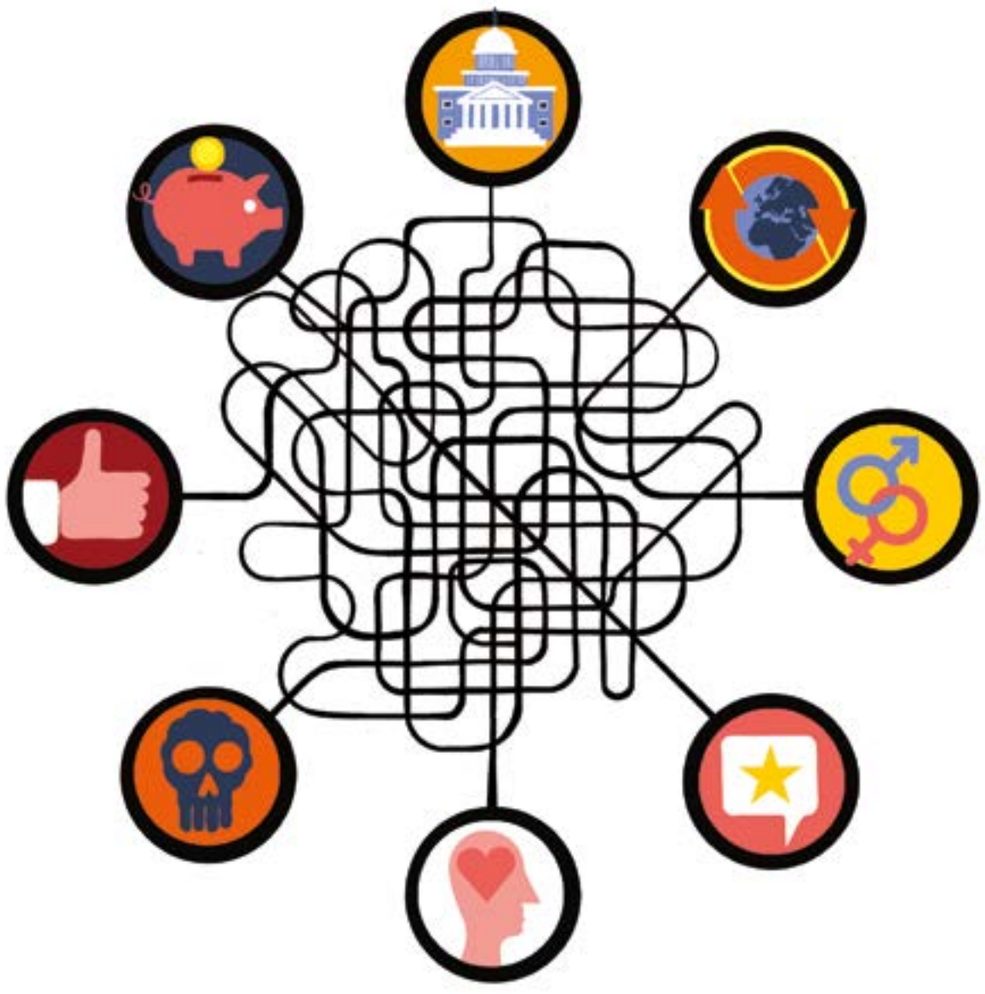
Como usuarios, no es mala idea acostumbrarnos a revisar las cabeceras o asuntos de los correos electrónicos que recibimos para saber cuál es el origen de un mensaje y ver si coincide con su remitente[5] y hacer uso de proveedores de correo electrónico que cifren los mensajes antes de ser enviados al servidor para su distribución[6]. Finalmente, antes de descargar contenido o acceder a enlaces incorporados en el cuerpo de un mensaje, conviene comprobar si dicho contenido o enlace puede suponer un problema seguridad[7].

Es aconsejable utilizar cuentas de correo electrónico de un solo uso o cuentas temporales para aquellas interacciones puntuales o de corta duración. Por ejemplo, en el registro en una web a cuya contenido queremos acceder solo una vez o en muy pocas ocasiones, aunque suponga más trabajo hacerse una cuenta nueva cada vez que la necesitemos.

Por otro lado, no se puede hablar de adecuada higiene digital sin una buena práctica en la generación y uso de contraseñas. Y eso necesariamente remite al uso de gestores de contraseñas y a una vigilancia activa de potenciales brechas de seguridad[8]. Un gestor de contraseñas es una aplicación que nos permite generar contraseñas de forma automática y guardarlas de forma segura utilizando una clave de cifrado derivada desde una contraseña maestra. Esta contraseña es la única que hemos de recordar o almacenar en un medio seguro (por ejemplo, un *pendrive* o disco duro externo).

El enfoque basado en cifrar la información antes de enviarla al proveedor de correo electrónico o a un sistema de almacenamiento en la nube, así como el uso de gestores de contraseñas y la rotación de cuentas de correo, caen dentro de lo que en seguridad se llama modelo de confianza cero o *Zero trust model*. Dicho modelo viene a decirnos que hemos de asumir que vamos a ser atacados, de forma que hemos de hacer todo lo posible para que, ante un eventual ataque, el impacto sobre nosotros sea mínimo. Este enfoque atañe a todo tipo de servicios o plataformas digitales, no solo al correo electrónico.

Rara vez leemos con detenimiento los términos de uso al empezar a usar un dispositivo o instalar una aplicación, incluso dando nuestro consentimiento



3. Que nadie conozca nuestros patrones de navegación

Por eso, conviene proteger nuestro patrón de navegación usando navegadores con una configuración *Zero Trust*, aplicable a cualquier herramienta con la que navegamos por internet. Guías como la proporcionada por INCIBE (Instituto Nacional de Ciberseguridad español) son de gran valor a la hora de configurar Zero Trust en nuestro navegador[9].

Si no protegemos nuestra privacidad, permitimos que se usen nuestros patrones de navegación para entrenar modelos avanzados de inteligencia artificial que, a su vez, se usan para diseñar campañas de *marketing* y de propaganda, así como para manipular usuarios con los que interactuamos o que tienen un comportamiento similar al nuestro a través del *phishing* o campañas de desinformación[10]. Conviene destacar la alta sofisticación de este tipo de ataques como resultado de la mejora de técnicas en la creación de *deepfakes*[11].

En la medida en que esto implica riesgos de seguridad para nuestro entorno y, por extensión, nuestra sociedad, no es aventurado afirmar que la protección de nuestra privacidad no es un derecho, sino que tenemos la obligación en primera persona de hacerlo[12]. En la economía de la atención que vivimos, nada es gratuito: nosotros somos el producto[13].

4. Nunca confiar, siempre verificar

De cara a evaluar la fiabilidad de un dominio web, hemos de asegurarnos de que accedemos a través de una comunicación cifrada mediante HTTPS[14], lo que nos permitirá comprobar el certificado digital del dominio que estamos visitando[15].

Sin embargo, el hecho de que un dominio haya sido registrado y cuente con un certificado válido no es suficiente garantía de que

su contenido sea fiable y de calidad. Es fácil encontrar sitios webs aparentemente legítimos que han sido utilizados para diseminar contenido fraudulento, muchas veces haciendo uso de la reputación y prestigio de otros. Los sistemas de verificación de noticias o *fact-checkers*, así como recursos como Wikipedia o la Wayback Machine, pueden ayudarnos a discernir la información de calidad.

Una muy buena praxis en la verificación de contenido *online* consiste en almacenar las páginas que visitamos mediante *snapshots* (copia de seguridad puntual de un sistema de archivos o base de datos) en la nube vía Wayback Machine (un servicio gratuito[16] con un esquema similar a Wikipedia) o creando nuestras propias capturas con herramientas como Update Scanner, Urlwatch o Change Detection. Estas aplicaciones, si las tenemos instaladas, nos avisan de cambios realizados en una página web, y sirven para ver el histórico de contenido *online* y saber cuándo se ha publicado nuevo contenido.

5. Copias de seguridad automáticas

Contar con respaldos o *backups* de nuestros datos, imágenes, documentos y recursos digitales es algo esencial, incluso innegociable. Lo ideal es que esta copia de seguridad se realice de forma automática.

Para los mensajes de correo electrónico personales conviene usar proveedores que cifren los mensajes antes de ser enviados al servidor

Sin entrar en detalle, en los retos asociados al *backup* de nuestros datos y sistemas, cabe subrayar que el sistema de respaldo por defecto en Android es el que de forma *gratuita* proporciona Google Drive. Dado que ya hemos advertido que nada es gratis, que nosotros somos el producto, conviene considerar que existen alternativas en local, ya sea usando un sistema NAS (Network Attached Storage) —un sistema de almacenamiento en red que permite almacenar y compartir ficheros[17]— o herramientas alternativas en la nube que implementan cifrado en el lado del cliente según el modelo *Zero trust*, como es el caso del servicio proporcionado por la empresa española Internxt[18].

6. Cifrado de extremo a extremo

En caso de usar Google Drive para las copias de seguridad de WhatsApp, conviene cerciorarse de activar el cifrado de extremo a extremo o E2E (*end-to-end*, un cifrado que hace que solo el emisor y el receptor de un mensaje puedan acceder a su contenido[19]) antes de realizar el *backup*.

La precaución sobre la activación del cifrado E2E en las aplicaciones de mensajería instantánea es algo que se suele obviar, en gran medida debido a la falta de conocimientos, o bien por una base de conocimientos muchas veces alimentada a través de fuentes de calidad no contrastada, algo recurrente en redes sociales. Sin ir más lejos, al usar Telegram asumimos que es una herramienta mucho más garantista en términos de protección de privacidad que otras aplicaciones de mensajería instantánea, cuando lo cierto es que existen claros indicios sobre la laxa protección de privacidad en Telegram[20] y es preferible que optemos por otras alternativas[21].

Hay otro segundo factor de interés sobre el cifrado E2E: su demonización[22]. El debate sobre la necesidad de impedir el cifrado de comunicaciones es una constante siempre que se analiza en el contexto de actividades ilegítimas, como el consumo de pornografía infantil[23] o el acceso a contenidos piratas. Aquí es preciso realizar un inciso: el uso inadecuado de una tecnología no hace que esa tecnología sea inadecuada, sino que llama a crear un marco de control y gobernanza de la misma, donde la persecución de abusos no lleve a la supresión de derechos fundamentales, como la privacidad o la neutralidad de red[24].

En una época plagada de opciones gratuitas para satisfacer nuestros deseos *ipso facto*, y a pesar de la avalancha informativa que recibimos a diario, estamos más desinformados y frustrados que nunca. Quizás el gran reto de nuestro tiempo sea vivir en el espacio digital aceptando los límites de lo natural y lo físico (con lo otro y con los otros), dedicando el debido tiempo para hacer de la reflexión una oportunidad para abrir nuevas vías de comprensión y de entendimiento, y adoptando medidas de seguridad para convertir juntos el *cibermundo* en un espacio habitable, sostenible habitable.

Autor

DAVID ARROYO GUARDEÑO
Investigador principal del Grupo de investigación en Ciberseguridad y Protección de la Privacidad (https://gicp.es), del Consejo Superior de Investigaciones Científicas. Su investigación y actividad docente se centra en el desarrollo de soluciones criptográficas para la protección de la privacidad, la lucha contra la desinformación y la defensa frente a ciberataques.

Bibliografía

Gamba, J., Rashed, M., Razaghpanah, A., Tapiador, J., Vallina-Rodríguez, N. *"An Analysis of Pre-Installed Android Software"* en *2020 IEEE Symposium on Security and Privacy (SP)* (2020, 1, pp. 1039-1055).

Kirschner, P. A., De Bruyckere, P. *"The myths of the digital native and the multitasker"* en *Teaching and Teacher Education* (2017, 67, pp. 135-142). Disponible en: https://doi.org/10.1016/j.tate.2017.06.001

Papadopoulos, P., Kourtellis, N., Rodríguez Rodríguez, P. y Laoutaris, N. *"If you are not paying for it, you are the product: how much do advertisers pay to reach you?"* en *Proceedings of the 2017 Internet Measurement Conference* (2017, pp. 142-156). Disponible en: https://dl.acm.org/doi/10.1145/3131365.3131397

Tomlinson, J. (ed.) *"Culture, Modernity and Immediacy"*. En: Beck, U., Sznaider, N. and Winter, R. (eds). *Global America? The Cultural Consequences of Globalization*. Liverpool, 2004; online edn, Liverpool Scholarship Online, 20 June 2013. Disponible en: https://doi.org/10.5949/liverpool/9780853239185.003.0004

Notas

1 Tomlinson, 2004.
2 Kirschner, De Bruyckere, 2017.
3 https://datareportal.com/reports/digital-2025-global-overview-report
4 Gamba *et al.*, 2020.
5 https://www.incibe.es/empresas/blog/dudas-legitimidad-correo-aprende-identificarlos
6 https://www.privacytools.io/privacy-email
7 https://www.virustotal.com/gui/home/upload
8 https://haveibeenpwned.com
9 https://www.incibe.es/ciudadania/formacion/guias/guia-de-navegadores-web
10 https://www.dsn.gob.es/sites/default/files/2025-01/CAPÍTULO%205%20TRABAJOS%20FORO%20CAMPAÑAS%20DE%20DESINFORMACIÓN.%20INICIATIVAS%20%202024.pdf
11 https://www.youtube.com/watch?v=01ffj0RgNmo
12 https://www.youtube.com/watch?v=3j9oARBlxmg
13 Papadopoulos *et al.*, 2017
14 https://www.incibe.es/ciudadania/blog/https-y-certificados-digitales-me-debo-fiar-de-todos
15 https://es.wikihow.com/verificar-un-certificado-SSL
16 https://www.insidephilanthropy.com/home/whos-funding-the-wayback-machine-saving-information-under-threat
17 https://www.redeszone.net/tutoriales/servidores/sistemas-operativos-servidores-nas
18 https://internxt.com/es
19 https://faq.whatsapp.com/490592613091019?helpref=faq_content
20 https://blog.cryptographyengineering.com/2024/08/25/telegram-is-not-really-an-encrypted-messaging-app
21 https://www.privacytools.io/privacy-messaging
22 https://maldita.es/malditatecnologia/20230526/dudas-legales-cifrado-extremo-extremo-prohibicion
23 https://www.patrick-breyer.de/en/posts/chat-control
24 https://theconversation.com/laliga-versus-cloudflare-hay-mejores-maneras-de-combatir-la-pirateria-251997

English

Six tips to take control of our online privacy.
THE HIGH COST OF FREE ONLINE SERVICES.

The digital world holds no mysteries for younger generations. However, the ease with which they navigate it can be misleading; it is essential to understand how technology makes us vulnerable in order to learn how to protect our data and privacy.

Keywords: *online privacy, security breaches, secure internet, password security, data protection*