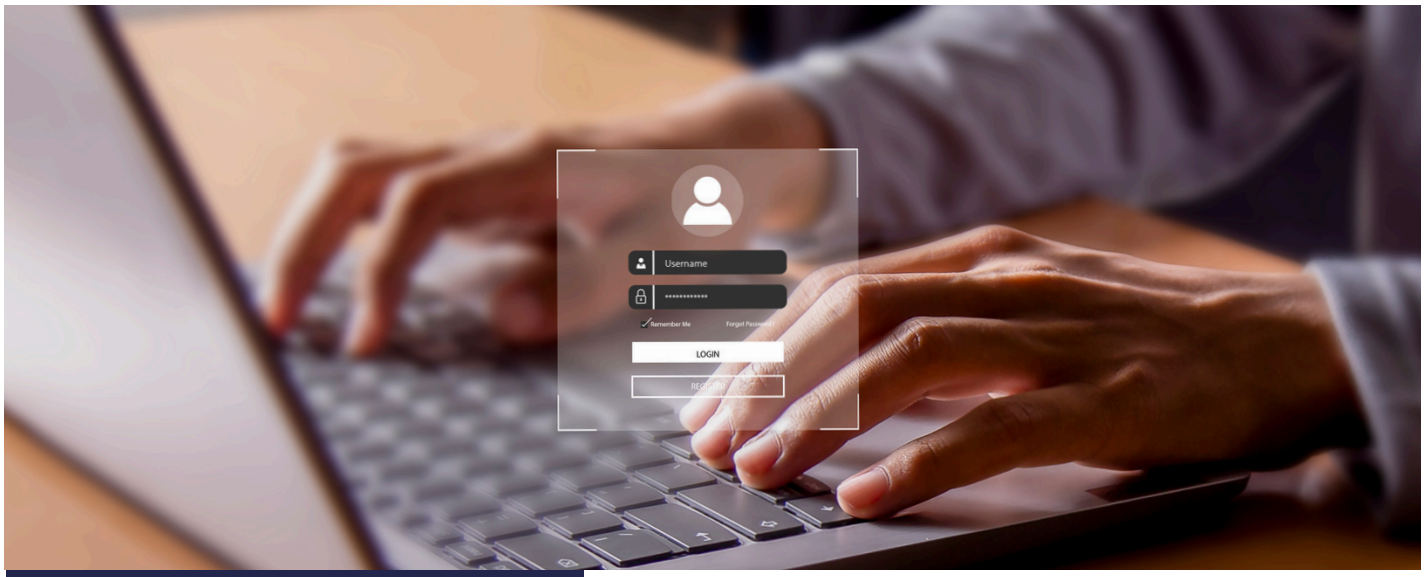
TU INFORMACIÓN, TU DECISIÓN

Aprende a cuidar tu privacidad digital

Hacia una cultura digital que promueva la paz y la transformación social
Colombia 2024



¿Sabias que...?

Cuidar de tus datos voluntarios e involuntarios en la red es de vital importancia para tener el control de tus decisiones, tus opiniones y conductas.

Parece de película, pero es real, tus datos pueden ser utilizados para influenciar en ti. Seguramente haz escuchado cuando alguien dice: "estaba buscando un producto en internet y ahora me llega mucha publicidad de eso".

Lo que sucede en este caso es que a partir de tus datos se crean perfiles de consumo y según ese perfil te llega publicidad.

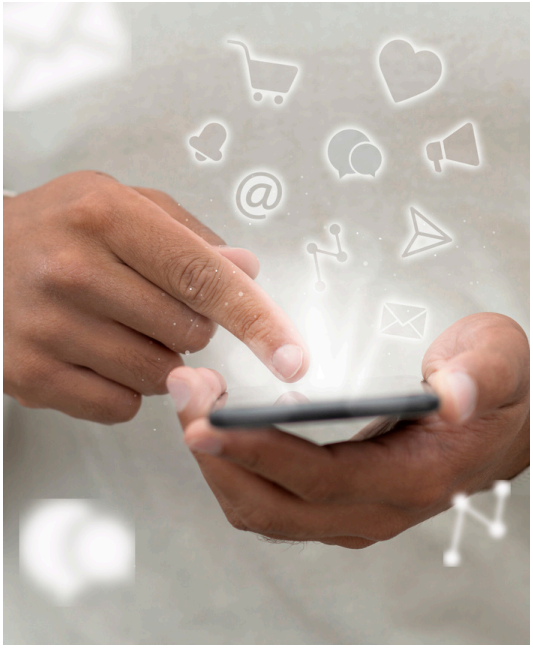
Pero lo complicado de todo esto es que también ocurre en escenarios de elección popular.

No es ficción...

En 2018 se reveló que la empresa de consultoría política Cambridge Analytica utilizó de manera indebida los datos personales de aproximadamente 87 millones de usuarios de Facebook sin su consentimiento, esto se hizo para dirigir mensajes políticos personalizados en campañas como la elección presidencial de Estados Unidos en 2016 y el referéndum del Brexit.

En este boletín aprenderás sobre como se usan tus datos personales y sensibles, así como la forma de prevenir que sean utilizados de forma no autorizada para influir en tus decisiones, conductas y opiniones.

¿Revisas los terminos de las Apps de tu celular?



De acuerdo con el estado general del uso de móviles, Internet y redes sociales en Colombia (Kepios, 2024), las aplicaciones más frecuentadas por los colombianos son: WhatsApp 92%, Facebook 89%, Instagram 86%, TikTok 67% y X 49%.

Como bien observas, en nuestro día a día, descargamos aplicaciones o accedemos a páginas que nos exigen autorizaciones para manejar nuestros datos personales. Sin embargo, a menudo pasamos por alto esta situación y nos desentendemos de los acuerdos sobre el uso de nuestra información.

Este tipo de prácticas pone en jaque nuestra privacidad y la de nuestros seres queridos, ya que en ocasiones otorgamos permiso no solo para el uso de nuestros datos, sino también de aquellos de terceros que habitan en nuestras redes sociales.

Compartimos datos involuntariamente a través de nuestros patrones de navegación, como los sitios visitados y los horarios. Esta información crea un perfil digital que contribuye a nuestra huella digital.

¿Para que se usan tus datos?

Los datos forjan nuestra huella digital, también conocida como huella electrónica o sombra digital. Este concepto alude a toda la información que dejamos al surcar las vastas aguas del Internet.

Por ejemplo, cada vez que nos registramos para crear un correo electrónico, nos inscribimos en un juego en línea o presentamos una solicitud de empleo, estamos dejando rastros. Asimismo, el tiempo que dedicamos a las redes sociales, los 'me gusta' que otorgamos y los enlaces que exploramos también suman a esta huella.

La huella digital activa se forja cuando ofrecemos de manera deliberada y consciente nuestra información personal, manifestándose así de forma voluntaria. Por otro lado, la huella digital pasiva se genera cuando aplicaciones, plataformas digitales y redes sociales recogen información sobre el usuario sin que este sea consciente de que tal recopilación está en marcha.

En este punto, es crucial adentrarse en un tema de suma importancia para la privacidad digital y la ciberseguridad: la ingeniería social, que en términos generales se puede entender como el conjunto de técnicas de manipulación que los ciberdelincuentes utilizan a partir de tu información.

Ingeniería social y sus riesgos

La ingeniería social se adentra en el estudio de los comportamientos psicológicos, sociológicos y estadísticos, con el propósito de identificar, ubicar, seleccionar y distribuir información a diversas comunidades humanas.

En ocasiones su objetivo es persuadir a las personas y sembrar la polarización en la sociedad a través de la difusión de información falsa o descontextualizada.

El aspecto más crucial de la ingeniería social es la esencia de los individuos: carácter, temperamento, creencias, aficiones, gustos, inclinaciones políticas, posición, conciencia y preparación académica, entre otros.

En resumen, la ingeniería social se relaciona con:

- La velocidad vertiginosa a la que fluye la información en Internet y cómo estas dinámicas moldean nuestras sociedades actuales.
- La abundancia de información en la red propicia su manipulación de forma sutil e imperceptible, permitiendo guiar comportamientos y alterar la percepción social de las personas.
- La cultura de la inmediatez, que restringe y limita nuestra capacidad crítica y reflexiva ante el consumo de información.

Pilas con la Inteligencia Artificial

Actualmente para la suplantación de identidad se están utilizando imágenes o archivos de voz manipulados con software de inteligencia artificial (IA) para parecer reales y auténticos.

Algunos de los riesgos asociados a la ingeniería social son:

Phishing
Consiste en engañar a las personas por medio de un correo electrónico en nombre de alguna entidad financiera, indicando la necesidad de actualización de datos. En dicho correo te envían un link o página web similar a la del banco con el ánimo de que dejes tu información confidencial.

Pharming
Consiste en engañar a las personas por medio de una página web fraudulenta, mediante la cual se suplanta la página de una entidad y por medio de ella se capturan credenciales de acceso (usuarios y clave) datos por medio de formularios de ingreso o registro falsos.

Smishing
Robo de información personal o financiera por medio de mensajes de texto con enlaces que redireccionan a páginas web falsas.

Vishing
A través de llamadas telefónicas los delincuentes se hacen pasar por una entidad financiera, comúnmente informando sobre un bloqueo o actualización de cuenta para solicitar información personal.

Suplantación de identidad
En los entornos digitales ocurre cuando una persona se hace pasar por otra, es decir, roba su información personal y construye perfiles falsos por medio de los cuales contacta a otros usuarios con el fin de agredir, robar, chantajear o incitar.

Si te encuentras bajo la sombra de alguno de estos riesgos, puedes denunciar a través del CAI Virtual de la Policía Nacional ingresando a:

www.caivirtual.policia.gov.co.

¿Cómo proteger mis datos?

- Usar una VPN (Red Privada Virtual, por sus siglas en inglés), herramienta que permite a los usuarios enviar y recibir datos de manera segura, como si estuvieran conectados a una red privada.
- Usar navegadores privados diseñados para ofrecer una mayor protección de la privacidad y seguridad en línea en comparación con los tradicionales. (mozilla.org o duckduckgo.com)
- Utilizar bloqueadores de rastreo para proteger la privacidad y limitar la recolección de datos en línea. Estas herramientas son diseñadas para prevenir que sitios web y anunciantes recopilen información sobre tu comportamiento en línea. Algunos de ellos son: DuckDuckGo Privacy Essentials o Ghostery, verifica la compatibilidad con tu navegador de preferencia.
- Acepta sólo solicitudes de conocidos en las redes sociales.
- Configura tus redes sociales en modo privado, esto te permitirá controlar quién ve lo que publicas o compartes.
- No compartas información con cualquier persona, ya sea en formularios, llamadas telefónicas o plataformas.
- Piensa antes de compartir o acceder a publicaciones de anuncios, sorteos y ofertas irresistibles.

ACTIVIDAD

Verifica si las claves que usas para tus distintas cuentas cumplen con lo siguiente:

- La longitud es fundamental: ¿Usas claves con al menos 8 caracteres?
  - Recuerda que usar al menos 8 caracteres hace más difícil descifrar tus contraseñas.
- ¿Combinas letras mayúsculas y minúsculas en tus claves?
  - Recuerda que usar este tipo de combinaciones hace más difícil descifrar tus contraseñas.
- ¿Utiliza símbolos o números que reemplacen letras?
  - Como cuando ciframos cartas de amor, juega y cambia letras por símbolos o números que sólo tu conozcas
- ¿Utiliza caracteres especiales como (*, $, %, +)?
  - Muchas páginas exigen esto por tu seguridad, aprovecha para reemplazar letras por alguno de estos símbolos

Recomendados

Si quieres conocer más acerca de casos en los que los datos de las personas han sido vulnerados y a partir de ellos fueron influenciados para tomar decisiones o expresar opiniones, te recomendamos ingresar a YouTube y buscar el video titulado **Cómo Cambridge Analytica analizó la personalidad de millones de usuarios de Facebook** o copiando y pegando el siguiente link en tu navegador web:
https://youtu.be/7831NGClsrM?si=C7vEeHRf04cNg6t6

En 2021 la Organización de Estados Americanos OEA publicó los **"Principios actualizados sobre la privacidad y la protección de datos personales"**, puedes buscarlo en tu buscador web con ese título para conocer acerca de los criterios internacionales que se han planteado para fortalecer las leyes de protección de datos personales o puedes copiar y pegar el siguiente link:
https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Para obtener más información sobre CIBERPAZ, visita los siguientes enlaces:

- https://ciberpaz.gov.co/portal/
- https://www.mintic.gov.co/portal/inicio/

Programa CiberPaz
Correo: contacto@ciberpaz.gov.co
Teléfono: +57 123 456 7890
Dirección: Calle 26 No. 57 - 50, Bogotá Colombia