



CONCIENCIA DIGITAL Y COMPORTAMIENTO SEGURO

ARTIFICIAL INTELLIGENCE PRESENTATION

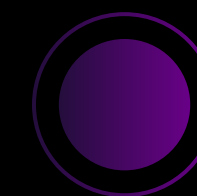
COMUNIDAD HIJAS DE MARIA
AUXILIADORA





BIENVENIDO A LA CONCIENCIA DIGITA

La conciencia digital es la capacidad de las personas para entender los riesgos y responsabilidades que existen al usar internet, dispositivos electrónicos y redes sociales. Implica saber cómo proteger la información personal, reconocer posibles amenazas en línea y utilizar la tecnología de manera responsable.





INTRODUCCION

El comportamiento seguro en el entorno digital consiste en aplicar buenas prácticas para evitar problemas como el robo de información, fraudes o accesos no autorizados. Esto incluye usar contraseñas seguras, no compartir datos personales con desconocidos, verificar la seguridad de los sitios web y mantener actualizados los dispositivos.

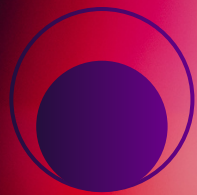
En conjunto, la conciencia digital y el comportamiento seguro permiten que las personas utilicen la tecnología de forma responsable, protegiendo su privacidad y evitando riesgos en el mundo digital.





ERRORES COMUNES QUE PONEN EN RIESGO TUS DATOS PERSONALES

- **USAR CONTRASEÑAS DEBILES:** Utilizar claves fáciles como fechas de nacimiento o "123456".
- **COMPARTIR DEMASIADA INFORMACION EN REDES SOCIALES:** Publicar datos personales como dirección, teléfono o documentos.
- **ABRIR ENLACES O CORREOS SOSPECHOSOS:** Puede tratarse de fraudes o intentos de robo de información.
- **DESCARGAR APLICACIONES DE FUENTES NO OFICIALES :** Algunas apps pueden contener virus o programas maliciosos.
- **NO CERRAR SESIONES IMPORTANTES EN DISPOSITIVOS AJENOS:** Otras personas pueden acceder a tu información.



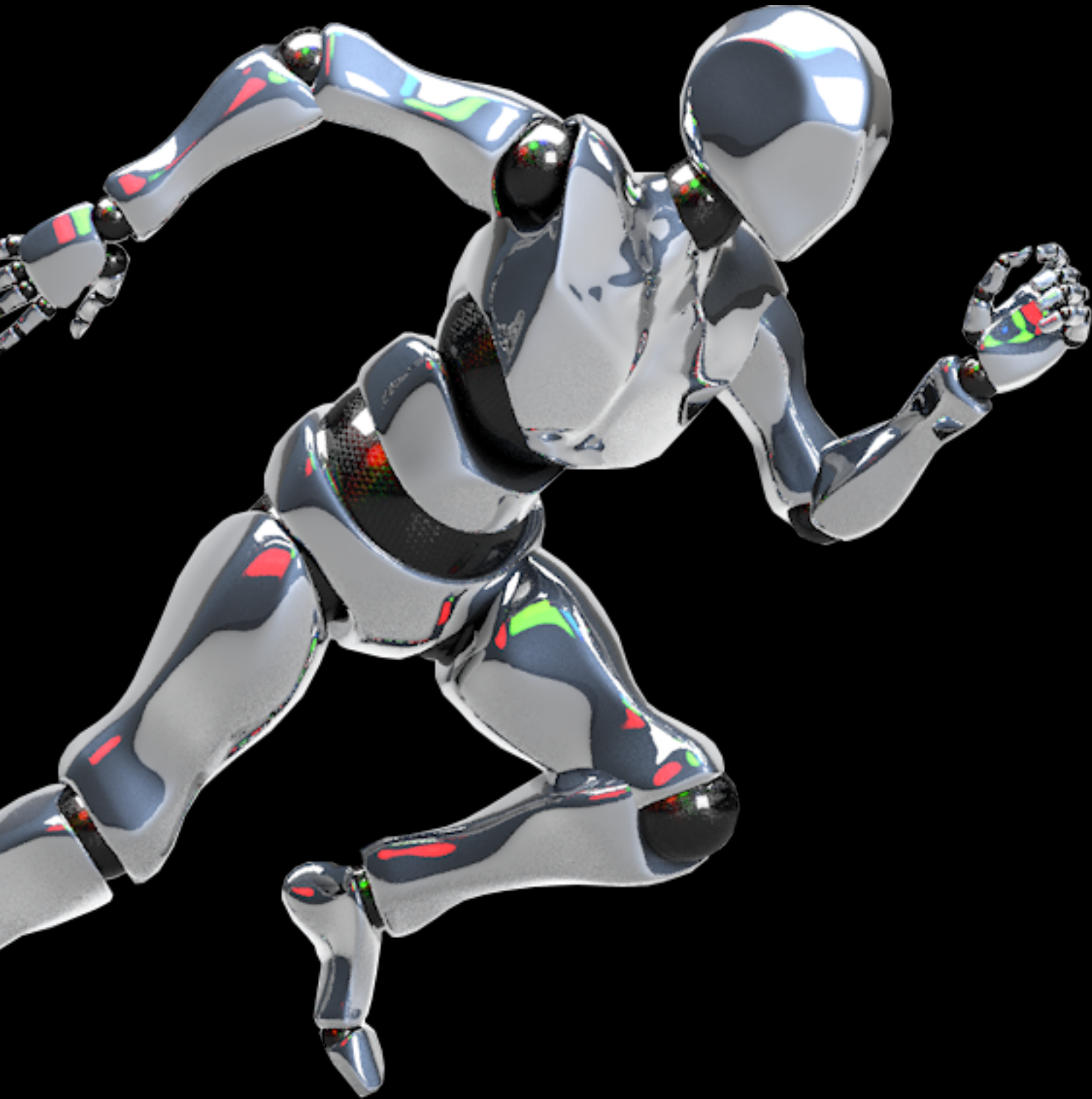
El “exceso de confianza digital” y sus consecuencias.

El exceso de confianza digital ocurre cuando las personas creen que en internet todo es seguro y, por ello, no toman precauciones al compartir información o usar plataformas digitales.

CONSECUENCIAS:

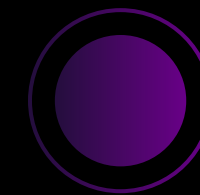
- Robo de datos personales.
- Suplantación de identidad.
- Fraudes o estafas en línea.
- Acceso no autorizado a cuentas personales.
- Pérdida de privacidad.





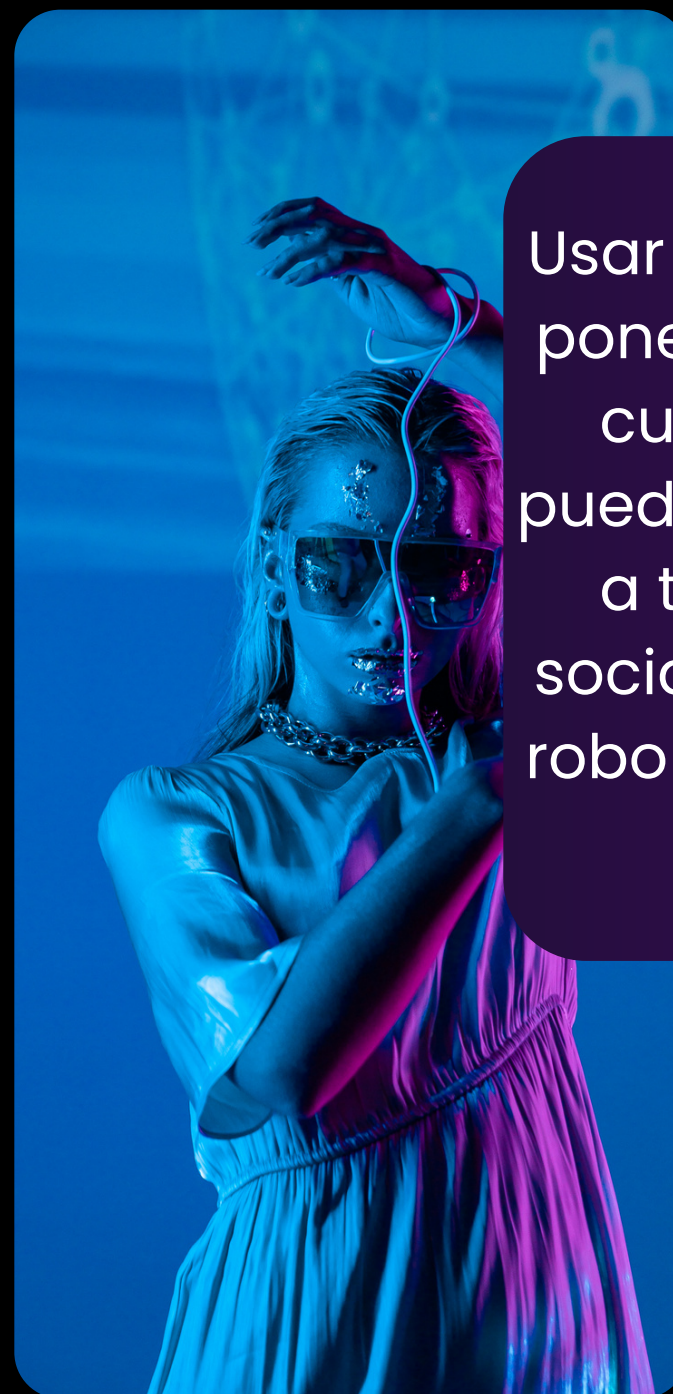
¿POR QUÉ NO DEBES COMPARTIR CÓDIGOS DE VERIFICACIÓN?

Los códigos de verificación son claves temporales que las plataformas envían para confirmar la identidad de una persona al ingresar a una cuenta o realizar algún cambio importante. No deben compartirse con nadie porque permiten acceder a cuentas personales como correos, redes sociales o aplicaciones bancarias. Si otra persona obtiene ese código, puede entrar a la cuenta, cambiar la contraseña y robar información personal. Por eso, los códigos de verificación son privados y deben mantenerse siempre en secreto.

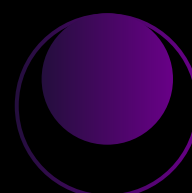




RIESGOS DE USAR LA MISMA CONTRASEÑA EN MÚLTIPLES PLATAFORMAS



Usar la misma contraseña en varias plataformas puede poner en riesgo tu información personal. Si una de esas cuentas es vulnerada o hackeada, los delincuentes pueden intentar usar esa misma contraseña para entrar a tus otras cuentas, como correo electrónico, redes sociales o aplicaciones bancarias. Esto puede provocar robo de información, pérdida de acceso a tus cuentas o incluso fraudes.





CÓMO IDENTIFICAR ENLACES SOSPECHOSOS.

- Revisar si la dirección web tiene errores de escritura o letras cambiadas.
- Desconfiar de enlaces enviados por personas desconocidas.
- Evitar enlaces que prometen premios, regalos o ofertas muy llamativas.
- No abrir enlaces que pidan contraseñas o datos personales.
- Verificar que el sitio tenga “https” y sea una página oficial.
- Tener cuidado con enlaces que generan urgencia como “haz clic ahora” o “tu cuenta será bloqueada”.

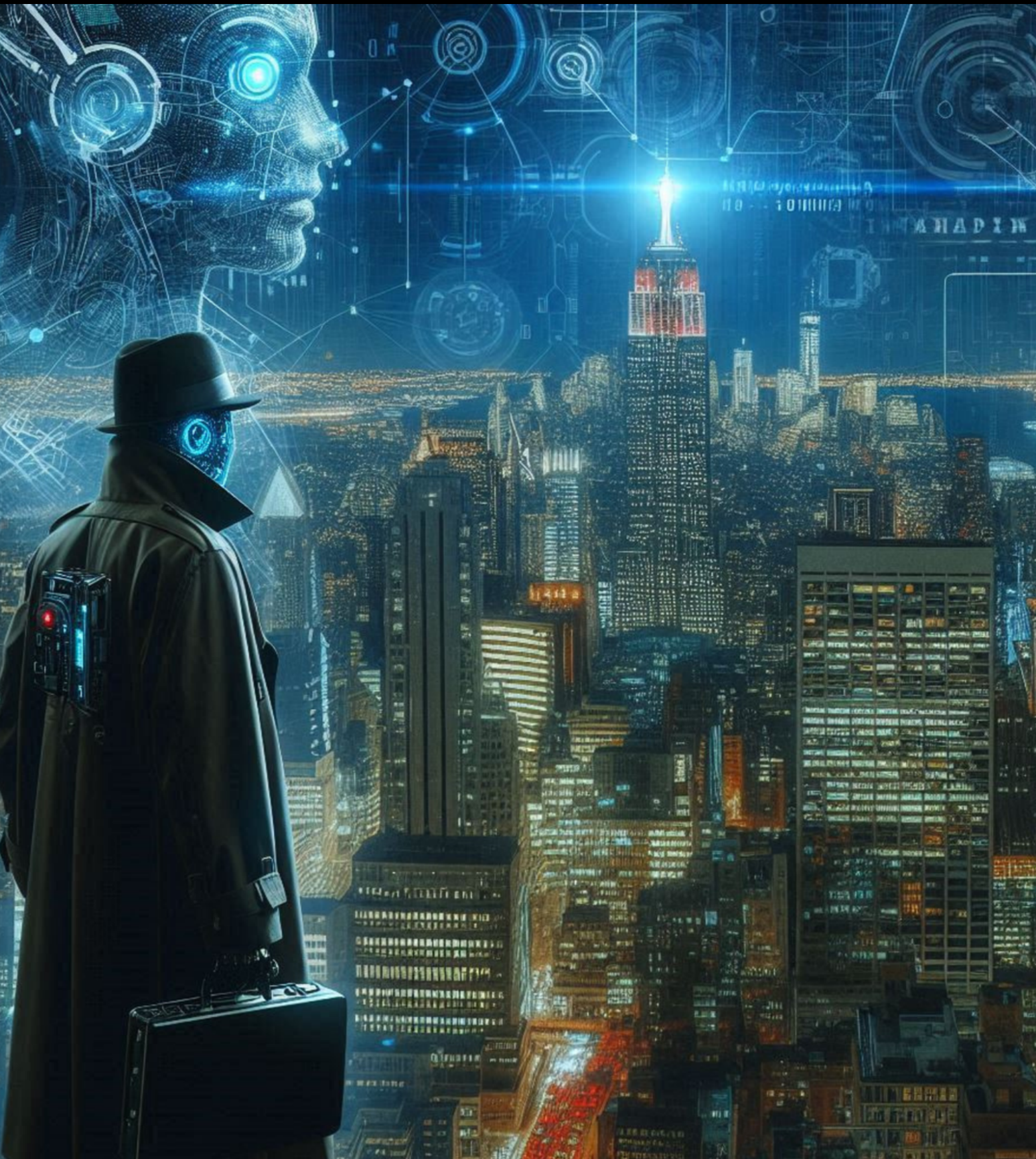


COMO SON LAS ENCUESTAS FALSAS Y RECOLECCIÓN INDEBIDA DE DATOS

- Son formularios o encuestas en internet que simulan ser oficiales para obtener información personal.
- Muchas veces prometen premios, bonos o regalos para que las personas participen.
- Pueden solicitar datos sensibles como número de documento, teléfono, correo o contraseñas.
- La información recolectada puede ser usada para fraudes, publicidad engañosa o suplantación de identidad.
- Nunca se deben proporcionar datos personales en encuestas de origen desconocido.

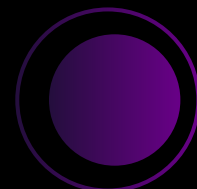
•

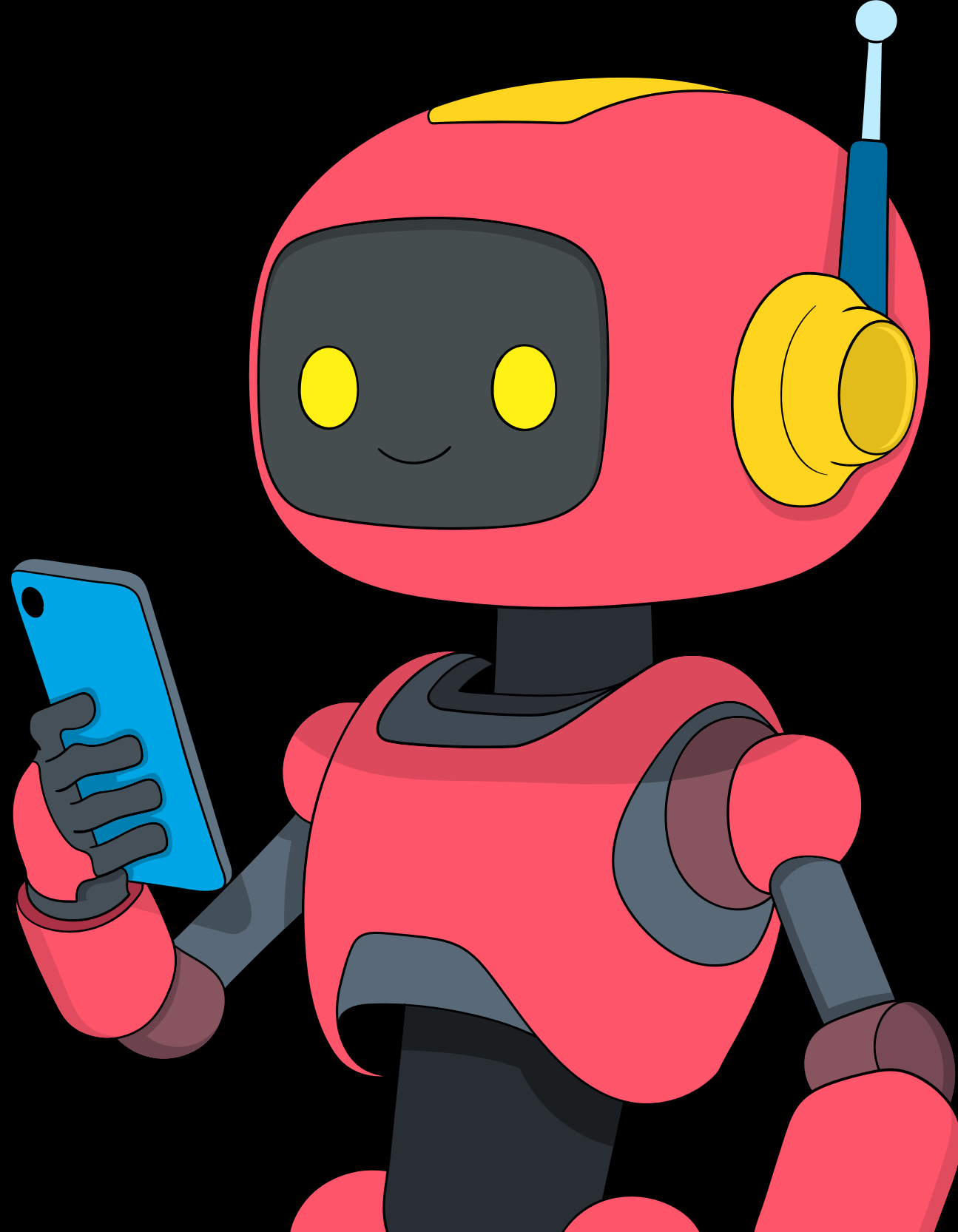




INFORMACIÓN PERSONAL QUE NUNCA DEBERÍAS PUBLICAR.

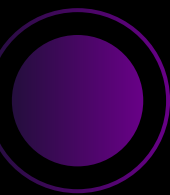
- Número de documento de identidad.
- Dirección de tu casa.
- Número de teléfono personal.
- Contraseñas de cuentas o correos electrónicos.
- Códigos de verificación que llegan a tu celular o correo.
- Datos bancarios o números de tarjetas.
- Información privada de tu familia.
- Ubicación en tiempo real o rutinas diarias.





TEST VIRALES EN REDES SOCIALES QUE ROBAN DATOS:

- Son juegos o cuestionarios que circulan en redes sociales.
- Suelen hacer preguntas sobre datos personales como nombre, fecha de nacimiento o gustos.
- Muchas veces piden iniciar sesión o autorizar acceso a la cuenta.
- La información puede ser usada para robar datos o suplantar identidades.
- Algunos también recopilan información del perfil y de los contactos.
- Por eso es importante evitar participar en test de origen desconocido.





MUCHAS GRACIAS

COMUNIDAD HIJAS DE
MARIA AXILIADORA

Los test virales en redes sociales pueden parecer divertidos, pero muchos recopilan tu información personal. Antes de participar, piensa si realmente es seguro compartir tus datos.

