RIESGO Y PROTECCIÓN DE LAS REDES SOCIALES.

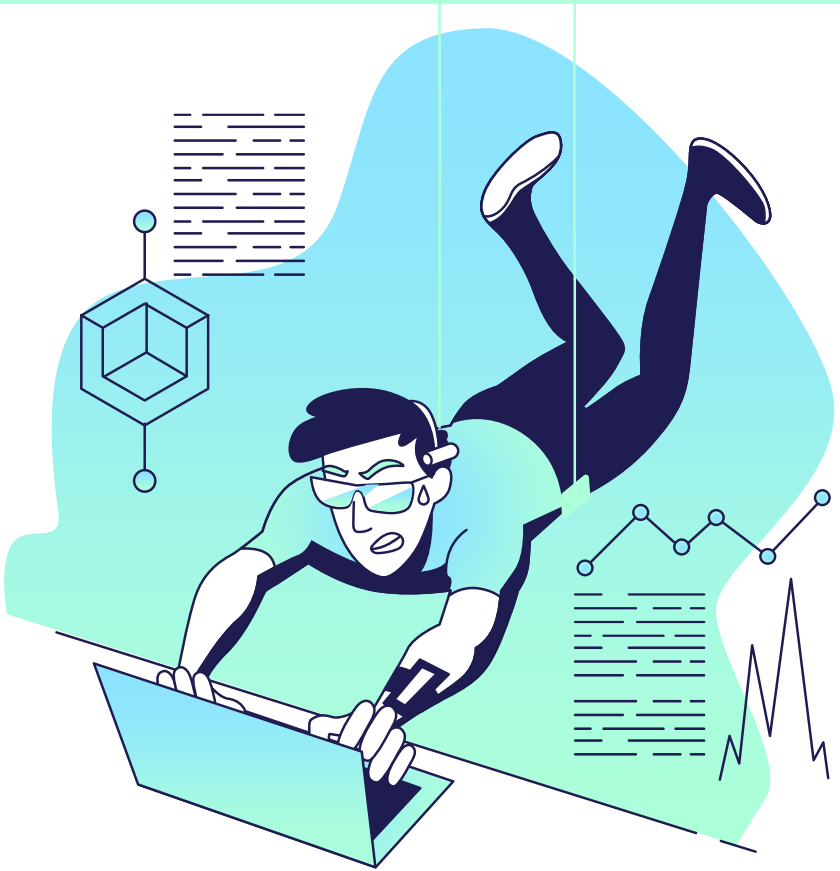
CONTENIDO DE LA PRESENTACIÓN

ÍNDICE

INTRODUCCIÓN

Las redes sociales son omnipresentes en nuestras vidas, pero su uso conlleva riesgos.

En esta presentación vamos a descubrir como protegernos.



01
Riesgos en Redes Sociales

RIESGOS EN REDES SOCIALES

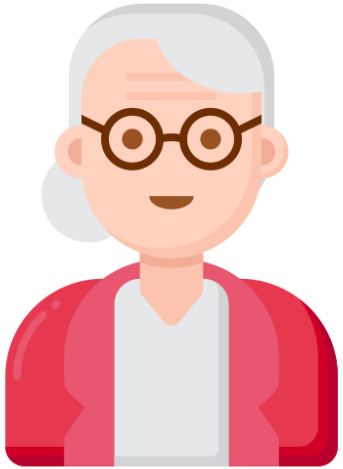
Las redes sociales, aunque conectan personas de todo el mundo, también presentan una serie de riesgos que deben abordarse para garantizar una experiencia en línea segura. Entre estos riesgos destacan:

1. **Pérdida de Privacidad:**
   - La información que compartimos puede ser utilizada de formas no deseadas.
   - Configuraciones de privacidad inadecuadas pueden exponer datos sensibles.
2. **Phishing y Ataques de Ingeniería Social:**
   - Correos electrónicos y mensajes falsos buscan obtener información confidencial.
   - Identificar estos intentos es crucial para evitar caer en trampas cibernéticas.
3. **Malware y Virus:**
   - Descargas no seguras y enlaces maliciosos pueden infectar dispositivos.
   - La protección antivirus es esencial para contrarrestar esta amenaza.

02
Perfiles Vulnerables

PERFILES VULNERABLES

Algunos perfiles son más vulnerables que otros. Niños, adolescentes y personas mayores pueden ser blanco de amenazas específicas. Proporcionaremos consejos para proteger a estos grupos:



1. **Niños y Adolescentes:**
    - Educación Digital: Fomentar la conciencia desde una edad temprana.
    - Configuraciones Parentales: Utilizar las herramientas de control parental para monitorear y limitar el acceso.
    - Comunicación Abierta: Establecer un diálogo abierto sobre la importancia de la seguridad en línea.
2. **Personas Mayores:**
    - Concienciación: Informar sobre los riesgos y tácticas de engaño en línea.
    - Privacidad: Enseñar a configurar y revisar las configuraciones de privacidad.
    - Actualizaciones Regulares: Mantener el software y las aplicaciones actualizadas para mejorar la seguridad.

03
Protección de la privacidad

PROTECCIÓN DE LA PRIVACIDAD

La privacidad es clave en las redes sociales. Exploraremos configuraciones de privacidad, contraseñas seguras y cómo limitar la información compartida públicamente.

1. **Configuraciones de Privacidad:**
   - Revisa y ajusta las configuraciones de privacidad en tu perfil.
   - Limita la visibilidad de información personal solo a aquellas personas de confianza.
2. **Contraseñas Fuertes y Únicas:**
   - Utiliza contraseñas robustas y diferentes para cada plataforma.
   - Cambia las contraseñas periódicamente para evitar accesos no autorizados.
3. **Minimiza la Información Pública:**
   - Comparte solo la información necesaria y evita detalles sensibles.
   - Ten cuidado con la sobreexposición de datos personales.

04 Reconociendo intentos de Phishing

RECONOCIMIENTO DE INTENTOS DE PHISHING

El phishing, un método común de ataque en redes sociales, implica engañar a los usuarios para que revelen información confidencial. Algunas medidas para reconocer y evitar intentos de phishing incluyen:

1. **Verificación de Enlaces:**
    - Antes de hacer clic, verifica la autenticidad de los enlaces.
    - Desconfía de URLs sospechosas o acortadas.
2. **Autenticación de Dos Factores (2FA):**
    - Habilita la autentificación de dos factores siempre que sea posible.
    - Añade una capa adicional de seguridad a tu cuenta.
3. **Desconfianza ante Mensajes Urgentes:**
    - Los ataques de phishing a menudo utilizan mensajes urgentes.
    - Si recibes un mensaje inesperado, verifica la autenticidad antes de tomar acciones.

05
Herramientas de seguridad

HERRAMIENTAS DE SEGURIDAD

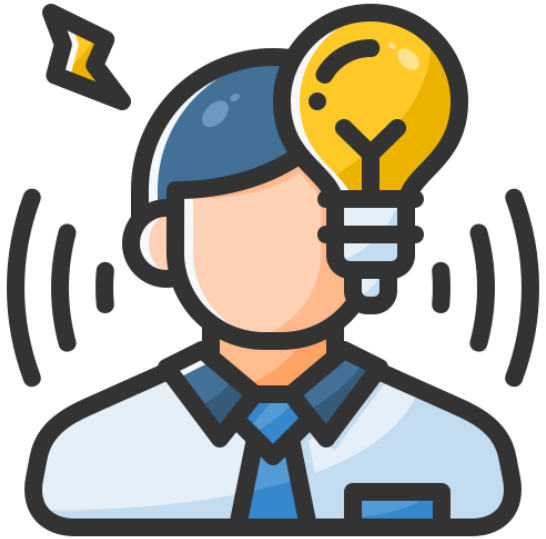
Para fortalecer la seguridad en tus redes sociales, es esencial contar con las herramientas adecuadas. Aquí te presentamos algunas medidas y herramientas efectivas:

1. **Antivirus y Software de Seguridad:**
    - Instala un antivirus confiable y mantenlo actualizado.
    - Utiliza software de seguridad para detectar y prevenir amenazas en tiempo real.
2. **Autentificación de Dos Factores (2FA):**
    - Activa la autenticación de dos factores siempre que sea posible.
    - Este método proporciona una capa adicional de seguridad al requerir una verificación adicional más allá de la contraseña.
3. **Actualizaciones Regulares de Software:**
    - Mantén actualizado el sistema operativo y todas las aplicaciones.
4. **Seguimiento de Inicios de Sesión:**
    - Revisa regularmente la actividad de inicio de sesión en tus cuentas.

06
Educación y concienciación

EDUCACIÓN Y CONCIENCIACIÓN

La educación y la concienciación son piedras angulares para una experiencia segura en redes sociales. Aquí te presentamos estrategias clave:



1. **Programas de Educación Digital:**
    - Participa en programas de educación digital para aprender sobre prácticas seguras en línea.
    - Familiarízate con los riesgos y las mejores prácticas.
2. **Concienciación sobre Ingeniería Social:**
    - Educa a los usuarios sobre las tácticas de ingeniería social.
    - Capacita a reconocer intentos de manipulación y engaño.
3. **Campañas de Concienciación:**
    - Participa y promueve campañas de concienciación sobre seguridad en redes sociales.
    - Comparte información valiosa con amigos y familiares.