Asignatura	Datos del alumno	Fecha
Seguridad en los Sistemas de Información	Apellidos: Jiménez Acosta	
	Nombre: Ronaldo	

Actividad 1. Delitos informáticos en fuentes abiertas

Objetivos

He utilizado el método de búsqueda recomendado en el documento, aplicando el comando **intitle:"Ronaldo Jiménez" "Web" site:linkedin.com.** Esta técnica me permitió localizar información detallada sobre mí, como mi lugar de origen, residencia actual, formación académica, certificaciones y historial laboral.

Además, al emplear el comando **inurl:jimcostdev filetype:pdf**, encontré mi currículum vitae en línea, que no solo contiene la información mencionada anteriormente, sino también mi dirección de correo electrónico.

Por último, al buscar por la palabra clave **"jimcostdev"**, identifiqué varias de mis redes sociales (GitHub, Instagram, YouTube, X, LinkedIn), así como fotos y mi sitio web personal (portafolio).

¿Es fácil realizar un delito informático con la información que he recopilado?
Sí, es relativamente fácil que un ciberdelincuente utilice la información que he recopilado para cometer un delito informático. Los datos que encontré, como mi lugar de origen, residencia actual, formación académica, certificaciones, historial laboral, y especialmente mi correo electrónico, podrían ser explotados de diversas maneras:

- ✓ **Suplantación de identidad:** Con esta información, un atacante podría hacerse pasar por mí en diferentes plataformas o servicios, lo que podría llevar a fraudes financieros o acceso no autorizado a mis cuentas.

Asignatura	Datos del alumno	Fecha
Seguridad en los Sistemas de Información	Apellidos: Jiménez Acosta	
	Nombre: Ronaldo	

- ✓ **Phishing dirigido (Spear Phishing):** El conocimiento detallado sobre mi vida personal y profesional podría ser utilizado para crear correos electrónicos fraudulentos altamente personalizados que parezcan legítimos, engañándome para que revele más información sensible o instale software malicioso.

- ✓ **Ataques a mis cuentas en redes sociales:** Al identificar mis redes sociales y portafolio, un atacante podría intentar acceder a estas cuentas para difundir desinformación, dañar mi reputación o atacar a mis contactos.

Riesgos que he identificado

- ✓ **Exposición de Información Sensible:** La divulgación de mis datos personales y profesionales podría ser explotada para realizar actividades maliciosas contra mí, como el robo de identidad o el acceso no autorizado a mis cuentas.

- ✓ **Ataques de Ingeniería Social:** La información que encontré facilita la elaboración de ataques de ingeniería social, donde un atacante podría manipularme a mí o a mis contactos para obtener más datos sensibles o acceso a sistemas.

- ✓ **Vulnerabilidad a Robo de Identidad:** La disponibilidad de mi CV y otros detalles personales aumenta el riesgo de que un delincuente utilice estos datos para crear cuentas a mi nombre o realizar actividades fraudulentas.

- ✓ **Abuso de Inteligencia Artificial (IA):** Con la información personal que he encontrado, los ciberdelincuentes podrían utilizar herramientas avanzadas de IA para crear deepfakes o clonar mi voz, lo que representa un nuevo nivel de amenaza.

- ✧ **Clonación de Voz:** Usando grabaciones o videos públicos donde hablo, un atacante podría utilizar herramientas de IA para clonar mi voz. Esto podría ser usado en fraudes telefónicos o para manipular a mis contactos, haciéndoles creer que realmente están hablando conmigo.

- ✧ **Deepfakes:** La IA también podría ser utilizada para crear videos falsos altamente realistas, donde parezca que estoy diciendo o haciendo algo que nunca hice. Estos videos podrían dañar mi reputación, ser usados en extorsión o manipular a otras personas.

¿Cómo creo que se podrían evitar estos riesgos?

- ✓ **Ajustes de Privacidad en Redes Sociales:** Necesito revisar y fortalecer la configuración de privacidad en todas mis redes sociales. Es importante limitar la cantidad de información visible públicamente, especialmente detalles como mi ubicación, empleo actual y contactos personales.

- ✓ **Monitoreo y Gestión de mi Presencia en Línea:** Debo revisar regularmente lo que está disponible sobre mí en línea y considerar eliminar información innecesaria o desactualizada. También, puedo configurar alertas de Google para recibir notificaciones si mi nombre aparece en nuevos resultados de búsqueda.

- ✓ **Uso de Servicios de Eliminación de Datos:** Sería conveniente utilizar servicios que me ayuden a eliminar o minimizar la cantidad de información personal que está disponible en línea.

- ✓ **Fortalecimiento de Contraseñas y Uso de Autenticación Multifactor:** Asegurarme de utilizar contraseñas seguras y únicas para todas mis cuentas en línea, y habilitar la autenticación multifactor (MFA) para añadir una capa extra de seguridad.

Asignatura	Datos del alumno	Fecha
Seguridad en los Sistemas de Información	Apellidos: Jiménez Acosta	
	Nombre: Ronaldo	

- ✓ **Concientización sobre Phishing y Deepfakes:** Debo educarme y educar a mis contactos sobre los riesgos de phishing y deepfakes, enseñando a reconocer correos electrónicos sospechosos y videos o audios que puedan ser falsos. Es crucial verificar la autenticidad del solicitante o del contenido antes de proporcionar información sensible o tomar cualquier acción.

- ✓ **Prevención Contra la Clonación de Voz:** Debería limitar la disponibilidad de grabaciones de mi voz en plataformas públicas. En conversaciones sensibles o importantes, estableceré métodos alternativos de verificación de identidad para evitar caer en fraudes basados en la clonación de voz.

Referencias:

https://support.microsoft.com/es-es/windows/prot%C3%A9jase-del-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44#:~:text=El%20phishing%20es%20un%20ataque,que%20fingen%20ser%20sitios%20leg%C3%ADtimos.

https://www.incibe.es/ciudadania/tematicas/virus-amenazas/suplantacion-de-identidad

https://www.computerweekly.com/es/noticias/366609413/Crece-el-uso-de-deepfakes-y-la-clonacion-de-voz