Homeland Security

Department of Homeland Security
Office of Partnership and Engagement (OPE)

Recursos para individuos bajo amenaza de doxing

16 de enero de 2024

¿QUÉ ES DOXING?

Doxing se refiere a la recopilación de información personal identificable de un individuo (PII, por sus siglas en inglés) y su divulgación pública con fines maliciosos, como la humillación pública, el acoso, el robo de identidad o el hostigamiento.

EJEMPLOS DE INFORMACIÓN SENSIBLE

- **Nombre completo**
- **Datos de contacto**
- **Dirección**
- **Miembros del grupo familiar**
- **Detalles del lugar de trabajo**
- **Información financiera**
- **Número de Seguro Social**

FUENTES HABITUALES DE INFORMACIÓN SENSIBLE

- **Publicaciones en redes sociales**
- **Registros de la propiedad y judiciales**
- **Anuncios de boda y obituarios**
- **Boletines informativos**
- **Conferencias públicas**
- **Foros web, blogs y foros de discusión**
- **Redes no protegidas**
- **Listas de inscripción electoral**

¿CÓMO PUEDO PROTEGERME DEL DOXING?

- **Tenga cuidado** con lo que publica sobre usted en internet, incluyendo fotos y vídeos, aunque sean temporales.
- **Elimine** la PII (dirección, fecha de nacimiento, número de teléfono, etc.) de sus perfiles en las redes sociales.
- **Revise** sus seguidores y rechace las solicitudes de cualquier persona que usted no conozca.
- **Solicite** la eliminación de sus datos personales de los sitios web de registros públicos. Entre los sitios web más conocidos se encuentran BeenVerified, FastPeopleSearch, Intelius, PeopleFinders, Spokeo, TruthFinder y Whitepages.
- **Elimine** las apps y las extensiones de navegador innecesarias para evitar la recopilación de sus datos personales.
- **Restringa** el localizador en aplicaciones y sitios web. Desactive los servicios de localización de cada aplicación o plataforma.
- **Active** la configuración de privacidad en redes sociales, aplicaciones y otros sitios web.
- **Instale** la verificación en dos pasos, utilice contraseñas complejas y no repita la misma contraseña para varias cuentas.

¿CÓMO PUEDO PROTEGERME DEL DOXING?

Solicite la eliminación de contenidos falsos, abusivos o amenazadores
Considere presentar una solicitud de eliminación a la plataforma o sitio web, de acuerdo con las normas y requisitos.

Documente lo que ocurre
Considere adoptar medidas para preservar las pruebas. Guarde todos los correos electrónicos, mensajes de voz y de texto que reciba, y haga capturas de pantalla o fotos de los comentarios en las redes sociales.

Notifique el incidente
Si usted ha recibido una amenaza contra su seguridad física o se siente hostigado penalmente, informe del incidente a los funcionarios locales de ley y orden público, así como a la plataforma de redes sociales o al administrador del sitio web.

RECURSOS Y GUÍAS ADICIONALES

Mejores prácticas y recursos de ciberseguridad de CISA: cisa.gov/cybersecurity

Guía CISA Cyber Essentials: cisa.gov/cyber-essentials

Consejo de CISA: Evitando la ingeniería social y los ataques de phishing: cisa.gov/tips/st04-014

Perspectivas de CISA: Mejorar la seguridad del correo electrónico y la web: cisa.gov/publication/enhance-email-and-web-security

Infografía de la guía sobre las amenazas de las redes sociales para el personal y las autoridades escolares: https://www.cisa.gov/resources-tools/resources/social-media-threat-guidance-school-staff-and-authorities-infographic

Si es víctima de un delito en línea, presente una queja **ante el Centro de Quejas de Delitos Cibernéticos (IC3) del FBI** en ic3.gov.