Recomendaciones para la **prevención y reducción** del riesgo de **Extorsión**

Los extorsionistas a menudo buscan **información sensible** que puedan usar en tu contra, como **información personal**, **fotografías**, **videos comprometedores** o **datos confidenciales**.

Estas recomendaciones pueden ayudarte a **usar la tecnología de forma más segura**.

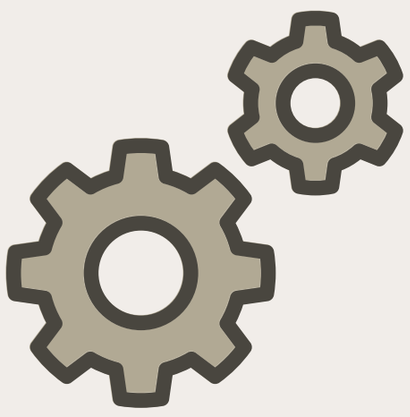
GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

Recomendaciones para la **prevención y reducción** del riesgo de **Extorsión**

Gran parte de tu **comunicación** podría ser potencialmente accesible.
Sólo comunica lo que sea necesario y **evita** comunicar **en exceso.**

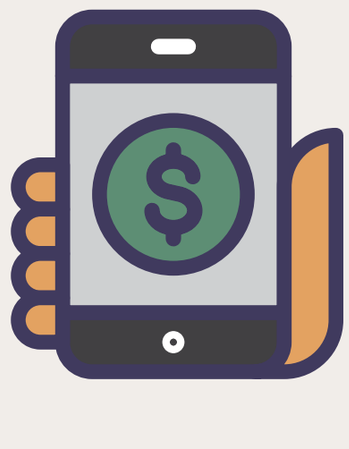
Ya sea en **línea** o **en persona**, no compartas ni publiques información en la esfera pública que pueda ser **utilizada en tu contra**, de tu familia, negocio o comunidad.

Confía en tus instintos, sé escéptico y cauteloso.



Familiarízate con las configuraciones de **privacidad** de las redes sociales, úsalas para **limitar el acceso a tu información personal**, como lista de amigos, ubicación, visibilidad de tus publicaciones.

Si estás enfrentando **desafíos financieros**, como **deudas o dificultades en negocios**, estos problemas podrían ser usados en tu contra, por lo que limita las comunicaciones en esta área a personas necesarias y de confianza.

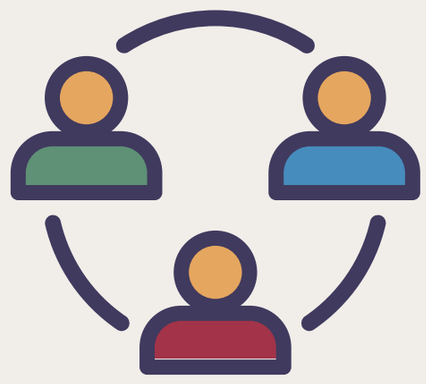


Recomendaciones para la **prevención y reducción** del riesgo de **Extorsión**

Idealmente, conéctate sólo a redes **WIFI de confianza.** Si necesitas conectarte a una red WIFI desconocida, **considera utilizar un VPN para mayor seguridad.**

Cuando recibas s**olicitudes de amistad** o invitaciones en línea, no las aceptes inmediatamente.

Analiza de quién proviene la solicitud y determina si es alguien conocido o una persona confiable en tu red.



Mantente alerta a los **intentos de phishing** en **correos electrónicos y mensajes** que soliciten información personal, confidencial o empresarial, **especialmente** como **contraseñas y detalles bancarios.** Verifica si son auténticos o no.

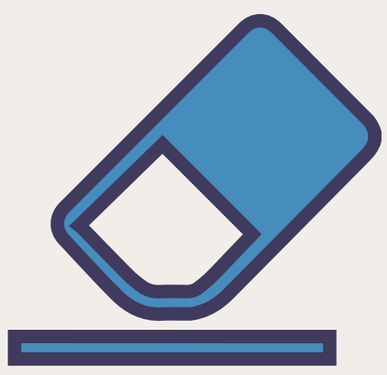
No compartas ninguna información que pueda dejarte vulnerable **personal o profesionalmente** con personas que no conoces en línea. Esto también se aplica en persona.

Recomendaciones para la **prevención y reducción** del riesgo de **Extorsión**

Mejora la seguridad en línea, usa **contraseñas fuertes y únicas**, cifrado de datos y **VPN para mejorar la seguridad**. Un VPN, o "Red Privada Virtual" ayuda a **proteger la privacidad y la seguridad** cuando navegas por Internet.

Imagina que Internet es como una gran autopista, donde circulan muchos automóviles (tu información) y cualquiera puede ver a dónde vas y qué llevas en tu automóvil.

Un VPN funciona como un túnel secreto bajo esa autopista.

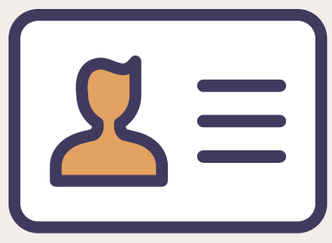


Siempre que sea posible, **elimina detalles personales sensibles en línea,** pero recuerda que estainformación aún puede ser recuperada incluso por alguien con conocimientos técnicos limitados.

Si usas dispositivos públicos o compartidos, **cierra la sesión en TODAS** las cuentas después de usarlas y **no guardes información sensible** o confidencial en estos discos duros.

Recomendaciones para la **prevención y reducción** del riesgo de **Extorsión**

Sé cauteloso con la **información personal** que compartes en las redes sociales como **direcciones, números de teléfono** e **información financiera.**



Identifica y protege las vulnerabilidades personales y empresariales.

Evita compartir imágenes íntimas en línea o por aplicaciones de mensajería ya que podrían ser usadas para extorsionar.

¿Te gustaría conocer mas acerca de este tema? Visita:

globalinitiative.net