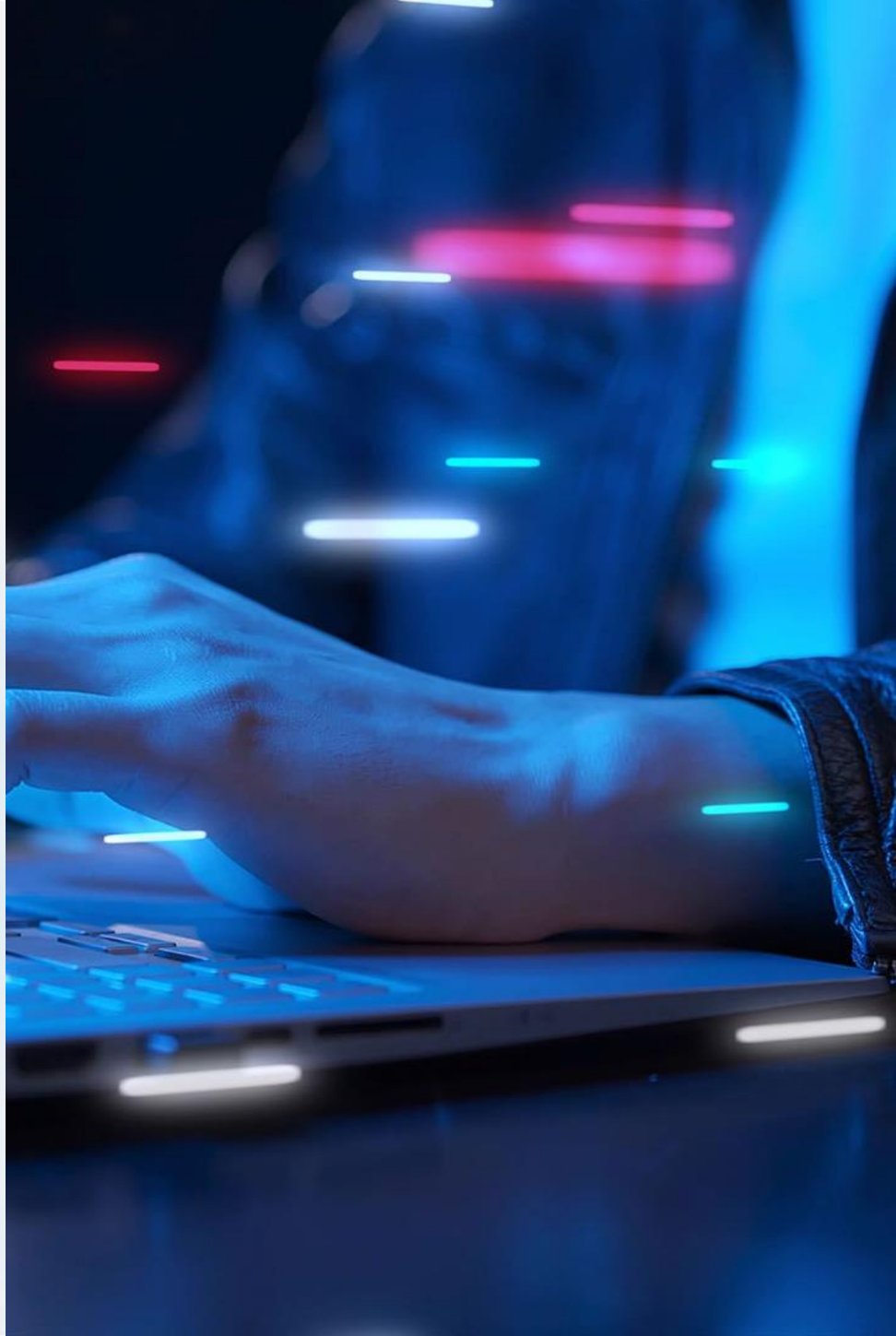
Delitos informáticos y cómo cómo protegerse

Los delitos informáticos se han vuelto muy comunes en nuestros días. Desde el Desde el robo de información personal hasta la extorsión, hay muchas formas en formas en que los ciberdelincuentes pueden causar daño. Aprende cómo cómo protegerte de estos delitos y mantener tus datos seguros.



Qué son los delitos informáticos

Virus informáticos

Código malicioso que se introduce introduce en tu dispositivo sin tu sin tu consentimiento, con el objetivo de dañar tus archivos y archivos y datos.

Robo de datos

Obtención ilegal de información información personal o financiera, financiera, como contraseñas o o números de tarjeta de crédito. crédito.

Suplantación de identidad identidad

Utilización de información personal para cometer fraudes, fraudes, abrir cuentas a nombre nombre de otros, o realizar otras otras fechorías.

Tipo de delitos informáticos

Email phishing

Método de ataque que engaña a los usuarios para que revelen información confidencial como contraseñas o datos contraseñas o datos bancarios. Suele llegar en forma de correo electrónico aparentemente legítimo.

Ransomware

Un tipo de virus informático que secuestra los datos del usuario y los libera sólo después de un pago de rescate. Es pago de rescate. Es una forma común de extorsión online.

DDoS

Ataque de denegación de servicio, en el que un sitio web es inundado con tráfico falso, y no puede accederse a él accederse a él hasta que el tráfico cese.

Ciberseguridad

Backups regulares

Mantener copias de seguridad de tus datos en un en un lugar seguro es clave para recuperarse de recuperarse de un ataque de ransomware.

Actualizaciones del software

Las actualizaciones del software suelen contener contener parches de seguridad para corregir corregir vulnerabilidades conocidas.

Inversión en seguridad

La inversión en medidas de seguridad como como firewalls, antivirus y software de seguridad seguridad de correo electrónico, puede marcar la marcar la diferencia.

Contraseñas seguras

Crear contraseñas fuertes y únicas, así como como cambiarlas regularmente, es crucial para para proteger tu información.

Cómo protegerse frente a los delitos informáticos

Protege tus dispositivos

Protege tus dispositivos con contraseñas fuertes y sofisticadas, sofisticadas, y mantén tu software software actualizado.

Conexiones seguras

Evita conectarte a redes Wi-Fi públicas, y en cambio, opta por por redes privadas y seguras.

Autenticación de dos factores

La autenticación de dos factores factores proporciona un segundo segundo nivel de verificación de de seguridad, fortaleciendo la protección de tu cuenta.

Consejos para evitar ser víctima víctima de un delito informático informático

No abras correos electrónicos sospechosos

Los correos electrónicos de remitentes desconocidos, con información incorrecta o incorrecta o de phishing, deben ser eliminados sin abrir.

No reveles información personal

No reveles información personal o financiera a nadie que no conozcas o no confíes no confíes plenamente.

No descargues archivos sospechosos

No descargues archivos de fuentes desconocidas.

¿Cómo proceder en caso de sufrir un delito informático?

Si sospechas que has sido víctima de un delito informático, sigue estos pasos:
pasos:

1. Mantén la calma y contacta inmediatamente a las autoridades pertinentes.
pertinentes.
2. Guarda toda la información posible, incluyendo capturas de pantalla de los mensajes o correos electrónicos que recibiste, y registra la dirección de correo electrónico o número de teléfono del remitente.
3. Revisa tus cuentas y cambia las contraseñas de las que hayas recibido
recibido correos electrónicos sospechosos.
4. Revisa tu ordenador con un buen software antivirus o lleva tu equipo a un especialista en seguridad informática.

Apoya tu proceso de remediaciones con:

ALINA

ALINA es un innovador chatbot impulsado por Inteligencia Artificial que te ayudará a resolver las remediaciones propuestas en este informe.

https://grupooruss.com/alina

¡Gracias!

www.grupooruss.com