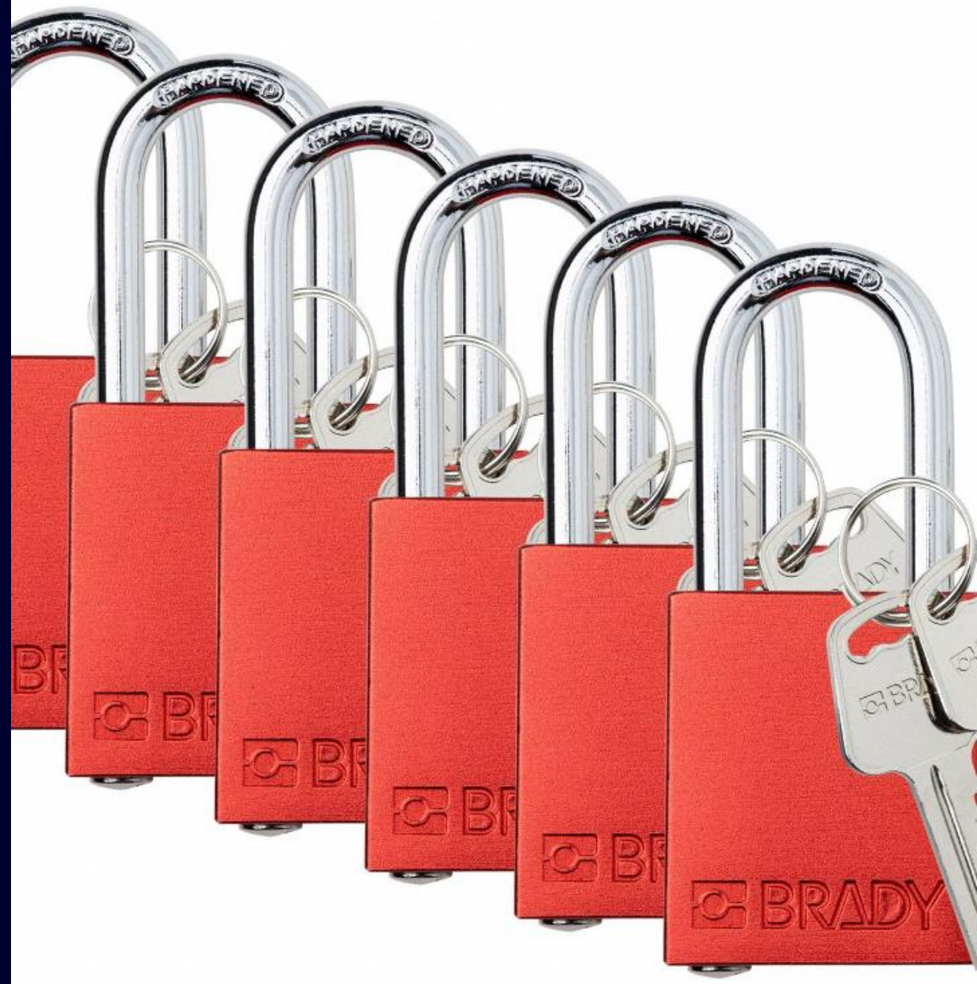
¡Protege tus redes sociales! sociales!

Mantén tu información personal y la de tu familia segura en línea.
Descubre aquí cómo protegerte de las amenazas en redes sociales.



Riesgos en las redes sociales

Fraude financiero

Los estafadores pueden usar tus datos personales para tratar de realizar transacciones bancarias.

Suplantación de identidad

Los ciberdelincuentes pueden usar tus datos para usurpar tu identidad y cometer cometer fraude.

Supervisión no autorizada

Las redes sociales pueden recopilar datos datos sobre tus hábitos y gustos, para luego venderlos a empresas de publicidad.

Acoso en línea

El anonimato en línea puede llevar a conductas abusivas y acoso, especialmente hacia menores.

Protegiendo tu información personal

Revisa tus amigos y seguidores

No agregues a personas que no conoces en la vida real y elimina a aquellos que parezcan sospechosos o que no interactúan con tus publicaciones.

Usa contraseñas robustas

Las contraseñas largas y combinadas con letras, números y caracteres especiales son más difíciles de descifrar.

No compartas información personal

No reveles tu dirección de casa, número telefónico y otra información privada en redes sociales.

Vigila tu actividad en línea línea

Comprueba con frecuencia quién ha accedido a tu perfil, qué dispositivos lo hicieron y desde qué ubicaciones geográficas.

Consejos para crear contraseñas seguras

1

No uses información personal

No uses nombres, fechas de nacimiento o información personal en tu contraseña.

2

Ten en mente un patrón secreto

Crea un patrón de palabras, letras y números que solo tú conozcas.

3

Combina diferentes caracteres

Usa letras minúsculas y mayúsculas, números y caracteres especiales como # y !.

Uso de la autenticación de dos factores

1

Paso 1

Agrega tu número de teléfono móvil móvil a tu cuenta de redes sociales. sociales.

Paso 2

2

Activa la autenticación de dos factores en la configuración de tu cuenta.

3

Paso 3

Cuando inicies sesión, recibirás un código de verificación en tu teléfono. Introdúcelo en el sitio web web o aplicación para iniciar sesión.

Cómo reconocer oportunidades de phishing

Revisa el remitente

El remitente debe tener un un dominio reconocido y no no usar un nombre genérico como "Soporte técnico".

Un correo sospechoso puede contener errores de de ortografía y gramática.

No abras enlaces desconocidos

No hagas clic en enlaces que no reconozcas, ya que pueden descargar malware malware en tu equipo o página de phishing.

Cuidado con las solicitudes urgentes

No respondas a correos electrónicos que te pidan información personal, credenciales o que sugieran una amenaza urgente.

Configuración de la privacidad de las publicaciones

Amigos cercanos

Checa tus opciones de privacidad y configúralas para que solo tus amigos cercanos puedan ver tus publicaciones.

Listas de acceso

Usa las listas de acceso para segmentar a tus amigos y controlar quién puede ver cada publicación.

No aceptes desconocidos

No agregues a personas a tu lista de amigos si no las conoces en la vida real o no contestan tus mensajes. mensajes.

La importancia de mantener actualizado actualizado el software de tus dispositivos dispositivos

Bugs y vulnerabilidades

Las actualizaciones de software pueden solucionar bugs y vulnerabilidades que que los ciberdelincuentes pueden aprovechar.

Mejora del rendimiento

Las actualizaciones de software pueden hacer que tu dispositivo funcione más rápido y eficientemente.

Nuevas características

Las actualizaciones pueden incluir nuevas características características y funciones de seguridad que hacen que que tu dispositivo sea más seguro y fácil de usar.

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