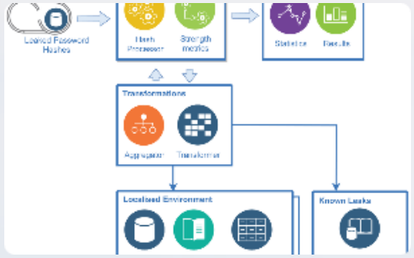
Ataques a las contraseñas: contraseñas: Cómo protegerse adecuadamente adecuadamente

En la era digital, proteger nuestras contraseñas es fundamental para mantener mantener nuestra información a salvo de los ciberdelincuentes.

Factores de riesgo asociados con contraseñas débiles débiles



Fugas de contraseñas

Cada vez es más común que las contraseñas se filtren o sean robadas en línea, lo que puede llevar al acceso no autorizado a tus cuentas.

Ataques de fuerza bruta

Algunos hackers usan programas programas que prueban diferentes combinaciones de contraseñas hasta descifrar la la correcta.

Phishing

Los ataques de phishing son correos electrónicos falsos que parecen provenir de un de un remitente legítimo, pero que intentan intentan hacerte revelar tu información de de inicio de sesión.

Contraseñas débiles

Las contraseñas simples o comunes son fáciles de descifrar y nos ponen en un riesgo un riesgo importante de invasión. Por ejemplo, "1234" o "password".

Cómo crear una contraseña segura

Longitud adecuada

Una contraseña segura debe contener al menos menos 12 caracteres.

Mezcla de caracteres

Combina letras (mayúsculas y minúsculas), números y símbolos como # o $ en tu contraseña. contraseña.

No uses información personal

Asegúrate de no usar información personal como como tu nombre o fecha de nacimiento en tu tu contraseña.

Actualiza tus contraseñas regularmente

Cambia tus contraseñas de forma regular para para evitar posibles robos de información.

Prácticas comunes de ataques a contraseñas

Ataque de phishing

Los atacantes posan de una entidad confiable – confiable – un banco por ejemplo – y envían envían mensajes que parecen legítimos para que para que todo el mundo cambie su contraseña. contraseña.

1

Ataque de diccionario

Los hackers utilizan programas que prueban muchas palabras comunes en lugar de intentar cada posible letra y número.

2

3

Ataque de fuerza bruta

Un ataque de fuerza bruta es cuando se intentan intentan todas las posibles combinaciones de de caracteres para descifrar una contraseña. contraseña.

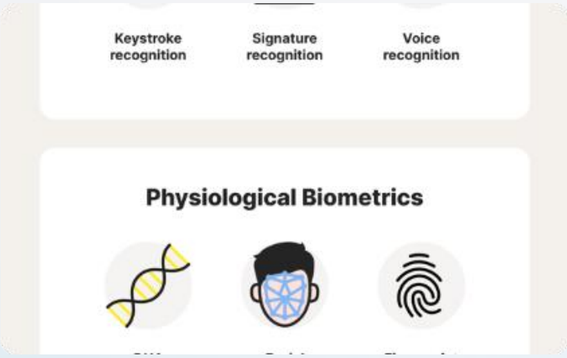
Herramientas recomendadas de autenticación

Autenticación de dos factores

Un segundo nivel de seguridad seguridad otorgado a las cuentas, cuentas, involucrando el uso de de un pin o una huella digital.

Gestor de contraseñas

Algunos softwares almacenan y generan contraseñas seguras automáticamente para que no tengas que recordarlas.



Autenticación Biométrica

Utiliza patrones únicos de huellas huellas dactilares, reconocimiento reconocimiento facial o escaneo escaneo de iris para identificarte identificarte sin la necesidad de de ingresar una contraseña.

Métodos de protección de datos

1

Encriptación

La encriptación es el proceso de codificar datos personales para que solo las personas autorizadas puedan verlos.

2

Antivirus / cortafuegos

Los cortafuegos te mantienen a salvo del tráfico en línea malicioso mientras que los programas programas anti-virus identifican y eliminan software dañino.

3

Seguridad de red

La seguridad de la red se refiere a cómo se asegura la transferencia segura de datos, a menudo a a menudo a través de una red común en línea.

Consejos importantes de seguridad en línea

1

Evita usar las mismas contraseñas

Los mismos inicios de sesión para todas tus tus cuentas pueden correr el riesgo de una una filtración masiva de datos.

2

Piensa antes de hacer click

Presta atención a los correos electrónicos no electrónicos no solicitados o enlaces que que parecen sospechosos.

3

Activa la autenticación de dos factores

Añade una segunda capa de seguridad en en todas tus cuentas importantes.

4

No reveles información personal

Límitate a compartir información personal personal solo con las personas que confías. confías.

5

Usa software actualizado

Te protege de las amenazas actuales en línea. línea.

6

Realiza copias de seguridad de tus tus datos

Guarda tus datos importantes en lugares lugares seguros.

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