Guía de ciberataques

ATAQUES A CONTRASEÑAS

Todo lo que debes saber a nivel usuario

Instituto Nacional
de Cancerología-ESE
Colombia
Por el control del cáncer

OBJETIVOS DE LOS CIBERATAQUES Y SUS CONSECUENCIAS PARA EL USUARIO

Los ciberdelincuentes se encuentran siempre al acecho de nuevas formas con las que atacarnos a los usuarios **aprovechándose de nuestro desconocimiento o vulnerabilidades en nuestras defensas.**
Sus objetivos son muchos **y pueden tener** ***distintas consecuencias para el usuario.***

TIPOS DE CIBERATAQUES

1

Ataques a contraseñas

Los ciberdelincuentes se sirven de *diversas técnicas y herramientas con las que atacar a nuestras credenciales*. **Los usuarios no siempre les dificultamos esta tarea, y solemos caer en malas prácticas que ponen en peligro nuestra seguridad:**

- **Utilizar** *la misma contraseña para distintos servicios*.
- **Utilizar** *contraseñas débiles, fáciles de recordar* **y de atacar**
- **Utilizar** *información personal a modo de contraseñas*, **como la fecha de nacimiento.**
- *Apuntarlas en notas* **o archivos sin cifrar.**
- *Guardar las contraseñas* **en webs o** *en el navegador.*
- **Y, finalmente,** *hacer uso de patrones sencillos*, **como ejemplo utilizar la palabra Cancer, seguida del año y un * o punto . Estos patrones acaban por popularizarse, facilitando aún más la tarea a los ciberdelincuentes.**

TIPOS DE CIBERATAQUES

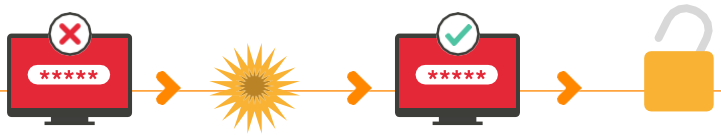
1 *Ataques a contraseñas*

Fuerza bruta | *Ataque por diccionario*

Fuerza bruta

¿Cómo funciona?

Consiste en adivinar nuestra contraseña a base de ensayo y error. *Los atacantes comienzan probando diferentes combinaciones con nuestros datos personales, en caso de conocerlos por otras vías. Luego, continúan haciendo combinaciones de palabras al azar, conjugando nombres, letras y números, hasta que dan con el patrón correcto, usando herramientas que prueban miles de combinaciones por minuto.*



¿Cuál es su objetivo?

El objetivo de los ciberdelincuentes siempre será conseguir la información almacenada en nuestras cuentas.
Dependiendo de si se trata de un correo electrónico, con el que obtener datos personales y contactos; una red social, con la que poder suplantar nuestra identidad; datos bancarios, con los que llevar a cabo transferencias o compras sin nuestro consentimiento; historia clínica y sistemas de apoyo para apoderarse de información de paciente o ciudadano, el atacante hará uso de esta información para su propio beneficio.

¿Cómo me protejo?

Como protección, *es fundamental mejorar la seguridad de las cuentas utilizando contraseñas robustas*. **Además,** *es conveniente aplicar el factor de autenticación múltiple*, **siempre que el servicio lo permita, y utilizar gestores de administración de contraseñas**

Aprende a gestionar tus contraseñas

El factor de autenticación doble y múltiple

Manual de contraseñas y control de Acceso - INC

TIPOS DE CIBERATAQUES

1 Ataques a contraseñas

Fuerza bruta | *Ataque por diccionario*

Ataque por diccionario

¿Cómo funciona?

Los ciberdelincuentes *utilizan un software que, de forma automática, trata de averiguar nuestra contraseña*. **Para ello, realiza diferentes comprobaciones, empezando con letras simples como "a", "AA" o "AAA" y, progresivamente, va cambiando a palabras más complejas.**

¿Cuál es su objetivo?

El objetivo de los ciberdelincuentes siempre será conseguir con la información almacenada en nuestras cuentas. Dependiendo de si se trata de un correo electrónico, con el que obtener datos personales y contactos, una red social, con la que poder suplantar nuestra identidad, o datos bancarios con los que llevar a cabo transferencias a su cuenta o realizar compras sin nuestro consentimiento, el atacante hará uso de esta información para su propio beneficio.

¿Cómo me protejo?

Como protección, *es fundamental mejorar la seguridad de las cuentas utilizando contraseñas robustas*. **Además, es conveniente aplicar el factor de autenticación múltiple, siempre que el servicio lo permita, y utilizar gestores de contraseñas.**

Una contraseña fácil, ¿pero cuántas cuentas comprometidas?

El factor de autenticación doble y múltiple

TIPOS DE CIBERATAQUES

1 Ataques a contraseñas

Fuerza bruta | *Ataque por diccionario*

Ataque por password spraying

¿Cómo funciona?

Los ciberdelincuentes obtienen **gran cantidad cuentas de usuario de una misma entidad ,** *y van probando con* **una pequeña cantidad de contraseñas para intentar acceder a uno o más servicios informáticos**

¿Cuál es su objetivo?

El objetivo de los ciberdelincuentes siempre será conseguir con la información almacenada en nuestras cuentas. Los atacantes usan los patrones de contraseñas mas comunes o populares, y combinaciones de nombres , años, cédulas, información publica en redes sociales, e información institucional entre otros, para probar el ingreso en todas las cuentas de correo de la entidad, que son publicas en cumplimiento de la Ley 1712 de 2014 (Ley de transparencia y del derecho al acceso a la información publica)

¿Cómo me protejo?

Como protección, *es fundamental mejorar la seguridad de las cuentas utilizando contraseñas robustas*. **Además, es conveniente aplicar el factor de autenticación múltiple, siempre que el servicio lo permita, y utilizar gestores de contraseñas. Las contraseñas se deben cambiar mínimo de manera trimestral.**

¿Pocas contraseñas para muchos usuarios ?

Las contraseñas deben ser GESTIONADAS DE FORMA SEGURA EN TODO SU CICLO DE VIDA: desde su creación, pasando por su almacenamiento y terminando por la destrucción.

Deben cumplir una serie de requisitos para que sean ROBUSTAS como TAMAÑO, TIPOS DE CARACTERES a incluir o su PERIODO DE VALIDEZ.

Cambiar las CONTRASEÑAS POR DEFECTO POR OTRAS CONSIDERADAS ROBUSTAS siempre es recomendable.

Los mecanismos de DOBLE FACTOR DE AUTENTICACIÓN "2FA" AUMENTAN LA SEGURIDAD DE LA CUENTA, son especialmente indicados para acceder a información sensible o servicios críticos.

Las contraseñas son un tipo de INFORMACIÓN PERSONAL E INTRANSFERIBLE, nadie a excepción de su propietario debe conocerlas.

Es recomendable utilizar UNA CONTRASEÑA PARA CADA SERVICIO, de esta manera en caso de robo solamente se comprometerá un servicio y no todos.

Los GESTORES DE CONTRASEÑAS son un tipo de herramienta que AYUDA A SU ADMINISTRACIÓN DE FORMA SEGURA, especialmente útiles cuando el número de contraseñas es elevado.

Fuente:

INCIBE - https://www.incibe.es

Instituto Nacional de Ciberseguridad (INCIBE), publicación de INCIBE bajo una licencia Reconocimiento Internacional de Creative Commons 4.0-No comercial-CompartirIgual. Texto completo de la licencia: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es_ES

OSI - Servicio de la Oficina de Seguridad del Internauta (OSI) - https://www.osi.es.