Caja de herramientas de ciberseguridad de la GCA: documento guía para las herramientas de «Renuncie a las contraseñas simples»

Uno de los métodos más comunes que emplean los delincuentes para obtener acceso a sus cuentas, su red o su información es iniciar sesión haciéndose pasar por usted. Es muy importante que utilice contraseñas (o frases de contraseña) únicas y seguras en cada una de sus cuentas, que guarde estas contraseñas en un lugar privado y que nunca las reutilice.

- Si emplea la misma contraseña en diferentes cuentas y un delincuente consigue hacerse con ella, tendrá acceso a todas esas cuentas.
    - *Intentará utilizar el mismo nombre de usuario y la misma contraseña en muchas aplicaciones de uso común.*

Los criminales cuentan con muchas técnicas para conocer sus contraseñas. Además, existe un mercado muy activo en Internet (la llamada *web oscura*) dispuesto a vender y comprar estos datos si una de las empresas con las que tiene cuenta ve comprometida su seguridad.

Estos métodos pueden ser:

- **Ataque por fuerza bruta**: se prueban todas las combinaciones posibles a través de procedimientos informáticos.
    - *Utilice contraseñas o frases de contraseña largas con caracteres especiales para que resulte más difícil.*
- **Ataque por diccionario**: es una variante del ataque por fuerza bruta que utiliza un diccionario con palabras, frases o contraseñas comunes.
    - *Utilice palabras o contraseñas que pueda recordar pero que no estén en ningún diccionario, no sean comunes y que nadie pueda relacionar con usted*
- **Relleno de credenciales**: una vez que los delincuentes consiguen comprometer una cuenta, utilizan el mismo nombre de usuario y la misma contraseña en otros lugares.
    - *Siempre que pueda, use una contraseña diferente en cada cuenta con otras medidas extra de protección (como la autenticación de doble factor o 2FA).*

- **Correo electrónico de phishing:** son correos cuyo asunto podría ser, por ejemplo, «Es el momento de restablecer la contraseña», y que contienen enlaces a sitios web malignos o registradores de pulsadores de teclas que se instalan al abrir un archivo adjunto (estos registradores espían el uso que se hace del teclado).

    - *Tenga cuidado al abrir un correo electrónico, al hacer clic en los enlaces o al descargar contenido desde un mensaje, aunque parezca provenir de una persona u organización que conoce.*

- **Ingeniería social**: los profesionales son muy hábiles manipulando las conversaciones y utilizan diferentes medios (llamadas de teléfono, mensajes de texto o redes sociales) para tratar de engañarle haciéndose pasar por otras personas y que revele sus contraseñas y otros datos personales.

    - *Nunca comparta con nadie su contraseña, ni partes de ella. Una empresa legítima no se lo pedirá.*

- **Adivinar manualmente la contraseña**: a través de los datos personales; por ejemplo, probando si se ha utilizado el nombre o la fecha de nacimiento en la contraseña.

    - *No utilice datos personales en las contraseñas. Piense en toda la información sobre usted que podría extraerse de las redes sociales e Internet y evite usarla en sus contraseñas.*

- **Espiar por encima del hombro**: en los lugares públicos o incluso en su puesto de trabajo, puede haber alguien espiando lo que hace.

    - *Compruebe quién está detrás o junto a usted, o si hay cámaras, especialmente cuando introduzca información confidencial.*

- **Interceptación**: las contraseñas pueden interceptarse en su paso por una red.

    - *Compruebe que el símbolo de candado* https *está presente en el sitio web y tenga cuidado cuando utilice conexiones wifi en lugares públicos, ya que pueden ser poco seguras o podría haber otras conexiones fraudulentas con un nombre parecido que permitieran ver la información que está transmitiendo.*

La capacidad de procesamiento de los equipos informáticos ha ido aumentando de forma exponencial con el tiempo, al igual que el uso de Internet y las redes sociales. Todo ello hace que resulte más fácil y rápido para los delincuentes acceder a nuestros datos:

	PC MacIntosh de Apple, 1984:	iMac 'Core i5' (estándar), 2019	Diferencia:
RAM:	128 K	8 G	Aumento del 64 500 000 %
Velocidad de procesamiento:	8 MHz	3 GHz	Un 37 400 % más rápido
Costo:	2 500 USD	1 500 USD	Reducción del 40 %

- Los rápidos avances tecnológicos les han dado a los ciberdelincuentes una posición de ventaja, y es que nunca había resultado tan rápido descifrar una contraseña como con los portátiles y programas modernos.
    - *Es necesario adaptarse a estos avances y utilizar contraseñas más largas y complejas, así como otras medidas de protección.*

Autenticación de doble factor (2FA)

La autenticación de doble factor aporta un nivel de protección adicional que dificulta enormemente a los atacantes el acceso a las cuentas. Para ello, se utiliza lo siguiente:

- Algo que se sabe:
    - Una contraseña
- Algo que se tiene:
    - Un token (Google Authenticator, Okta o RSA)
    - Un código de verificación que se envía al teléfono (SMS)
- Algo que se es:
    - El rostro o la huella digital (biometría)

La autenticación de doble factor necesita estos datos para permitir el acceso, lo que proporciona una capa de protección adicional.

Existen muchísimas recomendaciones para crear contraseñas o frases de contraseña largas y seguras. Con independencia de las que utilice, asegúrese de:

- Aplicar una política segura en toda la organización y un sistema que prohíba el uso de contraseñas poco seguras.
- No utilizar nombres de mascotas y otras contraseñas que podrían adivinarse a través de las redes sociales.
- Utilizar una contraseña diferente en cada cuenta.
- Explorar la posibilidad de utilizar un gestor de contraseñas para guardar las claves.

Otras recomendaciones:

- Actualice las contraseñas de las cuentas que se hayan visto comprometidas (puede comprobarlo con la aplicación Have I Been Pwned de la caja de herramientas).
- Elimine las cuentas y desinstale las aplicaciones que ya no se utilizan.
- No olvide utilizar contraseñas seguras y únicas en todas las cuentas.
- Habilite la autenticación de doble factor en todas las cuentas que lo permitan.
- Compruebe la configuración predeterminada del administrador en todos los dispositivos a los que se pueda acceder en remoto. Modifique siempre las contraseñas que vienen por defecto antes de usar el dispositivo o aplicación por primera vez, ya que son relativamente fáciles de adivinar.

Utilice las herramientas de «Renuncie a las contraseñas simples» para comprobar si alguna de sus cuentas se ha visto comprometida e implementar mejoras.

https://gcatoolkit.org/es/pequenas-empresas/renuncie-a-las-contrasenas-simples/