De contraseñas comunes y ocho mitos para aprender a estar más seguros en línea

Image not found or type unknown

Foto:Internet

La secuencia de dígitos 123456 sigue siendo en este 2020 la contraseña más común empleada por los usuarios en sus diferentes servicios en internet, de acuerdo con un estudio que cada año realiza la compañía NordPass.

Esta empresa cuenta con una solución informática para proteger nuestras contraseñas, con una versión gratis y otra de pago, y siempre presenta a finales de año una lista con las 200 claves más comunes, la cantidad de usuarios que las emplean (según los registros con NordPass) y el tiempo que se emplea en descifrarlas.

La clave 123456 requiere menos de un segundo para ser averiguada por un programa informático destinado a descifrar contraseñas y, según NordPass, más de dos millones de sus usuarios la usan. En segundo lugar aparece 123456789, la cual por ser más larga no deja de ser igual de fácil de adivinar por parte de los hackers.

Este año, como novedad, aparece picture1 entre las más usadas, completando el «podio» de las peores claves del año. Este es un ejercicio que busca abrir los ojos a aquellos confiados en que su contraseña es segura, o que no les tocará ser víctimas de hackers.

Por eso les propongo repasar ocho mitos alrededor de las contraseñas explicados por un experto de NordPass, Benjamin Scott.

No necesita preocuparse por las contraseñas si no tiene nada que ocultar

No tengo nada que ocultar, dicen muchas personas. Y así, establecen claves de acceso simples. Pero si se vieran afectadas por una brecha de seguridad, podrían ni siquiera darse cuenta cuando las conviertan en herramientas a la venia de un hacker malicioso. Por ejemplo, un pirata informático puede decidir

emplear tu correo electrónico para lanzar ataques de phishing, y los contactos o amigos del afectado podrían verse expuestos a ransomware u otros programas malignos.

Un hacker que descifre una contraseña tendría acceso a otras cuentas vinculadas en diferentes plataformas. Después de todo, las credenciales de correo electrónico y redes sociales se utilizan a menudo como mecanismos de inicio de sesión para sitios de terceros.

Está bien usar la misma contraseña en varias cuentas

Reutilizar contraseñas no es un movimiento inteligente. Es la misma razón por la que usted no desea utilizar una sola llave para su automóvil, oficina y apartamento. Si utiliza las mismas claves para varios sitios web un hackeo puede propagarse rápidamente.

Los números y los caracteres especiales fortalecen automáticamente la contraseña

Agregar números y símbolos a su contraseña ayudará, por supuesto, pero no en la medida en que muchos piensan. Los atacantes utilizan programas que pueden recorrer símbolos comunes y secuencias numéricas en milisegundos. Agregar 123 o remplazar la letra A con @ no hará mucho para ralentizar los softwares destinados a descifrar claves de acceso. Si bien es importante usar letras, números y símbolos completamente aleatorios, evitar patrones es esencial.

No es seguro escribir contraseñas

En un entorno empresarial o de oficina, es claramente vital que la información de la contraseña no se deje por ahí. Por otro lado, para las cuentas personales (redes sociales, por ejemplo, y correos electrónicos domésticos) realmente no es tan importante. Si alguien quiere secuestrar su cuenta de redes sociales o ingresar a su correo electrónico, es poco probable que viva cerca de usted. Un hacker puede sentarse en un dormitorio al otro lado del mundo y aun así lanzar un ataque. Mucho peor que escribir una contraseña es usar una simple y fácil de recordar. Esto último es sinónimo de fácil de descifrar.

Los verificadores de contraseñas en los sitios web siempre son confiables

Vaya a cualquier sitio web que tenga una evaluación de fuerza incorporada en el proceso de creación de contraseña. Descubrirá que al agregar una letra mayúscula y algunos números y símbolos, puede incrementar la calificación de su contraseña de débil a fuerte. No es así como funciona la seguridad por contraseña. El hacker que quiera ingresar a su correo electrónico utilizará herramientas sofisticadas. Puede comprobar cada palabra del diccionario en cuestión de segundos. Pasar por los nombres comunes y combinar cada uno con fechas comunes y patrones numéricos no le llevará mucho tiempo. Elegir P@ssword123 en lugar de «contraseña» hace muy poco para mejorar la seguridad, sea lo que sea lo que el verificador de fuerza de una web pueda decirle.

Olvidar su contraseña puede bloquearlo permanentemente de una cuenta

Esto solo sería cierto en circunstancias muy específicas. Para la gran mayoría de los usuarios de las plataformas protegidas con contraseña, recuperar una cuenta es bastante simple. Desde sitios de redes sociales como Instagram hasta centros de entretenimiento como Spotify, puede restablecer una contraseña olvidada con unos simples pasos.

Los usuarios siempre tienen la culpa de las infracciones de seguridad de las contraseñas

Es fácil culpar a los usuarios cuando sus cuentas son pirateadas o sus datos de inicio de sesión aparecen en línea. Sin embargo, las contraseñas débiles no siempre son la causa de estas infracciones. Muchos sitios web brindan consejos engañosos sobre lo que constituye una contraseña segura. La mayoría no se molesta en pedir a los usuarios que tomen precauciones adicionales. Peor aún, las contraseñas a veces se filtran en la web profunda cuando los archivos corporativos no están protegidos.

De hecho, puede averiguar si sus datos de inicio de sesión están disponibles en línea consultando el sitio web haveibeenpwned.com. Las empresas deben ser conscientes del papel que desempeñan para mantener seguras las contraseñas de los usuarios.

La complejidad siempre triunfa sobre la longitud

La complejidad es esencial, pero también lo es la longitud. Existe una razón por la que la mayoría de los sitios incluyen un número mínimo de caracteres para las contraseñas: cuanto más largos, mejor. Es más difícil hacer complejas las contraseñas cortas. Incluso una colección aleatoria de letras y símbolos se puede descifrar con relativa rapidez si solo tiene seis caracteres. La longitud y la complejidad son dos claves para una buena seguridad de las contraseñas. Si puedes concentrarte en ambos, entonces tu cuenta será mucho más difícil de hackear. (Tomado de Juventud Rebelde).

---

https://www.radiohc.cu/index.php/noticias/ciencias/241550-de-contrasenas-comunes-y-ocho-mitos-para-aprender-a-estar-mas-seguros-en-linea

Radio Habana Cuba