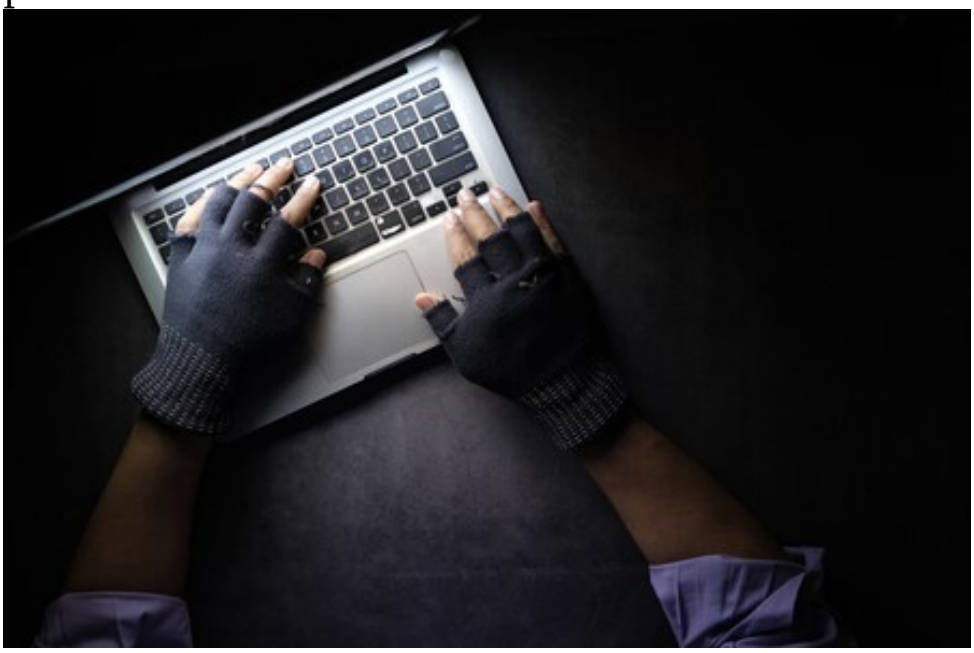
¿Cuánto tarda un hacker en averiguar tu contraseña?

Ya sabemos lo que tarda un hacker en averiguar tu contraseña por fuerza bruta. Da miedo.



ene-2023

JAVIER PASTOR

@javipas

En 2012 tener una contraseña de 10 caracteres con números, minúsculas y mayúsculas era bastante recomendable: los hackers podían tardar 106 años en averiguarla por métodos de fuerza bruta.

La cosa ha cambiado mucho en la última década. La potencia de las tarjetas gráficas con las que es posible acelerar el proceso ha

crecido de forma extraordinaria. De hecho, asusta: **esa misma contraseña ahora caería en tres semanas**.

La empresa de ciberseguridad Hive Systems lleva tiempo elaborando estos estudios, y en los últimos años se ha podido ver cómo efectivamente la recomendación es cada vez más exigente para los que crean nuevas contraseñas.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

De hecho, lo de usar números, mayúsculas y minúsculas ya no es suficiente, ahora es casi imprescindible:

1) usar una contraseña de al menos 12 caracteres y

2) usar además símbolos para crear contraseñas mucho más fuertes, aunque sean también mucho más difíciles de recordar.

Lo podemos ver rápidamente en la tabla siguiente, que además podemos comparar con las de 2020 y 2021 para sacar conclusiones evidentes: lo que creíamos que era una contraseña fuerte entonces **quizás no lo sea tanto ahora**.

LONGITUD	**2012**	**2021**	**2022**
10 CARACTERES NÚMEROS, MAYÚSCULAS Y MINÚSCULAS	106 años	7 meses	3 semanas
12 CARACTERES NÚMEROS, MAYÚSCULAS Y MINÚSCULAS	108.000 años	2.000 años	200 años
12 CARACTERES NÚMEROS, MAYÚSCULAS, MINÚSCULAS Y SÍMBOLOS	5 millones de años	34.000 años	3.000 años

LONGITUD	2012	2021	2022
12 CARACTERES NÚMEROS, MAYÚSCULAS, MINÚSCULAS Y SÍMBOLOS	193 billones de años	1 billón de años	92.000 años

Como indican en Hive Systems, las modernas tarjetas gráficas siguen siendo una buena forma de tratar de "romper" contraseñas, pero si uno realmente quiere acortar tiempos, lo ideal es **romperlas** "**en la nube**".

De hecho todos los datos utilizados aquí se refieren a ese método: esos tiempos de 2022 se basan en el uso de 8 GPUs NVIDIA A100 Tensor Core GPUs en Amazon Web Services a través de sus instancias P4 de EC2.

Nada mejor que una buena NVIDIA HGX A100 para romper contraseñas.

El costo de alquilar una hora esas instancias es de 32,77 dólares, pero claro, podríamos combinar varias. Esos tiempos son además los máximos posibles: es muy probable que acabáramos averiguando la contraseña antes si usáramos estos métodos.

Si no quieres gastar tanto, no pasa nada: servicios como vast.ai permiten alquilar ocho RTX 3090 **por 5,80 dólares la hora** —el precio varía según la demanda—, y con ellas también es posible hacer ataques de fuerza bruta realmente potentes. Suponemos que en pocos meses se ofrecerán las 4090, que son unas bestias rompiendo contraseñas, y multiplican por dos o más el rendimiento de las 3090 en estos escenarios.

Eso deja claro que un hacker motivado (y con fondos) puede acabar rompiendo contraseñas que creíamos razonablemente

fuertes. Nuestra **recomendación a la hora de crear nuevas contraseñas** es la siguiente:

1. 16 caracteres como mínimo.
2. Usar números, mayúsculas, minúsculas y símbolos.
3. Usar un gestor de contraseñas para recordar esas contraseñas fuertes.
4. Usar un método de autenticación en dos pasos.

El tercer consejo es evidente: es realmente complicado recordar esas contraseñas, así que contar con un gestor de contraseñas para esa gestión resulta casi imprescindible.

Y por supuesto, siempre que podamos lo ideal es además usar un sistema de autenticación en dos pasos (2FA). Si podemos evitar SMS mejor que mejor: lo más adecuado aquí sería utilizar aplicaciones tipo Authy o Google Authenticator, o dar el salto a tokens físicos como los de Yubikey.