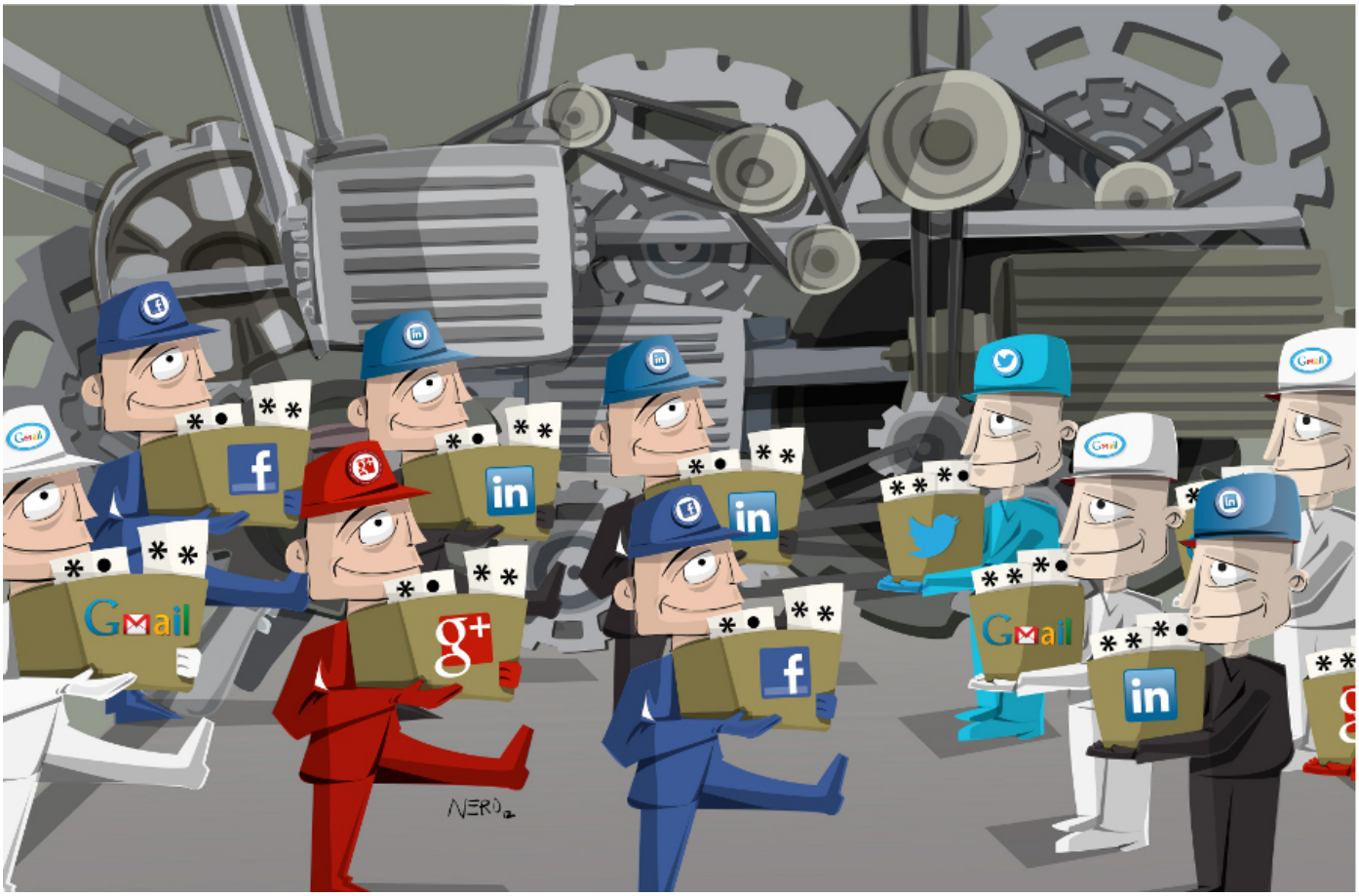
PASSWORD-FU: GUÍA FÁCIL PARA CONTRASEÑAS REALMENTE SEGURAS

Sergio Andrés Becerril

consejos

numero-15



“*DEBES UTILIZAR CONTRASEÑAS SEGURAS*”

Viejo mantra de seguridad

¿Cuántas veces hemos escuchado esta recomendación? Si has asistido a un curso, leído artículos (incluso los de esta revista) o tal vez escuchado un poco del tema de la seguridad informática, es casi seguro que has recibido este consejo más de una vez. Es una receta clásica que como los consejos de la abuelita, son más sencillos de decir que de seguir.

Pues bien, no te preocupes más. La siguiente es una sencilla guía de 3 pasos para que tus contraseñas sean (y se mantengan) siempre seguras. Explicaré un poco la razón detrás de estas recomendaciones, algunos puntos adicionales a considerar y cómo, tomados en conjunto, te ayudarán a resistir la mayoría de los embates contra tu seguridad.

1. Nunca utilices datos personales para crear tu contraseña

Recordemos que el propósito de las contraseñas es evitar accesos indeseados, no queremos que

cualquiera pueda leer nuestro correo, por ejemplo. Si utilizas información personal para crear tu contraseña (tu calle y número o tu fecha de nacimiento), estás aumentando la probabilidad de que alguien la adivine, ya que esta información es 1) fácil de obtener, pero sobre todo 2) muy comúnmente utilizada en contraseñas.

2. Una frase es mucho mejor que una 'contraseña'

- Pero (me dirán), ¿voy a tener que utilizar algo como 'b&kqAp5H' de contraseña? ¡*Nadie* se acuerda de esas cosas!- (con cierta razón).

Las supuestas contraseñas “seguras” son un ejemplo de buenas intenciones y pésimos métodos, porque los humanos no somos máquinas. Una persona recuerda algo mucho mejor si ese algo tiene sentido, una relación con su vida, etc. Después de todo, así funcionan nuestros cerebros.

Lo que es más, esa contraseña no es tan *segura* como parece. Además del (muy real y muy común) riesgo de ser apuntada en un post-it (algo así como dejar las llaves de la casa colgadas afuera de la entrada) un atacante con los medios apropiados la descubrirá en un santiamén. Específicamente, en 12 horas o menos[1].

¿Cuál es la solución entonces? Mi sugerencia: una frase de contraseña.

Consideremos la siguiente frase:

“Todos los días, gimnasio a las 8”

Tal vez es parte de tu rutina diaria o es un propósito de año nuevo. Como sea, una buena parte de ustedes se habrán identificado con esta frase. Y eso buscamos para no olvidarla. Ahora, ¿cómo utilizamos esto como contraseña? Muy sencillo. Quita acentos, espacios y escribe:

Todoslosdias,gimnasioalas8

Sorprendentemente, esta contraseña es ***un millón de cuatrillones de veces más segura*** que la que escribí al principio de esta sección - algo así como comparar una caja fuerte con una cajita de papel-. El mismo atacante que vulneró nuestra contraseña anterior en 12 horas tardaría miles, millones de años en encontrarla.

Tiene suficiente relación con nuestra vida como para recordarla fácilmente, pero no lo suficiente para que alguien la adivine.

Cada quien tendrá su propia fuente de inspiración para sus frases. Algunos utilizan frases de libros; otros, refranes populares. Conviene evitar una frase muy famosa; busca algo memorable únicamente para ti. La clave es la longitud: mientras más larga, mejor. Con 5 o 6 palabras usualmente basta. Esto lo discutimos a mayor detalle al final de este artículo, en la sección *"el tamaño sí importa".*

Lamentablemente, habrá sitios que no te permitirán contraseñas tan grandes (Outlook.com, anteriormente conocido como Hotmail, es uno de los principales culpables). Mi recomendación: abandona el servicio, o quéjate. Si es *imprescindible* que utilices el servicio utiliza una contraseña tan grande como te permita el sistema (en el caso de Outlook, el límite son 16 caracteres), pero considera al servicio como trascendentalmente inseguro.

3. Acomoda, rota y anota

¡Muy bien! Ya tenemos una guía para *crear* contraseñas seguras, que además son fáciles de recordar. Sin embargo, nos falta atender el resto de las recomendaciones comunes:

"Nunca utilices la misma contraseña en diferentes sitios"

"Debes cambiar tus contraseñas periódicamente (e.g. cada año)"

"Jamás apuntes tus contraseñas, mejor memorízalas"

Muchos expertos de seguridad me odiarán por lo que diré a continuación, pero la realidad es que puedes ignorar estas recomendaciones *bajo ciertas circunstancias*. Para ello, hay que entender qué se pretende con cada una y cómo podemos resolver cada problema con un enfoque diferente.

La razón por la cual se sugiere utilizar siempre una contraseña diferente es que, si un atacante logra obtener acceso a un servicio, podrá obtener acceso a otros sin mayor esfuerzo. En ocasiones, ¡no importa si tu contraseña es segura! Esto es porque a veces los atacantes logran vulnerar la seguridad de los proveedores y obtener acceso a **todas** las contraseñas. Un ejemplo es el reciente ataque a LinkedIn (junio 2012), donde las contraseñas de más de seis millones de usuarios de la red social fueron publicadas en Internet.

Aunque aquí la culpa yace en el proveedor, como usuarios podemos minimizar el riesgo. Utilizar

diferentes contraseñas hace justamente eso, porque garantiza que, aunque un atacante logre tener acceso a uno de tus servicios, no llegará más lejos[2].

Cambiar periódicamente las contraseñas sirve a un propósito similar: no importa qué tan bueno sea un atacante, si cambias el objetivo (i.e. tu contraseña) regularmente, frustrarás sus intentos por vulnerar tu seguridad.

Finalmente, evitar apuntar las contraseñas es la recomendación más sencilla de entender: evita que alguien (accidentalmente o a propósito) obtenga tus credenciales con mínimo esfuerzo.

¿Cómo le damos la vuelta a esto? El primer paso es **acomodar**. Debes acomodar todos los servicios que utilices con base a dos preguntas: **¿Contiene información crítica? ¿Es una puerta para otro servicio?**

La primera solo tú la puedes responder. Cada quien tendrá su definición de información crítica, aunque generalmente te diría que es algo que no puedes arriesgarte a perder (como tus declaraciones de impuestos) o a publicar (como tus correos privados). Recuerda que tu *identidad* también es muy valiosa. Considera, ¿qué podría lograr un atacante que obtuviera acceso a tu cuenta de Facebook, por ejemplo?

La segunda es más difícil de contestar. En esencia, una “puerta” es aquella cosa que te puede brindar acceso a otro servicio. El ejemplo clásico es tu cuenta de correo electrónico. ¿Por qué? Tu cuenta de correo electrónico se utiliza, entre otras cosas, para la recuperación de contraseñas de, probablemente, *todos los demás servicios*. Los atacantes saben esto y por eso consideran tu cuenta de correo uno de los premios más jugosos por obtener. Deberás buscar esas *puertas* y anotarlas.

Una vez que hayas hecho esto, podrás *acomodar* tus servicios respecto a su importancia. En mi caso:

Al centro está mi servicio más preciado: mi cuenta de correo principal. Tiene información crítica y es puerta para el resto de mis servicios. Ligeramente menos importantes son mis accesos a mis redes sociales, mi banco y mi servicio de compras en línea (no son “puertas”, pero sí tienen información crítica). Finalmente, mis servicios menos críticos (Netflix, Wordpress y Skype) están en el menor nivel de importancia.

Una vez *acomodados* tus servicios, puedes “**rotar”**.

Piensa en cada “nivel” de tus servicios como un mundo en sí mismo. Dentro de ese nivel, no debes repetir contraseñas y debes cambiarlas periódicamente. Pero, en vez de crear nuevas contraseñas cada que quieras cambiar tus servicios, puedes *rotarlas.* En mi caso, tengo 4 contraseñas diferentes en el segundo nivel. Cuando llega la hora de cambiarlas, simplemente roto: la contraseña de Twitter se convierte en la contraseña de mi banco, la contraseña de eBay en la contraseña de Twitter, etc.

También puedes rotar entre niveles, de arriba hacia abajo. ¿A qué me refiero? Cuando llega la hora de cambiar la contraseña de la cuenta de correo, es evidente que debo **crear** una nueva contraseña (después de todo, es mi servicio más sensible – debo ser más cuidadoso). ¿Qué hacer con la contraseña anterior? ¡Puedo rotarla hacia abajo! Digamos, a mi Facebook. Esto causaría que una contraseña de este nivel rotara hacia abajo y así sucesivamente.

De esta manera, mis contraseñas tienen un largo tiempo de vida (¡varios años!), lo que facilita su memorización, sin que esto haga que mis servicios sean más inseguros. Por supuesto, en el momento que descubra que algún servicio ha sido vulnerado, esa contraseña desaparece completamente de la rotación.

Aún así nos queda un reto: recordar qué contraseña le toca a qué servicio. El famoso “post-it de la muerte” puede aquí ser utilizado a nuestro favor. ¿Por qué? Pues porque si utilizas frases de contraseña, puedes **anotar** referencias a las frases, en vez de las contraseñas en sí. Por ejemplo, utilizando nuestra frase de contraseña (Todoslosdias,gimnasioalas8) podríamos anotar algo como: correo – gimnasio.

Para un atacante, esto tiene poca utilidad – la sola presencia de la palabra gimnasio no ayuda mucho, porque no es la contraseña en sí. Sin embargo, para ti cumple su propósito – te permite recordar fácilmente que, si quieres ingresar a tu correo, debes utilizar la frase que utiliza *gimnasio.*

Suena cansado y difícil, pero recuerda que son solo tres fases:

a) ACOMODA tus cuentas en niveles de importancia

b) ROTA las contraseñas *dentro de su mismo nivel o hacia abajo*

c) ANOTA las referencias entre servicios y contraseñas

SOLO PARA MECANÓGRAFOS: ¡DESPLAZA TUS MANOS!

Si eres mecanógrafo (es decir, que puedes escribir sin ver el teclado), este tip es para ti. Es tremendamente sencillo: desplaza tus manos uno o más lugares hacia la izquierda, derecha, arriba o abajo.

Por ejemplo, desplazando mis manos un lugar hacia arriba, puedo lograr que la contraseña que realizamos anteriormente:

Todoslosdias,gimnasioalas8

Se transforme en algo como esto:

%9e9wo9we8qwkt8jhqw89qoqw8

¡Inténtalo con tus propias contraseñas!

Y AHORA... ¿QUÉ SIGUE?

Siguiendo los tips anteriores, podrás memorizar más fácil tus contraseñas sin sacrificar nada en términos de seguridad. Estas ideas me han servido bien por más de 10 años y confío que las encontrarás útiles en el manejo de tus credenciales.

Un último consejo: todo esto es irrelevante si el sitio o sistema que utiliza tu contraseña es inseguro. Desconfía de sitios web que no utilicen https (busca un candadito en tu barra de direcciones; a veces es color verde, pero nunca debe ser color rojo) para procesar tus datos de inicio de sesión. Desconfía más de sitios que te piden contraseñas de tamaño pequeño. Si tienes dudas, utiliza una contraseña "desechable". Sobre todo, ejerce tu sentido común. Es buen consejo para cualquier reto en la vida.

EL TAMAÑO SÍ IMPORTA

Constantemente nos indican que nuestra contraseña debe contener caracteres especiales (como símbolos), además de letras mayúsculas, minúsculas y números. Esto se conoce como la *complejidad* de la contraseña y se puede calcular fácilmente.

Pensemos como un atacante. Si queremos adivinar una contraseña por *fuerza bruta* (probando sucesivamente cada posibilidad de contraseña), primero debemos definir el *espacio* o el universo de posibilidades. Supongamos que sabemos que las contraseñas requieren letras (mayúsculas y minúsculas), números y caracteres especiales. Por lo tanto, nuestro universo se compone de:

26 (letras minúsculas)

26 (letras mayúsculas)

10 (dígitos)

10 (símbolos – aquí estoy suponiendo, cada quien podrá dar un número diferente).

Entonces, la complejidad de esta contraseña no es más que la suma de estos números: 72.

Asombrosamente, el tamaño (o *longitud* de la contraseña) es más importante que su complejidad. Si te interesan las matemáticas detrás de esto, te bastará saber que la fórmula de la "fortaleza" de una contraseña se puede definir por la siguiente expresión:

COMPLEJIDAD LONGITUD

Es fácil notar que la longitud es más importante. Consideremos dos ejemplos: una contraseña tradicional, como 'b&kqAp5H' y una frase de contraseña: 'muypequeña'. La fortaleza de la primera es 72

y la de la segunda 26^{11}. A pesar de que nuestra frase de contraseña es muy pequeña (11 caracteres) y que solo contiene letras minúsculas, su fortaleza es 5 veces superior a la contraseña tradicional. Si agregamos una sola letra a la frase, la hacemos 132 veces más fuerte a ataques de fuerza bruta. ¿Dos letras más? 3,435 veces más fuerte.

No estoy argumentado que la complejidad es inútil (después de todo, es la mitad de la fórmula). Además, es probable que al crear tu contraseña te exijan utilizar letras mayúsculas, dígitos y símbolos. Mi recomendación es que no te preocupes por hacer tu contraseña algo muy *complejo*; como has visto, te conviene más hacerla más *grande*.

---

[1] Para más información consulta el apartado *"El tamaño sí importa*" al final de este artículo.

[2] Esto no es 100% correcto: sugiero leer sobre el ataque contra el escritor de la revista electrónica Wired, Mat Honan.
