

DADOWARE: mais segurança com frases-senha

DADOWARE é um método para gerar senhas mais seguras usando lápis, papel e dados para construir frases com palavras sorteadas deste livreto.

Você pode (e deve!) usar um gerenciador de senhas¹ para criar e armazenar senhas fortes para todas as suas contas. Mas para proteger seu arquivo de senhas o ideal é usar uma *frase-senha*. Uma frase-senha é formada por várias palavras, e é bem mais longa que uma senha comum. Se composta de palavras familiares, uma frase-senha pode ser mais fácil de lembrar que um monte de caracteres estranhos. E se todas as palavras forem escolhidas de forma aleatória, será bem difícil de quebrar.

O método Diceware™ foi inventado por Arnold G. Reinhold, autor de livros sobre informática. A parte mais complicada é ter uma lista de palavras para sortear lançando 5 dados. A lista precisa ter exatamente 7.776 (6⁵) palavras familiares. No site original do Diceware² não há uma lista de palavras em português, então resolvemos criar esta, que chamamos de **DADOWARE** para ficar mais fácil de explicar.

1 https://pt.wikipedia.org/wiki/Gerenciador_de_senha

2 <http://world.std.com/~reinhold/diceware.html>

Quantas palavras deve ter uma frase-senha?

O criador do Diceware recomenda um mínimo de **6** palavras. Veja a tabela para entender como evolui a força da senha (entropia de Shannon) considerando a lista de 7.776 palavras e o número de combinações possíveis:

número de palavras	número de possibilidades (p)	entropia (log ₂ p)	caracteres base 64
5	$7.776^5 = 2,8 \times 10^{19}$	64,6	11
6	$7.776^6 = 2,2 \times 10^{23}$	77,5	13
7	$7.776^7 = 1,7 \times 10^{27}$	90,5	16
8	$7.776^8 = 1,3 \times 10^{31}$	103,4	18

A última coluna mostra o tamanho de uma senha de força equivalente gerada a partir de 64 caracteres aleatórios.

Como sortear uma frase senha







Você precisa jogar 5 dados para sortear **cada** palavra – ou pode jogar só um dado 5 vezes para cada palavra.

- Os dois primeiros dados definem a página da lista de palavras. Por exemplo: 4 1 é a página **4,1**.
- Os dados restantes definem a palavra dentro da página: 5 6 3 (**563**) é **"joelho"** (na página **4,1**).

Repita o processo para **cada** palavra da frase-senha.

Exemplo completo: frase-senha de 6 palavras

Jogue 5 dados 6 vezes, ou um dado 30 vezes, anotando os resultados de 5 em 5. Veja este exemplo completo:

dados	página	palavra
	3,4	662 galera
	1,2	464 ama
	3,2	454 excitar
	4,5	564 muito
	6,2	655 subir
	2,3	532 comício

Frase-senha resultante:

galera ama excitar muito subir comício

Procedimento mais eficiente

O mais fácil é jogar os dados e ir anotando os números em grupos de cinco, para procurar as palavras depois. No exemplo anterior, você anotaria primeiro isso:

34 662 – 12 464 – 32 454 – 45 564 – 62 655 – 23 532

E depois procuraria as palavras, anotando assim:

galera – ama – excitar – muito – subir – comício

Para memorizar, imagine uma cena com as palavras.













Devo usar acentos em frases-senhas?

Você decide. Mas nem sempre o teclado está configurado corretamente antes de fazermos login em um sistema, então é mais prático evitar acentos. No exemplo anterior, você usaria a palavra “comicio” assim, sem o acento.

E se eu precisar de maiúsculas, dígitos ou caracteres especiais?

Você pode jogar um dado para escolher uma palavra da sua frase-senha e outro dado para escolher uma letra para escrever em maiúscula dentro daquela palavra.

Para acrescentar caracteres especiais, use um dado para escolher uma palavra e mais dois dados para escolher uma linha e uma coluna da tabela abaixo:

						
	!	@	#	\$	%	&
	*	()	-	_	+
	=	{	}	[]	
	<	>	,	.	:	;
	1	2	3	4	5	6
	7	8	9	0	\	?