

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.

Se você usa senhas fracas, não adianta ter um sistema criptográfico forte. Por isso é importante usar frases-senha (*passphrases*) para tudo que você quiser proteger de verdade no mundo digital. Uma frase-senha é bem mais longa que uma senha comum: dezenas de caracteres, em vez de 10 ou menos. Mas, se for composta por palavras comuns, pode ser muito mais fácil de lembrar. E se você usar palavras escolhidas aleatoriamente, será muito 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 (6^5) palavras comuns. No site original do Diceware¹ não há uma lista de palavras em português, então resolvemos criar esta, que chamamos de **DADOWARE** para ficar mais fácil de explicar.

1 <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: 4 1 365 é **"jazida"**, na página **4,1**.

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

Exemplo completo: frase-senha de 6 palavras

Joque 5 dados 6 vezes, ou um dado 30 vezes, anotando os resultados de 5 em 5. Eis o resumo do exemplo completo:

dados	página	palavra
    	3,4	544 galera
    	1,2	464 amanhã
    	3,2	454 fabril
    	4,5	566 naipe
    	6,2	665 suspiro
    	2,3	545 comício

Frase-senha resultante:

galera amanhã fabril naipe suspiro 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:

34544 – 12464 – 32454 – 45566 – 62665 – 23545

E depois procuraria as palavras, anotando assim:

galera – amanhã – fabril – naipe – suspiro – comício













Para memorizar, imagine uma cena com as palavras.

Devo usar acentos em frases-senhas?

Nem sempre o teclado está configurado corretamente antes de fazermos login em um sistema, então é melhor evitar acentos. No exemplo anterior, você usaria as palavras “amanha” e “comicio” assim, sem os acentos.

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	\	?