SplashData: 100 legrosszabb jelszó - 2017.

PCLinuxOS Magazine - 2018. január

: Paul Arnote (parnote)

Fotó: Santeri Viinamäki, Wikimedia Commons. Creative Commons Attribution-Share Alike 4.0 International license.

2017. december 19-én a SplashData kiadta a 2017. év 100 legrosszabb jelszaváról készült listáját. Úgy tűnik, az emberek nem tanulnak, a listában sok évente visszatérő van. A SlpashData jelszókezelő szoftvereket árul és 2010. óta állítja össze a gyenge jelszavak listáját. A listát a személyes adatokban az évek során történt kiszivárogtatásokból nyilvánosságra került információk alapján állították össze.

Nos, mielőtt tovább szaporítanánk a szót, íme a lista. Az első 25 jelszó esetében a jelszó mögötti szám a 2016-os legrosszabb jelszavak listájában elfoglalt helyhez képesti pozícióváltozást jelzi. Amennyiben egy jelszó új a listán, akkor a szám helyett a „new” felirat szerepel. Hasonlóképpen, azon jelszavaknál, amik pozíciója nem változott 2016-hoz képest, a megjegyzés „unchanged”.

Ha egy általad használt jelszó szerepel a lenti listán, elgondolkodhatsz a cseréjén. Láthatóan nem voltál olyan eredeti, mint amennyire kellene.

A szerkesztő megjegyzése: néhány jelszó úgy is mondhatnánk, hogy profán, vagyis a lista nem feltétlenül tekinthető „családbarátnak”. Ugyanakkor, a teljesség és a tényszerűség érdekében a listába bekerültek. A lista ilyen szavai akkor jelennek meg, ha a sorszám mögötti szöveget kijelölik.

1. 123456 (unchanged)
2. password (unchanged)
3. 12345678 (+1)
4. qwerty (+2)
5. 12345 (-2)
6. 123456789 (New)
7. letmein (New)
8. 1234567 (unchanged)
9. football (-4)
10. iloveyou (New)
11. admin (+4)
12. welcome (unchanged)
13. monkey (New)
14. login (-3)
15. abc123 (-1)
16. starwars (New)
17. 123123 (New)
18. dragon (+1)
19. passw0rd (-1)
20. master (+1)
21. hello (New)
22. freedom (New)
23. whatever (New)
24. qazwsx (New)
25. trustno1 (New)
26. 654321
27. jordan23
28. harley
29. password1
30. 1234
31. robert
32. matthew
33. jordan
34. asshole
35. daniel
36. andrew
37. lakers
38. andrea
39. buster
40. joshua
41. 1qaz2wsx
42. 12341234
43. ferrari
44. cheese
45. computer
46. corvette
47. blahblah
48. george
49. mercedes
50. 121212
51. maverick
52. fuckyou
53. nicole
54. hunter
55. sunshine
56. tigger
57. 1989
58. merlin
59. ranger
60. solo
61. banana
62. chelsea
63. summer
64. 1990
65. 1991
66. phoenix
67. amanda
68. cookie
69. ashley

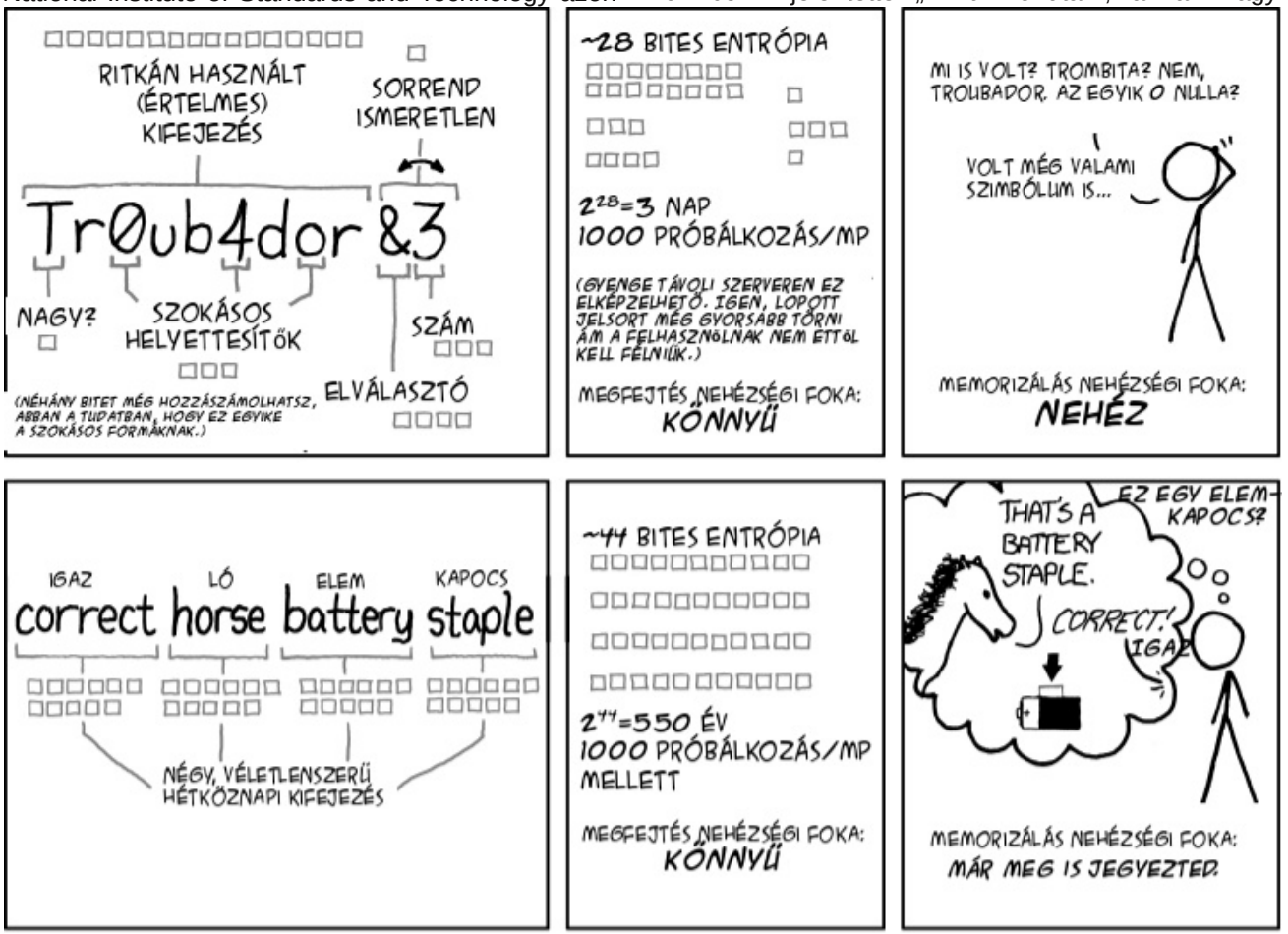
70. bandit
71. killer
72. aaaaaa
73. pepper
74. jessica
75. zaq1zaq1
76. jennifer
77. test
78. hockey
79. dallas
80. passwor
81. michelle
82. admin123
83. pussy
84. pass
85. asdf
86. william
87. soccer
88. london
89. 1q2w3e
90. 1992
91. biteme
92. maggie
93. querty
94. rangers
95. charlie
96. martin
97. ginger
98. golfer
99. yankees
100. thunder

Természetesen a visszatérő jelszavak továbbra is vezetik a listát, egy ideje már ott vannak. Mind az „123456”, mind a „password” a lista tetején, vagy annak közelében van, amióta készül a lista. A sporthoz kapcsolódó jelszavak („soccer”, vagy „football”), vagy a kedvenc csapatok („lakers”, „rangers”, vagy „yankees”) népszerűek maradtak. Idén, feltehetően egy teljesen új starwars rajongó generációnak bemutatott új Star Wars filmek hatására a „starwars” mint jelszó betört az első 20 legrosszabb jelszó közé. A „rage against the machine” jelenléte evidens az olyan jelszavakkal, mint „letmein” és „biteme”. A politikai vonal előretörése egyértelmű az olyan jelszavakkal mint „trustno1” és „freedom”. Továbbra is népszerűek az olyan billentyűkombinációk, mint az „1qaz2wsx” és a „qwerty” jelszavak.

A legjobb eljárás: mitől jó egy jelszó

Az elmúlt években úgy gondoltuk, hogy ezt könnyű megválaszolni. Ám, 2017 augusztusában Bill Burr a jelszavak világát ismét felforgatta. Bill Burr volt a National Institute of Standards and Technology azon alkalmazottja, aki 2003-ban kiadott egy jelentést, amellett síkra szállva, hogy a hacker-ek kizárása, félrevezetése érdekében speciális karaktereket, kis- és nagybetűket, illetve számokat vegyesen használjunk a jelszavakban. Írása gyakorlatilag azonnal jelszópolitikává lépett elő. Kimondta a VÉGSŐ SZÓT a jelszavakkal kapcsolatban. (Az erre vonatkozó USA Today cikket itt olvashatod el.)

Ám augusztusban Bill Burr egy Wall Stree Journal cikkben kijelentette „Amit mondtam, annak nagy



részét visszavonom.” A jelentése nem a való világ jelszavain, vagy gyakorlatán alapult. Sokkal inkább egy másik, 1980-ban kelt cikk inspirálta. Ám időközben a jelentés vált A szentírássá.

Bill Burr most azt javasolja, hogy felhasználók vonjanak össze négy véletlenszerű egyszerű szót ahelyett, hogy a szokásos kis-, nagybetűs, számos és különleges írásjelű keveréket használnának. Az itt látható XKCD képregény szépen összefoglalja miért és hogy lesz ez jobb.

De ne várd azt, hogy weblapok és más egyebek ugranak az új felfedezésre, mivel sok közülük továbbra is a „szabványos” keveréket várja, amit a 2003-as jelentés tett a jelszó szentírásává. Azok az „ajánlások” stabilan bebábozódtak a jelszavak világába akár egy „vallás” alapelvei. Végeredményben, 20 év kellett ahhoz, hogy ide eljussunk, és valószínűleg kétszer ennyi idő (vagy több) kell a hibás elképzelések elfelejtéséhez annak ellenére, hogy van jobb út. Oly sok rossz ötletnek sok időbe telik, mire elfelejtik.

Mindazonáltal látható, hogy sok felhasználó lusta a jelszavakkal. Ez egyértelmű a 2017. évi Legrosszabb Jelszavak Listájából. Nos, vannak módszerek magunk védelmére erős jelszavakkal. A tény tény marad, hogy nincs feltörhetetlen jelszó, ha van elég idő. Ám a cél az, hogy feltörés szempontjából elég bonyolult legyen, amitől a hekkerek egyszerűen feladják és továbblépnek a következő szerencsétlenre, békén hagyva az adataidat. Ki tudja? Lehet, hogy a következő szerencsétlen jelszava rajta van a legrosszabb jelszavak listáján.

Használj jelszókezelőt. Hogy melyik legyen függ attól, hogy megbízol-e a felhőben, vagy sem, illetve milyen kényelmi szintet keresel. Ha egyazon jelszókezelőt akarsz használni több eszközön (ki az aki manapság nem használ több eszközt), akkor felhő alapú megoldásra van szükséged. Talán a LastPass a csúcs, ami egy webböngésző bővítmény. Emlékezni fog az összes jelszavadra azoknál a weblapoknál, amelyek kérnek és segít véletlenszerű biztonságos jelszót generálni az új weblapok számára. Csak a „mester” jelszóra kell emlékezned. Ne légy amnéziás, mert még a LastPass emberei sem képesek visszafejteni a jelszavaidat, ha elfelejted a „mester” jelszót. Nagy valószínűséggel, még a „mester” jelszavad BIRTOKÁBAN sem képesek, vagy tudják visszanyerni a jelszavaidat.

Ha helyi, nem felhő alapú megoldást szeretnél inkább, telepítheted a KeeppassX-et, ami a PCLinuxOS tárolójában is megtalálható. Nagyon hasonlít a működése a LastPass-éhoz, felhő nélkül. A jelszavaid a merevlemezeden, titkosított fájlban lesznek mentve.

Vannak más jelszókezelők is a piacon. Ha valamelyik nem feltétlenül felel meg az elvárásaidnak, próbálj ki egy másikat. Csak arra vigyázz, kibe helyezed a bizalmadat.

Ne használd ugyanazt a jelszót több weblapon. Ennek magától értetődőnek kellene lennie, de mindig előfordul szerte a világban. Először is, az emberek a szokásaik rabjai. Másodszor, sokkal „egyszerűbb” egy, vagy két jelszót megjegyezni, amit a web egészén használsz. Természetesen könnyebb neked, és könnyebb hozzáférni a személyes adataidhoz is – a hekkereknek (ha ezt el kell magyaráznom neked, akkor te egyáltalán nem törődsz az adataid biztonságával). Ha egy hekker megszerzi egy jelszavadat, megpróbálja majd használni másik oldalon is. Minden oldalon egyedi jelszavad legyen (ami még kedvesebbé és kívánatosabbá teszi a fent említett jelszókezelőket).

Kerüld a popkultúrát és a személyes „kincstárat”. A popkultúra szavai, mint a kedvenc sport, csapat, film, filmszereplő, színész stb. mindig népszerű választások, amikor olyan jelszót keresnek, ami a személyes ízlést és „belsőt” tükrözi vissza. Kerüld ezeket, mert valószínűleg nem te vagy az egyetlen kedvelője, aki az adott popkultúra szavát vagy kifejezését választja. Ha csak te vagy, akkor az nem pop kultúra.

Hasonlóképpen kerüld a személyes „kincstárat”. Ez azt jelenti, hogy kerüld a születési, házassági és évfordulós dátumokat, gyerekek, házi kedvencek, kedvenc ételek neveit és minden egyebet, ami köztudott, vagy könnyen kideríthető rólad.

Összegzés

Úgy tűnik, hogy adatszivárgások egyre gyakrabban fordulnak elő. Valójában, az adatszivárgások túlságosan is általánossá váltak. Érthető, mivel a TE személyes adataid kívánatos valuta a hekkerek és a gátlástalan emberek számára csakúgy, mint a világ különböző kormányainak. A legismertebb vállalatok között, amelyeknél adatszivárgás történt 2017-ben, szerepel a Verizon, a Saks Fith Avenue, a Deloitte és az Uber. Ne felejtkezzünk el a hatalmas Equifax adatszivárgásról, ami emberek millióinak adatait fedte fel. Az adatszivárgási statisztikák nem tartalmazzák a Yahoo!-nak nevezett évente visszatérő szivárgást és a felnőtt oldalakat.

TE vagy az egyetlen személy, akit valóban érdekel az adataid védelme. Bármennyire is meg akarnak győzni az ellenkezőjéről, a cégek ténylegesen teljes mértékben csak a részvényeseik iránti lojálisak. A személyes adataid védelme tőled indul – és így is történik – és VELED ér véget. Ha nem törődsz a jelszavaiddal (gyenge, hatástalan, mindenfelé használt jelszó) azt fogod kapni, amit megérdemelsz. Valószínűleg nem fog tetszeni, amit eredményeképpen begyűjtesz.