

Record of Important Things

If found, please return to:

Simply, people can no longer remember passwords good enough to reliably defend against dictionary attacks, and are much more secure if they choose a password too complicated to remember and then write it down. We're all good at securing small pieces of paper. I recommend that people write their passwords down on a small piece of paper, and keep it with their other valuable small pieces of paper: in their wallet.

Bruce Schneier

Authentication credentials

1. 9.

2. 10.

3. 11.

4. 12.

5. 13.

6. 14.

7. 15.

8. 16.

17. Secure passphrases with Diceware

24. Security questions

1

Web site

Login or E-mail address

Passwords used

Date

Notes

Web site

Login or E-mail address

Passwords used

Date

Notes

Web site

Login or E-mail address

Passwords used

Date

Notes

Web site

Login or E-mail address

Passwords used

Date

Notes

Web site

Login or E-mail address

Passwords used

Date

Notes

Web site

Login or E-mail address

Passwords used

Date

Notes

Web site

Login or E-mail address

Passwords used

Date

Notes

Web site

Login or E-mail address

Passwords used

Date

Notes

Web site

Login or E-mail address

Passwords used

Date

Notes

Web site

Login or E-mail address

Passwords used

Date

Notes

Web site

Login or E-mail address

Passwords used

Date

Notes

Web site

Login or E-mail address

Passwords used

Date

Notes

Web site

Login or E-mail address

Passwords used

Date

Notes

Web site

Login or E-mail address

Passwords used

Date

Notes

Web site

Login or E-mail address

Passwords used

Date

Notes

Web site

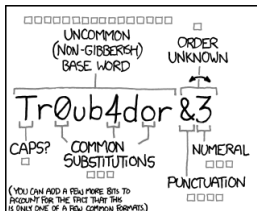
Login or E-mail address

Passwords used

Date

Notes

Secure passphrases with Diceware



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

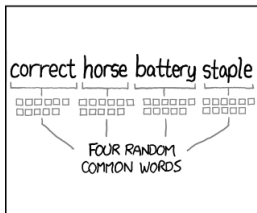
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CRACKING A STOLEN MATH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O's WAS A ZERO?

AND THERE WAS SOME SYMBOL....

DIFFICULTY TO REMEMBER: HARD



~44 BITS OF ENTROPY

$2^{44} = 530 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: HARD

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

What is a Diceware passphrase?

A passphrase is a bunch of words and characters that you type into your computer to let it know for sure that *the person typing is you*. Passphrases differ from passwords only in length.

Diceware is a method for picking passphrases which uses dice to select words at random from a special list. Each word in the list is preceded by a four digit number. All the digits are between one and six, allowing you to use the outcomes of four dice rolls to select a word from the list.

Directions

- 1 Decide how many words you want in your passphrase. A five-word passphrase provides a level of security *much* higher than the passwords most people use. For NSA-proof security, use seven words.
- 2 Roll all four dice at once and write the results down, reading from left to right, on a scrap of paper. Make as many of these four-digit groups as you want words in your passphrase.
- 3 Flip to the word list and look up the corresponding word next to each four-digit number.
- 4 The words you have found are your new passphrase!
- 5 Come up with a way to remember your phrase. It might be a story, mental picture, or sentence that will remind you of the phrase you generated.

Example

Suppose you want a five-word passphrase. You will need 5×4 or 20 dice rolls. Let's say they come out as:

1, 6, 6, 6, 5, 1, 5, 6, 5, 3, 5, 6, 3, 2, 2, 3, 5, 6, 2, 6.

Write the results on a scrap of paper in groups of four:

1 6 6 6

5 1 5 6

5 3 5 6

3 2 2 3

5 6 2 6

You then look up each group of five rolls in the Diceware word list by finding the number in the list and writing down the word next to the number:

1666 cognitive

5156 poetic

5356 ribbon

3223 garlic

5626 smelliness

Your passphrase would then be:

cognitive poetic ribbon garlic smelliness

This passphrase is one of the 3,656,158,440,062,976 (6^{20}) alternatives that could have been chosen by this method.

- 1111 aardvark
 1112 abandoned
 1113 abbreviate
 1114 abdomen
 1115 abhorrence
 1116 abiding
 1121 abnormal
 1122 abrasion
 1123 absorbing
 1124 abundant
 1125 abyss
 1126 academy
 1131 accountant
 1132 acetone
 1133 achiness
 1134 acid
 1135 acoustics
 1136 acquire
 1141 acrobat
 1142 actress
 1143 acuteness
 1144 aerosol
 1145 aesthetic
 1146 affidavit
 1151 afloat
 1152 afraid
 1153 aftershave
 1154 again
 1155 agency
 1156 aggressor
 1161 aghast
 1162 agitate
 1163 agnostic
 1164 agonizing
 1165 agreeing
 1166 aidless
 1211 aimlessly
 1212 ajar
 1213 alarmclock
 1214 albatross
 1215 alchemy
 1216 alfalfa
 1221 algae
 1222 aliens
 1223 alkaline
 1224 almanac
 1225 alongside
 1226 alphabet
 1231 already
 1232 also
 1233 altitude
 1234 aluminum
 1235 always
 1236 amazingly
 1241 ambulance
 1242 amendment
 1243 amiable
 1244 ammunition
 1245 amnesty
 1246 amoeba
 1251 amplifier
 1252 amuser
 1253 anagram
 1254 anchor
 1255 android
 1256 anesthesia
 1261 angelfish
 1262 animal
 1263 anklet
 1264 announcer
 1265 anonymous
 1266 answer
 1311 antelope
 1312 anxiety
 1313 anyplace
 1314 aorta
 1315 apartment
 1316 apnea
 1321 apostrophe
 1322 apple
 1323 apricot
 1324 aquamarine
 1325 arachnid
 1326 arbitrate
 1331 ardently
 1332 arena
 1333 argument
 1334 aristocrat
 1335 armchair
 1336 aromatic
 1341 arrowhead
 1342 arsonist
 1343 artichoke
 1344 asbestos
 1345 ascend
 1346 aseptic
 1351 ashamed
 1352 asinine
 1353 asleep
 1354 asocial
 1355 asparagus
 1356 astronaut
 1361 asymmetric
 1362 atlas
 1363 atmosphere
 1364 atom
 1365 atrocious
 1366 attic
 1411 atypical
 1412 auctioneer
 1413 auditorium
 1414 augmented
 1415 auspicious
 1416 automobile
 1421 auxiliary
 1422 avalanche
 1423 avenue
 1424 aviator
 1425 avocado
 1426 awareness
 1431 awhile
 1432 awkward
 1433 awning
 1434 awoke
 1435 axially
 1436 azalea
 1441 babbling
 1442 backpack
 1443 badass
 1444 bagpipe
 1445 bakery
 1446 balancing
 1451 bamboo
 1452 banana
 1453 barracuda
 1454 basket
 1455 bathrobe
 1456 bathzooka
 1461 blade
 1462 blender
 1463 blimp
 1464 blouse
 1465 blurred
 1466 boathyard
 1511 bobcat
 1512 body
 1513 bogusness
 1514 bohemian
 1515 boiler
 1516 bonnet
 1521 boots
 1522 borough
 1523 bossiness
 1524 bottle
 1525 bouquet
 1526 boxlike
 1531 breath
 1532 briefcase
 1533 broom
 1534 brushes
 1535 bubblegum
 1536 buckle
 1541 buddhist
 1542 buffalo
 1543 bullfrog
 1544 bunny
 1545 busboy
 1546 buzzard
 1551 cabin
 1552 cactus
 1553 cadillac
 1554 cafeteria
 1555 cage
 1556 cahoots
 1561 cajoling
 1562 cakewalk
 1563 calculator
 1564 camera
 1565 canister
 1566 capsule
 1611 carrot
 1612 cashew
 1613 cathedral
 1614 caucasian
 1615 caviar
 1616 ceasefire
 1621 cedar
 1622 celery
 1623 cement
 1624 census
 1625 ceramics
 1626 cesspool
 1631 chalkboard
 1632 cheesecake
 1633 chimney
 1634 chlorine
 1635 chopsticks
 1636 chrome
 1641 chute
 1642 cilantro
 1643 cinnamon
 1644 circle
 1645 cityscape
 1646 civilian
 1651 clay
 1652 clergyman
 1653 clipboard
 1654 clock
 1655 clubhouse
 1656 coathanger
 1661 cobweb
 1662 coconut
 1663 codeword
 1664 coexistent
 1665 coffee cake
 1666 cognitive
 2111 cohabitate
 2112 collarbone
 2113 computer
 2114 confetti
 2115 copier
 2116 cornea
 2121 cosmetics
 2122 cotton
 2123 couch
 2124 coverless
 2125 coyote
 2126 coziness
 2131 crawfish
 2132 crewmember
 2133 crib
 2134 croissant
 2135 crumble
 2136 crystal
 2141 cubical
 2142 cucumber
 2143 cuddly
 2144 cufflink
 2145 cuisine
 2146 culprits
 2151 cup
 2152 curry
 2153 cushion
 2154 cuticle
 2155 cybernetic
 2156 cyclist
 2161 cylinder
 2162 cymbal
 2163 cynicism
 2164 cypress
 2165 cytoplasm
 2166 dachshund
 2211 daffodil
 2212 dagger
 2213 dairy
 2214 dalmatian
 2215 dandelion
 2216 dartboard
 2221 dastardly
 2222 datebook
 2223 debugger
 2224 dawn
 2225 daytime
 2226 dazzler
 2231 dealer
 2232 debris
 2233 decal
 2234 dedicate
 2235 deepness
 2236 defrost
 2241 degree
 2242 dehydrator
 2243 deliverer
 2244 democrat
 2245 dentist
 2246 deodorant
 2251 depot
 2252 deranged
 2253 desktop
 2254 detergent
 2255 device
 2256 dexterity
 2261 diamond
 2262 dibs
 2263 dictionary
 2264 diffuser
 2265 digit
 2266 dilated
 2311 dimple
 2312 dinnerware
 2313 dioxide
 2314 diploma
 2315 directory
 2316 dishcloth
 2321 ditto
 2322 dividers
 2323 dizziness
 2324 doctor
 2325 dodge
 2326 doll
 2331 dominoes
 2332 donut
 2333 doorstep
 2334 dorsal
 2335 double
 2336 downstairs
 2341 dozed
 2342 drainpipe
 2343 dresser
 2344 driftwood
 2345 droppings
 2346 drum
 2351 dryer
 2352 dubiously
 2353 duckling
 2354 duffel
 2355 dugout
 2356 dumpster
 2361 duplex
 2362 durable
 2363 dustpan
 2364 dutiful
 2365 duvet
 2366 dwarfism

2411 dwelling	2624 evacuation	3241 gesture	3454 hygienist
2412 dwindling	2625 evergreen	3242 getaway	3455 hypnotist
2413 dynamite	2626 evidence	3243 geyser	3456 ibuprofen
2414 dyslexia	2631 evolution	3244 ghoulishly	3461 icepack
2415 eagerness	2632 exam	3245 gibberish	3462 icing
2416 earlobe	2633 excerpt	3246 giddiness	3463 iconic
2421 easel	2634 exerciser	3251 giftshop	3464 identical
2422 eavesdrop	2635 exfoliate	3252 gigabyte	3465 idiocy
2423 ebook	2636 exhale	3253 gimmick	3466 idly
2424 eccentric	2641 exist	3254 giraffe	3511 igloo
2425 echoless	2642 exorcist	3255 giveaway	3512 ignition
2426 eclipse	2643 explode	3256 gizmo	3513 iguana
2431 ecosystem	2644 exquisite	3261 glasses	3514 illuminate
2432 ecstasy	2645 exterior	3262 gleeful	3515 imaging
2433 edged	2646 exuberant	3263 glisten	3516 imbecile
2434 editor	2651 fabric	3264 glove	3521 imitator
2435 educator	2652 factory	3265 glucose	3522 immigrant
2436 eelworm	2653 faded	3266 glycerin	3523 imprint
2441 eerie	2654 failsafe	3311 gnarly	3524 iodine
2442 effects	2655 falcon	3312 gnomish	3525 ionosphere
2443 egg nog	2656 family	3313 goatskin	3526 ipad
2444 egomaniac	2661 fanfare	3314 goggles	3531 iphone
2445 ejection	2662 fasten	3315 goldfish	3532 iridescent
2446 elastic	2663 faucet	3316 gong	3533 irksome
2451 elbow	2664 favorite	3321 goody	3534 iron
2452 elderly	2665 feasibly	3322 gorgeous	3535 irrigation
2453 elephant	2666 february	3323 gosling	3536 island
2454 elfishly	3111 federal	3324 gothic	3541 isotope
2455 eliminator	3112 feedback	3325 gourmet	3542 issueless
2456 elk	3113 feigned	3326 governor	3543 italicize
2461 elliptical	3114 feline	3331 grape	3544 itemizer
2462 elongated	3115 femur	3332 greyhound	3545 itinerary
2463 elsewhere	3116 fence	3333 grill	3546 itunes
2464 elusive	3121 ferret	3334 groundhog	3551 ivory
2465 elves	3122 festival	3335 grumbling	3552 jabbering
2466 emancipate	3123 fettuccine	3336 guacamole	3553 jackrabbit
2511 embroidery	3124 feudalist	3341 guerrilla	3554 jaguar
2512 emcee	3125 feverish	3342 guitar	3555 jailhouse
2513 emerald	3126 fiberglass	3343 gullible	3556 jalapeno
2514 emission	3131 fictitious	3344 gumdrop	3561 jamboree
2515 emoticon	3132 fiddle	3345 gurgling	3562 janitor
2516 emperor	3133 figurine	3346 gusto	3563 jarring
2521 emulate	3134 fillet	3351 gutless	3564 jasmine
2522 enactment	3135 finalist	3352 gymnast	3565 jaundice
2523 enchilada	3136 fiscally	3353 gynecology	3566 jawbreaker
2524 endorphin	3141 fixture	3354 gyration	3611 jaywalker
2525 energy	3142 flashlight	3355 habitat	3612 jazz
2526 enforcer	3143 fleshiness	3356 hacking	3613 jealous
2531 engine	3144 flight	3361 haggard	3614 jeep
2532 enhance	3145 florist	3362 haiku	3615 jelly
2533 enigmatic	3146 flypaper	3363 halogen	3616 jeopardize
2534 enjoyably	3151 foamless	3364 hamburger	3621 jersey
2535 enlarged	3152 focus	3365 handgun	3622 jetski
2536 enormous	3153 foggy	3366 happiness	3623 jezebel
2541 enquirer	3154 folksong	3411 hardhat	3624 jiffy
2542 enrollment	3155 fondue	3412 hastily	3625 jigsaw
2543 ensemble	3156 footpath	3413 hatching	3626 jingling
2544 entryway	3161 fossil	3414 haughty	3631 jobholder
2545 enunciate	3162 fountain	3415 hazelnut	3632 jockstrap
2546 envoy	3163 fox	3416 headband	3633 joggling
2551 enzyme	3164 fragment	3421 hedgehog	3634 john
2552 epidemic	3165 freeway	3422 hefty	3635 joinable
2553 equipment	3166 fridge	3423 heinously	3636 jokingly
2554 erasable	3211 frosting	3424 helmet	3641 journal
2555 ergonomic	3212 fruit	3425 hemoglobin	3642 jovial
2556 erratic	3213 fryingpan	3426 henceforth	3643 joystick
2561 eruption	3214 gadget	3431 herbs	3644 jubilant
2562 escalator	3215 gainfully	3432 hesitation	3645 judiciary
2563 eskimo	3216 gallstone	3433 hexagon	3646 juggle
2564 esophagus	3221 gamekeeper	3434 hubcap	3651 juice
2565 espresso	3222 gangway	3435 huddling	3652 jujitsu
2566 essay	3223 garlic	3436 huff	3653 jukebox
2611 estrogen	3224 gaslight	3441 hugeness	3654 jumpiness
2612 etching	3225 gathering	3442 hullabaloo	3655 junkyard
2613 eternal	3226 gauntlet	3443 human	3656 juror
2614 ethics	3231 gearbox	3444 hunter	3661 justifying
2615 etiquette	3232 gecko	3445 hurricane	3662 juvenile
2616 eucalyptus	3233 gem	3446 hushing	3663 kabob
2621 eulogy	3234 generator	3451 hyacinth	3664 kamikaze
2622 euphemism	3235 geographer	3452 hybrid	3665 kangaroo
2623 euthanize	3236 gerbil	3453 hydrant	3666 karate

4111 kayak	4324 mammal	4541 obliterate	5154 pneumonia
4112 keepsake	4325 mango	4542 obnoxious	5155 podiatrist
4113 kennel	4326 mapmaker	4543 observer	5156 poetic
4114 kerosene	4331 marbles	4544 obtain	5161 pogo
4115 ketchup	4332 massager	4545 obvious	5162 poison
4116 khaki	4333 matchstick	4546 occupation	5163 poking
4121 kickstand	4334 maverick	4551 oceanic	5164 policeman
4122 kilogram	4335 maximum	4552 octopus	5165 poncho
4123 kimono	4336 mayonnaise	4553 ocular	5166 popcorn
4124 kingdom	4341 moaning	4554 office	5211 porcupine
4125 kiosk	4342 mobilize	4555 oftentimes	5212 postcard
4126 kissing	4343 moccasin	4556 oiliness	5213 poultry
4131 kite	4344 modify	4561 ointment	5214 powerboat
4132 kleenex	4345 moisture	4562 older	5215 prairie
4133 knapsack	4346 molecule	4563 olympics	5216 pretzel
4134 kneecap	4351 momentum	4564 omissible	5221 princess
4135 knickers	4352 monastery	4565 omnivorous	5222 propeller
4136 koala	4353 moonshine	4566 oncoming	5223 prune
4141 krypton	4354 mortuary	4611 onion	5224 pry
4142 laboratory	4355 mosquito	4612 onlooker	5225 pseudo
4143 ladder	4356 motorcycle	4613 onstage	5226 psychopath
4144 lakefront	4361 mousetrap	4614 onward	5231 publisher
4145 lantern	4362 movie	4615 onyx	5232 pucker
4146 laptop	4363 mower	4616 oomph	5233 pueblo
4151 laryngitis	4364 mozzarella	4621 opaquely	5234 pulley
4152 lasagna	4365 muckiness	4622 opera	5235 pumpkin
4153 latch	4366 mudflow	4623 opium	5236 punchbowl
4154 laundry	4411 mugshot	4624 opossum	5241 puppy
4155 lavender	4412 mule	4625 opponent	5242 purse
4156 laxative	4413 mummy	4626 optical	5243 pushup
4161 lazybones	4414 mundane	4631 opulently	5244 putt
4162 lecturer	4415 muppet	4632 oscillator	5245 puzzle
4163 leftover	4416 mural	4633 osmosis	5246 pyramid
4164 leggings	4421 mustard	4634 ostrich	5251 python
4165 leisure	4422 mutation	4635 otherwise	5252 quarters
4166 lemon	4423 myriad	4636 ought	5253 quesadilla
4211 length	4424 myspace	4641 outhouse	5254 quilt
4212 leopard	4425 myth	4642 ovation	5255 quote
4213 leprechaun	4426 nail	4643 oven	5256 racoon
4214 lettuce	4431 namesake	4644 owlsh	5261 radish
4215 leukemia	4432 nanosecond	4645 oxford	5262 ragweed
4216 levers	4433 napkin	4646 oxidize	5263 railroad
4221 lewdness	4434 narrator	4651 oxygen	5264 rampantly
4222 liability	4435 nastiness	4652 oyster	5265 rancidity
4223 library	4436 natives	4653 ozone	5266 rarity
4224 licorice	4441 nautically	4654 pacemaker	5311 raspberry
4225 lifeboat	4442 navigate	4655 padlock	5312 ravishing
4226 lightbulb	4443 nearest	4656 pageant	5313 rearrange
4231 likewise	4444 nebula	4661 pajamas	5314 rebuilt
4232 lilac	4445 nectar	4662 palm	5315 receipt
4233 limousine	4446 nefarious	4663 pamphlet	5316 reentry
4234 lint	4451 negotiator	4664 pantyhose	5321 refinery
4235 lioness	4452 neither	4665 paprika	5322 register
4236 lipstick	4453 nemesis	4666 parakeet	5323 rehydrate
4241 liquid	4454 neoliberal	5111 passport	5324 reimburse
4242 listless	4455 nephew	5112 patio	5325 rejoicing
4243 litter	4456 nervously	5113 pauper	5326 rekindle
4244 liverwurst	4461 nest	5114 pavement	5331 relic
4245 lizard	4462 netting	5115 payphone	5332 remote
4246 llama	4463 neuron	5116 pebble	5333 renovator
4251 luau	4464 nevermore	5121 peculiarly	5334 reopen
4252 lubricant	4465 nextdoor	5122 pedometer	5335 reporter
4253 lucidity	4466 nicotine	5123 pegboard	5336 request
4254 ludicrous	4511 niece	5124 pelican	5341 rerun
4255 luggage	4512 nimbleness	5125 penguin	5342 reservoir
4256 lukewarm	4513 nintendo	5126 peony	5343 retriever
4261 lullaby	4514 nirvana	5131 pepperoni	5344 reunion
4262 lumberjack	4515 nuclear	5132 peroxide	5345 revolver
4263 lunchbox	4516 nugget	5133 pesticide	5346 rewrite
4264 luridness	4521 nuisance	5134 petroleum	5351 rhapsody
4265 luscious	4522 nullify	5135 pewter	5352 rhetoric
4266 luxurious	4523 numbing	5136 pharmacy	5353 rhino
4311 lyrics	4524 nuptials	5141 pheasant	5354 rhubarb
4312 macaroni	4525 nursery	5142 phonebook	5355 rhyme
4313 maestro	4526 nutcracker	5143 phrasing	5356 ribbon
4314 magazine	4531 nylon	5144 physician	5361 riches
4315 mahogany	4532 oasis	5145 plank	5362 ridden
4316 maimed	4533 oat	5146 pledge	5363 rigidity
4321 majority	4534 obediently	5151 plotted	5364 rimmed
4322 makeover	4535 obituary	5152 plug	5365 riptide
4323 malformed	4536 object	5153 plywood	5366 riskyly

- 5411 ritzy
 5412 riverboat
 5413 roamer
 5414 robe
 5415 rocket
 5416 romancer
 5421 ropelike
 5422 rotisserie
 5423 roundtable
 5424 royal
 5425 rubber
 5426 rudderless
 5431 rugby
 5432 ruined
 5433 rulebook
 5434 rummage
 5435 running
 5436 rupture
 5441 rustproof
 5442 sabotage
 5443 sacrifice
 5444 saddlebag
 5445 saffron
 5446 sainthood
 5451 saltshaker
 5452 samurai
 5453 sandworm
 5454 sapphire
 5455 sardine
 5456 sassy
 5461 satchel
 5462 sauna
 5463 savage
 5464 saxophone
 5465 scarf
 5466 scenario
 5511 schoolbook
 5512 scientist
 5513 scooter
 5514 scrapbook
 5515 sculpture
 5516 scythe
 5521 secretary
 5522 sedative
 5523 segregator
 5524 seismology
 5525 selected
 5526 semicolon
 5531 senator
 5532 septum
 5533 sequence
 5534 serpent
 5535 sesame
 5536 settler
 5541 severely
 5542 shack
 5543 shelf
 5544 shirt
 5545 shovel
 5546 shrimp
 5551 shuttle
 5552 shyness
 5553 siamese
 5554 sibling
 5555 siesta
 5556 silicon
 5561 simmering
 5562 singles
 5563 sisterhood
 5564 sitcom
 5565 sixfold
 5566 sizable
 5611 skateboard
 5612 skeleton
 5613 skies
 5614 skulk
 5615 skylight
 5616 slapping
 5621 sled
 5622 slingshot
 5623 sloth
 5624 slumbering
 5625 smartphone
 5626 smelliness
 5631 smitten
 5632 smokestack
 5633 smudge
 5634 snapshot
 5635 sneezing
 5636 sniff
 5641 snowsuit
 5642 snugness
 5643 speakers
 5644 sphinx
 5645 spider
 5646 splashing
 5651 sponge
 5652 sprout
 5653 spur
 5654 spyglass
 5655 squirrel
 5656 statue
 5661 steamboat
 5662 stingray
 5663 stopwatch
 5664 strawberry
 5665 student
 5666 stylus
 6111 suave
 6112 subway
 6113 suction
 6114 suds
 6115 suffocate
 6116 sugar
 6121 suitcase
 6122 sulphur
 6123 superstore
 6124 surfer
 6125 sushi
 6126 swan
 6131 sweatshirt
 6132 swimwear
 6133 sword
 6134 sycamore
 6135 syllable
 6136 symphony
 6141 synagogue
 6142 syringes
 6143 systemize
 6144 tablespoon
 6145 taco
 6146 tadpole
 6151 taekwondo
 6152 tagalong
 6153 takeout
 6154 tallness
 6155 tamale
 6156 tanned
 6161 tapestry
 6162 tarantula
 6163 tastebud
 6164 tattoo
 6165 tavern
 6166 thaw
 6211 theater
 6212 thimble
 6213 thorn
 6214 throat
 6215 thumb
 6216 thwarting
 6221 tiara
 6222 tidbit
 6223 tiebreaker
 6224 tiger
 6225 timid
 6226 tinsel
 6231 tiptoeing
 6232 tirade
 6233 tissue
 6234 tractor
 6235 tree
 6236 tripod
 6241 trousers
 6242 trucks
 6243 tryout
 6244 tubeless
 6245 tuesday
 6246 tugboat
 6251 tulip
 6252 tumbleweed
 6253 tupperware
 6254 turtle
 6255 tusk
 6256 tutorial
 6261 tuxedo
 6262 tweezers
 6263 twins
 6264 tyrannical
 6265 ultrasound
 6266 umbrella
 6311 umpire
 6312 unarmored
 6313 unbuttoned
 6314 uncle
 6315 underwear
 6316 unevenness
 6321 unflavored
 6322 ungloved
 6323 unhinge
 6324 unicycle
 6325 unjustly
 6326 unknown
 6331 unlocking
 6332 unmarked
 6333 unnoticed
 6334 unopened
 6335 unpaved
 6336 unquenched
 6341 unroll
 6342 unscrewing
 6343 untied
 6344 unusual
 6345 unveiled
 6346 unwrinkled
 6351 unyielding
 6352 unzip
 6353 upbeat
 6354 upcountry
 6355 update
 6356 upfront
 6361 upgrade
 6362 upholstery
 6363 upkeep
 6364 upload
 6365 uppercut
 6366 upright
 6411 upstairs
 6412 uptown
 6413 upwind
 6414 uranium
 6415 urban
 6416 urchin
 6421 urethane
 6422 urgent
 6423 urologist
 6424 username
 6425 usher
 6426 utensil
 6431 utility
 6432 utmost
 6433 utopia
 6434 utterance
 6435 vacuum
 6436 vagrancy
 6441 valuables
 6442 vanquished
 6443 vaporizer
 6444 varied
 6445 vaseline
 6446 vegetable
 6451 vehicle
 6452 velcro
 6453 vendor
 6454 vertebrate
 6455 vestibule
 6456 veteran
 6461 vexingly
 6462 vicinity
 6463 videogame
 6464 viewfinder
 6465 vigilante
 6466 village
 6511 vinegar
 6512 violet
 6513 viperfish
 6514 virus
 6515 visor
 6516 vitamins
 6521 vivacious
 6522 vixen
 6523 vocalist
 6524 vogue
 6525 voicemail
 6526 volleyball
 6531 voucher
 6532 voyage
 6533 vulnerable
 6534 waffle
 6535 wagon
 6536 wakeup
 6541 walrus
 6542 wanderer
 6543 wasp
 6544 water
 6545 waving
 6546 wheat
 6551 whisper
 6552 wholesaler
 6553 wick
 6554 widow
 6555 welder
 6556 wifeless
 6561 wikipedia
 6562 wildcat
 6563 windmill
 6564 wipeout
 6565 wired
 6566 wishbone
 6611 wizardry
 6612 wobbliness
 6613 wolverine
 6614 womb
 6615 woolworker
 6616 workbasket
 6621 wound
 6622 wrangle
 6623 wreckage
 6624 wristwatch
 6625 wrongdoing
 6626 xerox
 6631 xylophone
 6632 yacht
 6633 yahoo
 6634 yard
 6635 yearbook
 6636 yesterday
 6641 yiddish
 6642 yield
 6643 yoyo
 6644 yodel
 6645 yogurt
 6646 yuppie
 6651 zealot
 6652 zebra
 6653 zepplin
 6654 zestfully
 6655 zigzagged
 6656 zillion
 6661 zipping
 6662 zirconium
 6663 zodiac
 6664 zombie
 6665 zookeeper
 6666 zucchini

Security questions

Shouldn't I never write my password down?

In today's world, major corporations are hacked every week, and distributed cracking networks can break complex passwords in record time. It's safest to use a strong, unique password for each account you hold, but this makes memorization impractical.

Once, people were told not to write passwords down, ever, but the consensus among security professionals has evolved. You're better at protecting this book than corporations are at securing their password databases.

Can I just pick my own words from the list?

No. Humans are terrible at being unpredictable, and hackers are great at exploiting predictability. The primary reason that Diceware creates secure passwords is that you have no agency in the process.

Should I leave spaces between the words?

Yes. It makes your passphrase more secure, and easier to type.

How many words should I use in my passphrase?

The most important accounts, such as email, e-commerce and financial sites, should use at least five words.

Encrypted drives storing sensitive personal and financial documents should use seven words.

Less critical accounts, like social media, can use three words provided the passwords are unique.

My passphrase was rejected because it is too long, or because it lacks capitalization and numbers.

You may shorten words to no less than three letters without affecting the security of your passphrase. You may also replace words with their associated 4 digit number. You may *not* choose different words.

Capitalization adds a very small amount of security; if required, pick a memorable word to capitalize.

What if I lose this book?

The real purpose of this book is to provide you with the tools to generate strong, memorable passwords that are

unbreakable by the world's most powerful computers. It need not be the only place that you record them.

Are password managers like 1Password safe?

Yes, as long as the master password is strong & secure. For example, if Google Chrome is configured to store your password, make sure that you have a strong Google password, and don't leave your account logged in on computers or mobile devices that are not physically secure. The same is true of Safari and iCloud, Internet Explorer and Windows Live, etc.

Who invented Diceware?

Diceware was invented by Arnold G. Reinhold, a computer scientist in Cambridge, MA. It was first published to Usenet's *sci.crypt.research* on August 1st, 1995. For lots more information, visit <https://goo.gl/xobzeV>.

This book implements a simplified version developed by the Electronic Frontier Foundation (EFF) in 2016.

What is the danger in reusing a password?

Imagine that you used the same password for an online clothing store, and your email provider. Months later, the clothing store is hacked and your password is stolen. The hackers login to your email and find correspondence from your bank. They use the bank website to reset your online banking password, and intercept the confirmation email. Next, they use the bank website to order checks in your name, initiate transfers, etc.

This story illustrates why the security of your email ranks above others in importance: for hackers, it is the gateway to all your accounts.

How can I find out if my password has been stolen?

Visit haveibeenpwned.com, and type in your email address. This helpful site tracks the data leaks released by hackers, and maintains a database of email addresses hacked and what kind of data was stolen.

If your email tests positive, immediately change the password for the sites listed *and* any sites that might have shared the same password.

What is two-factor authentication?

Two-factor authentication enhances your password by sending a code to your phone or another device, which you must supply in order to be authorized. This ensures that even if someone has your password, they also need to have your phone.

It's a good idea to set up two-factor authentication on any account linked to your bank account or credit cards.

The US Government no longer recommends SMS for two-factor authentication, due to the ease with which text messages can be intercepted. Mobile apps such as Google Authenticator are more secure.

What is phishing?

Phishing is when a hacker sends you an email message which appears to be from an organization you have a relationship with, but is actually a trap to make you give up your password.

Phishing emails typically warn you that something is wrong with your account, a delivery, or another kind of transaction, and urge you to open a document or log in via a link. They can be very realistic and insidious.

Always check the URL in any emailed links you click, and be sure that they take you to the site you expect.

What is social engineering?

Social engineering is when a hacker contacts a company you do business with and pretends to be you. Often this means telling customer service that you have lost your password, and trying to convince the representative to change it or otherwise unlock your account.

The best protection against social engineering is to avoid easily-guessed security questions, such as your mother's maiden name. When asked for such information, generate a Diceware password instead.

How can I stay safe online?

Above all, practice good operational security (*opsec*). Be suspicious and careful online.

Minimize the number of accounts you open, and always choose the best account security available. Keep track

of the accounts you open, close unused accounts, and change passwords on active accounts regularly. Prefer to shop with businesses that have strong online safeguards, and take advantage of identity protection and online shopping protection services offered by reputable financial institutions.

What to do if I've been hacked?

The resources at crashoverridenetwork.com and at staysafeonline.org are a good starting point. They provide tools to help determine whether you have been hacked and can help you to regain control over your online accounts.

Record of Important Things

Compiled & edited by Wade Brainerd

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 license.

XKCD comic from:
<https://xkcd.com/936/>

Diceware by Arnold G. Reinhold from:
<http://world.std.com/~reinhold/diceware.html>

Diceware word list from:
<https://www.eff.org/deeplinks/2016/07/new-wordlists-random-passphrases>
https://www.eff.org/files/2016/09/08/eff_short_wordlist_2_0.txt

The L^AT_EX source code for this book is located at:
<https://github.com/wadetb/dicebook>