

Record of Important Things



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 CTO, Resilient

Index

1 Record of authentication credentials and other notes

1 _____ 2 _____

3 _____ 4 _____

5 _____ 6 _____

7 _____ 8 _____

9 _____ 10 _____

11 _____ 12 _____

13 _____ 14 _____

15 _____ 16 _____

17 _____ 18 _____

19 _____ 20 _____

21 _____ 22 _____

23 _____ 24 _____

25 _____ 26 _____

27 _____ 28 _____

29 _____ 30 _____

31 _____ 32 _____

33 _____ 34 _____

35 _____ 36 _____

37 _____ 38 _____

39 _____ 40 _____

41 _____ 42 _____

43 _____ 44 _____

45 _____ 46 _____

47 _____ 48 _____

49 Cryptographically-secure passphrases with Diceware

57 Questions & answers regarding online security

Web site

Login or E-mail address

Password(s) used

Date

Notes

2

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used	Date
------------------	------

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used	Date
------------------	------

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used	Date
------------------	------

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used	Date
------------------	------

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used	Date
------------------	------

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used	Date
------------------	------

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used	Date
------------------	------

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used	Date
------------------	------

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Web site

Login or E-mail address

Password(s) used

Date

Notes

Cryptographically-secure passphrases with Diceware

<p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>ORDER UNKNOWN</p> <p>Tr0ub4dor&3</p> <p>CAPS? COMMON SUBSTITUTIONS NUMERICAL PUNCTUATION</p> <p>(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS)</p>	<p>~28 BITS OF ENTROPY</p> <p>$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$</p> <p>(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CRACKING A STOKEN HOPKIN IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)</p> <p>DIFFICULTY TO GUESS: EASY</p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p> <p>DIFFICULTY TO REMEMBER: HARD</p>
<p>correct horse battery staple</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p>$2^{44} = 530 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$</p> <p>DIFFICULTY TO GUESS: HARD</p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT!</p> <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

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 in to 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 that 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.
- 2 Roll all four dice at once and write the results down, reading from left to right, on a scrap 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 that you have found are your new passphrase! If you wish, roll the dice one more time to choose one word to Capitalize, and again for a digit to add to the end.
- 5 Come up with a way to remember your phrase. It might be a story, scenario, or sentence that that can remind you of the particular words you chose, in order.

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, and 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 (about 2^{51}) alternatives that could have been chosen by this method.

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

2235 deepness	2426 eclipse	2621 eulogy	3212 fruit
2236 defrost	2431 ecosystem	2622 euphemism	3213 fryingpan
2241 degree	2432 ecstasy	2623 euthanize	3214 gadget
2242 dehydrator	2433 edged	2624 evacuation	3215 gainfully
2243 deliverer	2434 editor	2625 evergreen	3216 gallstone
2244 democrat	2435 educator	2626 evidence	3221 gamekeeper
2245 dentist	2436 eelworm	2631 evolution	3222 gangway
2246 deodorant	2441 eerie	2632 exam	3223 garlic
2251 depot	2442 effects	2633 excerpt	3224 gaslight
2252 deranged	2443 eggnog	2634 exerciser	3225 gathering
2253 desktop	2444 egomaniac	2635 exfoliate	3226 gauntlet
2254 detergent	2445 ejection	2636 exhale	3231 gearbox
2255 device	2446 elastic	2641 exist	3232 gecko
2256 dexterity	2451 elbow	2642 exorcist	3233 gem
2261 diamond	2452 elderly	2643 explode	3234 generator
2262 dibs	2453 elephant	2644 exquisite	3235 geographer
2263 dictionary	2454 elfishly	2645 exterior	3236 gerbil
2264 diffuser	2455 eliminator	2646 exuberant	3241 gesture
2265 digit	2456 elk	2651 fabric	3242 getaway
2266 dilated	2461 elliptical	2652 factory	3243 geyser
2311 dimple	2462 elongated	2653 faded	3244 ghoulishly
2312 dinnerware	2463 elsewhere	2654 failsafe	3245 gibberish
2313 dioxide	2464 elusive	2655 falcon	3246 giddiness
2314 diploma	2465 elves	2656 family	3251 giftshop
2315 directory	2466 emancipate	2661 fanfare	3252 gigabyte
2316 dishcloth	2511 embroidery	2662 fasten	3253 gimmick
2321 ditto	2512 emcee	2663 faucet	3254 giraffe
2322 dividers	2513 emerald	2664 favorite	3255 giveaway
2323 dizziness	2514 emission	2665 feasibly	3256 gizmo
2324 doctor	2515 emoticon	2666 february	3261 glasses
2325 dodge	2516 emperor	3111 federal	3262 gleeful
2326 doll	2521 emulate	3112 feedback	3263 glisten
2331 dominoes	2522 enactment	3113 feigned	3264 glove
2332 donut	2523 enchilada	3114 feline	3265 glucose
2333 doorstep	2524 endorphin	3115 femur	3266 glycerin
2334 dorsal	2525 energy	3116 fence	3311 gnarly
2335 double	2526 enforcer	3121 ferret	3312 gnomish
2336 downstairs	2531 engine	3122 festival	3313 goatskin
2341 dozed	2532 enhance	3123 fettuccine	3314 goggles
2342 drainpipe	2533 enigmatic	3124 feudalism	3315 goldfish
2343 dresser	2534 enjoyably	3125 feverish	3316 gong
2344 driftwood	2535 enlarged	3126 fiberglass	3321 gooey
2345 droppings	2536 enormous	3131 fictitious	3322 gorgeous
2346 drum	2541 enquirer	3132 fiddle	3323 gosling
2351 dryer	2542 enrollment	3133 figurine	3324 gothic
2352 dubiously	2543 ensemble	3134 fillet	3325 gourmet
2353 duckling	2544 entryway	3135 finalist	3326 governor
2354 duffel	2545 enunciate	3136 fiscally	3331 grape
2355 dugout	2546 envoy	3141 fixture	3332 greyhound
2356 dumpster	2551 enzyme	3142 flashlight	3333 grill
2361 duplex	2552 epidemic	3143 fleshiness	3334 groundhog
2362 durable	2553 equipment	3144 flight	3335 grumbling
2363 dustpan	2554 erasable	3145 florist	3336 guacamole
2364 dutiful	2555 ergonomic	3146 flypaper	3341 guerrilla
2365 duvet	2556 erratic	3151 foamless	3342 guitar
2366 dwarfism	2561 eruption	3152 focus	3343 gullible
2411 dwelling	2562 escalator	3153 foggy	3344 gumdrop
2412 dwindling	2563 eskimo	3154 folksong	3345 gurgling
2413 dynamite	2564 esophagus	3155 fondue	3346 gusto
2414 dyslexia	2565 espresso	3156 footpath	3351 gutless
2415 eagerness	2566 essay	3161 fossil	3352 gymnast
2416 earlobe	2611 estrogen	3162 fountain	3353 gynecology
2421 easel	2612 etching	3163 fox	3354 gyration
2422 eavesdrop	2613 eternal	3164 fragment	3355 habitat
2423 ebook	2614 ethics	3165 freeway	3356 hacking
2424 eccentric	2615 etiquette	3166 fridge	3361 haggard
2425 echoless	2616 eucalyptus	3211 frosting	3362 haiku

3363 halogen	3554 jaguar	4145 lantern	4336 mayonnaise
3364 hamburger	3555 jailhouse	4146 laptop	4341 moaning
3365 handgun	3556 jalapeno	4151 laryngitis	4342 mobilize
3366 happiness	3561 jamboree	4152 lasagna	4343 moccasin
3411 hardhat	3562 janitor	4153 latch	4344 modify
3412 hastily	3563 jarring	4154 laundry	4345 moisture
3413 hatchling	3564 jasmine	4155 lavender	4346 molecule
3414 haughty	3565 jaundice	4156 laxative	4351 momentum
3415 hazelnut	3566 jawbreaker	4161 lazybones	4352 monastery
3416 headband	3611 jaywalker	4162 lecturer	4353 moonshine
3421 hedgehog	3612 jazz	4163 leftover	4354 mortuary
3422 hefty	3613 jealous	4164 leggings	4355 mosquito
3423 heinously	3614 jeep	4165 leisure	4356 motorcycle
3424 helmet	3615 jelly	4166 lemon	4361 mousetrap
3425 hemoglobin	3616 jeopardize	4211 length	4362 movie
3426 henceforth	3621 jersey	4212 leopard	4363 mower
3431 herbs	3622 jetski	4213 leprechaun	4364 mozzarella
3432 hesitation	3623 jezebel	4214 lettuce	4365 muckiness
3433 hexagon	3624 jiffy	4215 leukemia	4366 mudflow
3434 hubcap	3625 jigsaw	4216 levers	4411 mugshot
3435 huddling	3626 jingling	4221 lewdness	4412 mule
3436 huff	3631 jobholder	4222 liability	4413 mummy
3441 hugeness	3632 jockstrap	4223 library	4414 mundane
3442 hullabaloo	3633 jogging	4224 licorice	4415 muppet
3443 human	3634 john	4225 lifeboat	4416 mural
3444 hunter	3635 joinable	4226 lightbulb	4421 mustard
3445 hurricane	3636 jokingly	4231 likewise	4422 mutation
3446 hushing	3641 journal	4232 lilac	4423 myriad
3451 hyacinth	3642 jovial	4233 limousine	4424 myspace
3452 hybrid	3643 joystick	4234 lint	4425 myth
3453 hydrant	3644 jubilant	4235 lioness	4426 nail
3454 hygienist	3645 judiciary	4236 lipstick	4431 namesake
3455 hypnotist	3646 juggle	4241 liquid	4432 nanosecond
3456 ibuprofen	3651 juice	4242 listless	4433 napkin
3461 icepack	3652 jujitsu	4243 litter	4434 narrator
3462 icing	3653 jukebox	4244 liverwurst	4435 nastiness
3463 iconic	3654 jumpiness	4245 lizard	4436 natives
3464 identical	3655 junkyard	4246 llama	4441 nautically
3465 idiocy	3656 juror	4251 luau	4442 navigate
3466 idly	3661 justifying	4252 lubricant	4443 nearest
3511 igloo	3662 juvenile	4253 lucidity	4444 nebula
3512 ignition	3663 kabob	4254 ludicrous	4445 nectar
3513 iguana	3664 kamikaze	4255 luggage	4446 nefarious
3514 illuminate	3665 kangaroo	4256 lukewarm	4451 negotiator
3515 imaging	3666 karate	4261 lullaby	4452 neither
3516 imbecile	4111 kayak	4262 lumberjack	4453 nemesis
3521 imitator	4112 keepsake	4263 lunchbox	4454 neophyte
3522 immigrant	4113 kennel	4264 luridness	4455 nephew
3523 imprint	4114 kerosene	4265 luscious	4456 nervously
3524 iodine	4115 ketchup	4266 luxurious	4461 nest
3525 ionosphere	4116 khaki	4311 lyrics	4462 netting
3526 ipad	4121 kickstand	4312 macaroni	4463 neuron
3531 iphone	4122 kilogram	4313 maestro	4464 nevermore
3532 iridescent	4123 kimono	4314 magazine	4465 nextdoor
3533 irksome	4124 kingdom	4315 mahogany	4466 nicotine
3534 iron	4125 kiosk	4316 maimed	4511 niece
3535 irrigation	4126 kissing	4321 majority	4512 nimbleness
3536 island	4131 kite	4322 makeover	4513 nintendo
3541 isotope	4132 kleenex	4323 malformed	4514 nirvana
3542 issueless	4133 knapsack	4324 mammal	4515 nuclear
3543 italicize	4134 kneecap	4325 mango	4516 nugget
3544 itemizer	4135 knickers	4326 mapmaker	4521 nuisance
3545 itinerary	4136 koala	4331 marbles	4522 nullify
3546 itunes	4141 krypton	4332 massager	4523 numbing
3551 ivory	4142 laboratory	4333 matchstick	4524 nuptials
3552 jabbering	4143 ladder	4334 maverick	4525 nursery
3553 jackrabbit	4144 lakefront	4335 maximum	4526 nutcracker

4531 nylon	5122 pedometer	5313 rearrange	5464 saxophone
4532 oasis	5123 pegboard	5314 rebuilt	5465 scarf
4533 oat	5124 pelican	5315 receipt	5466 scenario
4534 obediently	5125 penguin	5316 reentry	5511 schoolbook
4535 obituary	5126 peony	5321 refinery	5512 scientist
4536 object	5131 pepperoni	5322 register	5513 scooter
4541 obliterate	5132 peroxide	5323 rehydrate	5514 scrapbook
4542 obnoxious	5133 pesticide	5324 reimburse	5515 sculpture
4543 observer	5134 petroleum	5325 rejoicing	5516 scythe
4544 obtain	5135 pewter	5326 rekindle	5521 secretary
4545 obvious	5136 pharmacy	5331 relic	5522 sedative
4546 occupation	5141 pheasant	5332 remote	5523 segregator
4551 oceanic	5142 phonebook	5333 renovator	5524 seismology
4552 octopus	5143 phrasing	5334 reopen	5525 selected
4553 ocular	5144 physician	5335 reporter	5526 semicolon
4554 office	5145 plank	5336 request	5531 senator
4555 oftentimes	5146 pledge	5341 rerun	5532 septum
4556 oiliness	5151 plotted	5342 reservoir	5533 sequence
4561 ointment	5152 plug	5343 retriever	5534 serpent
4562 older	5153 plywood	5344 reunion	5535 sesame
4563 olympics	5154 pneumonia	5345 revolver	5536 settler
4564 omissible	5155 podiatrist	5346 rewrite	5541 severely
4565 omnivorous	5156 poetic	5351 rhapsody	5542 shack
4566 oncoming	5161 pogo	5352 rhetoric	5543 shelf
4611 onion	5162 poison	5353 rhino	5544 shirt
4612 onlooker	5163 poking	5354 rhubarb	5545 shovel
4613 onstage	5164 policeman	5355 rhyme	5546 shrimp
4614 onward	5165 poncho	5356 ribbon	5551 shuttle
4615 onyx	5166 popcorn	5361 riches	5552 shyness
4616 oomph	5211 porcupine	5362 ridden	5553 siamese
4621 opaquely	5212 postcard	5363 rigidity	5554 sibling
4622 opera	5213 poultry	5364 rimmed	5555 siesta
4623 opium	5214 powerboat	5365 riptide	5556 silicon
4624 opossum	5215 prairie	5366 riskily	5561 simmering
4625 opponent	5216 pretzel	5411 ritzy	5562 singles
4626 optical	5221 princess	5412 riverboat	5563 sisterhood
4631 opulently	5222 propeller	5413 roamer	5564 sitcom
4632 oscillator	5223 prune	5414 robe	5565 sixfold
4633 osmosis	5224 pry	5415 rocket	5566 sizable
4634 ostrich	5225 pseudo	5416 romancer	5611 skateboard
4635 otherwise	5226 psychopath	5421 ropelike	5612 skeleton
4636 ought	5231 publisher	5422 rotisserie	5613 skies
4641 outhouse	5232 pucker	5423 roundtable	5614 skulk
4642 ovation	5233 pueblo	5424 royal	5615 skylight
4643 oven	5234 pulley	5425 rubber	5616 slapping
4644 owlsh	5235 pumpkin	5426 rudderless	5621 sled
4645 oxford	5236 punchbowl	5431 rugby	5622 slingshot
4646 oxidize	5241 puppy	5432 ruined	5623 sloth
4651 oxygen	5242 purse	5433 rulebook	5624 slumbering
4652 oyster	5243 pushup	5434 rummage	5625 smartphone
4653 ozone	5244 putt	5435 running	5626 smelliness
4654 pacemaker	5245 puzzle	5436 rupture	5631 smitten
4655 padlock	5246 pyramid	5441 rustproof	5632 smokestack
4656 pageant	5251 python	5442 sabotage	5633 smudge
4661 pajamas	5252 quarters	5443 sacrifice	5634 snapshot
4662 palm	5253 quesadilla	5444 saddlebag	5635 sneezing
4663 pamphlet	5254 quilt	5445 saffron	5636 sniff
4664 pantyhose	5255 quote	5446 sainthood	5641 snowsuit
4665 paprika	5256 racoon	5451 saltshaker	5642 snugness
4666 parakeet	5261 radish	5452 samurai	5643 speakers
5111 passport	5262 ragweed	5453 sandworm	5644 sphinx
5112 patio	5263 railroad	5454 sapphire	5645 spider
5113 pauper	5264 rampantly	5455 sardine	5646 splashing
5114 pavement	5265 rancidity	5456 sassy	5651 sponge
5115 payphone	5266 rarity	5461 satchel	5652 sprout
5116 pebble	5311 raspberry	5462 sauna	5653 spur
5121 peculiarly	5312 ravishing	5463 savage	5654 spyglass

5655 squirrel	6232 tirade	6365 uppercut	6542 wanderer
5656 statue	6233 tissue	6366 upright	6543 wasp
5661 steamboat	6234 tractor	6411 upstairs	6544 water
5662 stingray	6235 tree	6412 uptown	6545 waving
5663 stopwatch	6236 tripod	6413 upwind	6546 wheat
5664 strawberry	6241 trousers	6414 uranium	6551 whisper
5665 student	6242 trucks	6415 urban	6552 wholesaler
5666 stylus	6243 tryout	6416 urchin	6553 wick
6111 suave	6244 tubeless	6421 urethane	6554 widow
6112 subway	6245 tuesday	6422 urgent	6555 wielder
6113 suction	6246 tugboat	6423 urologist	6556 wifeless
6114 suds	6251 tulip	6424 username	6561 wikipedia
6115 suffocate	6252 tumbleweed	6425 usher	6562 wildcat
6116 sugar	6253 tupperware	6426 utensil	6563 windmill
6121 suitcase	6254 turtle	6431 utility	6564 wipeout
6122 sulphur	6255 tusk	6432 utmost	6565 wired
6123 superstore	6256 tutorial	6433 utopia	6566 wishbone
6124 surfer	6261 tuxedo	6434 utterance	6611 wizardry
6125 sushi	6262 tweezers	6435 vacuum	6612 wobbliness
6126 swan	6263 twins	6436 vagrancy	6613 wolverine
6131 sweatshirt	6264 tyrannical	6441 valuables	6614 womb
6132 swimwear	6265 ultrasound	6442 vanquished	6615 woolworker
6133 sword	6266 umbrella	6443 vaporizer	6616 workbasket
6134 sycamore	6311 umpire	6444 varied	6621 wound
6135 syllable	6312 unarmored	6445 vaseline	6622 wrangle
6136 symphony	6313 unbuttoned	6446 vegetable	6623 wreckage
6141 synagogue	6314 uncle	6451 vehicle	6624 wristwatch
6142 syringes	6315 underwear	6452 velcro	6625 wrongdoing
6143 systemize	6316 unevenness	6453 vendor	6626 xerox
6144 tablespoon	6321 unflavored	6454 vertebrae	6631 xylophone
6145 taco	6322 ungloved	6455 vestibule	6632 yacht
6146 tadpole	6323 unhinge	6456 veteran	6633 yahoo
6151 taekwondo	6324 unicycle	6461 vexingly	6634 yard
6152 tagalong	6325 unjustly	6462 vicinity	6635 yearbook
6153 takeout	6326 unknown	6463 videogame	6636 yesterday
6154 tallness	6331 unlocking	6464 viewfinder	6641 yiddish
6155 tamale	6332 unmarked	6465 vigilante	6642 yield
6156 tanned	6333 unnoticed	6466 village	6643 yo-yo
6161 tapestry	6334 unopened	6511 vinegar	6644 yodel
6162 tarantula	6335 unpaved	6512 violin	6645 yogurt
6163 tastebud	6336 unquenched	6513 viperfish	6646 yuppie
6164 tattoo	6341 unroll	6514 virus	6651 zealot
6165 tavern	6342 unscrewing	6515 visor	6652 zebra
6166 thaw	6343 untied	6516 vitamins	6653 zeppelin
6211 theater	6344 unusual	6521 vivacious	6654 zestfully
6212 thimble	6345 unveiled	6522 vixen	6655 zigzagged
6213 thorn	6346 unwrinkled	6523 vocalist	6656 zillion
6214 throat	6351 unyielding	6524 vogue	6661 zipping
6215 thumb	6352 unzip	6525 voicemail	6662 zirconium
6216 thwarting	6353 upbeat	6526 volleyball	6663 zodiac
6221 tiara	6354 upcountry	6531 voucher	6664 zombie
6222 tidbit	6355 update	6532 voyage	6665 zookeeper
6223 tiebreaker	6356 upfront	6533 vulnerable	6666 zucchini
6224 tiger	6361 upgrade	6534 waffle	
6225 timid	6362 upholstery	6535 wagon	
6226 tinsel	6363 upkeep	6536 wakeup	
6231 tiptoeing	6364 upload	6541 walrus	

Questions & answers regarding online security

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 word 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 on a mobile phone.

How many words should I use in my passphrase?

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

Other accounts like social media can reasonably use three words, provided each password is used only once.

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 manager apps 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 on computers or mobile devices that are not physically secure. The same is true of Safari and iCloud, Internet Explorer and Windows Live, etc.

PasswordSafe (<https://pwsafe.org/>) and its accompanying mobile apps provide a good alternative password manager that is not tied to a web browser or e-mail account.

Who invented Diceware?

Diceware was invented by Arnold G. Reinhold, a computer scientist living in Cambridge, MA. Diceware was first published to Usenet's `sci.crypt.research` on August 1st, 1995. For more information, visit <http://world.std.com/reinhold/diceware.html>.

This book implements a simplified version developed by the Electronic Frontier Foundation (EFF) which uses only four dice and is optimized for typing on mobile phones.

What is the danger in re-using a password?

Imagine that you used the same password for an online clothing store, and your e-mail provider. Months later, the clothing store is hacked and your password 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 sent by your bank. From here, they use the bank website to order checks in your name, initiate transfers, etc.

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

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

Visit <https://haveibeenpwned.com/> or a similar site, and type in your e-mail address. They track the data leaks released by hackers, and can identify which e-mail addresses were hacked, and how much data was released.

If your e-mail tests positive, immediately change the password

for the sites listed *and* any sites that might have used 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 then have to type in 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.

What is phishing?

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

Phishing e-mails typically warn you that something is wrong with your account, and urge you to log in via a link. They can be very realistic and insidious.

Always check the URL in any e-mailed links you click, and make sure that they take you to the site you expect. Better yet, ignore links in e-mails and go directly to the website for the organization.

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 using easily-guessed security questions, such as your mother's maiden name. When offered an opportunity to enter such security questions, 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 frequently.

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 services.

What to do if I've been hacked?

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