

If found, please return to:



# 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	_____	13 _____
2	_____	14 _____
3	_____	15 _____
4	_____	16 _____
5	_____	17 _____
6	_____	18 _____
7	_____	19 _____
8	_____	20 _____
9	_____	21 _____
10	_____	22 _____
11	_____	23 _____
12	_____	24 _____

25	_____	37	_____
26	_____	38	_____
27	_____	39	_____
28	_____	40	_____
29	_____	41	_____
30	_____	42	_____
31	_____	43	_____
32	_____	44	_____
33	_____	45	_____
34	_____	46	_____
35	_____	47	_____
36	_____	48	_____

49 Cryptographically-secure passphrases with Diceware

59 Questions & answers regarding online security

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

---

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

---

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

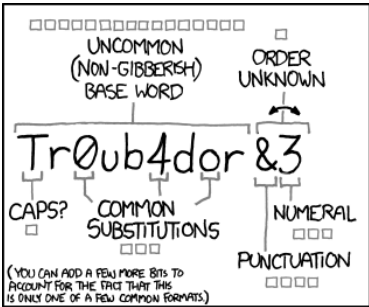
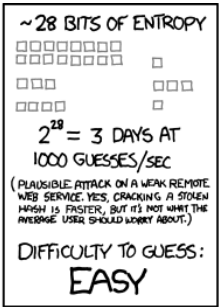

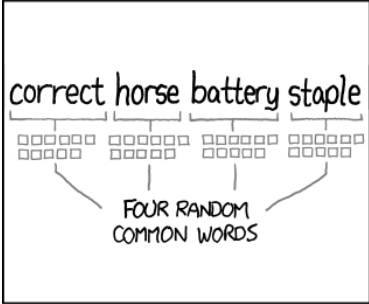

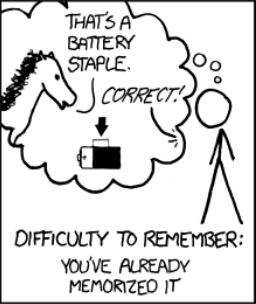
Date

---

Notes

---

# Secure passphrases with Diceware

 <p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>ORDER UNKNOWN</p> <p>Tr0ub4dor &amp;3</p> <p>CAPS? COMMON SUBSTITUTIONS NUMERAL 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><math>2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}</math></p> <p>(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CRACKING A STOLEN HASH 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><math>2^{44} = 530 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}</math></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.

Comic by <https://xkcd.com/> © ⓘ

## 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 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 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!
- 5 Come up with a way to remember your phrase. It might be a story, mental picture, or sentence that can remind you of the phrase you generated.

## Example

Suppose you want a five-word passphrase. You will need  $5 \times 4$  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 (about  $2^{51}$ ) alternatives that could have been chosen by this method.



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

2163 cynicism	2345 droppings	2531 engine	3113 feigned
2164 cypress	2346 drum	2532 enhance	3114 feline
2165 cytoplasm	2351 dryer	2533 enigmatic	3115 femur
2166 dachshund	2352 dubiously	2534 enjoyably	3116 fence
2211 daffodil	2353 duckling	2535 enlarged	3121 ferret
2212 dagger	2354 duffel	2536 enormous	3122 festival
2213 dairy	2355 dugout	2541 enquirer	3123 fettuccine
2214 dalmatian	2356 dumpster	2542 enrollment	3124 feudalist
2215 dandelion	2361 duplex	2543 ensemble	3125 feverish
2216 dartboard	2362 durable	2544 entryway	3126 fiberglass
2221 dastardly	2363 dustpan	2545 enunciate	3131 fictitious
2222 datebook	2364 dutiful	2546 envoy	3132 fiddle
2223 daughter	2365 duvet	2551 enzyme	3133 figurine
2224 dawn	2366 dwarfish	2552 epidemic	3134 fillet
2225 daytime	2411 dwelling	2553 equipment	3135 finalist
2226 dazzler	2412 dwindling	2554 erasable	3136 fiscally
2231 dealer	2413 dynamite	2555 ergonomic	3141 fixture
2232 debris	2414 dyslexia	2556 erratic	3142 flashlight
2233 decal	2415 eagerness	2561 eruption	3143 fleshiness
2234 dedicate	2416 earlobe	2562 escalator	3144 flight
2235 deepness	2421 easel	2563 eskimo	3145 florist
2236 defrost	2422 eavesdrop	2564 esophagus	3146 flypaper
2241 degree	2423 ebook	2565 espresso	3151 foamless
2242 dehydrator	2424 eccentric	2566 essay	3152 focus
2243 deliverer	2425 echoless	2611 estrogen	3153 foggy
2244 democrat	2426 eclipse	2612 etching	3154 folksong
2245 dentist	2431 ecosystem	2613 eternal	3155 fondue
2246 deodorant	2432 ecstasy	2614 ethics	3156 footpath
2251 depot	2433 edged	2615 etiquette	3161 fossil
2252 deranged	2434 editor	2616 eucalyptus	3162 fountain
2253 desktop	2435 educator	2621 eulogy	3163 fox
2254 detergent	2436 eelworm	2622 euphemism	3164 fragment
2255 device	2441 eerie	2623 euthanize	3165 freeway
2256 dexterity	2442 effects	2624 evacuation	3166 fridge
2261 diamond	2443 eggnog	2625 evergreen	3211 frosting
2262 dibs	2444 egomaniac	2626 evidence	3212 fruit
2263 dictionary	2445 ejection	2631 evolution	3213 fryingpan
2264 diffuser	2446 elastic	2632 exam	3214 gadget
2265 digit	2451 elbow	2633 excerpt	3215 gainfully
2266 dilated	2452 elderly	2634 exerciser	3216 gallstone
2311 dimple	2453 elephant	2635 exfoliate	3221 gamekeeper
2312 dinnerware	2454 elfishly	2636 exhale	3222 gangway
2313 dioxide	2455 eliminator	2641 exist	3223 garlic
2314 diploma	2456 elk	2642 exorcist	3224 gaslight
2315 directory	2461 elliptical	2643 explode	3225 gathering
2316 dishcloth	2462 elongated	2644 exquisite	3226 gauntlet
2321 ditto	2463 elsewhere	2645 exterior	3231 gearbox
2322 dividers	2464 elusive	2646 exuberant	3232 gecko
2323 dizziness	2465 elves	2651 fabric	3233 gem
2324 doctor	2466 emancipate	2652 factory	3234 generator
2325 dodge	2511 embroidery	2653 faded	3235 geographer
2326 doll	2512 emcee	2654 failsafe	3236 gerbil
2331 dominoes	2513 emerald	2655 falcon	3241 gesture
2332 donut	2514 emission	2656 family	3242 getaway
2333 doorstep	2515 emoticon	2661 fanfare	3243 geyser
2334 dorsal	2516 emperor	2662 fasten	3244 ghoulishly
2335 double	2521 emulate	2663 faucet	3245 gibberish
2336 downstairs	2522 enactment	2664 favorite	3246 giddiness
2341 dozed	2523 enchilada	2665 feasibly	3251 giftshop
2342 drainpipe	2524 endorphan	2666 february	3252 gigabyte
2343 dresser	2525 energy	3111 federal	3253 gimmick
2344 driftwood	2526 enforcer	3112 feedback	3254 giraffe

3255 giveaway	3441 hugeness	3623 jezebel	4165 leisure
3256 gizmo	3442 hullabaloo	3624 jiffy	4166 lemon
3261 glasses	3443 human	3625 jigsaw	4211 length
3262 gleeful	3444 hunter	3626 jingling	4212 leopard
3263 glisten	3445 hurricane	3631 jobholder	4213 leprechaun
3264 glove	3446 hushing	3632 jockstrap	4214 lettuce
3265 glucose	3451 hyacinth	3633 jogging	4215 leukemia
3266 glycerin	3452 hybrid	3634 john	4216 levers
3311 gnarly	3453 hydrant	3635 joinable	4221 lewdness
3312 gnomish	3454 hygienist	3636 jokingly	4222 liability
3313 goatskin	3455 hypnotist	3641 journal	4223 library
3314 goggles	3456 ibuprofen	3642 jovial	4224 licorice
3315 goldfish	3461 icepack	3643 joystick	4225 lifeboat
3316 gong	3462 icing	3644 jubilant	4226 lightbulb
3321 goopy	3463 iconic	3645 judiciary	4231 likewise
3322 gorgeous	3464 identical	3646 juggle	4232 lilac
3323 gosling	3465 idiocy	3651 juice	4233 limousine
3324 gothic	3466 idly	3652 jujitsu	4234 lint
3325 gourmet	3511 igloo	3653 jukebox	4235 lioness
3326 governor	3512 ignition	3654 jumpiness	4236 lipstick
3331 grape	3513 iguana	3655 junkyard	4241 liquid
3332 greyhound	3514 illuminate	3656 juror	4242 listless
3333 grill	3515 imaging	3661 justifying	4243 litter
3334 groundhog	3516 imbecile	3662 juvenile	4244 liverwurst
3335 grumbling	3521 imitator	3663 kabob	4245 lizard
3336 guacamole	3522 immigrant	3664 kamikaze	4246 llama
3341 guerrilla	3523 imprint	3665 kangaroo	4251 luau
3342 guitar	3524 iodine	3666 karate	4252 lubricant
3343 gullible	3525 ionosphere	4111 kayak	4253 lucidity
3344 gumdrop	3526 ipad	4112 keepsake	4254 ludicrous
3345 gurgling	3531 iphone	4113 kennel	4255 luggage
3346 gusto	3532 iridescent	4114 kerosene	4256 lukewarm
3351 gutless	3533 irksome	4115 ketchup	4261 lullaby
3352 gymnast	3534 iron	4116 khaki	4262 lumberjack
3353 gynecology	3535 irrigation	4121 kickstand	4263 lunchbox
3354 gyration	3536 island	4122 kilogram	4264 luridness
3355 habitat	3541 isotope	4123 kimono	4265 luscious
3356 hacking	3542 issueless	4124 kingdom	4266 luxurious
3361 haggard	3543 italicize	4125 kiosk	4311 lyrics
3362 haiku	3544 itemizer	4126 kissing	4312 macaroni
3363 halogen	3545 itinerary	4131 kite	4313 maestro
3364 hamburger	3546 itunes	4132 kleenex	4314 magazine
3365 handgun	3551 ivory	4133 knapsack	4315 mahogany
3366 happiness	3552 jabbering	4134 kneecap	4316 maimed
3411 hardhat	3553 jackrabbit	4135 knickers	4321 majority
3412 hastily	3554 jaguar	4136 koala	4322 makeover
3413 hatchling	3555 jailhouse	4141 krypton	4323 malformed
3414 haughty	3556 jalapeno	4142 laboratory	4324 mammal
3415 hazelnut	3561 jamboree	4143 ladder	4325 mango
3416 headband	3562 janitor	4144 lakefront	4326 mapmaker
3421 hedgehog	3563 jarring	4145 lantern	4331 marbles
3422 hefty	3564 jasmine	4146 laptop	4332 massager
3423 heinously	3565 jaundice	4151 laryngitis	4333 matchstick
3424 helmet	3566 jawbreaker	4152 lasagna	4334 maverick
3425 hemoglobin	3611 jaywalker	4153 latch	4335 maximum
3426 henceforth	3612 jazz	4154 laundry	4336 mayonnaise
3431 herbs	3613 jealous	4155 lavender	4341 moaning
3432 hesitation	3614 jeep	4156 laxative	4342 mobilize
3433 hexagon	3615 jelly	4161 lazybones	4343 moccasin
3434 hubcap	3616 jeopardize	4162 lecturer	4344 modify
3435 huddling	3621 jersey	4163 leftover	4345 moisture
3436 huff	3622 jetski	4164 leggings	4346 molecule

4351 momentum	4533 oat	5115 payphone	5261 radish
4352 monastery	4534 obediently	5116 pebble	5262 ragweed
4353 moonshine	4535 obituary	5121 peculiarly	5263 railroad
4354 mortuary	4536 object	5122 pedometer	5264 rampantly
4355 mosquito	4541 obliterate	5123 pegboard	5265 rancidity
4356 motorcycle	4542 obnoxious	5124 pelican	5266 rarity
4361 mousetrap	4543 observer	5125 penguin	5311 raspberry
4362 movie	4544 obtain	5126 peony	5312 ravishing
4363 mower	4545 obvious	5131 pepperoni	5313 rearrange
4364 mozzarella	4546 occupation	5132 peroxide	5314 rebuilt
4365 muckiness	4551 oceanic	5133 pesticide	5315 receipt
4366 mudflow	4552 octopus	5134 petroleum	5316 reentry
4411 mugshot	4553 ocular	5135 pewter	5321 refinery
4412 mule	4554 office	5136 pharmacy	5322 register
4413 mummy	4555 oftentimes	5141 pheasant	5323 rehydrate
4414 mundane	4556 oiliness	5142 phonebook	5324 reimburse
4415 puppet	4561 ointment	5143 phrasing	5325 rejoicing
4416 mural	4562 older	5144 physician	5326 rekindle
4421 mustard	4563 olympics	5145 plank	5331 relic
4422 mutation	4564 omissible	5146 pledge	5332 remote
4423 myriad	4565 omnivorous	5151 plotted	5333 renovator
4424 myspace	4566 oncoming	5152 plug	5334 rerun
4425 myth	4611 onion	5153 plywood	5335 reporter
4426 nail	4612 onlooker	5154 pneumonia	5336 request
4431 namesake	4613 onstage	5155 podiatrist	5341 rerun
4432 nanosecond	4614 onward	5156 poetic	5342 reservoir
4433 napkin	4615 onyx	5161 pogo	5343 retriever
4434 narrator	4616 oomph	5162 poison	5344 reunion
4435 nastiness	4621 opaquely	5163 poking	5345 revolver
4436 natives	4622 opera	5164 policeman	5346 rewrite
4441 nautically	4623 opium	5165 poncho	5351 rhapsody
4442 navigate	4624 opossum	5166 popcorn	5352 rhetoric
4443 nearest	4625 opponent	5211 porcupine	5353 rhino
4444 nebula	4626 optical	5212 postcard	5354 rhubarb
4445 nectar	4631 opulently	5213 poultry	5355 rhyme
4446 nefarious	4632 oscillator	5214 powerboat	5356 ribbon
4451 negotiator	4633 osmosis	5215 prairie	5361 riches
4452 neither	4634 ostrich	5216 pretzel	5362 ridden
4453 nemesis	4635 otherwise	5221 princess	5363 rigidity
4454 neoliberal	4636 ought	5222 propeller	5364 rimmed
4455 nephew	4641 outhouse	5223 prune	5365 riptide
4456 nervously	4642 ovation	5224 pry	5366 riskily
4461 nest	4643 oven	5225 pseudo	5411 ritzy
4462 netting	4644 owlsh	5226 psychopath	5412 riverboat
4463 neuron	4645 oxford	5231 publisher	5413 roamer
4464 nevermore	4646 oxidize	5232 pucker	5414 robe
4465 nextdoor	4651 oxygen	5233 pueblo	5415 rocket
4466 nicotine	4652 oyster	5234 pulley	5416 romancer
4511 niece	4653 ozone	5235 pumpkin	5421 ropelike
4512 nimbleness	4654 pacemaker	5236 punchbowl	5422 rotisserie
4513 nintendo	4655 padlock	5241 puppy	5423 roundtable
4514 nirvana	4656 pageant	5242 purse	5424 royal
4515 nuclear	4661 pajamas	5243 pushup	5425 rubber
4516 nugget	4662 palm	5244 putt	5426 rudderless
4521 nuisance	4663 pamphlet	5245 puzzle	5431 rugby
4522 nullify	4664 pantyhose	5246 pyramid	5432 ruined
4523 numbing	4665 paprika	5251 python	5433 rulebook
4524 nuptials	4666 parakeet	5252 quarters	5434 rummage
4525 nursery	5111 passport	5253 quesadilla	5435 running
4526 nutcracker	5112 patio	5254 quilt	5436 rupture
4531 nylon	5113 pauper	5255 quote	5441 rustproof
4532 oasis	5114 pavement	5256 racoon	5442 sabotage

5443 sacrifice	5625 smartphone	6211 theater	6353 upbeat
5444 saddlebag	5626 smelliness	6212 thimble	6354 upcountry
5445 saffron	5631 smitten	6213 thorn	6355 update
5446 sainthood	5632 smokestack	6214 throat	6356 upfront
5451 saltshaker	5633 smudge	6215 thumb	6361 upgrade
5452 samurai	5634 snapshot	6216 thwarting	6362 upholstery
5453 sandworm	5635 sneezing	6221 tiara	6363 upkeep
5454 sapphire	5636 sniff	6222 tidbit	6364 upload
5455 sardine	5641 snowsuit	6223 tiebreaker	6365 uppercut
5456 sassy	5642 snugness	6224 tiger	6366 upright
5461 satchel	5643 speakers	6225 timid	6411 upstairs
5462 sauna	5644 sphinx	6226 tinsel	6412 uptown
5463 savage	5645 spider	6231 tiptoeing	6413 upwind
5464 saxophone	5646 splashing	6232 tirade	6414 uranium
5465 scarf	5651 sponge	6233 tissue	6415 urban
5466 scenario	5652 sprout	6234 tractor	6416 urchin
5511 schoolbook	5653 spur	6235 tree	6421 urethane
5512 scientist	5654 spyglass	6236 tripod	6422 urgent
5513 scooter	5655 squirrel	6241 trousers	6423 urologist
5514 scrapbook	5656 statue	6242 trucks	6424 username
5515 sculpture	5661 steamboat	6243 tryout	6425 usher
5516 scythe	5662 stingray	6244 tubeless	6426 utensil
5521 secretary	5663 stopwatch	6245 tuesday	6431 utility
5522 sedative	5664 strawberry	6246 tugboat	6432 utmost
5523 segregator	5665 student	6251 tulip	6433 utopia
5524 seismology	5666 stylus	6252 tumbleweed	6434 utterance
5525 selected	6111 suave	6253 tupperware	6435 vacuum
5526 semicolon	6112 subway	6254 turtle	6436 vagrancy
5531 senator	6113 suction	6255 tusk	6441 valuables
5532 septum	6114 suds	6256 tutorial	6442 vanquished
5533 sequence	6115 suffocate	6261 tuxedo	6443 vaporizer
5534 serpent	6116 sugar	6262 tweezers	6444 varied
5535 sesame	6121 suitcase	6263 twins	6445 vaseline
5536 settler	6122 sulphur	6264 tyrannical	6446 vegetable
5541 severely	6123 superstore	6265 ultrasound	6451 vehicle
5542 shack	6124 surfer	6266 umbrella	6452 velcro
5543 shelf	6125 sushi	6311 umber	6453 vendor
5544 shirt	6126 swan	6312 unarmored	6454 vertebrae
5545 shovel	6131 sweatshirt	6313 unbuttoned	6455 vestibule
5546 shrimp	6132 swimwear	6314 uncle	6456 veteran
5551 shuttle	6133 sword	6315 underwear	6461 vexingly
5552 shyness	6134 sycamore	6316 unevenness	6462 vicinity
5553 siamese	6135 syllable	6321 unflavored	6463 videogame
5554 sibling	6136 symphony	6322 ungloved	6464 viewfinder
5555 siesta	6141 synagogue	6323 unhinge	6465 vigilante
5556 silicon	6142 syringes	6324 unicycle	6466 village
5561 simmering	6143 systemize	6325 unjustly	6511 vinegar
5562 singles	6144 tablespoon	6326 unknown	6512 violin
5563 sisterhood	6145 taco	6331 unlocking	6513 viperfish
5564 sitcom	6146 tadpole	6332 unmarked	6514 virus
5565 sixfold	6151 taekwondo	6333 unnoticed	6515 visor
5566 sizable	6152 tagalong	6334 unopened	6516 vitamins
5611 skateboard	6153 takeout	6335 unpaved	6521 vivacious
5612 skeleton	6154 tallness	6336 unquenched	6522 vixen
5613 skies	6155 tamale	6341 unroll	6523 vocalist
5614 skulk	6156 tanned	6342 unscrewing	6524 vogue
5615 skylight	6161 tapestry	6343 untied	6525 voicemail
5616 slapping	6162 tarantula	6344 unusual	6526 volleyball
5621 sled	6163 tastebud	6345 unveiled	6531 voucher
5622 slingshot	6164 tattoo	6346 unwrinkled	6532 voyage
5623 sloth	6165 tavern	6351 unyielding	6533 vulnerable
5624 slumbering	6166 thaw	6352 unzip	6534 waffle

6535 wagon	6562 wildcat	6625 wrongdoing	6652 zebra
6536 wakeup	6563 windmill	6626 xerox	6653 zeppelin
6541 walrus	6564 wipeout	6631 xylophone	6654 zestfully
6542 wanderer	6565 wired	6632 yacht	6655 zigzagged
6543 wasp	6566 wishbone	6633 yahoo	6656 zillion
6544 water	6611 wizardry	6634 yard	6661 zipping
6545 waving	6612 wobbliness	6635 yearbook	6662 zirconium
6546 wheat	6613 wolverine	6636 yesterday	6663 zodiac
6551 whisper	6614 womb	6641 yiddish	6664 zombie
6552 wholesaler	6615 woolworker	6642 yield	6665 zookeeper
6553 wick	6616 workbasket	6643 yoyo	6666 zucchini
6554 widow	6621 wound	6644 yodel	
6555 wielder	6622 wrangle	6645 yogurt	
6556 wifeless	6623 wreckage	6646 yuppie	
6561 wikipedia	6624 wristwatch	6651 zealot	



# Notes about 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.

## **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.

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



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

### **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, provided the shortened version remains unique within the word list. 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 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 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 1<sup>st</sup>, 1995. For lots more information, see <https://google/xobzeV>.

This book implements a simplified version developed by the Electronic Frontier Foundation (EFF) in 2016, which uses only four dice.

## **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 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 e-mail 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](https://haveibeenpwned.com), 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 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 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.

## 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 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 [www.crashoverridenetwork.com](http://www.crashoverridenetwork.com) and [staysafeonline.org](http://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.

---

## 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](https://www.eff.org/files/2016/09/08/eff_short_wordlist_2_0.txt)

The L<sup>A</sup>T<sub>E</sub>X source code for this book is located at:

<https://github.com/wadetb/dicebook>