

**"Those Dang Passwords –
They're Just Driving Me Crazy!"**

**Some Introductory Remarks For
A Panel on Passwords in Portland,
Organized By *The Oregonian***

Joe St Sauver, Ph.D.

Disclaimer: All opinions strictly my own

Tonight's Focus? Those Dang PASSWORDS!

most popular passwords

1111 111111 112233 123 123!@# 123.321 123.com 123123 1234
12345 123456 1234567 12345678 123456789
1234567890 123465 1234qwer 123abc 123qwe 123qwe!@# 123qwe123
123qweasd 142536 147147 1q2w3e 1q2w3e4r 1q2w3e4r5t 1qaz2wsx
1qaz@WSX 1qazxsw2 225588 2wsx3edc 654321 666666 8812345 88888888 Admin@123
P@ssw0rd P@ssword Passw0rd \001 a123456 aa123456 abc123
abcd1234 admin admin1 admin123 admin@123 administrator apple
changeme cisco data firewall huawei iloveyou letmein linux manager
master master123 monitor oracle p@ssw0rd pass pass123 passw0rd passwd
password password1 q1w2e3 q1w2e3r4 q1w2e3r4t5 qazxsw
qwel123 qwel123!@# qweasd qwer1234 qwerty r00t redhat root
root1 root123 root123!@# root1234 root@123 rootme rootpass
rootroot samsung server system temporal test test123 toor welcome
zaq12wsx

Source: <https://www.dragonresearchgroup.org/insight/sshpwauth-cloud.html>

Do YOU Use Any Of Those Passwords? (Or Any OTHER Weak Passwords?)

- I sure hope not!
- Those are the passwords that the Dragon Research Group (DRG) found hacker/crackers try most often when guessing the passwords of ssh (secure shell) accounts.
- Why do attackers try those passwords? The passwords on that list include some known default passwords (that may never have gotten changed), plus passwords that are empirically known to be popular with many average users. Users may use them for their email accounts, or for accounts at online merchants, etc.
- If you use one of those passwords (or any other simple password, including any word from a dictionary), it's just a matter of time until bad things happen.

Why Do The Bad Guys *Want* Passwords?

- In most cases, it's nothing personal, it's "just business."
- Most cybercrime is monetarily motivated: hacking your accounts is just a way for a cyber criminal to make a buck.
- Maybe they'll "just" send spam from your account.
- Then again, maybe they'll clean out your bank account.
- So **HOW** do bad guys steal your passwords?

The Malware Problem

- **Malware is the most common way that passwords get popped.**
- If your computer does get infected with some types of malicious software, that malware may snoop and report on whatever you type – including your secret passwords.
- It's therefore critical that you strive to keep your computer **malware free** (one good option is to use an operating system that doesn't get hit by malware much, since antivirus really isn't all that effective any more).
- Regardless of which operating system you use, make sure you keep everything patched up-to-date! (Try Secunia PSI on your personal Windows systems, see http://secunia.com/vulnerability_scanning/personal/)

A Few Other Attacks Against Passwords

- Maybe we'll just "look over your shoulder" as you type your password in at a meeting (or maybe you'll sit under a conveniently-placed ceiling-mounted security camera!)
- Maybe you'll "volunteer" your password if we just ask you to tell us (e.g., social engineering/phishing attacks).
- Maybe your password is being transmitted over the Internet in clear text (e.g., unencrypted) -- if so, maybe we can try to eavesdrop upon it ("sniff it") as it goes past.
- If I have physical access to your system, maybe we'll just plug in a USB hardware key logger, and intercept everything you type (including your password) that way.
- There are a million ways that plain old passwords can easily fail...

Password Resets: Another Weak Spot

- I'm sure everyone here has had to reset a password at least once. You know how that tends to work – normally you see one of two options:
 - You supply answers to trivia questions ("What's your favorite football team?" – how hard is *that* to guess?) Attackers may also look up trivia on social media sites.
 - The other common alternative? You get a "password reset link" sent to an email account you've preregistered. Does that make you feel a little nervous? It should.
- If I can just get control of your email account, I can then try to "reset" the passwords to all your other accounts.

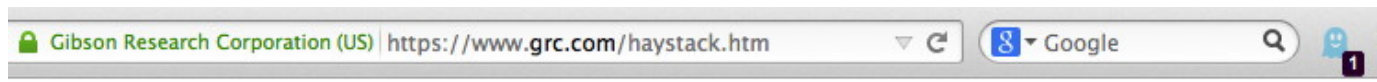
One Option: Avoid Creating Accounts

- The simplest step: **if possible, avoid creating accounts in the first place. Resist "signing up."**
- If you don't have a username and password for a site, there's nothing to get hacked, and you've got one less account to worry about.
- Of course, if you don't sign in, you may not be able to access some content or some services.
- However, if you don't "sign in" (and if you don't accept cookies, etc.), it also becomes harder for marketers to track your online activities.

When You Have No Option...

- Sometimes you have no choice but to create an account and password.
- When that's the case, create a username and password that's unique to **just** that site.
- You and I both know what a "good" password "should" look like, right?
- It should be "long" (but somehow still easy to remember), while being formed from a "rich character set" including upper & lower case letters, numbers, plus punctuation or oddball symbols (e.g., .,?!;:~@#\$\$%^&*~+="/|\<>[](){})

A Sample "Complex" Password



GRC's Interactive Brute Force Password "Search Space" Calculator

(*NOTHING* you do here ever leaves your browser. What happens here, stays here.)

☒ 3 Uppercase ☒ 6 Lowercase ☒ 1 Digit ☒ 3 Symbols 13 Characters

This|5^MYp@ss

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10+33 = 95
Search Space Length (Characters):	13 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	51,880,316, 927,184,027,554,126,495
Search Space Size (as a power of 10):	5.19×10^{25}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	16.50 trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	1.65 hundred thousand centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	1.65 hundred centuries

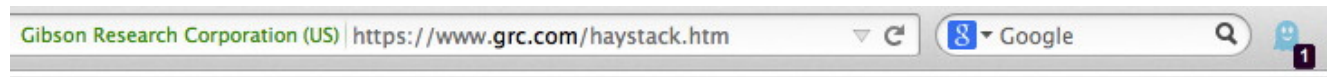
Note that typical attacks will be online password guessing
limited to, at most, a few hundred guesses per second.

One *Slight* Problem With Complex Passwords

- **People have a hard time remembering complex strings.**
For example, I bet you don't remember the password I just showed you on the preceding slide... or do you?
- People being people, they tend to use easier-to-remember passwords, instead. For example, perhaps they set their password to something like "baseball" or "hockey"
- While that's easier to remember, it's also easy to brute force, or even to just guess through a dictionary attack.

[What's a dictionary attack? Try all the words in the dictionary as possible passwords. FWIW, there are only about 250,000 words even in a big English dictionary, so that's a pretty short list for an attacker to try...]

Sample Six Character Password



GRC's Interactive Brute Force Password "Search Space" Calculator

(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)

☒ No Uppercase ☒ 6 Lowercase ☐ No Digits ☐ No Symbols 6 Characters

hockey

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26
Search Space Length (Characters):	6 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	321,272,406
Search Space Size (as a power of 10):	3.21×10^8

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	3.72 days
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	0.00321 seconds
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	0.00000321 seconds

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

Passphrases To The Rescue (Maybe)

- While people have a hard time remembering random unpronounceable strings with numbers and weird characters and odd capitalization, most people CAN remember a relatively long "passphrase..."
- Pass phrases can be a more secure alternative, at least if:
 - the site you're logging into allows you to use long passwords (some will, some may not)
 - the site allows you to use words from the dictionary in your password (again, some may, some may not)
 - your pass phrase isn't a well known cliché or otherwise overly common ("a penny saved is a penny earned")

Sample 36 Character Passphrase

Gibson Research Corporation (US) | <https://www.grc.com/haystack.htm> Google

GRC's Interactive Brute Force Password "Search Space" Calculator

(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)

☐ No Uppercase ☒ 31 Lowercase ☐ No Digits ☒ 5 Symbols 36 Characters

oat meal is nutritious and delicious

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+33 = 59
Search Space Length (Characters):	36 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	5,729,232,372, 459,098,666,549,656,927, 180,282,234,474,814,812, 596,145,669,014,757,320
Search Space Size (as a power of 10):	5.73×10^{63}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	1.82 thousand trillion trillion trillion trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	18.22 million trillion trillion trillion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	18.22 thousand trillion trillion trillion centuries

Note that typical attacks will be online password guessing
limited to, at most, a few hundred guesses per second.

Another Problem: Lots of Accounts

- Another problems is that we all have **too many** accounts to keep straight. So what do people do?
 - Maybe you use the same username and password "everywhere..." When that happens, if an attacker can crack your username and password on one site, they can use it on on all the sites where you have accounts.
 - People may save their passwords (insecurely) in their web browsers...
 - Still other users just give up and continually "reset" their passwords every time they need to login.
- Is there *no better solution* if you have lots of accounts?

← → https://www.schneier.com/blog/archives/2005/06/write_down_your.html Google

Write Down Your Password

Microsoft's Jesper Johansson [urged](#) people to write down their passwords.

This is good advice, and I've been saying it for years.

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.


Tags: [passwords](#), [usability](#)

[Posted on June 17, 2005 at 8:40 AM](#) • 139 Comments

☐ Like ☐ Tweet ☐ +1 ☐ i ☐ ⚙

☒ blog ☐ essays ☐ whole site

Subscribe

About Bruce Schneier



Important Note From Joe: this only works if you trust those who have access to the content of your wallet, and you never lose your wallet...

Additional Important Note From Joe: this is NOT a recommendation that you should tape your username and password to the side of your computer where anyone walking by can see it!

Or Maybe Try A Password Manager?

www.pcmag.com/article2/0,2817,2407168,00.asp

PC NEWS / OPINIONS / FEATURES / DEALS / HOW-TO / BUSINESS / SUBSCRIBE

Search for products, news, tips...

ALL REVIEWS LAPTOPS TABLETS PHONES APPS SOFTWARE SECURITY PRINTERS CAMERAS HDTVS

The Best Password Managers

BY NEIL J. RUBENKING AUGUST 22, 2014

In these days of hacks, Heartbleed, and endless breaches, a strong, unique, and often-changed password for every site is even more imperative. A password manager can help you attain that goal.

SHARES

Name	LastPass 3.0	LastPass 3.0 Premium	Dashlane 3	RoboForm Everywhere 7	Intuitive Password 2.9	Keeper Password Manager & Digital Vault 8	Norton Identity Safe	PasswordBox	RoboForm Desktop 7	Sticky Password 7
Editor Rating	★★★★★ EDITOR'S CHOICE	★★★★★ EDITOR'S CHOICE	★★★★★ EDITOR'S CHOICE	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
Lowest Price	\$0.00 LastPass	\$12.00 LastPass		\$9.95 RoboForm				\$0.00 Amazon	\$29.95 RoboForm	
Platforms	Windows, Mac, Linux	Android, iOS, Windows, Mac, Blackberry, Windows Phone, Symbian, Linux	Android, iOS, Windows, Mac	Android, iOS, Windows, Mac, Windows Phone, Linux	Web	Android, iOS, Windows, Mac, Web, Windows Phone, Linux, Kindle, Nook	Android, iOS, Windows	Android, iOS, Windows, Mac, Kindle	Windows, Mac	Android, iOS, Windows
Password Strength Report	Yes	Yes	Yes	No	Yes	No	No	No	No	No
Secure Password Sharing	Yes	Yes	Yes	No	Yes	Yes	No	Yes	No	No
	Read the Review	Read the Review	Read the Review	Read the Review	Read the Review	Read the Review	Read the Review	Read the Review	Read the Review	Read the Review

Online merchants and other supposedly secure websites can't be relied on to keep your personal information safe. Even sites using decent security practices may

Multifactor: Better Than Passwords Alone

- If you use an ATM card you're already familiar with one type of multifactor authentication: you need to supply your ATM card (something you have), PLUS you need to supply your PIN code (something you know).
- Two factor authentication for your computer accounts works in a similar way: after you login as you normally would with your username and password, the service you're logging into might contact you via your registered cell phone to confirm that it's "really you."
- You might need to enter a six digit code that they give you; other times you may simply push "ok" button on your phone to signal that you really want to proceed.
- If the sites you use offer some sort of multifactor authentication, ***please, USE IT!***

www.google.com/landing/2step/#tab=how-it-protects

Google

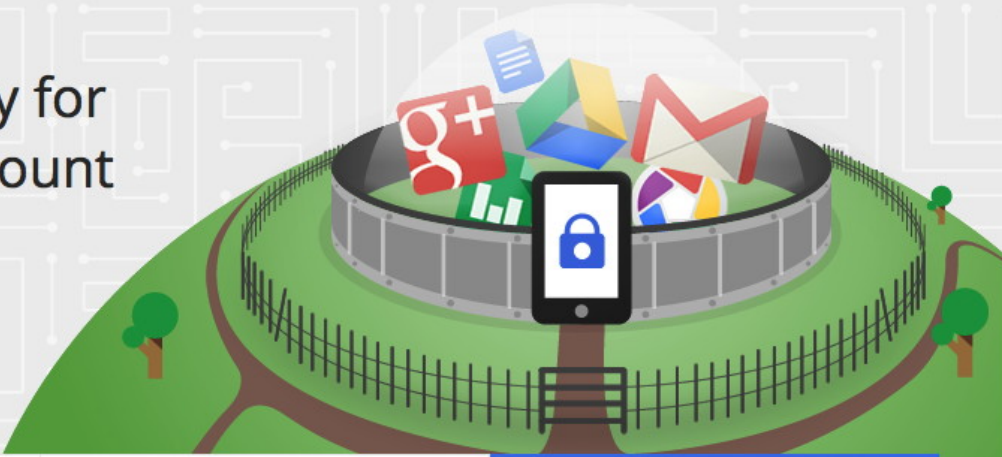
Google 2-Step Verification

Get Started

Home Features Help

Stronger security for your Google Account

With 2-Step Verification, you'll protect your account with both your password and your phone

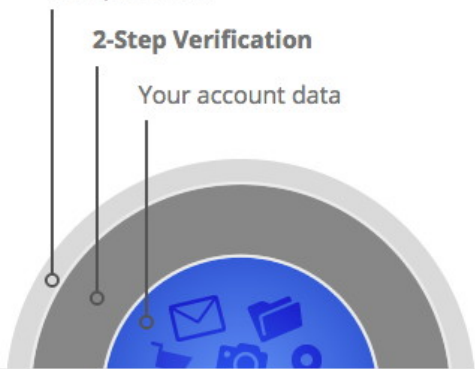


Why you need it How it works How it protects you

Your password

2-Step Verification

Your account data



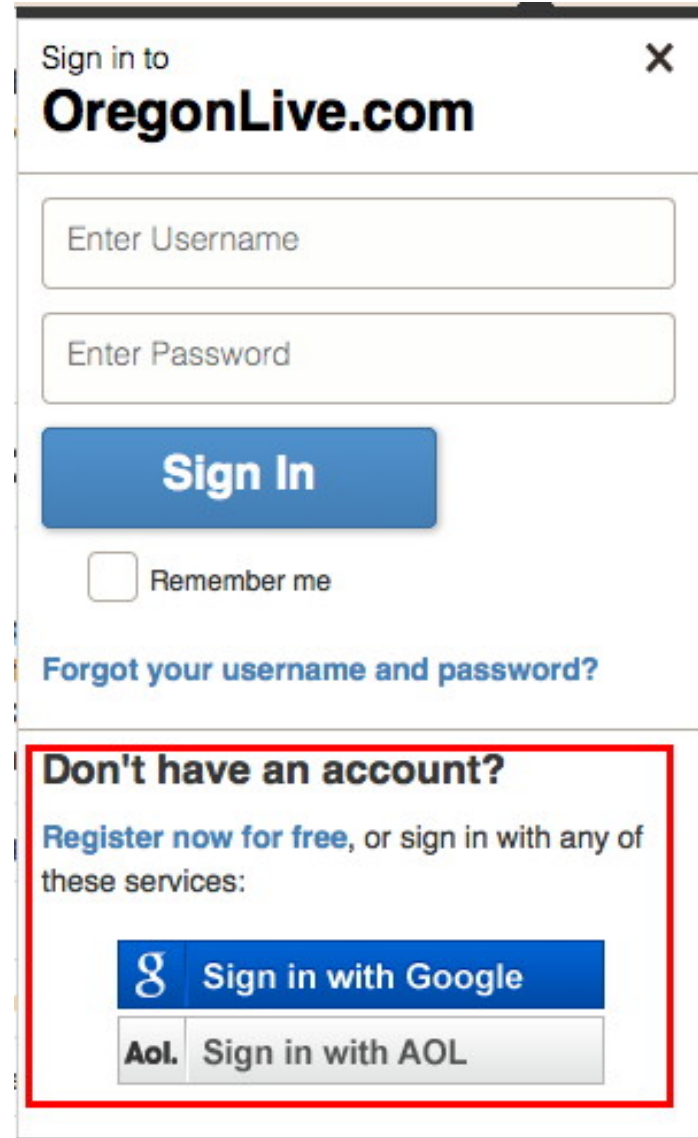
An extra layer of security

Most people only have one layer – their password – to protect their account. With 2-Step Verification, if a bad guy hacks through your password layer, he'll still need your phone to get into your account.

Another Alternative... Federated Auth

- You could also try using "federated auth."
- For example, you may have noticed that some sites will let you login with your credentials from another site (such as Facebook or Google).

That's usually a sign that you're at a site that's doing some type of federated authentication.



The image shows a web form for signing in to OregonLive.com. At the top, it says "Sign in to OregonLive.com" with a close button (X). Below this are two input fields: "Enter Username" and "Enter Password". A blue "Sign In" button is positioned below the password field. Under the button is a checkbox labeled "Remember me". A link "Forgot your username and password?" is located below the checkbox. At the bottom, a red-bordered box contains the text "Don't have an account?" followed by "Register now for free, or sign in with any of these services:". Below this text are two buttons: "Sign in with Google" (with the Google logo) and "Sign in with AOL" (with the AOL logo).

Important Notes About Federated Auth

- Federated authentication is NOT the same as just using the same username and the same password on multiple sites! Doing THAT is a **REALLY BAD** idea. (Fortunately, federated auth is NOT the same thing at all!)
- Some illegitimate sites may try to trick you into thinking that you're doing federated authentication when you're really not (this is a not uncommon phishing ploy). Pay very careful attention to the site you're actually logging into!
- Logging in with social media credentials may share more about you and your friends than you realize or intend. The best types of federated authentication strictly limit the information about you that get shared with 3rd party sites to just the minimum amount necessary. (Other types of federated auth may simply share way, way, too much)

Conclusion: It's Your Choice.

What Will You Choose To Do?

- Many users ignore cyber security issues. That's probably not you, or you wouldn't be here tonight.
- Others will take modest steps, such as at least making sure your computer is virus free and patched up-to-date, and maybe trying a password manager.
- A still smaller group of people may decide to do whatever it takes to live a "security-oriented lifestyle" (including using multifactor authentication).
- And a few may become so discouraged that they decide to stop using the Internet altogether (but that's a shame – there's a lot of terrific benefits to using the Internet)
- What will **YOU** choose to do?