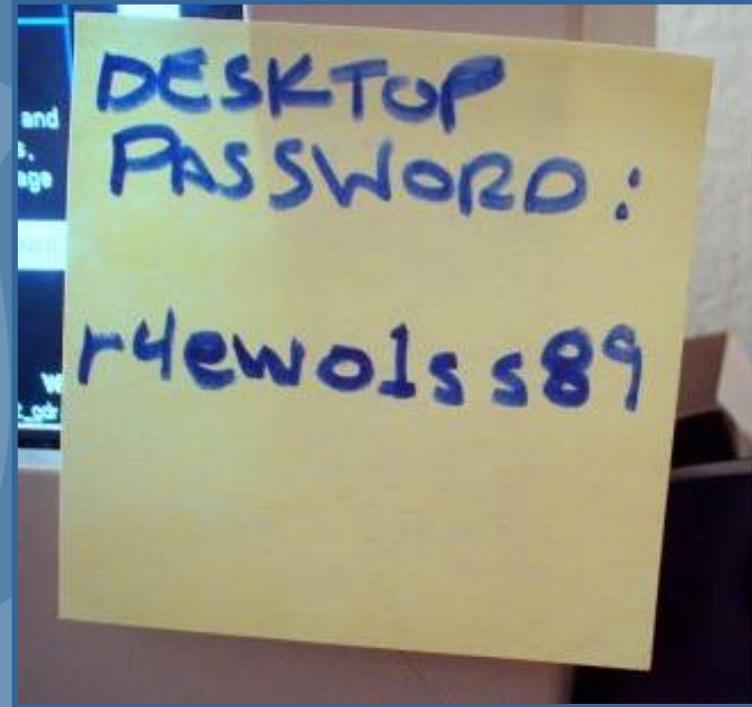


~~Password~~ Management 201

passphrase



June 2013

Information Security and Privacy Office

City of Phoenix



Ripped from the Headlines

- Account information breached for 50,000,000 Living Social users
 - Customer names
 - eMail addresses
 - Birthdates
 - Hashed and salted passwords

LivingSocial recently experienced a cyber-attack on our computer systems that resulted in unauthorized access to some customer data from our servers. We are actively working with law enforcement to investigate this issue.

The information accessed includes names, email addresses, date of birth for some users, and encrypted passwords -- technically 'hashed' and 'salted' passwords. We never store passwords in plain text.

The database that stores customer credit card information was not affected or accessed.

Although your LivingSocial password would be difficult to decode, we want to take every precaution to ensure that your account is secure, so we are expiring your old password and requesting that you create a new one.

For your security, please create a new password by clicking the button below.

[change your password now](#)

2013-04-05	Incident Occurred
2013-04-12	Incident Discovered By Organization
2013-04-26	Organization Reports Incident



Pop Quiz

- What's a hashed password?
- Extra credit: What's salt on a hashed password?
 - (Other than tasty)





Hash Function

- One-way encryption – can't decrypt
 - **Has no key**
- Primary use is for message integrity
 - By comparing hash values, you can see if message sent = message received





Why Hash?

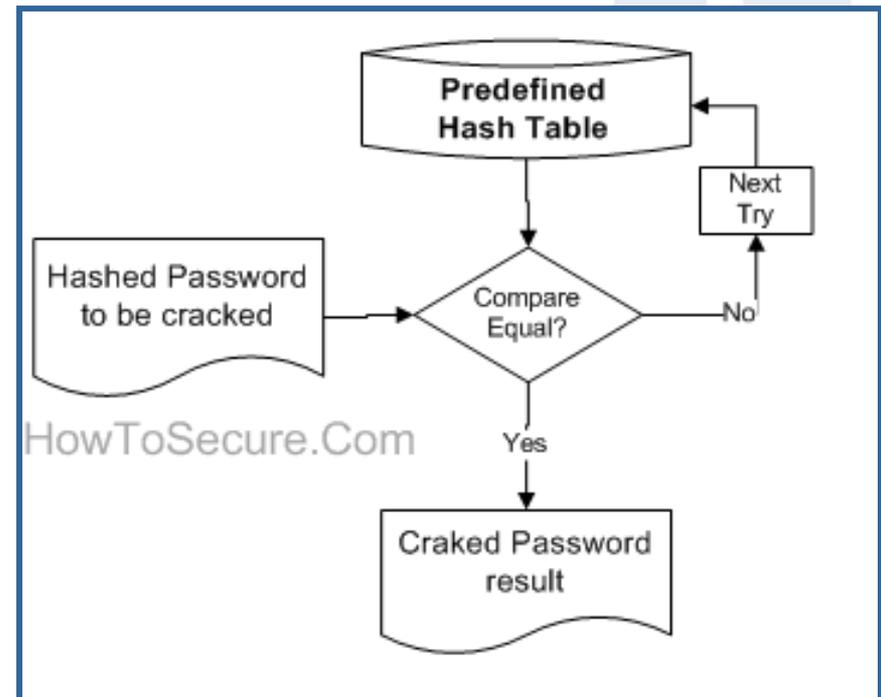
Keep Original Data Confidential

- Passwords are commonly hashed
- Password files actually contain hash of your password – not the password itself
 - When you log in, the computer hashes your password and compares the hash value to the hash value of the password that's on file



So How Do Hackers Crack Passwords?

- Brute force – try every combination of characters
- Use tables of pre-hashed passwords (rainbow tables)
 - Use a hash algorithm and hash the dictionary and the 500 top passwords
 - Steal a password file
 - Compare the file (hashed passwords) to the list (hashed words)





Defend Against Password Hackers: Salted Hash

- Salting adds a string of random characters to the passwords before they are hashed, so that each one has a unique hash
 - Hacker has to crack every user's password individually, even if there are a lot of duplicate passwords





Why Worry – Living Social Passwords Were Encrypted

chanman819 | Smack-Fu Master, in training

[jump to post](#)

The problem is that password encryption or storage security measures should not be viewed as some kind of fortified bulwark that actively keeps out all but the most determined attackers.

A password breach should be viewed as a raging inferno in a building and any security measures in place are analogous to fire-resistant building materials and sprinklers in a warehouse full of flammable goods - they only buy time for the occupants to escape, they don't make it safe to remain inside the burning building.

- Comment on article about Living Social breach



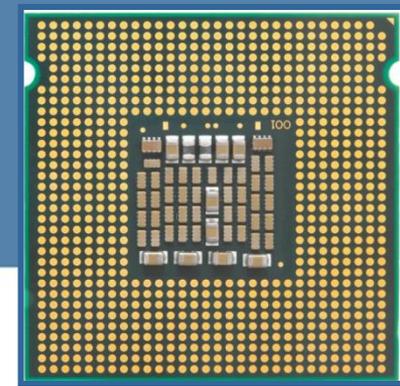
Pop Quiz

- What's a CPU?
- What's a GPU?





CPU and GPU



- Central Processing Unit
 - “Brain” of a computer that performs the arithmetical, logical, and input/output operations of the system

- Graphics Processing Unit
 - Like the CPU, GPU is a single-chip processor
 - Used primarily for computing 3D functions, like lighting effects, object transformations, and 3D motion
 - Designed to take the “load” off the CPU

- Speed is how fast the processor can perform calculations
 - Speed is limited by the number of transistors built into a processor, parallel connections to other processors, the capacity of the bus to transmit data back and forth from the CPU to memory, and other hardware specifications



CPU vs GPU

CPU

- 9 million transistors (Pentium III)
- 2.4 billion calculations per second (in general, for a 2.4 gigahertz CPU)

GPU

- 22 million transistors (Nvidia GeForce 256)
- 200 billion operations a second (Quadro, designed for CAD applications)

Why do we care?

A PC running a single AMD Radeon HD7970 GPU, for example, can try on average **8.2 billion password combinations each second**, depending on the algorithm used to encrypt/hash them



Brute Force Attacks Today



- Today any 7 character password can be cracked by brute force **in hours** using a regular personal computer with a GPU graphics card
- Using a normal CPU, it take 24 seconds to crack a five character random password, like “xnZyr”
 - Rate of 9.8 million password guesses per second
- Adding a GPU graphics card, it takes **1 second** to break the same password



Test Your Password

- Type a password with the same characteristics as your password
 - Length, case, special characters, numbers...
- <http://howsecureismypassword.net/>
- Test “Phoenix1”
 - Meets our Password Standard



HOW SECURE IS MY PASSWORD?



SHOW SETTINGS

Your password would be cracked almost

Instantly

[Tweet Result]

HIDE DETAILS

Length: 8 characters

Character Combinations: 62

Calculations Per Second: 4 billion

Possible Combinations: 218 trillion

COMMON PASSWORD: IN THE TOP 3080 MOST USED PASSWORDS

Your password is very commonly used. It would be cracked almost instantly.



HOW SECURE IS MY PASSWORD?



SHOW SETTINGS

It would take a desktop PC about
26 million years
to crack your password

[Tweet Result]

HIDE DETAILS

Length: 13 characters

Character Combinations: 77

Calculations Per Second: 4 billion

Possible Combinations: 3 septillion



Ilene15Amazing!

HOW SECURE IS MY PASSWORD?



SHOW SETTINGS

It would take a desktop PC about
157 billion years
to crack your password

[Tweet Result]

HIDE DETAILS

Length: 15 characters

Character Combinations: 77

Calculations Per Second: 4 billion

Possible Combinations: 19 octillion



The Same Rules Apply: Turn the Volume to Eleven

- Longer is stronger
 - Microsoft recommends **14 characters**
- More complexity is better
 - Include upper case, lower case, punctuation, symbols, and numbers
 - Password cracking software checks for common letter-to-symbol conversions, such as “to” → 2
- Use different passwords
 - Work is different from banking is different from social media is different from email is different from spouse’s
- Change your passwords often
 - Set an automatic reminder for yourself to change passwords on your high-risk accounts at least every three months



Remember...

i shall use strong passwords.

I shall! u53 \$4r0ng-p@5sw0rdz!

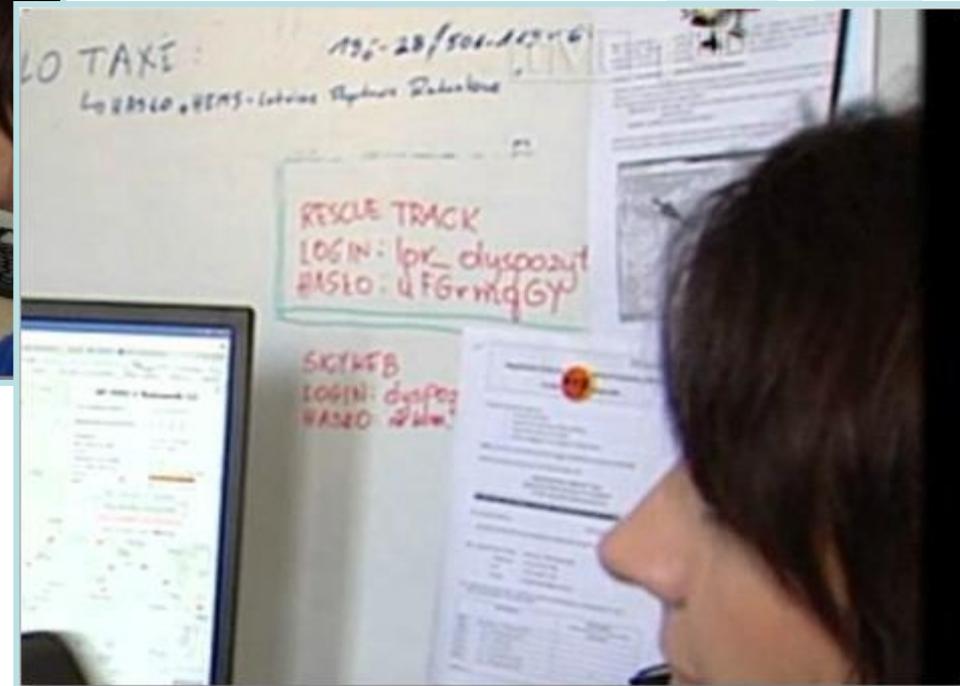
x	0	x
0	x	x
0	0	x

Strong passwords are a minimum of 8 characters in length & include uppercase, lowercase, numbers & special characters.



Tip: Before being interviewed on TV, wipe passwords off whiteboard

- The following screenshot is from a broadcast on TVP (Polish television)



Hasło is Polish for “Password”



More Cowbell (Supplemental Info)

City of Phoenix



The Power of Social Media

- April 23: AP Twitter account was hacked
- False message claimed there had been two explosions at the White House and that President Obama had been injured
- Just after 1 p.m. ET, the Dow Jones industrial average dropped about 130 points
 - It quickly bounced back as the truth came out

REPORT: AP TWITTER ACCOUNT HACKED...

Says Obama injured in White House explosion...

DOW Tanks on Fake Tweet...





So In Response to the Twitter PW Hack...

www.ismytwitterpasswordsecure.com

IS YOUR TWITTER PASSWORD SECURE?

It's a scary world right now, guys. Your Twitter password can cause the Dow Jones to drop nearly 150 points and compel dozens of blogs to write breathless posts about the future of online journalism. You should be worried.

In order to help everyone out a little, we've created an algorithm that will examine your password and tell you if it's secure enough. Spoiler alert: it isn't.

 Remember me - [Forgot password?](#)



If You Enter Anything, You Get...

www.ismytwitterpasswordsecure.com

**NO NO NO NO NO
NO NO NO DON'T BE AN IDIOT.**

Do you see "twitter.com" in the address bar? No, you don't. Don't ever type your login and password to Twitter on a site that isn't twitter.com. Same with Facebook. And LinkedIn. I guess what I'm trying to say here is, don't be an idiot.

 Tweet 3,535

Made, with apologies, by Alastair Coote. No offense to anyone that has been caught by a phishing attack. We all have our bad moments.



Why Password Management is Important



- Scale and speed of cyber-attacks is escalating
 - 855 data breach incidents: 174 million compromised records (2011)
- Average annualized cost of cybercrime to U.S. organizations is now \$8.9 million
 - Up 6% from last year
- 30,000 URLs (websites) are infected every day
 - 80% of those infected sites are legitimate
- 85% percent of all malware comes from the web
 - Includes viruses, worms, spyware, adware and Trojans
- Drive-by downloads have become the top web threat



Top 25 leaked passwords of 2012

1.password (unchanged)	2.123456 (unchanged)	3.12345678 (unchanged)	4.abc123 (up one)	5.qwerty (down one)
6.monkey (unchanged)	7.letmein (up one)	8.dragon (up two)	9.111111 (up three)	10.baseball (up one)
11.iloveyou (up two)	12.trustno1 (down three)	13.1234567 (down six)	14.sunshine (up one)	15.master (down one)
16.123123 (up four)	17. <u>welcome</u> (new entry!)	18.shadow (up one)	19.ashley (down three)	20.football (up five)
21. <u>jesus</u> (new entry!)	22.michael (up two)	23. <u>ninja</u> (new entry!)	24. <u>mustang</u> (new entry!)	25. <u>password1</u> (new entry!)



Avoid Common Password Pitfalls



- Avoid creating passwords that use
 - Dictionary words in any language
 - Words spelled backwards, common misspellings, and abbreviations
 - Sequences or repeated characters. Examples: 12345678, 222222, abcdefg, or adjacent letters on your keyboard (qwerty)
 - Personal information
 - Examples: Your name, family names and birthdates, driver's license, dog's SSN, or similar information

Test Your Password		Minimum Requirements
Password:	<input type="text" value="Phoenix20"/>	<ul style="list-style-type: none"> • Minimum 8 characters in length • Contains 3/4 of the following items: <ul style="list-style-type: none"> - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	<input type="checkbox"/>	
Score:	<div style="background-color: yellow; width: 64%; display: inline-block;">64%</div>	
Complexity:	Strong	

Test Your Password		Minimum Requirements
Password:	<input type="text" value="@Ph03nix20"/>	<ul style="list-style-type: none"> • Minimum 8 characters in length • Contains 3/4 of the following items: <ul style="list-style-type: none"> - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	<input type="checkbox"/>	
Score:	<div style="background-color: green; width: 99%; display: inline-block;">99%</div>	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	$+(n*4)$	<input type="text" value="9"/>	+ 36
Uppercase Letters	Cond/Incr	$+\left(\frac{len-n}{2}\right)$	<input type="text" value="1"/>	+ 16
Lowercase Letters	Cond/Incr	$+\left(\frac{len-n}{2}\right)$	<input type="text" value="6"/>	+ 6
Numbers	Cond	$+(n*4)$	<input type="text" value="2"/>	+ 8
Symbols	Flat	$+(n*6)$	<input type="text" value="0"/>	0
Middle Numbers or Symbols	Flat	$+(n*2)$	<input type="text" value="1"/>	+ 2
Requirements	Flat	$+(n*2)$	<input type="text" value="4"/>	+ 8

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	$+(n*4)$	<input type="text" value="10"/>	+ 40
Uppercase Letters	Cond/Incr	$+\left(\frac{len-n}{2}\right)$	<input type="text" value="1"/>	+ 18
Lowercase Letters	Cond/Incr	$+\left(\frac{len-n}{2}\right)$	<input type="text" value="4"/>	+ 12
Numbers	Cond	$+(n*4)$	<input type="text" value="4"/>	+ 16
Symbols	Flat	$+(n*6)$	<input type="text" value="1"/>	+ 6
Middle Numbers or Symbols	Flat	$+(n*2)$	<input type="text" value="3"/>	+ 6
Requirements	Flat	$+(n*2)$	<input type="text" value="5"/>	+ 10

Deductions				
Letters Only	Flat	$-n$	<input type="text" value="0"/>	0
Numbers Only	Flat	$-n$	<input type="text" value="0"/>	0
Repeat Characters (Case Insensitive)	Comp	-	<input type="text" value="0"/>	0
Consecutive Uppercase Letters	Flat	$-(n*2)$	<input type="text" value="0"/>	0
Consecutive Lowercase Letters	Flat	$-(n*2)$	<input type="text" value="5"/>	- 10
Consecutive Numbers	Flat	$-(n*2)$	<input type="text" value="1"/>	- 2
Sequential Letters (3+)	Flat	$-(n*3)$	<input type="text" value="0"/>	0
Sequential Numbers (3+)	Flat	$-(n*3)$	<input type="text" value="0"/>	0
Sequential Symbols (3+)	Flat	$-(n*3)$	<input type="text" value="0"/>	0

Deductions				
Letters Only	Flat	$-n$	<input type="text" value="0"/>	0
Numbers Only	Flat	$-n$	<input type="text" value="0"/>	0
Repeat Characters (Case Insensitive)	Comp	-	<input type="text" value="2"/>	- 1
Consecutive Uppercase Letters	Flat	$-(n*2)$	<input type="text" value="0"/>	0
Consecutive Lowercase Letters	Flat	$-(n*2)$	<input type="text" value="2"/>	- 4
Consecutive Numbers	Flat	$-(n*2)$	<input type="text" value="2"/>	- 4
Sequential Letters (3+)	Flat	$-(n*3)$	<input type="text" value="0"/>	0
Sequential Numbers (3+)	Flat	$-(n*3)$	<input type="text" value="0"/>	0
Sequential Symbols (3+)	Flat	$-(n*3)$	<input type="text" value="0"/>	0

Legend
Exceptional: Exceeds minimum standards. Additional bonuses are applied.
Sufficient: Meets minimum standards. Additional bonuses are applied.
Warning: Advisory against employing bad practices. Overall score is reduced.
Failure: Does not meet the minimum standards. Overall score is reduced.

Legend
Exceptional: Exceeds minimum standards. Additional bonuses are applied.
Sufficient: Meets minimum standards. Additional bonuses are applied.
Warning: Advisory against employing bad practices. Overall score is reduced.
Failure: Does not meet the minimum standards. Overall score is reduced.



**LONGER
PASSWORDS**

MAKE

**STRONGER
PASSWORDS**



<http://pwnedList.com/>



Prevent account hijacking today!

29,577,575

e-mail address & password combinations collected

2,208 credentials leaks collected
966,231,281 passwords collected
168,602,891 emails collected

Have your accounts been compromised? Find out.

PwnedList is a tool that allows an average person to check if their accounts have been compromised. You can read more about where our data comes from [here](#). Just enter an email address associated with any of your accounts to see if it's on our list. Data entered is not stored, re-used, or given to any third parties. Don't trust us? You can also use a SHA-512 hash of your email as input. Just don't forget to lowercase all characters first.



The Truth about Data Breaches

MOST AREN'T...

Like you see in the movies. The chances are that you're not facing genius hackers exploiting your fancy new mobile and cloud services.

HIGH TECH

Most attacks are actually quite unsophisticated and conducted from a distance — often Eastern Europe. Only 7% involve physical attacks — and most of those are ATM skims.

79%

OF ATTACKS ARE OPPORTUNIST

INSIDE JOBS

Fewer attacks than ever are deliberate "inside jobs" by employees or partners misusing privileges — though lost devices is a common cause.

5%

OF ATTACKS INVOLVE MISUSE OF PRIVILEGES

SPOTTED INTERNALLY

Most breaches go undetected by the affected company; they're often pointed out by law enforcement, auditors or payment card companies.

8%

OF INCIDENTS DISCOVERED BY INTERNAL STAFF

MOST ARE...

Pretty mundane. They rely on simple vulnerabilities like weak passwords and web exploits — and often sit unnoticed for years.

EASILY PREVENTABLE

Easy-to-guess passwords are one of the most common exploits used by criminals.

97%

OF ATTACKS AVOIDABLE BY SIMPLE OR INTERMEDIATE CONTROLS

DUE TO HUMAN ERROR

When attacks are targeted, humans are often the weak point. Watch out for phishing and other social engineering attacks.

22%

OF INCIDENTS IN LARGER ORGANIZATIONS INVOLVED SOCIAL TACTICS

ABOUT THE MONEY

Criminals want money — so POS systems and customer payment details are the most common targets.

96%

OF ATTACKS ARE MOTIVATED BY FINANCIAL OR PERSONAL GAIN

LONG TERM

While attacks typically breach security within minutes, they're often not spotted for months or even years.

85%

OF ATTACKS TOOK WEEKS OR MORE TO DISCOVER

- Source: Verizon Data Breach Report, 2004–2012