Password Management 201

Passphrase

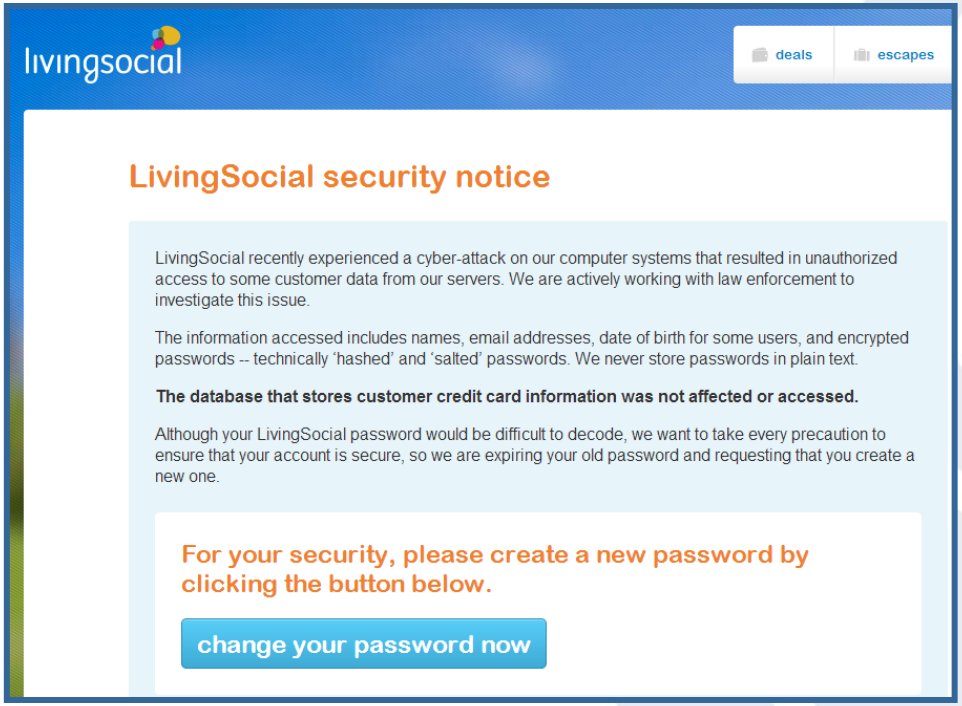
June 2013

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



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

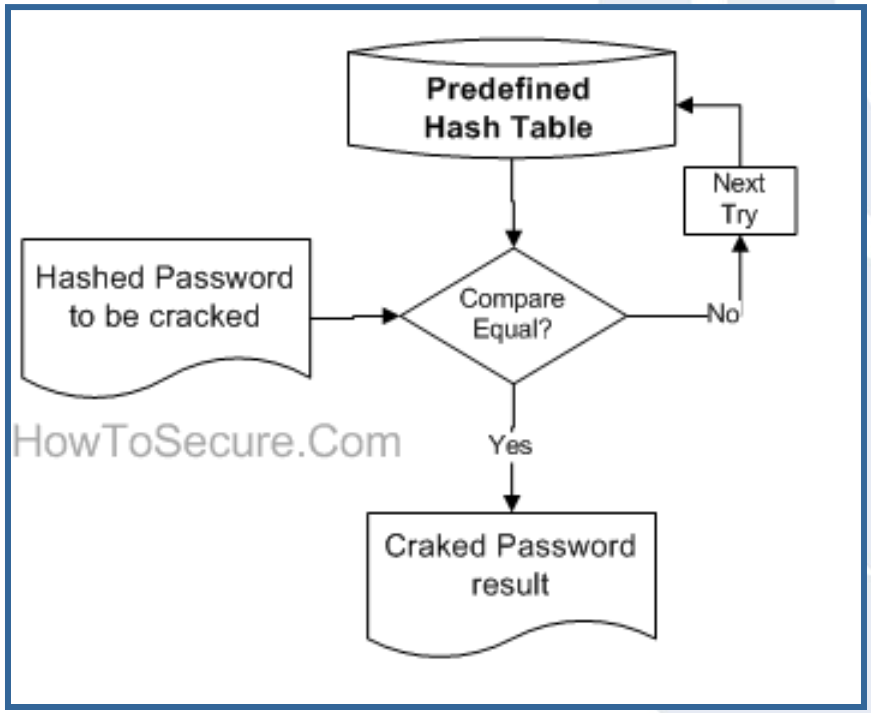
- One-way encryption – can't decrypt
  - Has no key
- Primary use is for message integrity
  - By comparing hash values, you can see if message sent = message received

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.

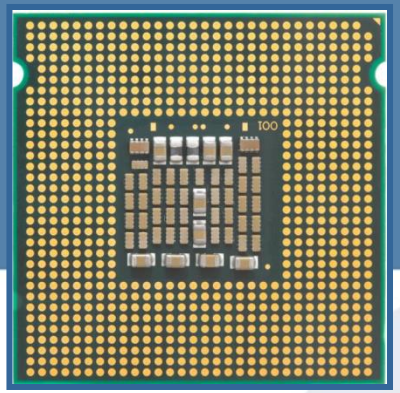
A password breach should be viewed as a raging inferno in a building and any security measures in place are analogous to fire-resistant building materials and sprinklers in a warehouse full of flammable goods - they only buy time for the occupants to escape, they don't make it safe to remain inside the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

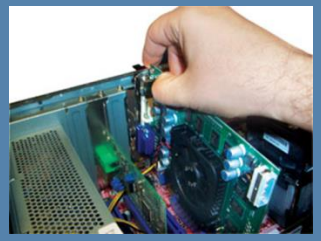
GPU

- 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

Phoenix1


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.

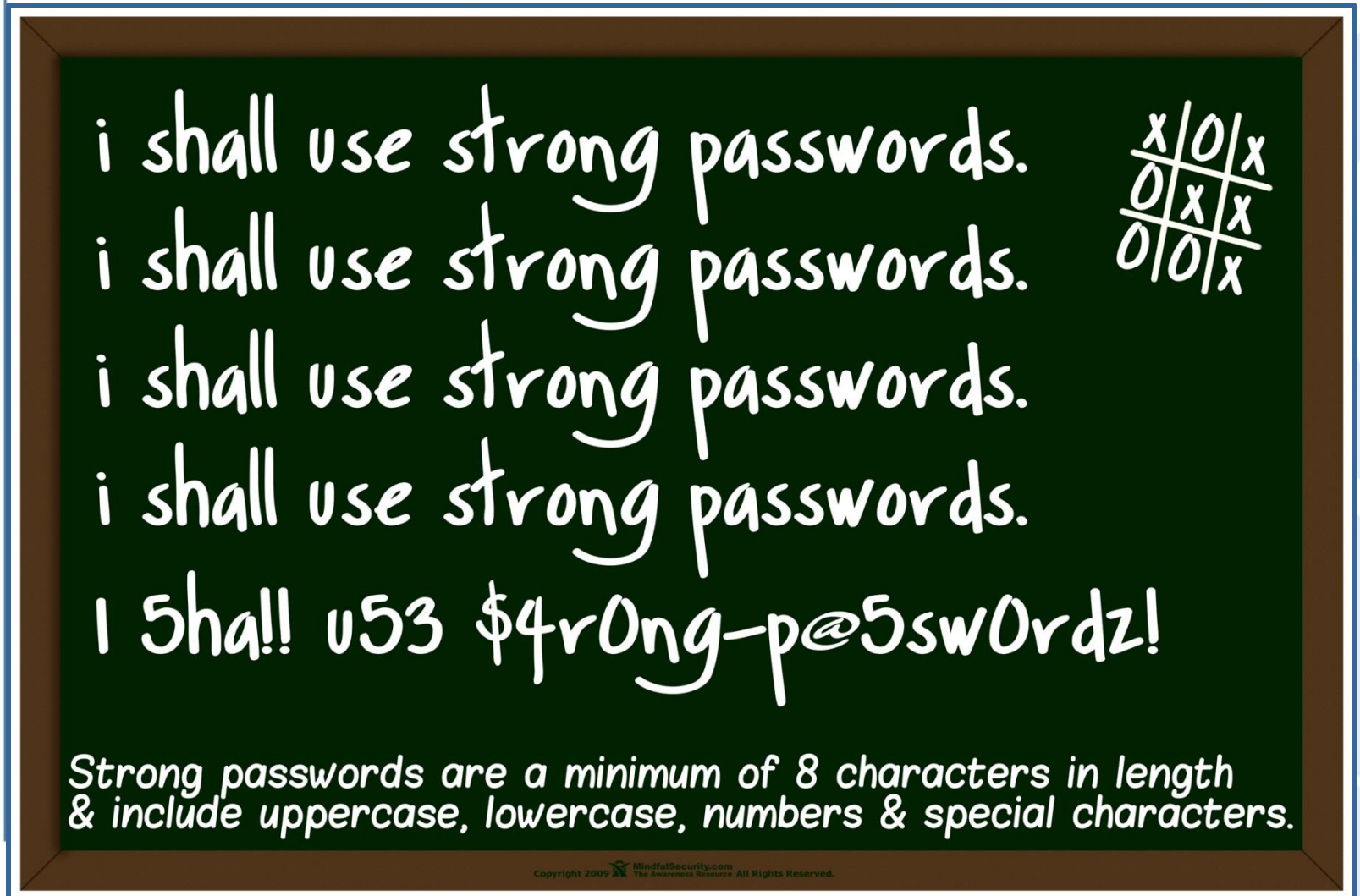
RandellisGr8!

Ilene15Amazing!

The Same Rules Apply:
Turn the Volume to Eleven

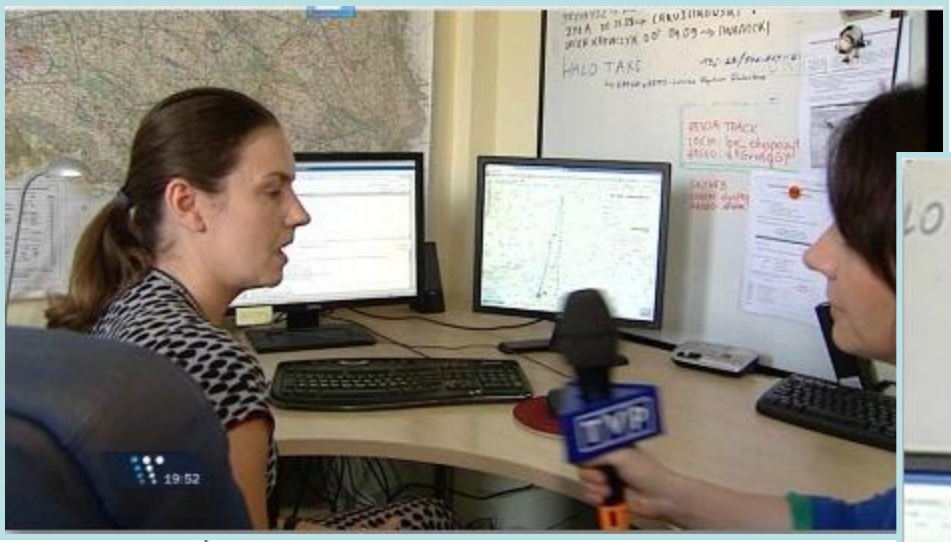
- Longer is stronger
  - Microsoft recommends 14 characters
- More complexity is better
  - Include upper case, lower case, punctuation, symbols, and numbers
  - Password cracking software checks for common letter-to-symbol conversions, such as “to” → 2
- Use different passwords
  - Work is different 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

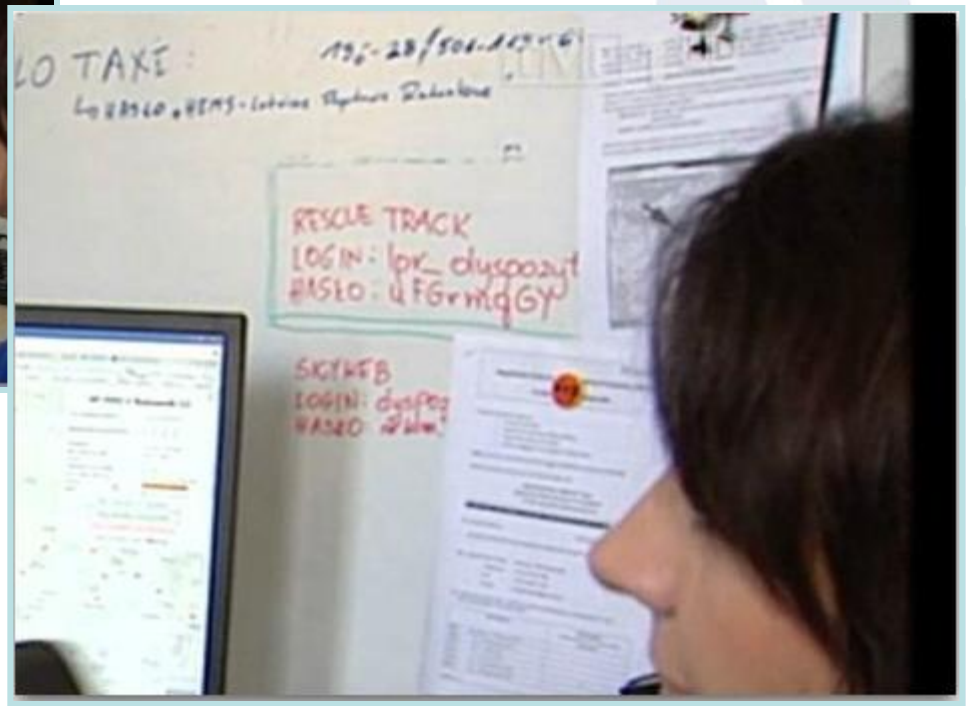
Remember…


i shall use strong passwords.
i shall use strong passwords.
i shall use strong passwords.
i shall use strong passwords.
I 5ha!! u53 $4rOng-p@5swOrdz!
Strong passwords are a minimum of 8 characters in length & include uppercase, lowercase, numbers & special characters.
Copyright 2009 MindfulSecurity.com The Awareness Resource All Rights Reserved.

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)

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…

If You Enter Anything, You Get…

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.welcome (new entry!)	18.shadow (up one)	19.ashley (down three)	20.football (up five)
21.jesus (new entry!)	22.michael (up two)	23.ninja (new entry!)	24.mustang (new entry!)	25.password1 (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:	Phoenix20	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	64%	
Complexity:	Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	9	+ 36
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 16
Lowercase Letters	Cond/Incr	+((len-n)*2)	6	+ 6
Numbers	Cond	+(n*4)	2	+ 8
Symbols	Flat	+(n*6)	0	0
Middle Numbers or Symbols	Flat	+(n*2)	1	+ 2
Requirements	Flat	+(n*2)	4	+ 8
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	0	0
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	5	- 10
Consecutive Numbers	Flat	-(n*2)	1	- 2
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	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.

Test Your Password		Minimum Requirements
Password:	@Ph03nix20	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	99%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	10	+ 40
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 18
Lowercase Letters	Cond/Incr	+((len-n)*2)	4	+ 12
Numbers	Cond	+(n*4)	4	+ 16
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	2	- 4
Consecutive Numbers	Flat	-(n*2)	2	- 4
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	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.


LONGER
PASSWORDS
MAKE
STRONGER
PASSWORDS
Copyright 2010 MindfulSecurity.com The Awareness Resource All Rights Reserved.

http://pwnedlist.com/

pwned List

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

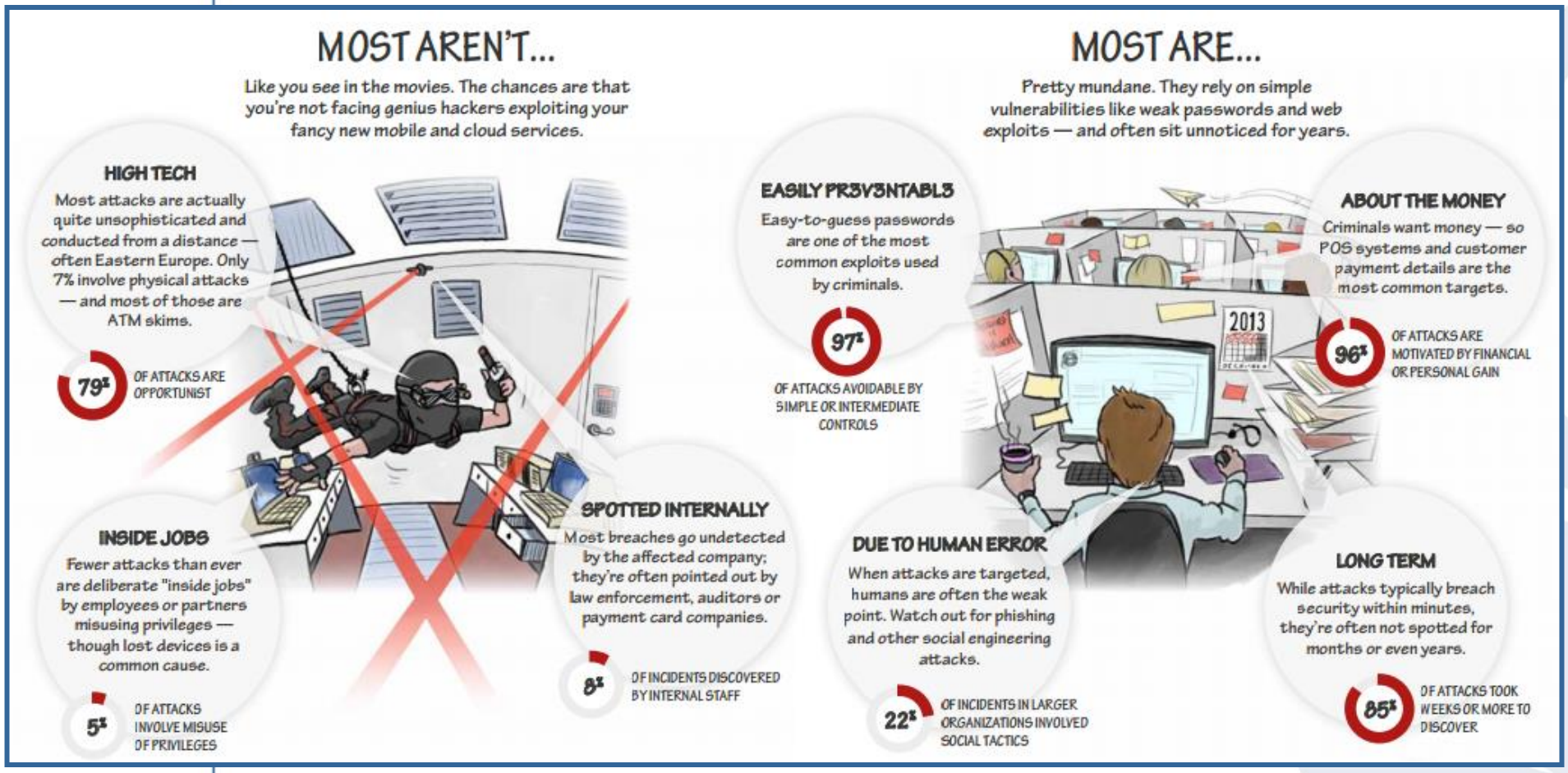
Have your accounts been compromised? Find out.

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.

Email

CHECK

The Truth about Data Breaches



- Source: Verizon Data Breach Report, 2004–2012