(Almost) everything about passwords that OWASP won’t teach you.

Per Thorsheim
OWASP Cheat Sheets

- Password Storage Cheat Sheet
- Authentication Cheat Sheet
- Forgot Password Cheat Sheet
- Pinning Cheat Sheet
Things I hate:
1. Vandalism
2. Irony
3. Lists.
Work / Life Flowchart.
(As a CISO)
Account creation form @ikea

Please enter preferred username + password.
Online bank in Kuwait

Password

- The password remains your most important line of protection. It is used for login and to perform transactions in KFHOnline. Please keep it to yourself.
- We highly recommend that you use the provided virtual keyboard with randomly ordered keys to deter others from identifying your password.

Please enter the password

Password: [Enter]
Usability in a nutshell
Per Thorsheim
Phone: +47 90 99 92 59
Lovasbakken 37
N-5145 Fyllingsdalen
Norway
Passwords are *everywhere*
Woo hoo! Your password has been changed! Please be sure to memorize it or note it in a safe place.

Proceed to your account

username: QwEAsDzxC!2#4
password: WPA PSK: 'EndJGhJgwcsNDcxN2BvVGPLZCWXdQU363VC'
WPS PIN: '39740328'

INTERNET – GUEST NET IN THE RECEPTION has installed an internet guest net in the reception area.
17yr teens – pick your PIN

Girls
1996

Boys
1337
1996
Digit distribution for PINs

4-digit memorable

4-digit non-memorable

7-digit memorable

Digit 0 is not «random» enough?

Digit 6 is hard to remember?

Thank you to Andrey Bogdanov, Sondre Rønjom & Jan Fredrik Leversund for great help!
A birthday present every eleven wallets? The security of customer-chosen banking PINs
http://www.cl.cam.ac.uk/~jcb82/doc/BPA12-FC-banking_pin_security.pdf
http://www.cl.cam.ac.uk/~jcb82/doc/BPA12-FC-banking_pin_security-slides_ss.pdf

Daniel Amitay: 
http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes

Radical.org/pinmap
By @kluzz

Heatmapping PINs

Rockyou

iPhone

Physical access
Control system
Look, and you shall see... PINs.
Guess What?

YOU ARE PREDICTABLE!
What's the value of a password?
Consequences?

Tuesday, June 5, 2012, on Twitter:

CrackMeIfYouCan Something BIG is brewing. CHANGE YOUR PASSWORD NOW on all major sites. Yes, those CAPS are on purpose ;)  
8:00 PM Jun 5th from web
Lessons from Linkedin

LINKEDIN: BASE WORDS

The Linkedin list containing 5.8 million unique password hashes is now over 90% cracked. These are the top words users are basing their passwords on.

TOP 15 BASE WORDS USED IN LINKEDIN PASSWORDS

<table>
<thead>
<tr>
<th>Base Word</th>
<th>Unique User Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>linkedin</td>
<td>56,193</td>
</tr>
<tr>
<td>love</td>
<td>21,042</td>
</tr>
<tr>
<td>anna</td>
<td>12,996</td>
</tr>
<tr>
<td>pask</td>
<td>8058</td>
</tr>
<tr>
<td>linked</td>
<td>7909</td>
</tr>
<tr>
<td>jack</td>
<td>7298</td>
</tr>
<tr>
<td>blue</td>
<td>7234</td>
</tr>
<tr>
<td>john</td>
<td>6676</td>
</tr>
<tr>
<td>mark</td>
<td>5535</td>
</tr>
<tr>
<td>mike</td>
<td>5424</td>
</tr>
<tr>
<td>chris</td>
<td>5050</td>
</tr>
<tr>
<td>nick</td>
<td>4731</td>
</tr>
<tr>
<td>paul</td>
<td>4499</td>
</tr>
<tr>
<td>password</td>
<td>4489</td>
</tr>
</tbody>
</table>

BAD PASS PHRASES FOUND ON LINKEDIN

- You’ll never walk alone
- The light shines in the darkness
- The word truth sets you free
- Save the cheerleader save the world
- There is no tore but what we make
- Jesus chavez supernar
- Big trouble in little china
- What the fck is happening
- Forever blowing bubbles
- Work smarter not harder
- You are my sunshine <3
- I need a vacation
- You get what you give
- crispness appliance
- Everything is destroyed

LINKEDIN: POP COLORS

The leaked list containing over 5.8 million password hashes from Linkedin is now over 90% cracked. These are the top colors represented in users’ passwords.

- Black: 281
- Red: 417
- Blue: 304
- Green: 665
- Purple: 398
- Yellow: 998

TOP COLORS USED IN LINKEDIN PASSWORDS

- Black: 281
- Red: 417
- Blue: 304
- Green: 665
- Purple: 398
- Yellow: 998

- Numbers = unique user passwords
- * Can this be connected to Linkedin?
Mobile Usability #1

Oh Please GOD, NO CAPTCHAS ON PHONES! EVER!

Keys to small.

FINGERS TOO BIG!

Oh Please GOD, NO CAPTCHAS ON PHONES! EVER!

Introduction to app should include security features?

PIN on Phone = equals PIN on Dropbox! (Why no other options for the paranoid?)
Foursquare — Verify mail account
Unknown address, or wrong format?
Can we verify mail addresses?
Default do not show password?
Do not remember password?
Display password option = GOOD! (Default on?)
Tip For Mobile Usability:

Johansen 56426736
The password you entered is not valid

Please note that the password must respect the following rules:

- It must contain between 7 and 32 characters. Use only characters from the following set: ! # $ % & * ( ) + , - . / 0123456789 : ; < = > ? @ ABCDEFGHIJKLMNOPQRSTUVWXYZ [ ] _ ` abcdefghijklmnopqrstuvwxyz { } ~
- It must contain at least 1 lowercase letter(s) (abcdefghiklmnopqrstuvwxyz).
- It must contain at least 1 capital letter(s) (ABCDEFGHIJKLMNOPQRSTUVWXYZ).
- It must contain at least 1 numeric character(s) (0123456789).
- It must not contain more than 2 identical consecutive characters (AAA, iii, $$$$$ ...).
- It must not contain your user name.
- It must not contain your email address.
- It must not contain your first name.
- It must not contain your last name.

STARTING TODAY, ALL PASSWORDS MUST CONTAIN LETTERS, NUMBERS, DOODLES, SIGN LANGUAGE AND SQUIRREL NOISES.
Google kontoer

Google kontonavn og passord lar deg bruke alt fra Google.

Bruk Google på din

Konfigurer profilen din og innstillinger.

Passordtyper: For kort

Bruk minst åtte tegn, ikke bruk et passord fra et annet nettsted, eller noe allfor opplagt, som navnet på kjæledyrnet ditt. Hvorfor?

Ta med deg alt

Bytt mellom enheter, og fortsett der du slapp.
Give sound advice -- Recommend 2FA
«Secret» Mail + Phone #

Facebook 2FA in use! 😊
Starttls.info

RFC 2487 -> RFC 3207

Transparent opportunistic encryption using SSL/TLS between to SMTP servers

RFC requires public servers to accept sending & receiving plaintext

Self-signed, expired, SSLv2, RC4, MD5, Anonymous DH, 40-56 bits encryption keys...

We’ve found the dark side of SSL!
(please contribute by testing domains.)
Operation Face Factor

- Unique opportunity (!)
- 5000+ «headshots»
- Passwords + other information available
- Analyze!
Categorization

Sex

Glasses (Y/N)

Hair color

Facial hair

Facial hair
No
Mustache
Small beard
Full beard
«Porn donut»
«Unix Guru»

Hair color
No 😊
«Blond»
Superblond
Brunette
Redhead
«Silver fox»
... and the results?

Women prefer length.

Men prefer wider selection (entropy).

«Unix gurus» have the worst passwords.
Getting hacked may be good?
PasswordsCon
Las Vegas, Aug 5-6
co-located with BSidesLV
Trondheim (Norge)
Dec 7-8
passwordscon.org
Applied Risk Analysis
A final note + video

«Never write down your password»
Thank you!

- in/thorsheim
- securitynirvana.blogspot.com
- @thorsheim
- /GodPraksis
- /user/thorsheim
- per.thorsheim
- Available on RedPhone for Android