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

Per Thorsheim

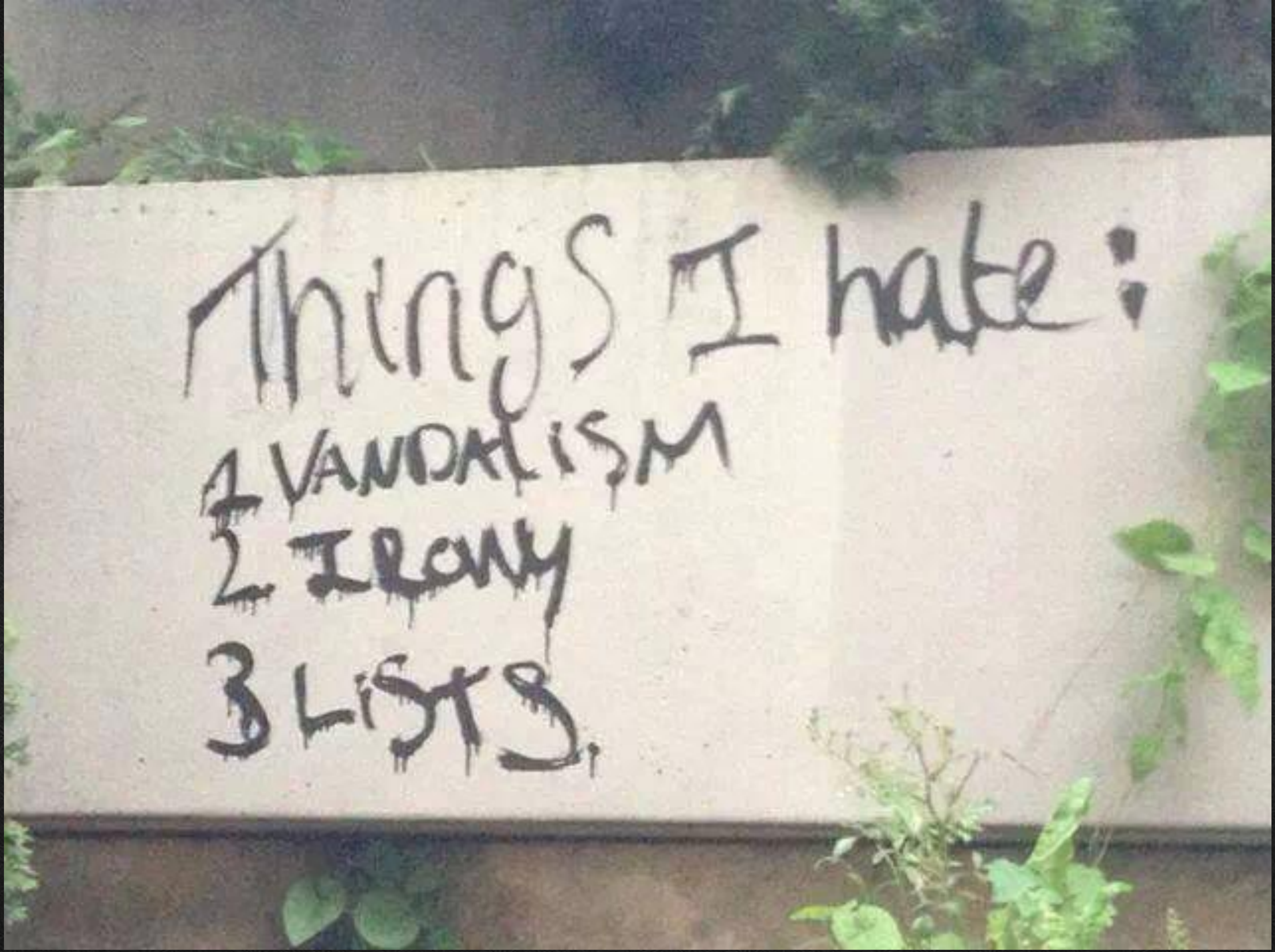
OWASP Cheat Sheets

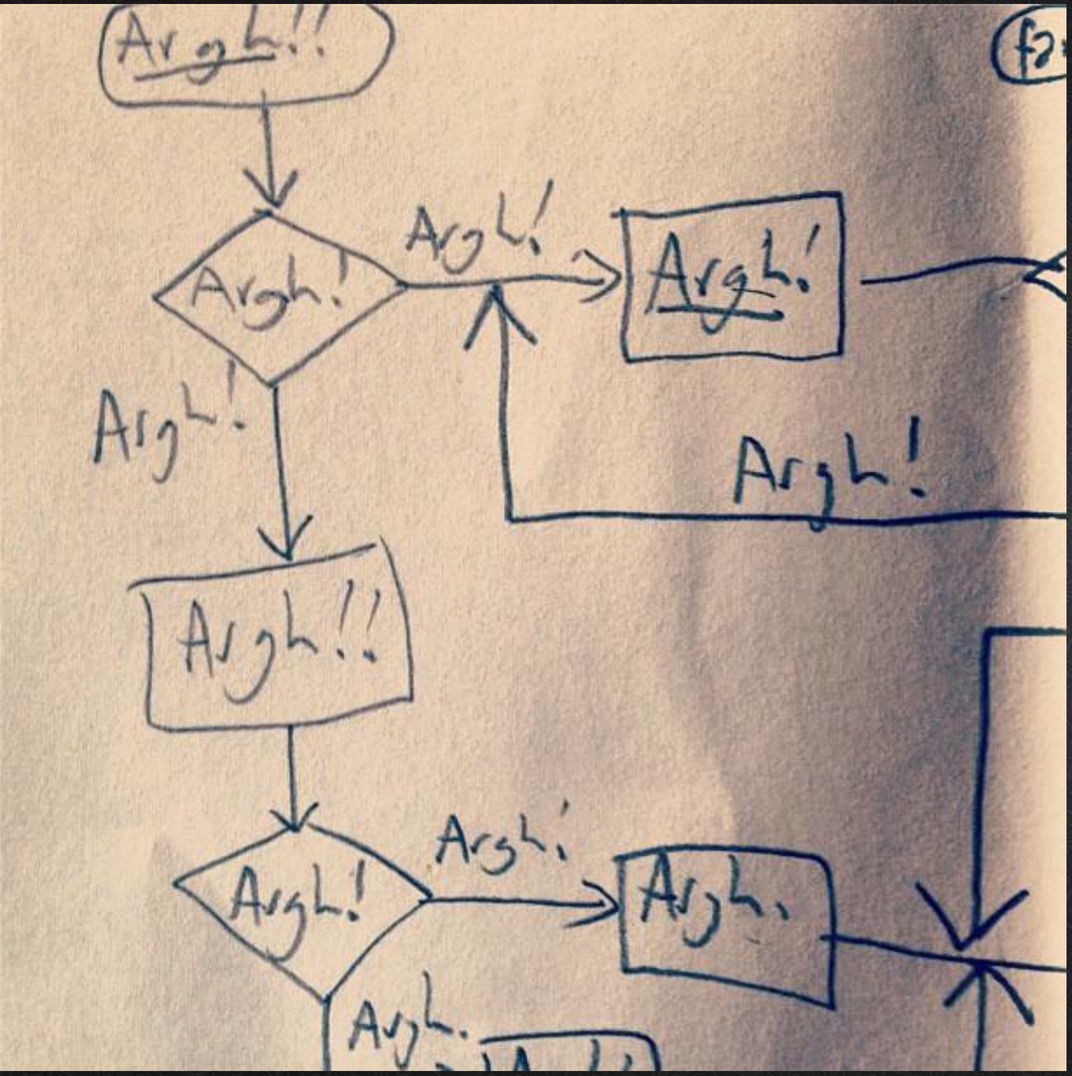
Password Storage Cheat Sheet

Authentication Cheat Sheet

Forgot Password Cheat Sheet

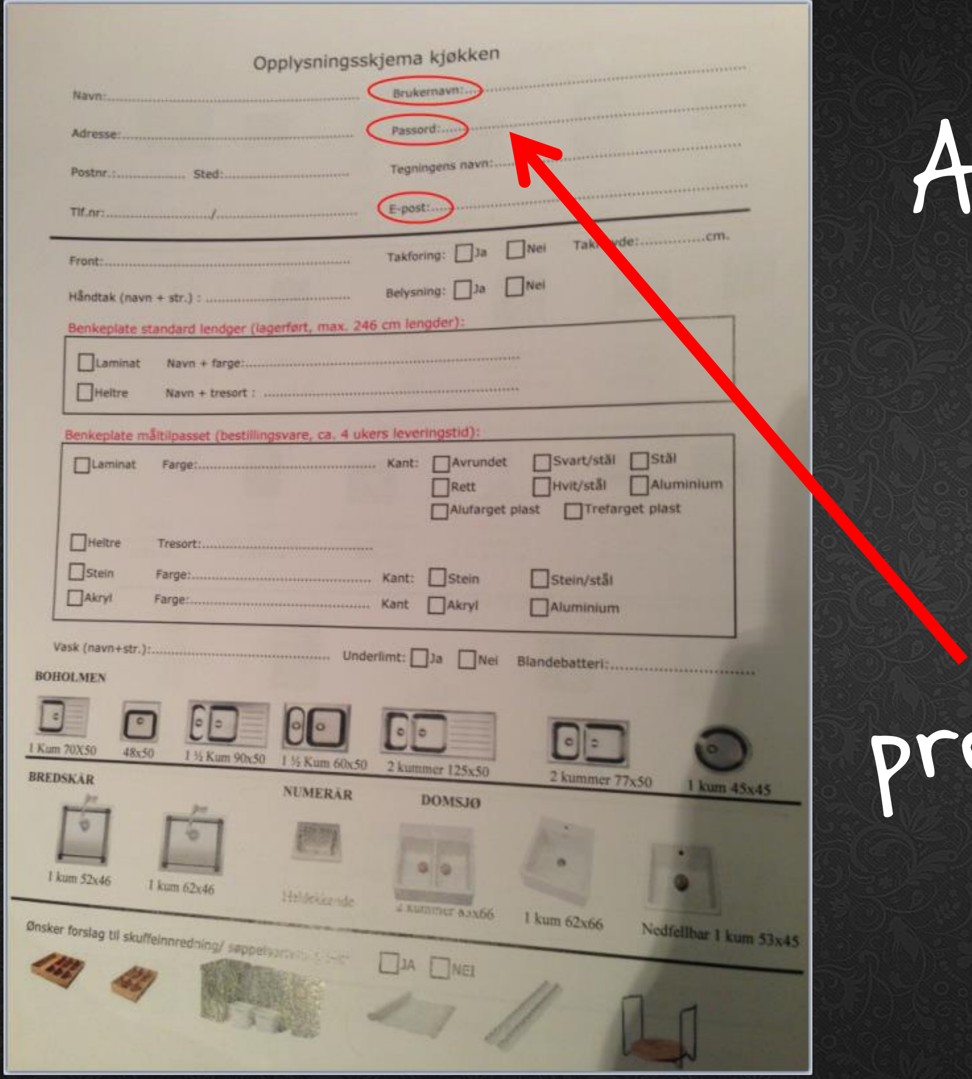
Pinning Cheat Sheet


Things I hate:
1 VANDALISM
2 IRONY
3 LISTS.



Work / Life Flowchart.

(As a CISO)



Opplysningsskjema kjøkken

Navn:........................ Brukernavn:........................

Adresse:........................ Passord:........................

Postnr.:.............. Sted:.............. Tegningens navn:........................

Tlf.nr:............/............ E-post:........................

Front:........................ Takforing: □Ja □Nei Takhøyde:..............cm.

Håndtak (navn + str.) : .... Belysning: □Ja □Nei

Benkeplate standard lengder (lagerført, max. 246 cm lengder):

□Laminat Navn + farge:........................

□Heltre Navn + tresort : ....

Benkeplate måltilpasset (bestillingsvare, ca. 4 ukers leveringstid):

□Laminat Farge:........................ Kant: □Avrundet □Svart/stål □Stål

□Rett □Hvit/stål □Aluminium

□Alufarget plast □Trefarget plast

□Heltre Tresort:........................

□Stein Farge:........................ Kant: □Stein □Stein/stål

□Akryl Farge:........................ Kant □Akryl □Aluminium

Vask (navn+str.):........................ Underlimt: □Ja □Nei Blandebatteri:........................

BOHOLMEN

1 Kum 70X50 48x50 1 ½ Kum 90x50 1 ½ Kum 60x50 2 kummer 125x50 2 kummer 77x50 1 kum 45x45

BREDSKÄR NUMERÄR DOMSJØ

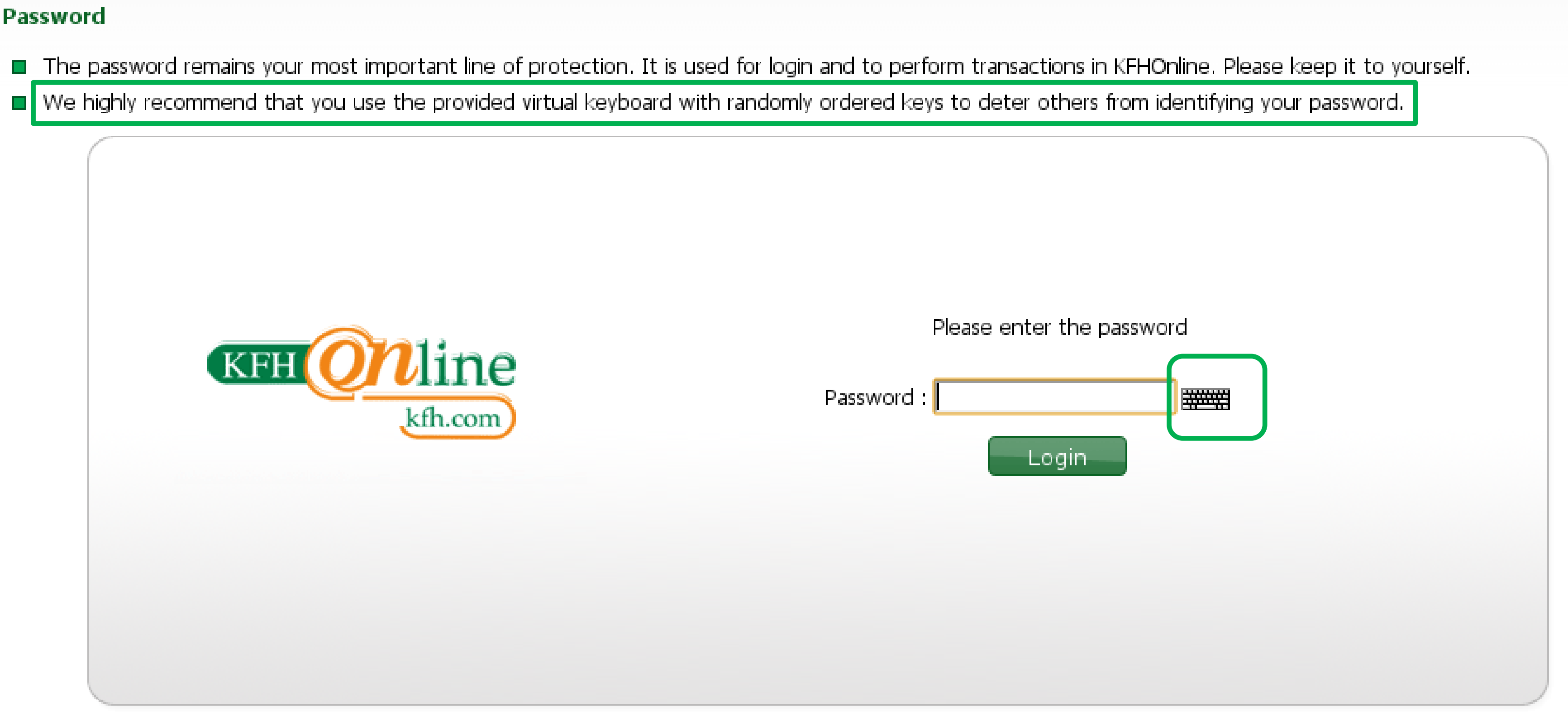
1 kum 52x46 1 kum 62x46 Heldekkende 2 kummer 83x66 1 kum 62x66 Nedfellbar 1 kum 53x45

Ønsker forslag til skuffeinnredning/ søppelsortering □JA □NEI

Account creation form @ikea

Please enter preferred username + password.

Online bank in Kuwait



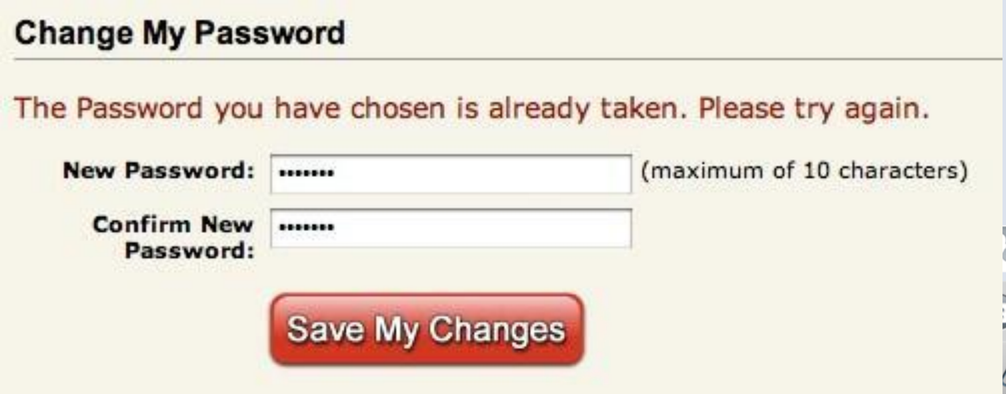
Password

- 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 :

Usability in a nutshell

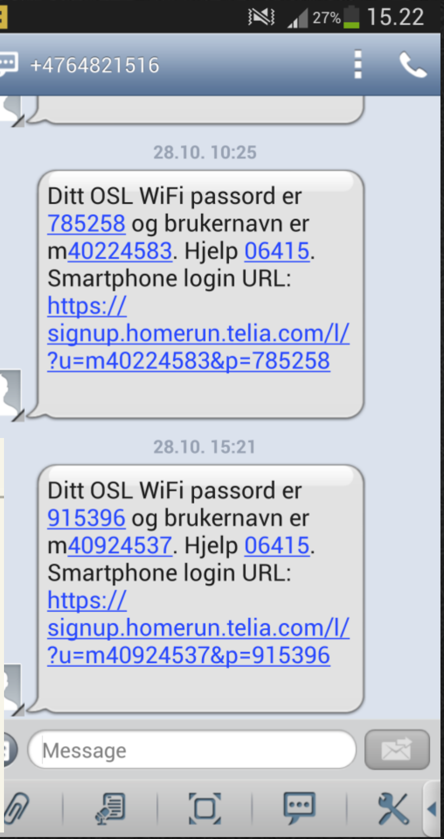


Change My Password

The Password you have chosen is already taken. Please try again.

New Password: ••••••• (maximum of 10 characters)

Confirm New Password: •••••••



28.10. 10:25

Ditt OSL WiFi passord er 785258 og brukernavn er m40224583. Hjelp 06415. Smartphone login URL: https://signup.homerun.telia.com/l/?u=m40224583&p=785258

28.10. 15:21

Ditt OSL WiFi passord er 915396 og brukernavn er m40924537. Hjelp 06415. Smartphone login URL: https://signup.homerun.telia.com/l/?u=m40924537&p=915396

1234

3268

5555

Per Thorsheim
Phone: +47 90 99 92 59
Lovasbakken 37
N-5145 Fyllingsdalen
Norway

8822

1971

8192

1433

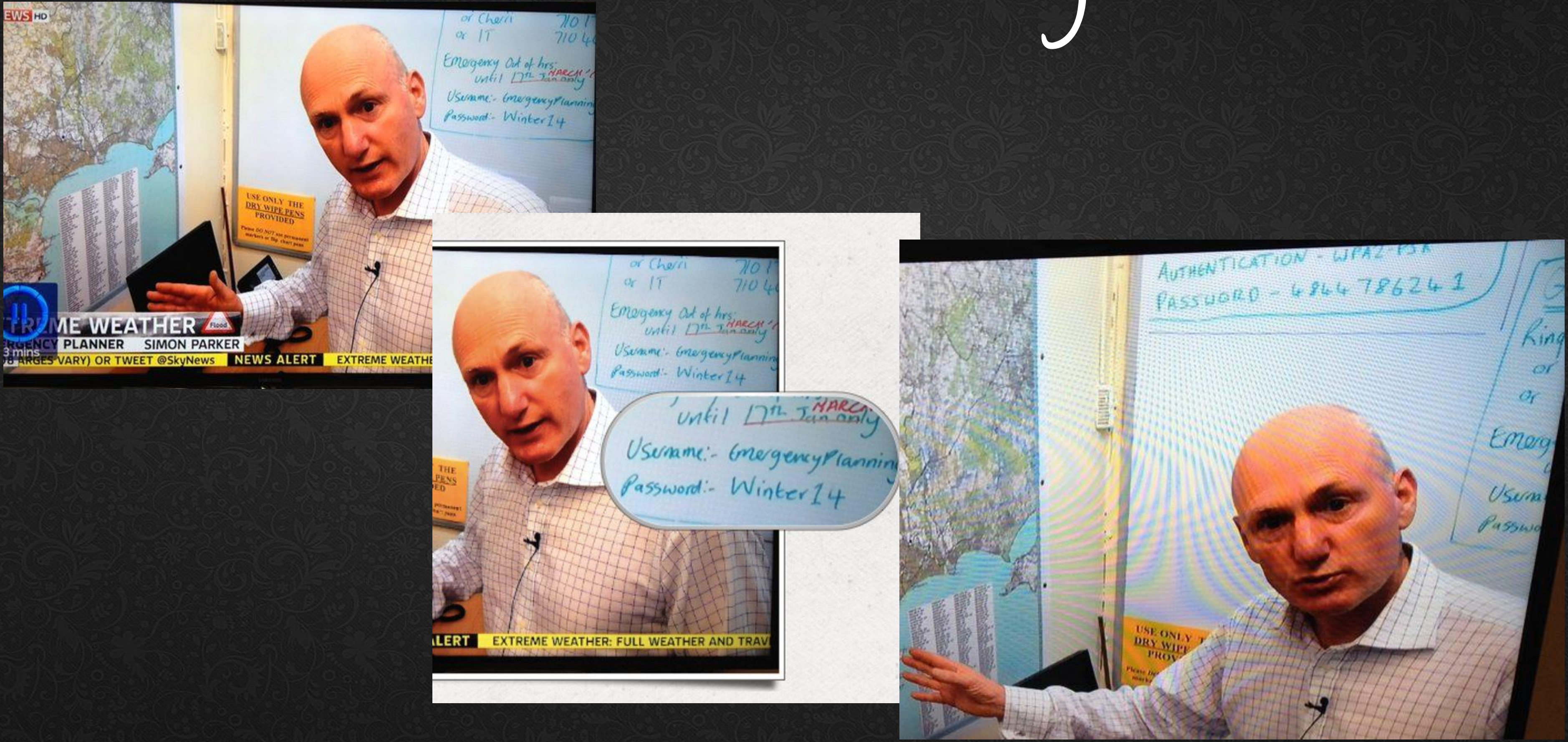
8897

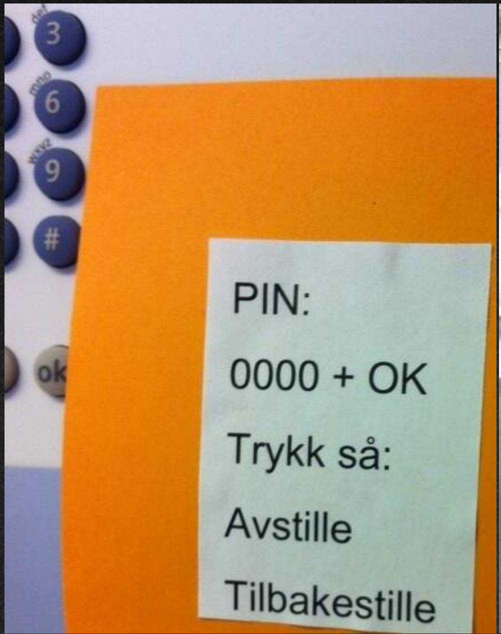
9999

5600

0000

Passwords are *everywhere*


EWS HD
or Cheri 710
or IT 710 4
Emergency Out of hrs
until 17th Jan only MARCH
Usename:- EmergencyPlanning
Password:- Winter14
USE ONLY THE DRY WIPE PENS PROVIDED
TREME WEATHER Flood
ERGENCY PLANNER SIMON PARKER
ARGES VARY) OR TWEET @SkyNews
NEWS ALERT
EXTREME WEATHER: FULL WEATHER AND TRAV
AUTHENTICATION - WPA2-PSK
PASSWORD - 4864478624 1



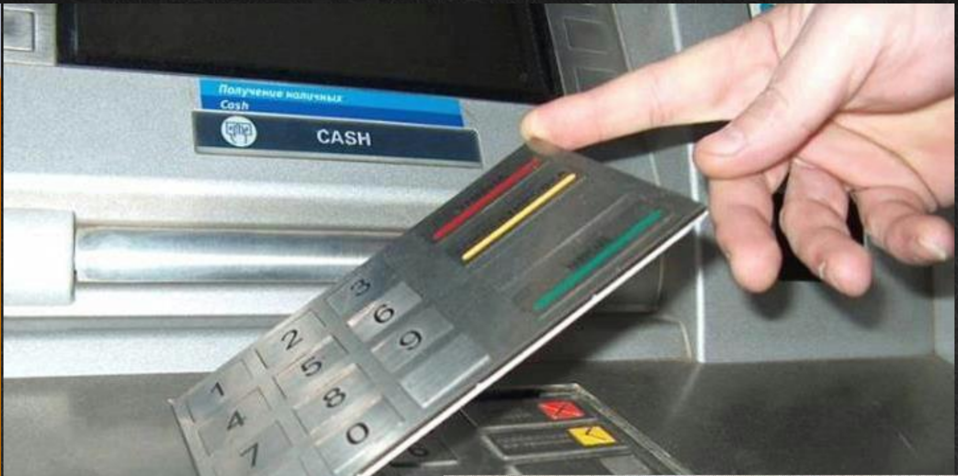
PIN:

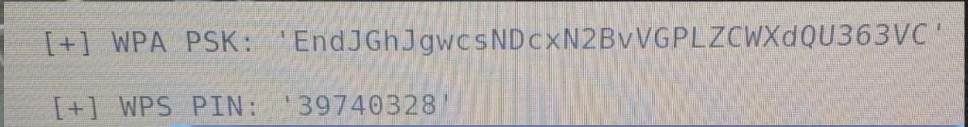
0000 + OK

Trykk så:

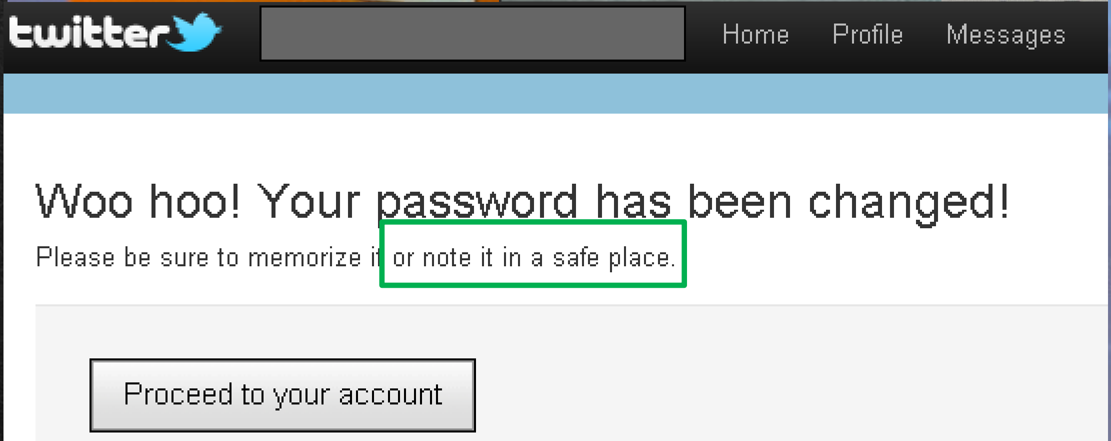
Avstille

Tilbakestille





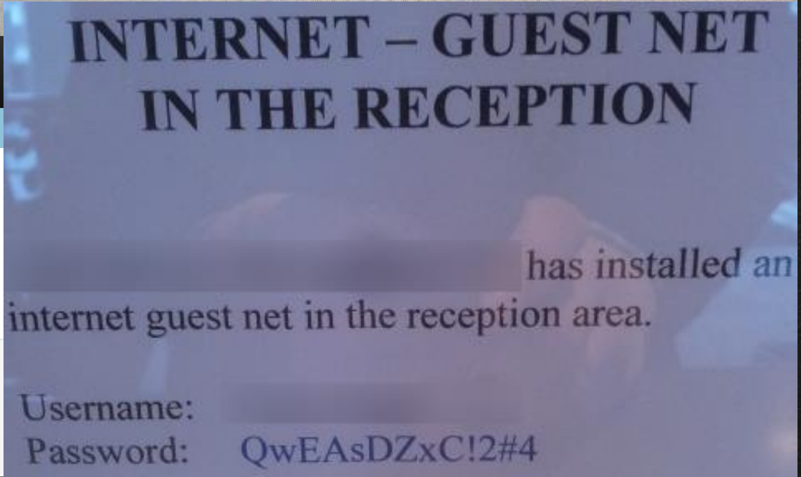
```
[+] WPA PSK: 'EndJGhJgwcsNDcxN2BvVGPLZCWXdQU363VC'
 [+] WPS PIN: '39740328'
```



Woo hoo! Your password has been changed!

Please be sure to memorize it or note it in a safe place.

Proceed to your account



INTERNET – GUEST NET IN THE RECEPTION

[redacted] has installed an internet guest net in the reception area.

Username: [redacted]
Password: QwEAsDZxC!2#4

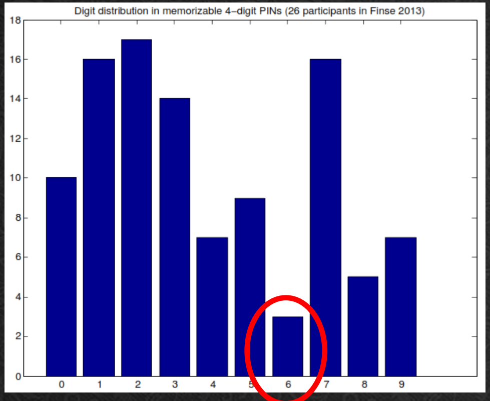
17yr teens – pick your PIN

Girls
1996

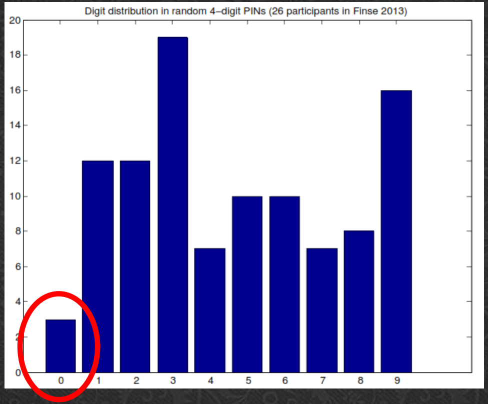
Boys
1337
1996

Digit distribution for PINs

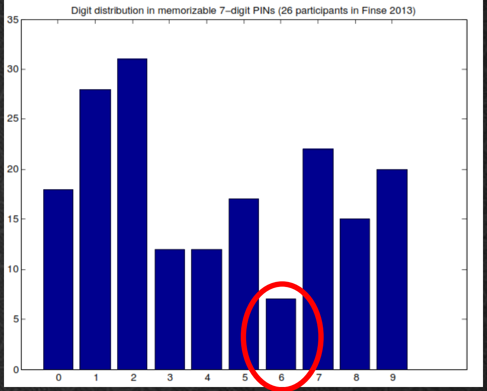
4-digit memorable



4-digit non-memorable



7-digit memorable



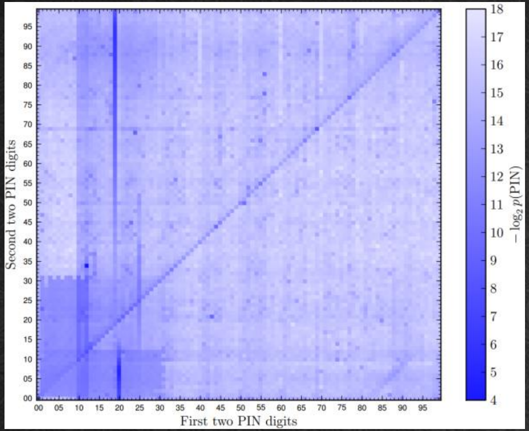
Digit 0 is not «random» enough?

Digit 6 is hard to remember?

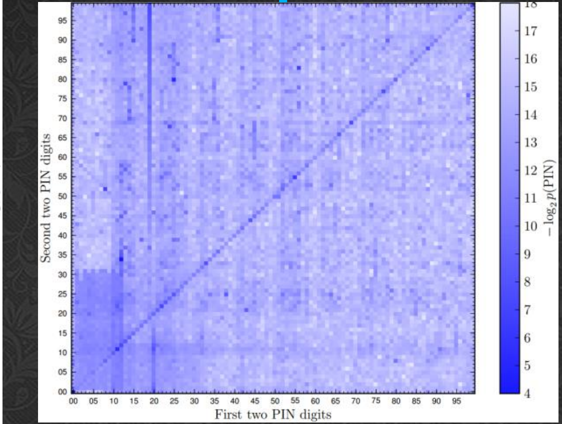
Thank you to Andrey Bogdanov, Sondre Rønjom & Jan Fredrik Leversund for great help!

Heatmapping PINs

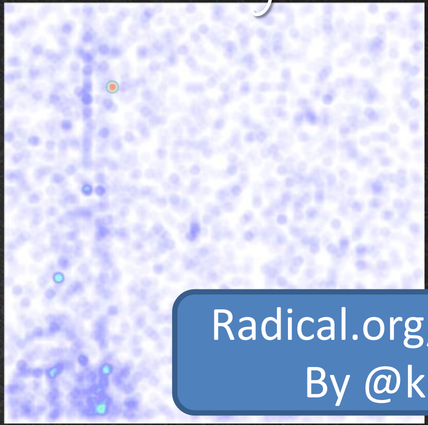
Rockyou



iPhone



Physical access Control system

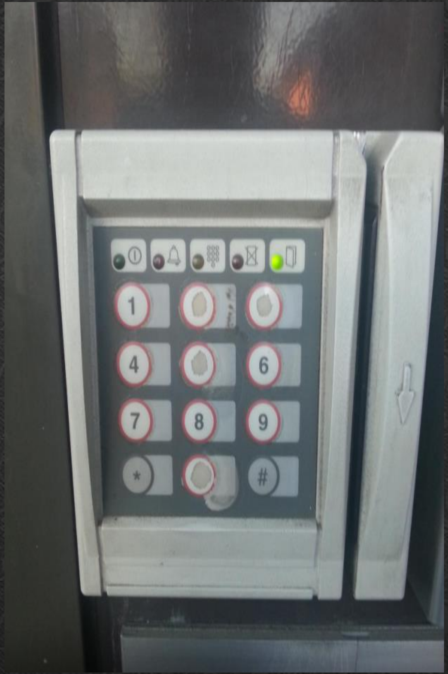


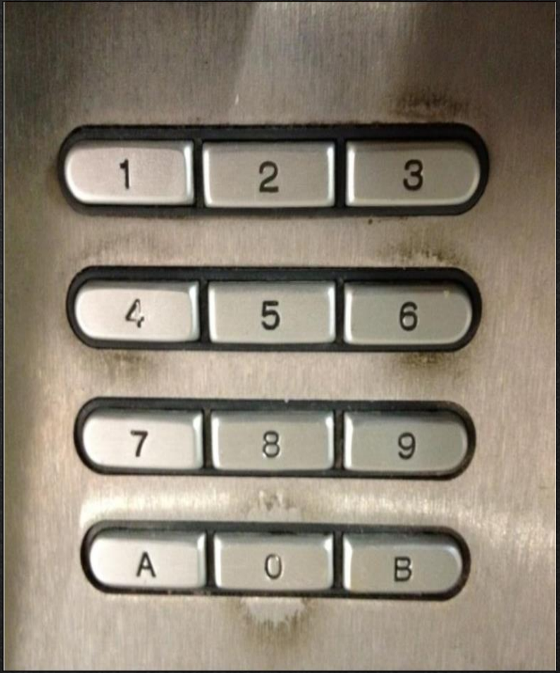
Radical.org/pinmap
By @kluzz

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

Look, and you shall see... PINs.

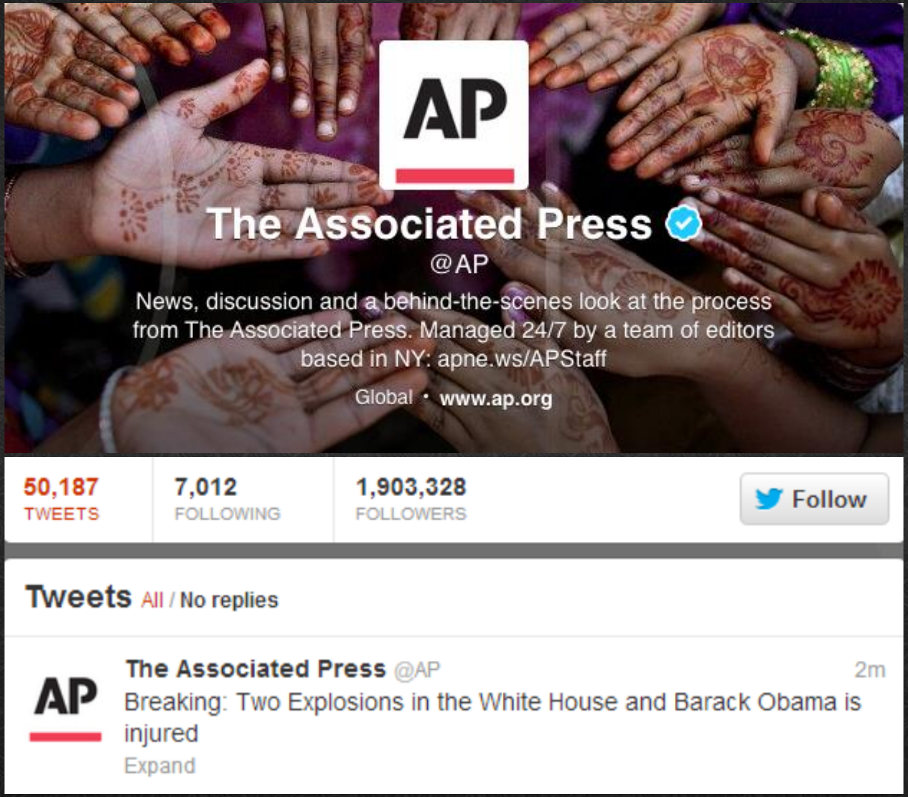




Guess What?

YOU ARE PREDICTABLE!

What's the value of a password?



The Associated Press

@AP

News, discussion and a behind-the-scenes look at the process from The Associated Press. Managed 24/7 by a team of editors based in NY: apne.ws/APStaff

Global · www.ap.org

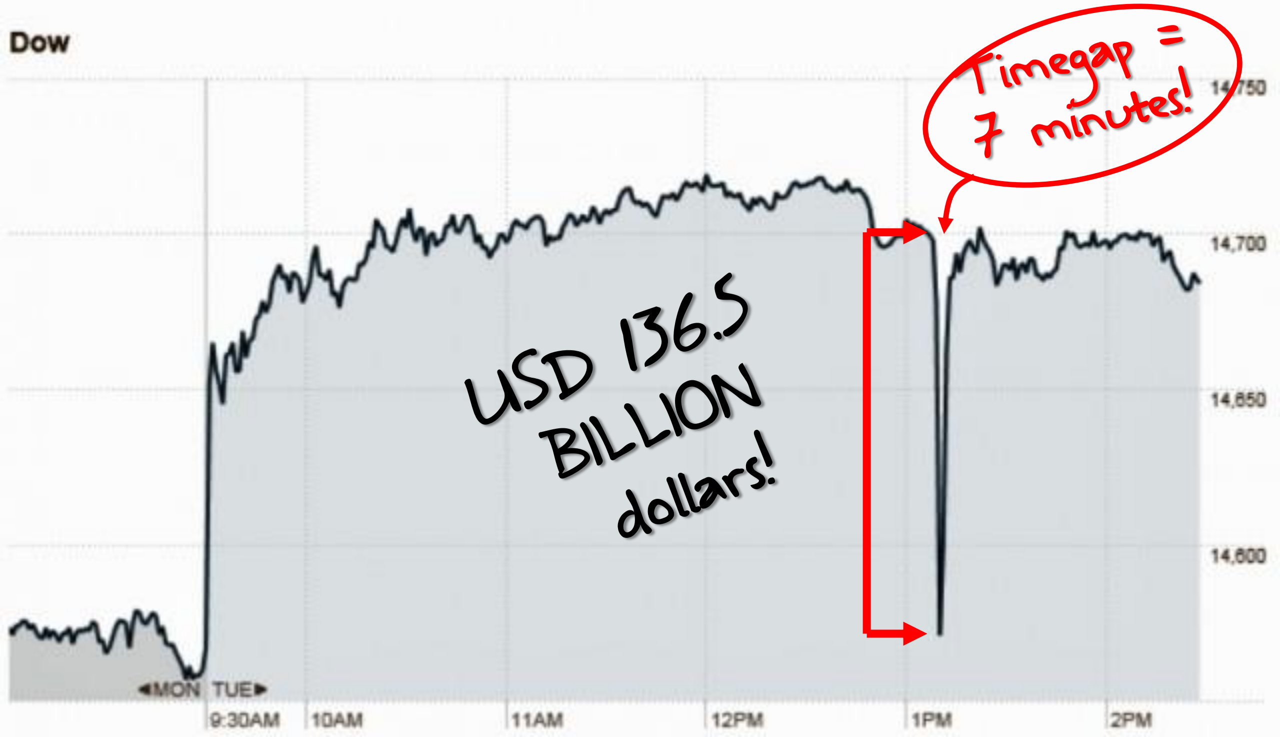
50,187 TWEETS | 7,012 FOLLOWING | 1,903,328 FOLLOWERS

Tweets All / No replies

The Associated Press @AP 2m

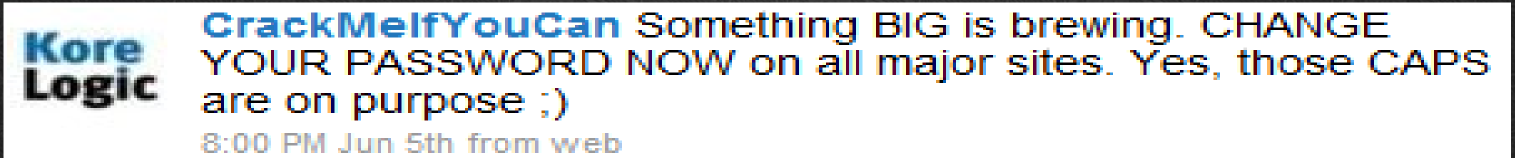
Breaking: Two Explosions in the White House and Barack Obama is injured

Consequences?



http://arstechnica.com/security/2013/04/hacked-ap-twitter-feed-rocks-market-after-sending-false-news-flash/

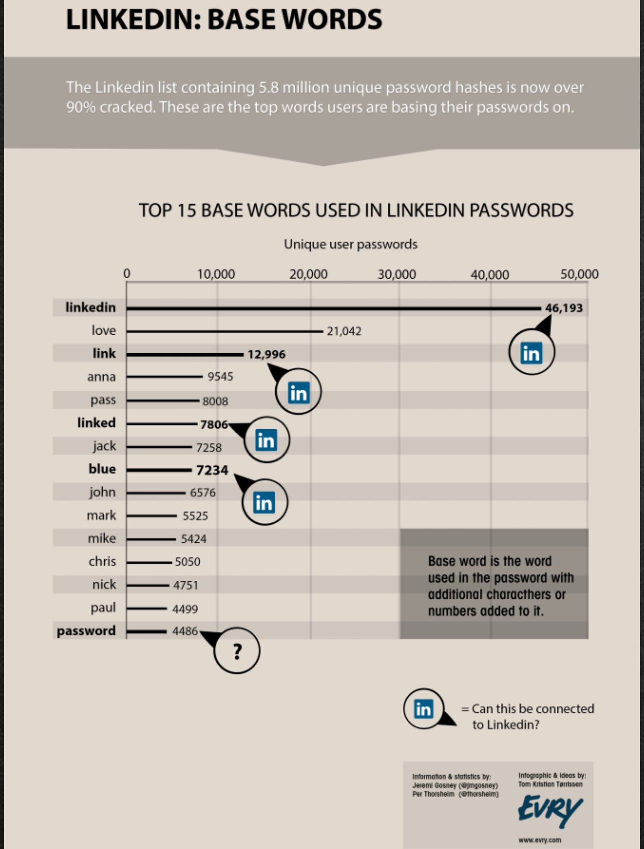
Tuesday, June 5, 2012, on Twitter:



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

Base word is the word used in the password with additional charocthers or numbers added to it.

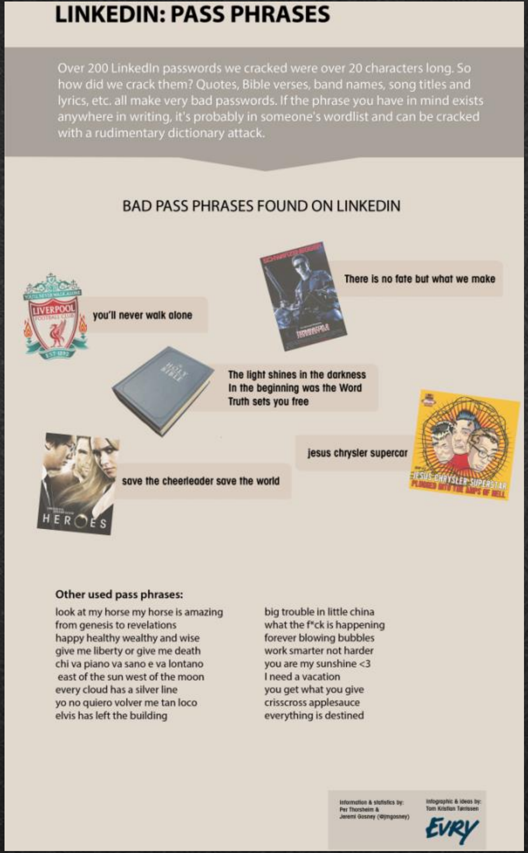
= Can this be connected to Linkedin?

Information & statistics by:
Jeremi Gosney (@jmgosney)
Per Thorsheim (@thorsheim)

Infographic & ideas by:
Tom Kristian Tørrissen

Evry

www.evry.com



LINKEDIN: PASS PHRASES

Over 200 LinkedIn passwords we cracked were over 20 characters long. So how did we crack them? Quotes, Bible verses, band names, song titles and lyrics, etc. all make very bad passwords. If the phrase you have in mind exists anywhere in writing, it's probably in someone's wordlist and can be cracked with a rudimentary dictionary attack.

BAD PASS PHRASES FOUND ON LINKEDIN

you'll never walk alone

There is no fate but what we make

The light shines in the darkness
In the beginning was the Word
Truth sets you free

jesus chrysler supercar

save the cheerleader save the world

Other used pass phrases:

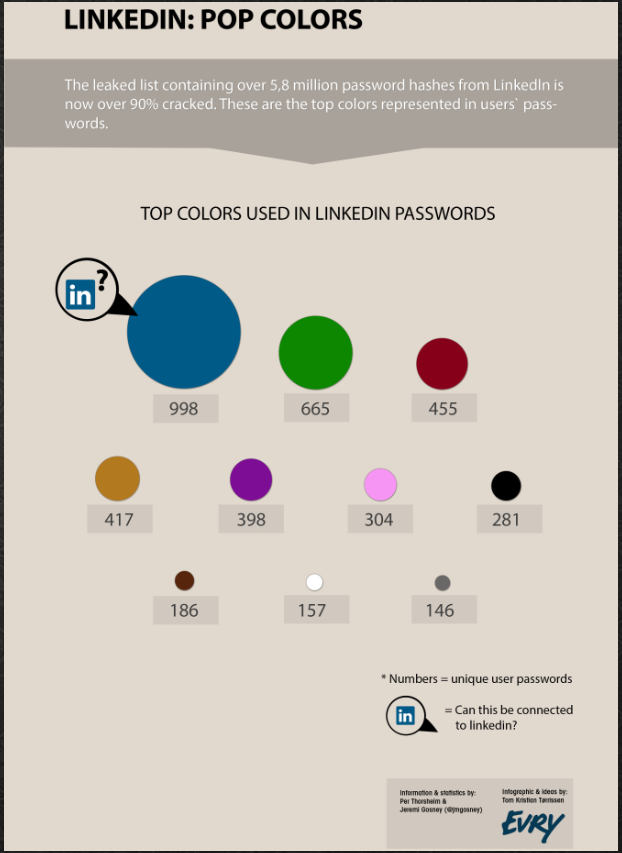
look at my horse my horse is amazing
from genesis to revelations
happy healthy wealthy and wise
give me liberty or give me death
chi va piano va sano e va lontano
east of the sun west of the moon
every cloud has a silver line
yo no quiero volver me tan loco
elvis has left the building

big trouble in little china
what the f*ck is happening
forever blowing bubbles
work smarter not harder
you are my sunshine <3
I need a vacation
you get what you give
crisscross applesauce
everything is destined

Information & statistics by:
Per Thorsheim &
Jeremi Gosney (@jmgosney)

Infographic & ideas by:
Tom Kristian Tørrissen

Evry



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.

TOP COLORS USED IN LINKEDIN PASSWORDS

* Numbers = unique user passwords

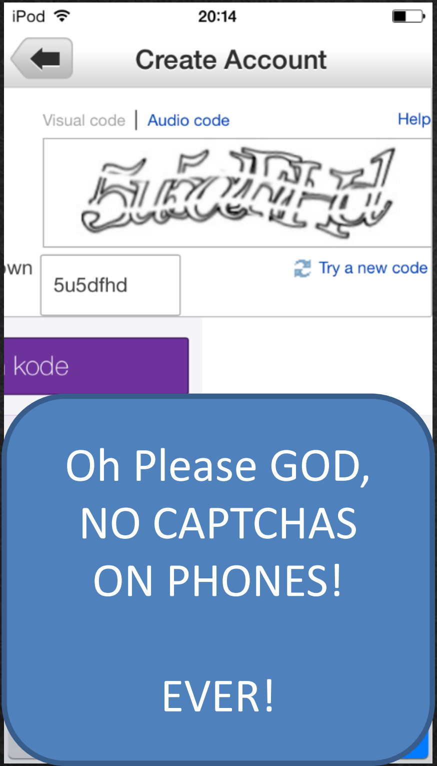
= Can this be connected to linkedin?

Information & statistics by:
Per Thorsheim &
Jeremi Gosney (@jmgosney)

Infographic & ideas by:
Tom Kristian Tørrissen

Evry

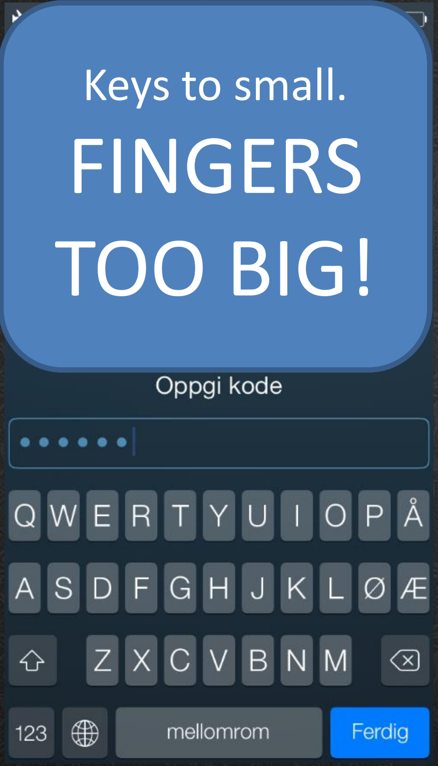
Mobile Usability #1



wn 5u5dfhd

Oh Please GOD, NO CAPTCHAS ON PHONES!

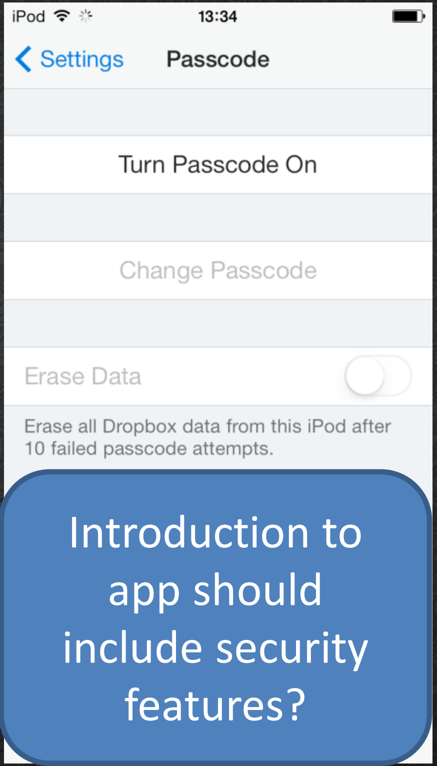
EVER!



Oppgi kode ••••••

Keys to small.

FINGERS TOO BIG!



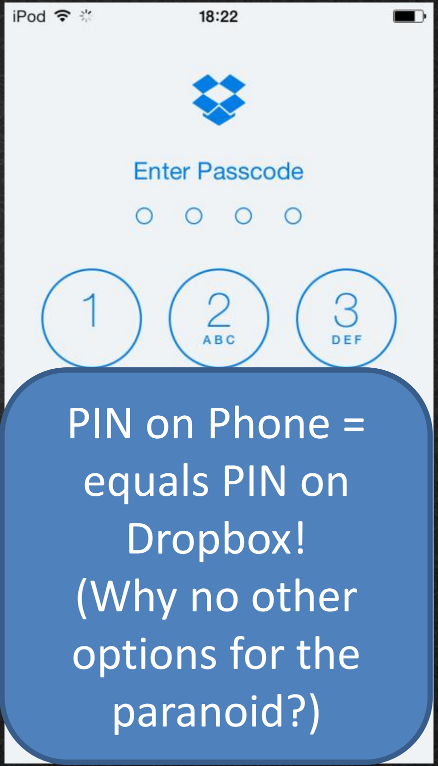
Turn Passcode On

Change Passcode

Erase Data ○

Erase all Dropbox data from this iPod after 10 failed passcode attempts.

Introduction to app should include security features?

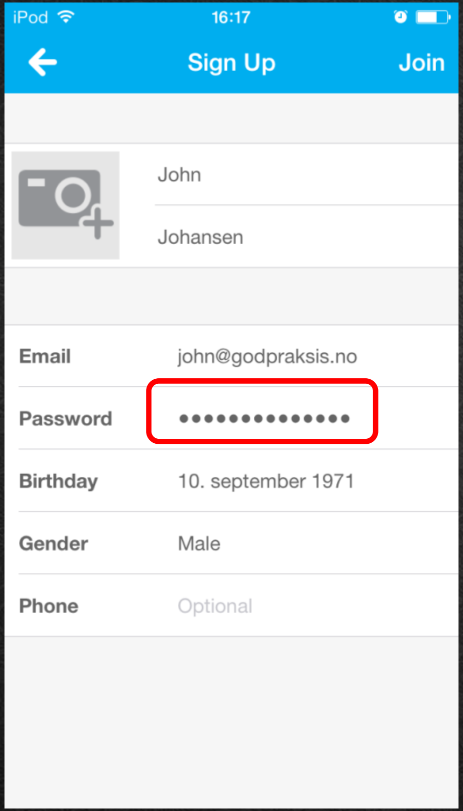


Enter Passcode

○ ○ ○ ○

PIN on Phone = equals PIN on Dropbox! (Why no other options for the paranoid?)

Foursquare – Verify mail account



John

Johansen

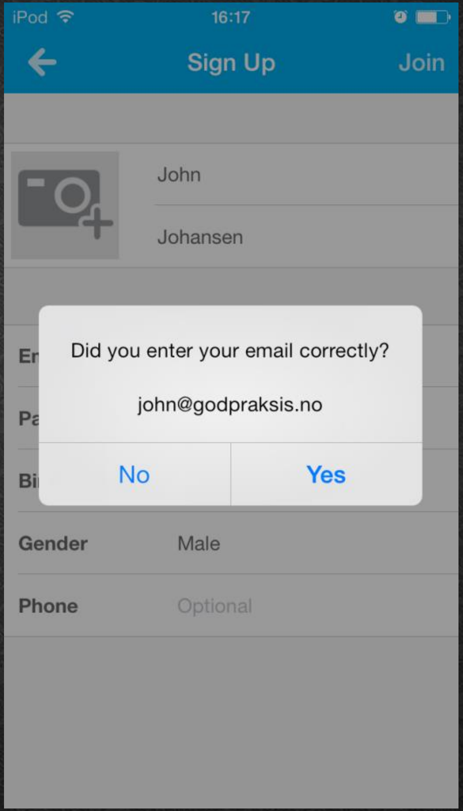
Email john@godpraksis.no

Password ••••••••••••••

Birthday 10. september 1971

Gender Male

Phone Optional



John

Johansen

Did you enter your email correctly?

john@godpraksis.no

No Yes

Er

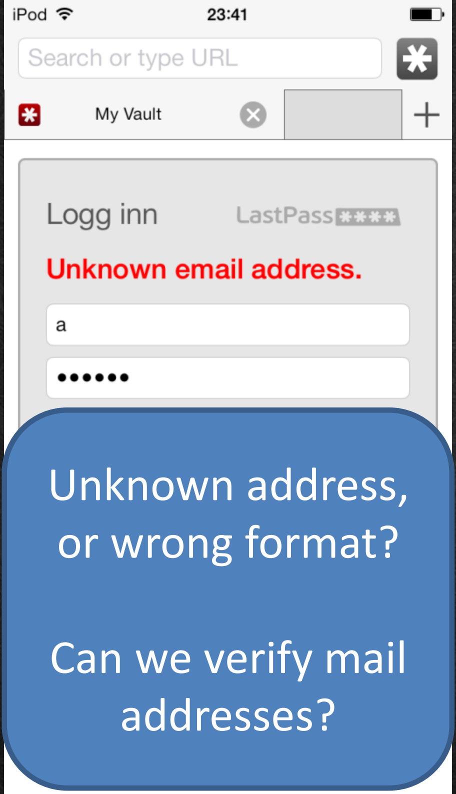
Pa

Bi

Gender Male

Phone Optional

Lastpass – iOS & Android



iPod 23:41

Search or type URL

My Vault

Logg inn LastPass****

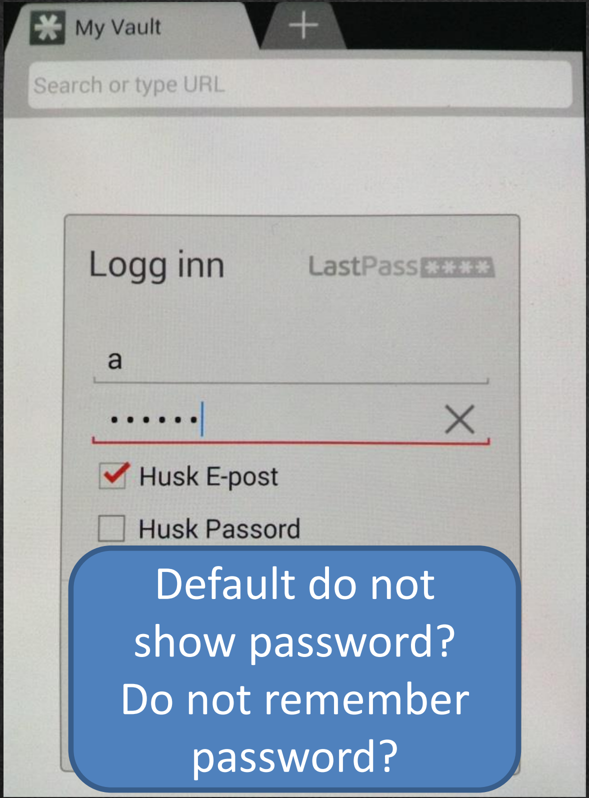
Unknown email address.

a

••••••

Unknown address, or wrong format?

Can we verify mail addresses?



My Vault

Search or type URL

Logg inn LastPass****

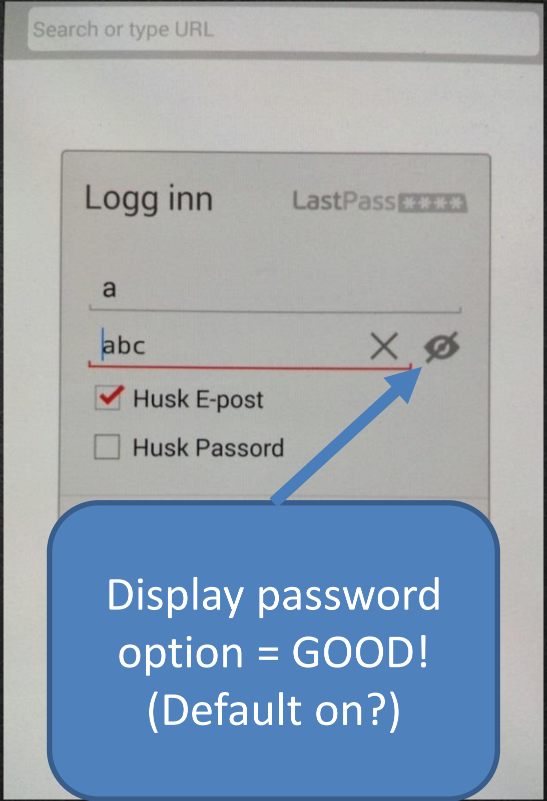
a

••••••

☑ Husk E-post

□ Husk Passord

Default do not show password? Do not remember password?



Search or type URL

Logg inn LastPass****

a

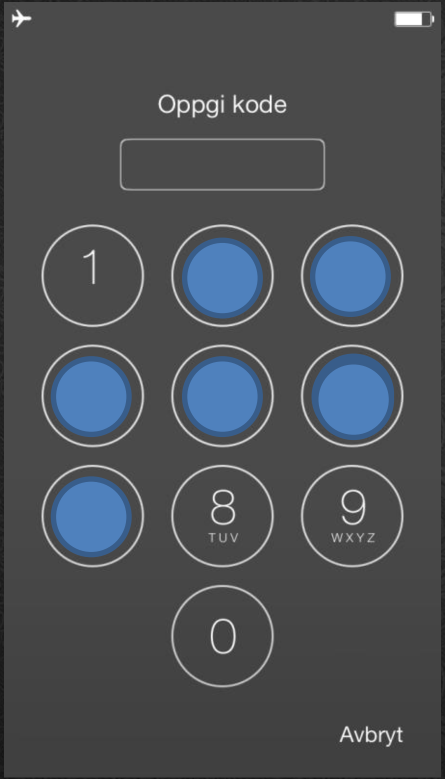
abc

☑ Husk E-post

□ Husk Passord

Display password option = GOOD! (Default on?)

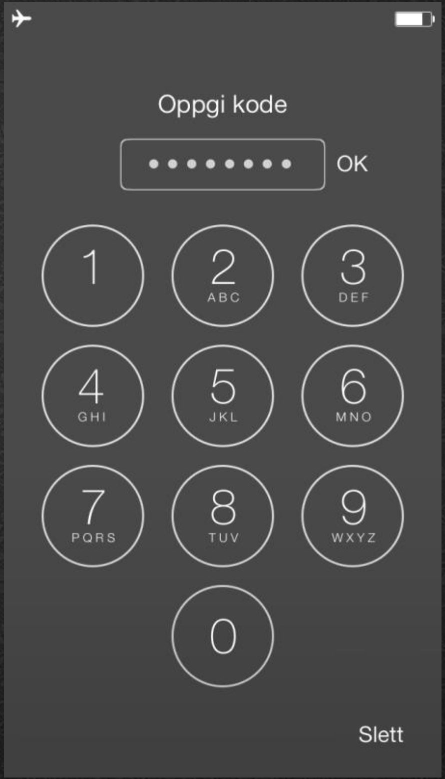
Tip For Mobile Usability:


Oppgi kode

=

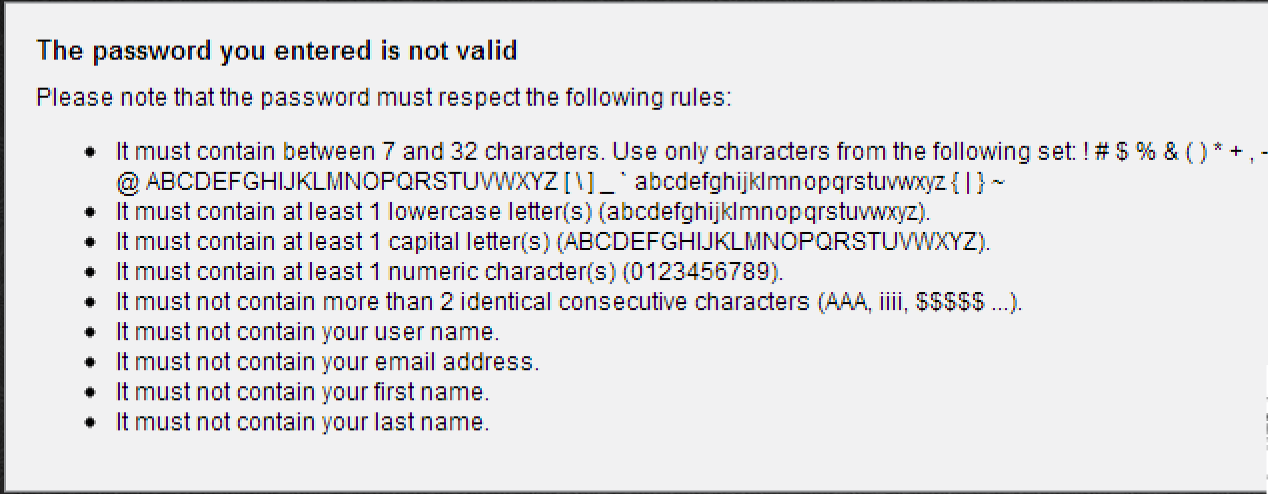
Johansen

56426736


Oppgi kode

••••••••

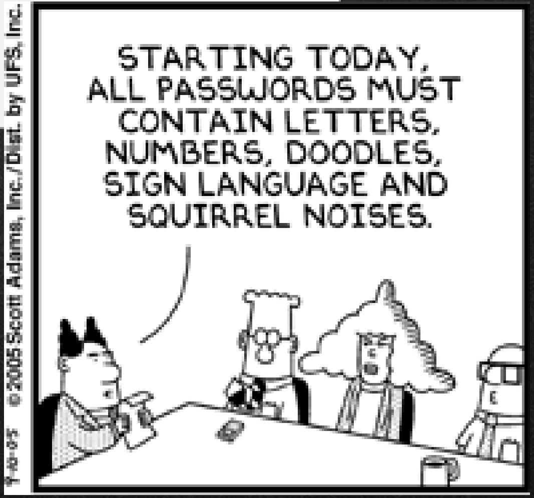
Password Meters



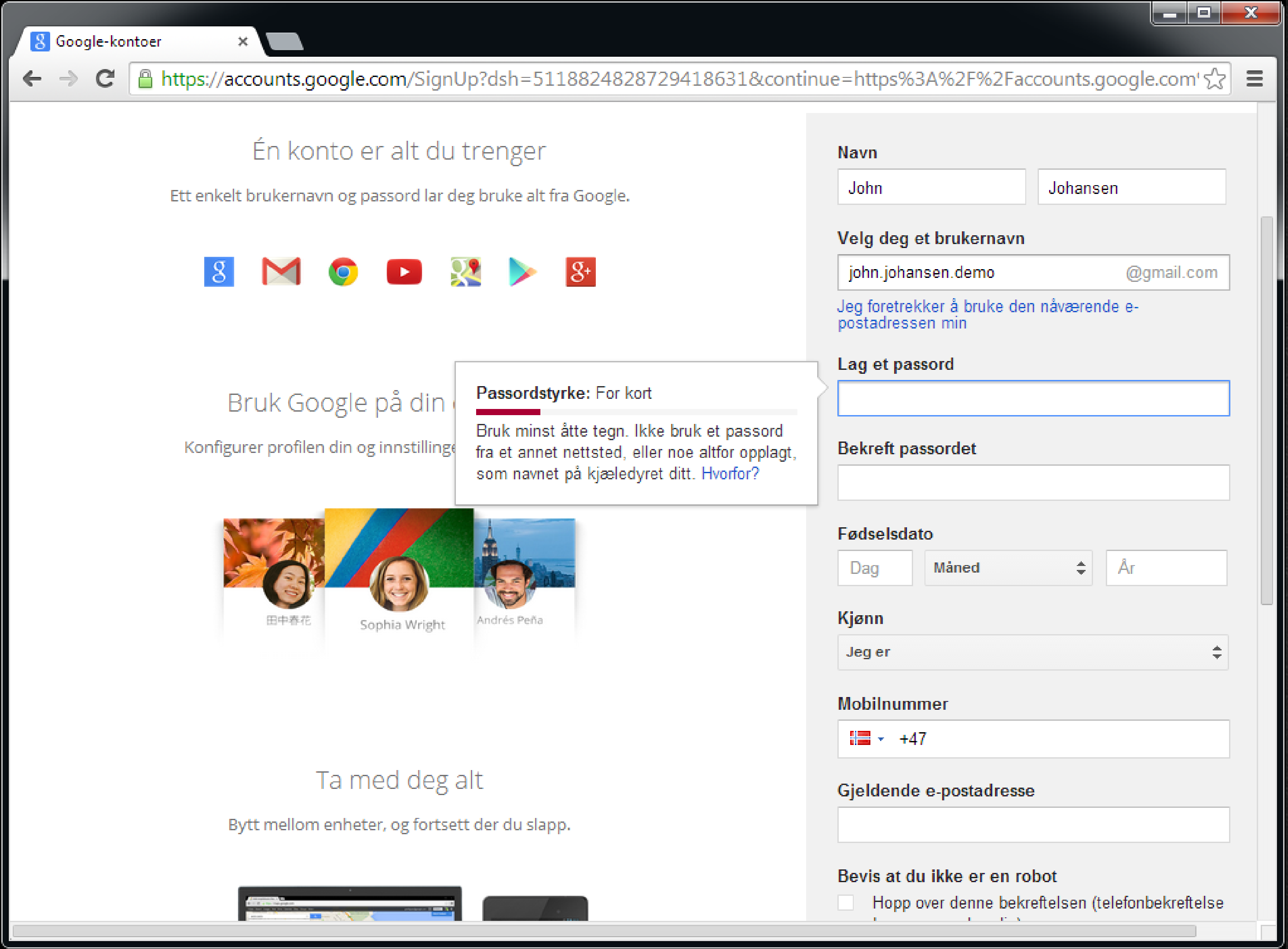
The password you entered is not valid

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) (abcdefghijklmnopqrstuvwxyz).
- 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, iiii, $$$$$ ...).
- 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.
9-10-05 © 2005 Scott Adams, Inc./Dist. by UFS, Inc.

Google account creation



Google-kontoer

https://accounts.google.com/SignUp?dsh=5118824828729418631&continue=https%3A%2F%2Faccounts.google.com'

Én konto er alt du trenger

Ett enkelt brukernavn og passord lar deg bruke alt fra Google.

Bruk Google på din

Konfigurer profilen din og innstillinge

Sophia Wright

Andrés Peña

Ta med deg alt

Bytt mellom enheter, og fortsett der du slapp.

Passordstyrke: For kort

Bruk minst åtte tegn. Ikke bruk et passord fra et annet nettsted, eller noe altfor opplagt, som navnet på kjæledyret ditt. Hvorfor?

Navn

John | Johansen

Velg deg et brukernavn

john.johansen.demo @gmail.com

Jeg foretrekker å bruke den nåværende e-postadressen min

Lag et passord

Bekreft passordet

Fødselsdato

Dag | Måned | År

Kjønn

Jeg er

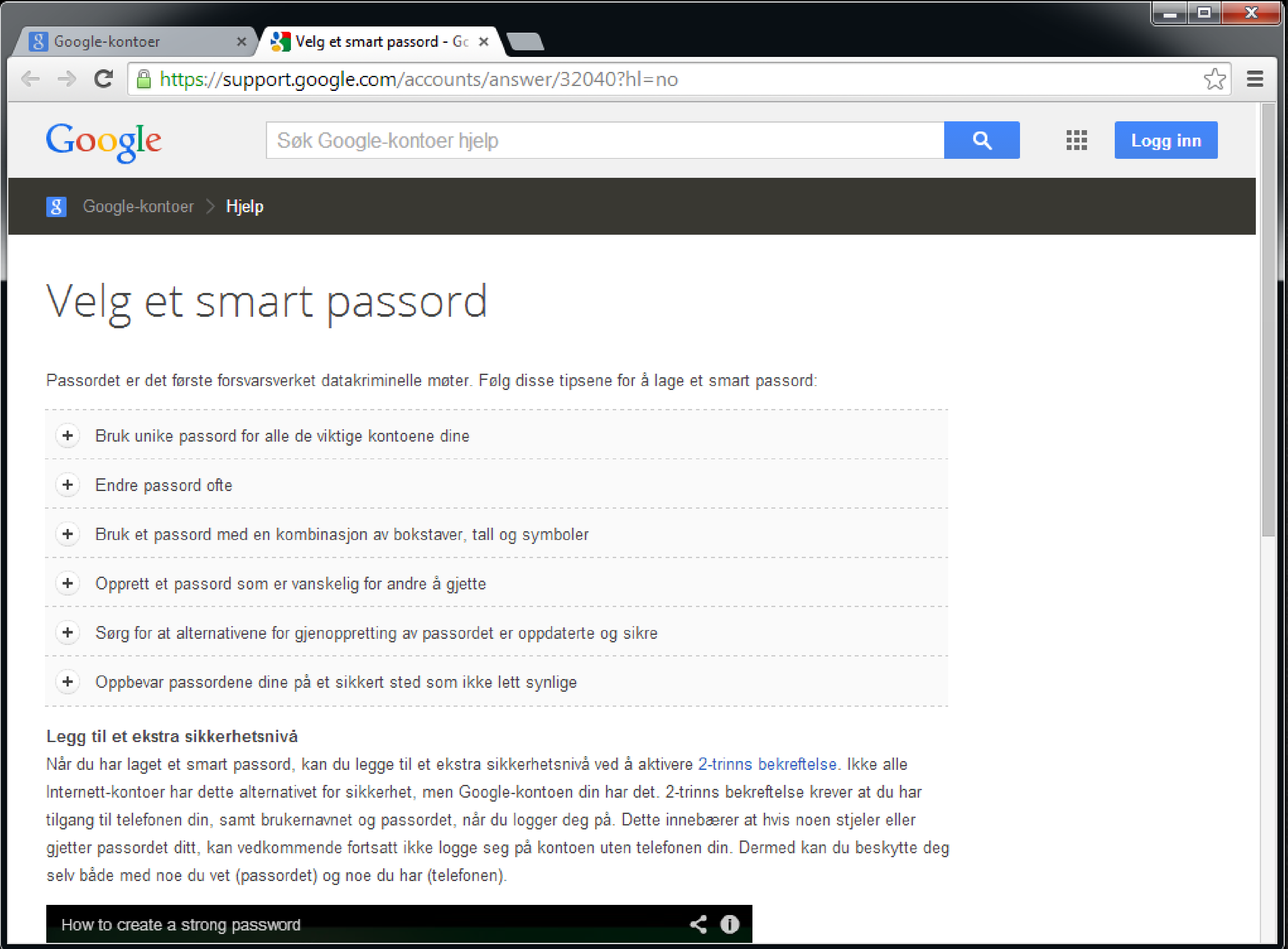
Mobilnummer

+47

Gjeldende e-postadresse

Bevis at du ikke er en robot

□ Hopp over denne bekreftelsen (telefonbekreftelse


Google-kontoer
Velg et smart passord - Gc
https://support.google.com/accounts/answer/32040?hl=no
Google
Søk Google-kontoer hjelp
Logg inn
Google-kontoer
Hjelp
How to create a strong password

Velg et smart passord

Passordet er det første forsvarsverket datakriminelle møter. Følg disse tipsene for å lage et smart passord:

- + Bruk unike passord for alle de viktige kontoene dine
- + Endre passord ofte
- + Bruk et passord med en kombinasjon av bokstaver, tall og symboler
- + Opprett et passord som er vanskelig for andre å gjette
- + Sørg for at alternativene for gjenoppretting av passordet er oppdaterte og sikre
- + Oppbevar passordene dine på et sikkert sted som ikke lett synlige

Legg til et ekstra sikkerhetsnivå

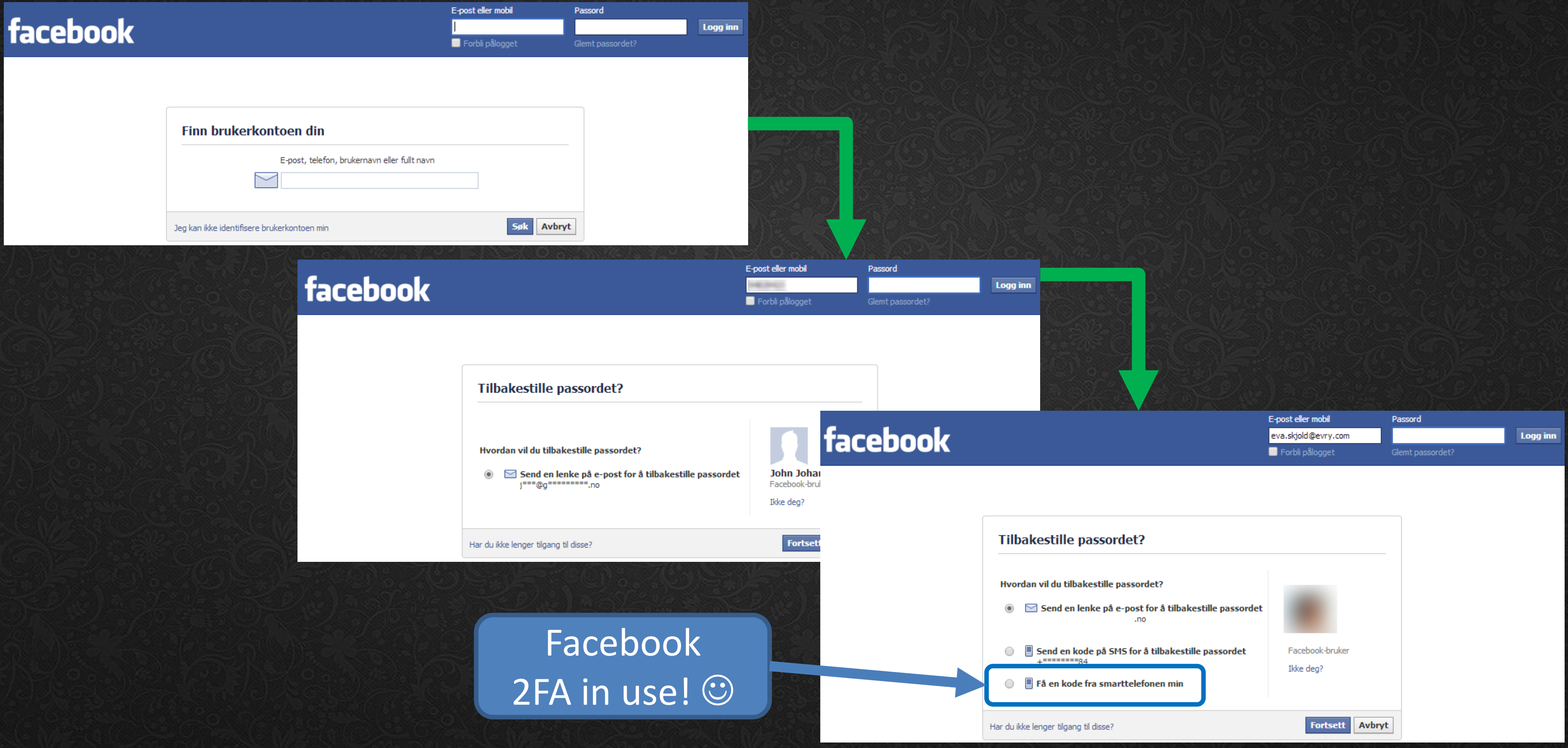
Når du har laget et smart passord, kan du legge til et ekstra sikkerhetsnivå ved å aktivere 2-trinns bekreftelse. Ikke alle Internett-kontoer har dette alternativet for sikkerhet, men Google-kontoen din har det. 2-trinns bekreftelse krever at du har tilgang til telefonen din, samt brukernavnet og passordet, når du logger deg på. Dette innebærer at hvis noen stjeler eller gjetter passordet ditt, kan vedkommende fortsatt ikke logge seg på kontoen uten telefonen din. Dermed kan du beskytte deg selv både med noe du vet (passordet) og noe du har (telefonen).

Give sound advice

--

Recommend 2FA

«Secret» Mail + Phone



facebook

E-post eller mobil

Passord

Logg inn

□ Forbli pålogget

Glemt passordet?

Finn brukerkontoen din

E-post, telefon, brukernavn eller fullt navn

Jeg kan ikke identifisere brukerkontoen min

Søk | Avbryt

facebook

E-post eller mobil: [redacted]

Passord

Logg inn

□ Forbli pålogget

Glemt passordet?

Tilbakestille passordet?

Hvordan vil du tilbakestille passordet?

● Send en lenke på e-post for å tilbakestille passordet
j***@g*********.no

John Johan
Facebook-bru
Ikke deg?

Har du ikke lenger tilgang til disse?

Fortsett

facebook

E-post eller mobil: eva.skjold@evry.com

Passord

Logg inn

□ Forbli pålogget

Glemt passordet?

Tilbakestille passordet?

Hvordan vil du tilbakestille passordet?

● Send en lenke på e-post for å tilbakestille passordet
.no

○ Send en kode på SMS for å tilbakestille passordet
+********84

○ Få en kode fra smarttelefonen min

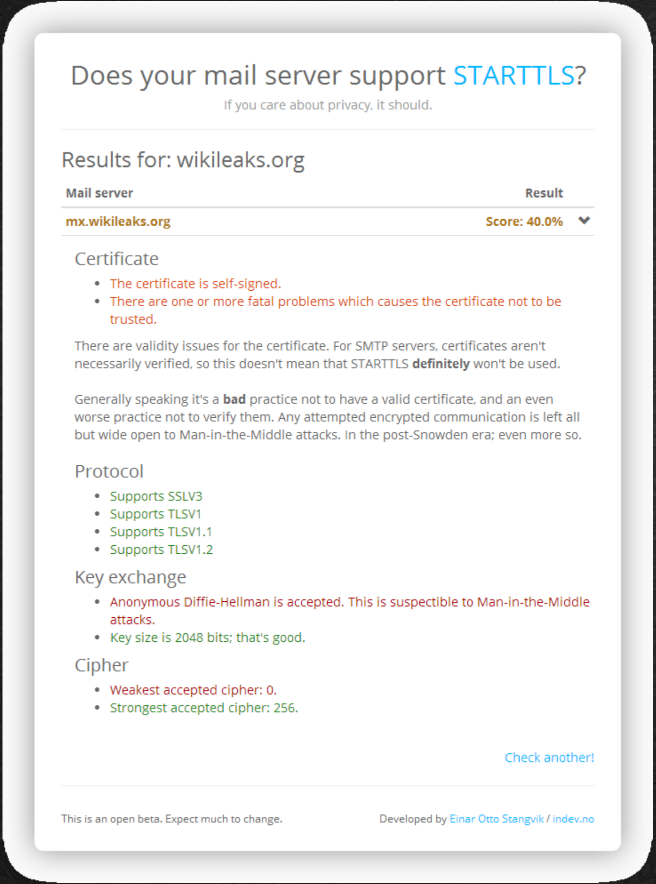
Facebook-bruker
Ikke deg?

Har du ikke lenger tilgang til disse?

Fortsett | Avbryt

Facebook
2FA in use! ☺

Starttls.info



Does your mail server support STARTTLS?

If you care about privacy, it should.

Results for: wikileaks.org

Mail server	Result
mx.wikileaks.org	Score: 40.0%

Certificate

- The certificate is self-signed.
- There are one or more fatal problems which causes the certificate not to be trusted.

There are validity issues for the certificate. For SMTP servers, certificates aren't necessarily verified, so this doesn't mean that STARTTLS **definitely** won't be used.

Generally speaking it's a **bad** practice not to have a valid certificate, and an even worse practice not to verify them. Any attempted encrypted communication is left all but wide open to Man-in-the-Middle attacks. In the post-Snowden era; even more so.

Protocol

- Supports SSLV3
- Supports TLSV1
- Supports TLSV1.1
- Supports TLSV1.2

Key exchange

- Anonymous Diffie-Hellman is accepted. This is suspectible to Man-in-the-Middle attacks.
- Key size is 2048 bits; that's good.

Cipher

- Weakest accepted cipher: 0.
- Strongest accepted cipher: 256.

This is an open beta. Expect much to change.

Developed by Einar Otto Stangvik / indev.no

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

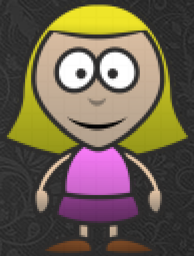
- Unique opportunity (!)
- 5000+ «headshots»
- Passwords + other information available
- Analyze!

Categorization

Facial hair

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

Sex
Glasses (Y/N)
Hair color
Facial hair



Hair color

No ☺
«Blond»
Superblond
Brunette
Redhead
«Silver fox»

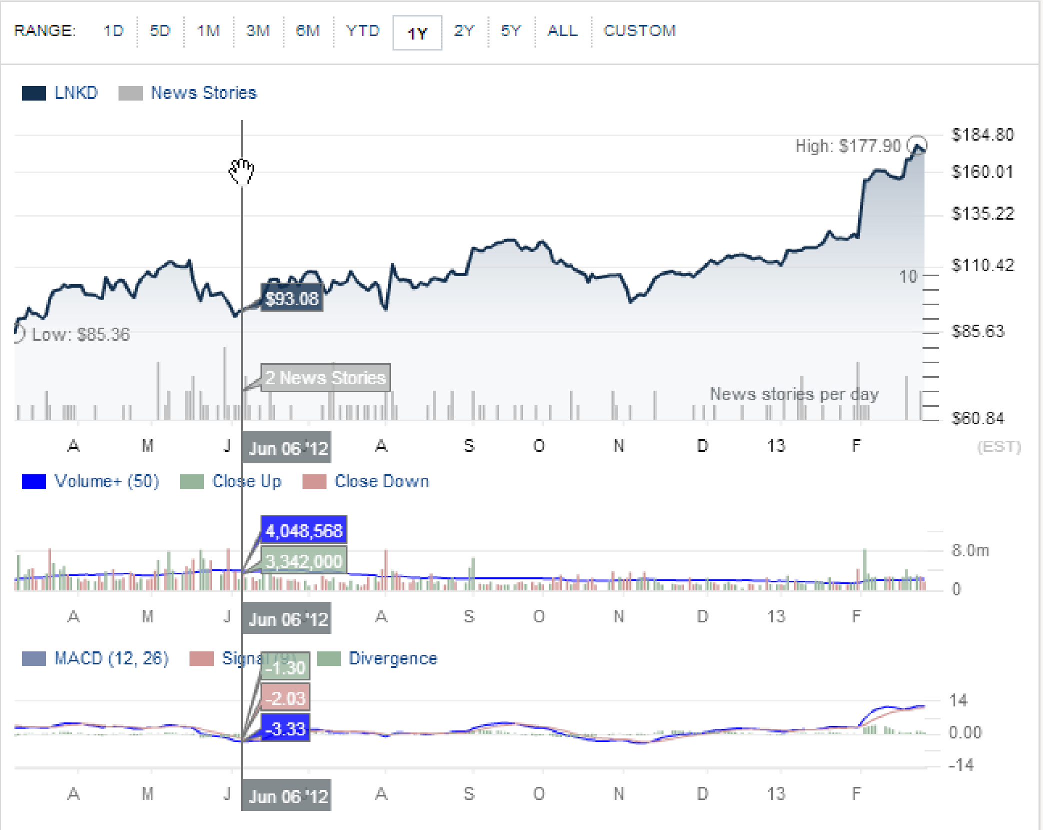
… and the results?

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