Keep your device to yourself

Per Thorsheim
Security Advisor
God Praksis

Twitter: @thorsheim

Background

24.01.13: Trend Micro reports that 60% of working Norwegian have use a personal smartphone, PC or pad to handle work-related information.

My chronicle at Computerworld, 25.01.2013: «Hold dingsen din for deg selv»

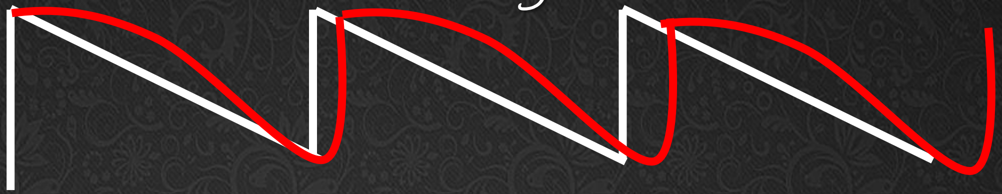
...And articles in Advokatbladet Sept 2011 & April 2012

Definitions

- Bring Your Own Device - BYOD
  - «Use your own equipment to do your job»

- Mobile Device Management – MDM
  - Software for controlling mobile devices
    - Tracking, remote deletion, maintenance, control, limitations

Devices get:



Damaged (?)

Not returned or destroyed

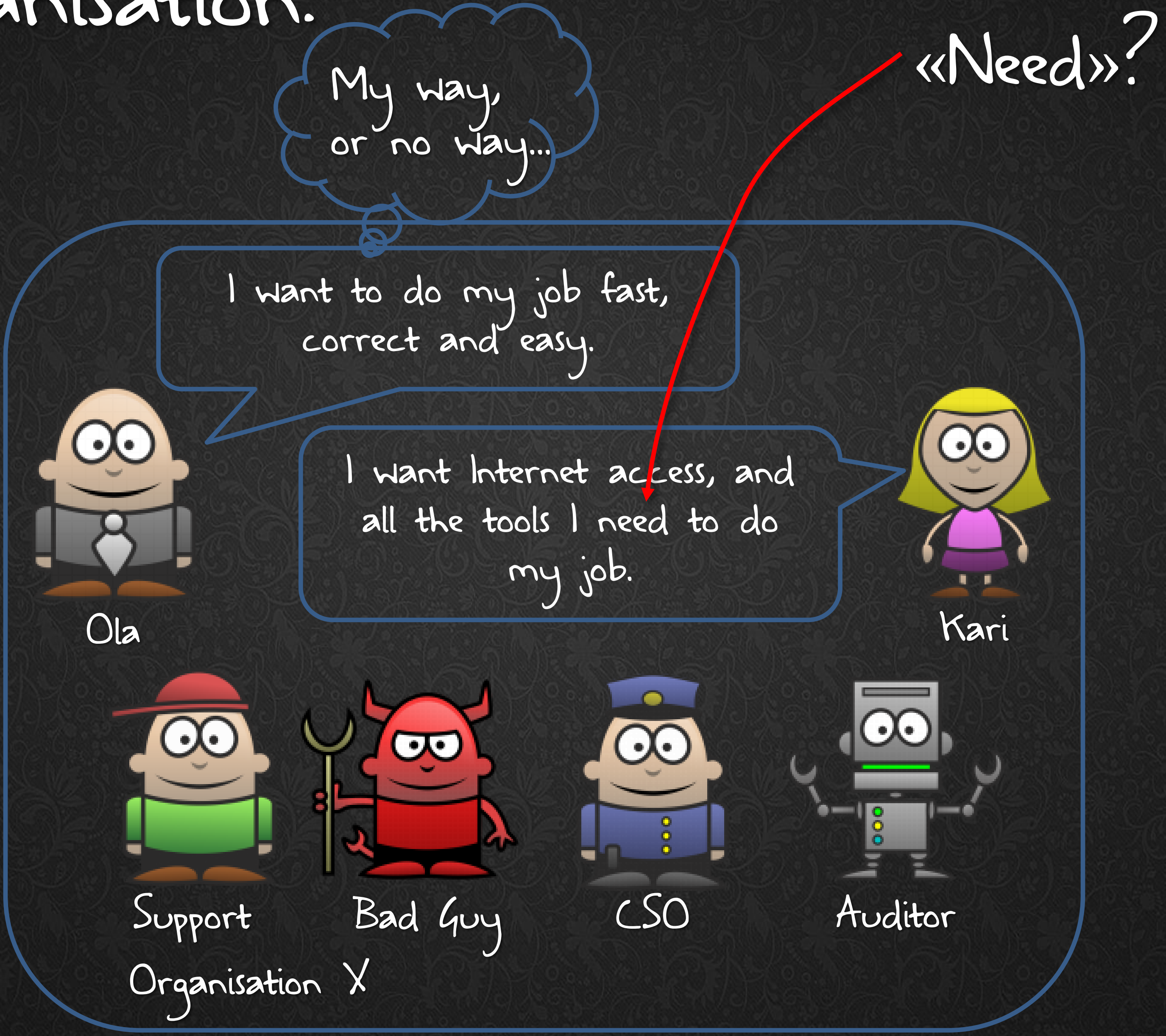
Lost (?)

Not found again

Stolen!

No reporting to police

Organisation:



My way, or no way...

«Need»?

I want to do my job fast, correct and easy.

I want Internet access, and all the tools I need to do my job.

Ola

Kari

Support

Bad Guy

CSO

Auditor

Organisation X

What do ~~you~~ I have on ~~your~~ my iPad?

Apple / iTunes konto

Gmail + IMAP mail

Twitter, Facebook

Google+, Linkedin

Skype, Dropbox

Google Drive

Norwegian reiseapp

SATS app, Netflix

Sprout Social / Klout

Norsk Tipping / Buypass

Storage / Backup

iCloud

Apple-ID

Passord

□ La meg forbli pålogget

News, Spotify, LastPass

Vine, BankID, Kindle

Digipost, iZettle, Evernote

Finn iPhone

WolframAlpha, FINN.no

Bergen Taxi, Instagram

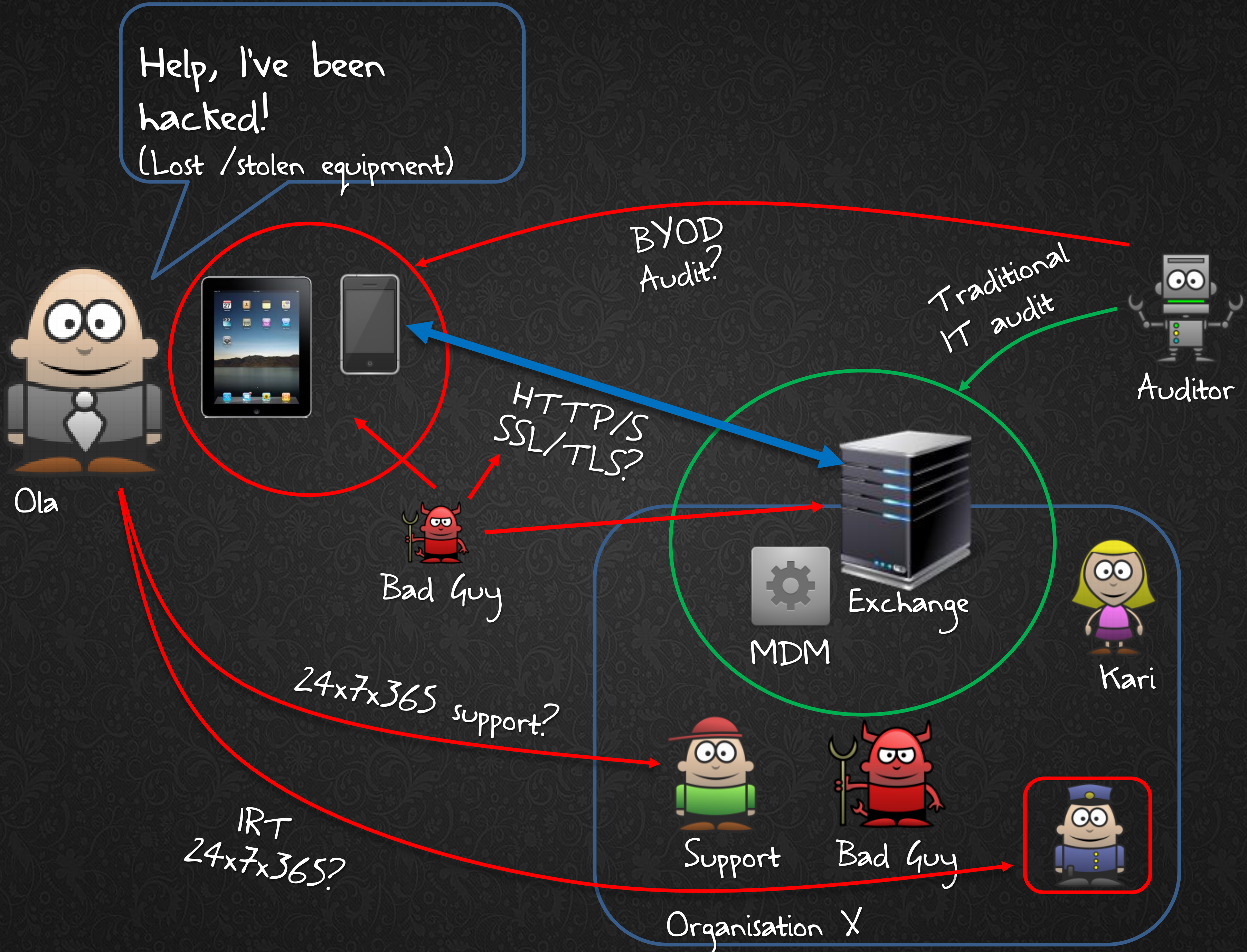
Bank app

+ config, usrnames & pwds for: VPN, WLAN

🟩 Offers 2FA authentication

🟨 Requires 2FA authentication

Red = § Personally sensitive info and/or financial risk



Help, I've been hacked!
(Lost /stolen equipment)

BYOD Audit?

Traditional IT audit

Auditor

HTTP/S SSL/TLS?

Ola

Bad Guy

Exchange

MDM

Kari

24x7x365 support?

IRT 24x7x365?

Support

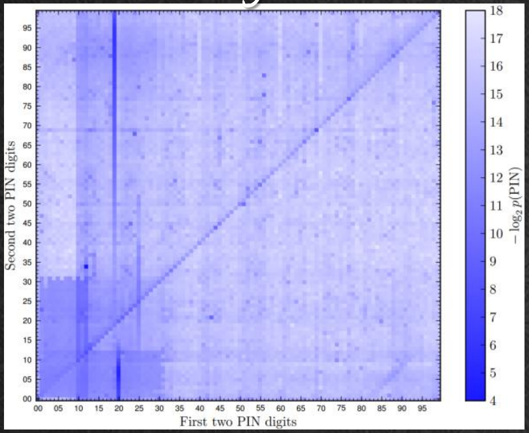
Bad Guy

Organisation X

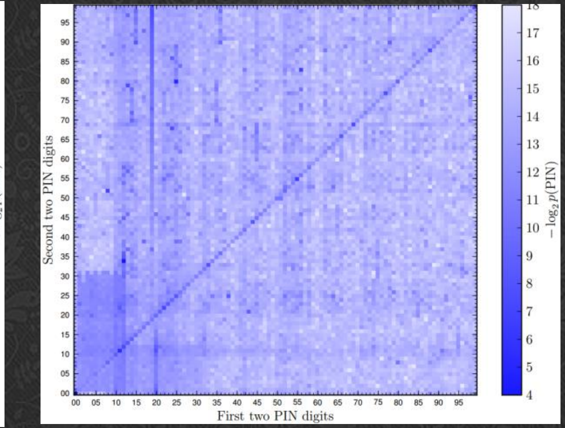
Mobile Device - Client Side Risk

- Usually a 4-digit PIN

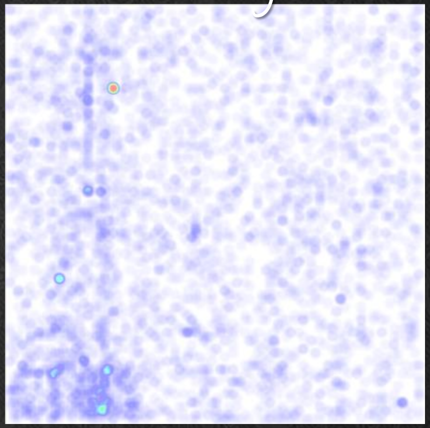
Rockyou



iPhone

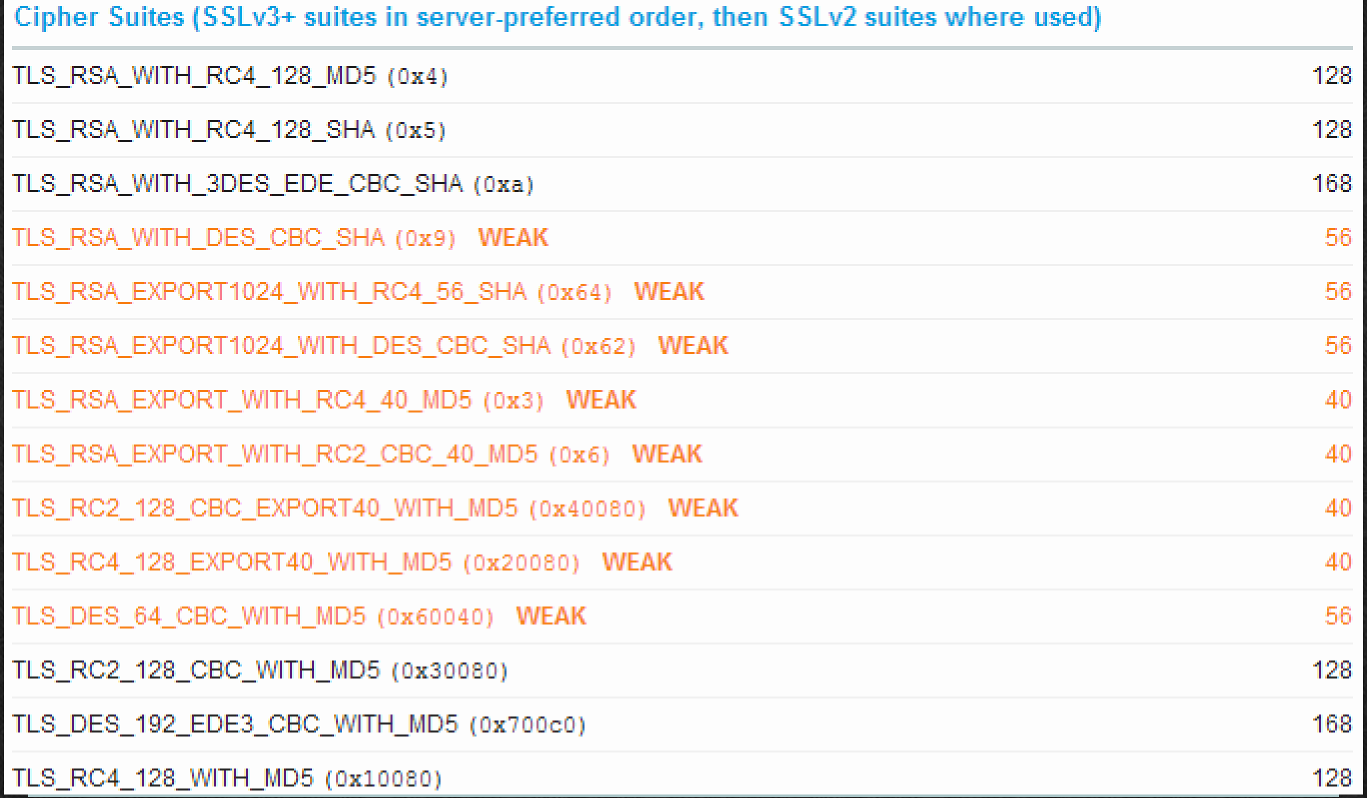


Physical access
Control system



  - User selected PIN: Top100 used by «most»
  - Apple iOS: 4-digit PIN kan be cracked in <40 min
- Device/memcard encryption not possible
- MDM often depends on being online (gsm/wifi)

Client – Server Comms Risk



Cipher Suites (SSLv3+ suites in server-preferred order, then SSLv2 suites where used)

TLS_RSA_WITH_RC4_128_MD5 (0x4)	128
TLS_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	168
TLS_RSA_WITH_DES_CBC_SHA (0x9) **WEAK**	56
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA (0x64) **WEAK**	56
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (0x62) **WEAK**	56
TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x3) **WEAK**	40
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x6) **WEAK**	40
TLS_RC2_128_CBC_EXPORT40_WITH_MD5 (0x40080) **WEAK**	40
TLS_RC4_128_EXPORT40_WITH_MD5 (0x20080) **WEAK**	40
TLS_DES_64_CBC_WITH_MD5 (0x60040) **WEAK**	56
TLS_RC2_128_CBC_WITH_MD5 (0x30080)	128
TLS_DES_192_EDE3_CBC_WITH_MD5 (0x700c0)	168
TLS_RC4_128_WITH_MD5 (0x10080)	128

(www.ssllabs.com – free check of SSL config on webservers)

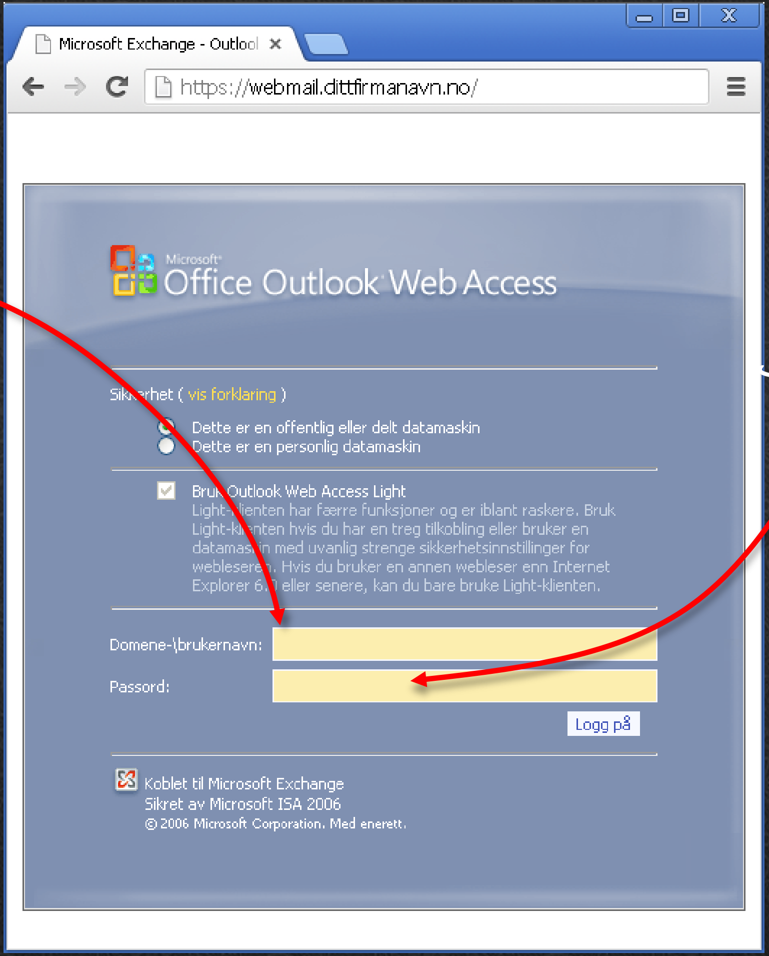
(Apple) Cloud Security

Demo time.

http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/
http://www.tv2.no/nyheter/innenriks/nakne-tenaaringsjenter-selges-paa-nett-3961421.html

Server Side Risk: OWA

Call helpdesk, get username!



Microsoft Exchange - Outlool ×
https://webmail.dittfirmanavn.no/
Microsoft Office Outlook Web Access

Sikkerhet (vis forklaring)

● Dette er en offentlig eller delt datamaskin
○ Dette er en personlig datamaskin

☑ Bruk Outlook Web Access Light
Light-klienten har færre funksjoner og er iblant raskere. Bruk Light-klienten hvis du har en treg tilkobling eller bruker en datamaskin med uvanlig strenge sikkerhetsinnstillinger for webleseren. Hvis du bruker en annen webleser enn Internet Explorer 6.0 eller senere, kan du bare bruke Light-klienten.

Domene-\brukernavn:

Passord:

Logg på

Koblet til Microsoft Exchange
Sikret av Microsoft ISA 2006
© 2006 Microsoft Corporation. Med enerett.

Automated password guessing is «easy».

Free tools on the Internet has automation modules readily available.

Norwegian Data Protection Authority:

Right of access does not apply to equipment that workers themselves own.

This means that the employer does not have legal access to documents stored in the employee's private equipment, even if this equipment from time to time may be used for work-related activities.

www.datatilsynet.no/Global/05_regelverk/epostforskriften_merknader.pdf

MDM Legal Access

Employer can not:

- Obtain a list of:
  - Apps
  - Catalog/file names
  - Document names
- Read / change:
  - Documents
  - Pictures
  - Videos
  - Sound files

Employer can:

- Require PIN/Password
- Require encryption

Grey areas:

- Tracking
- Remote lock
- Remote wipe
- Config control (audit)

Recommendations

- Employer buys & owns all equipment needed
- Written & acknowleged procedures for legal access
- 24x7 incident handling group (IRT)
  - May include lock / wipe / delete
- Secure client-server communication
  - No defaults, please!
- Good practice SSL/TLS config on server
  - No defaults, please!
- Personal use of cloud services should be avoided for work-related info & tasks.

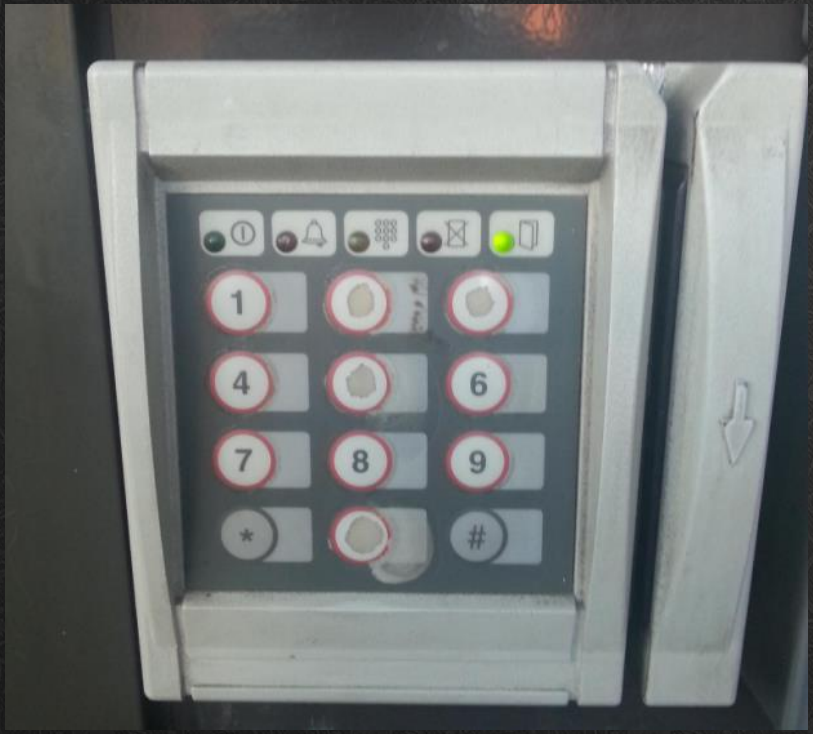
Password stuff.

Per Thorsheim
Security Advisor
God Praksis

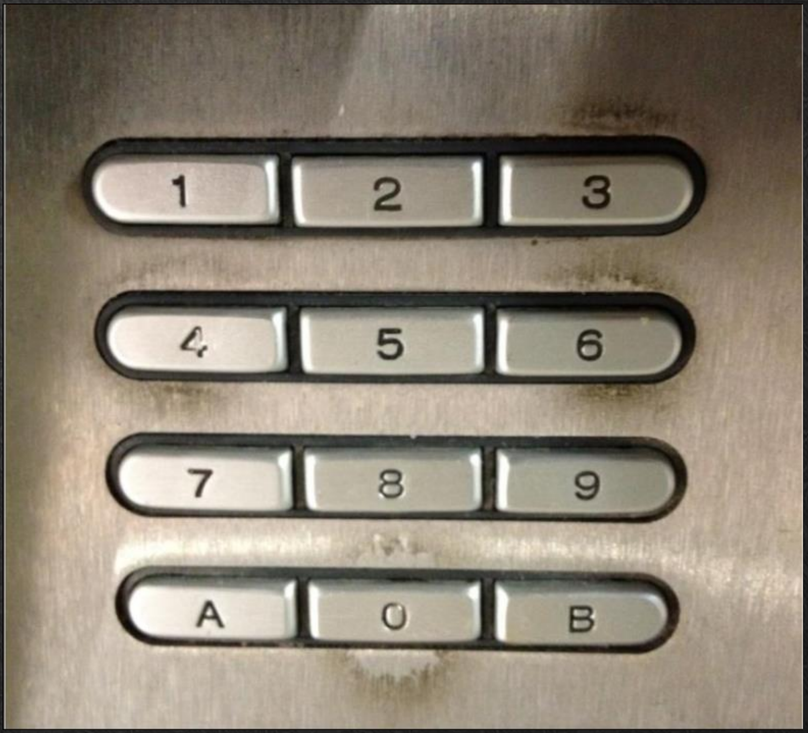
Twitter: @thorsheim

PIN pads

(Somewhere not important)



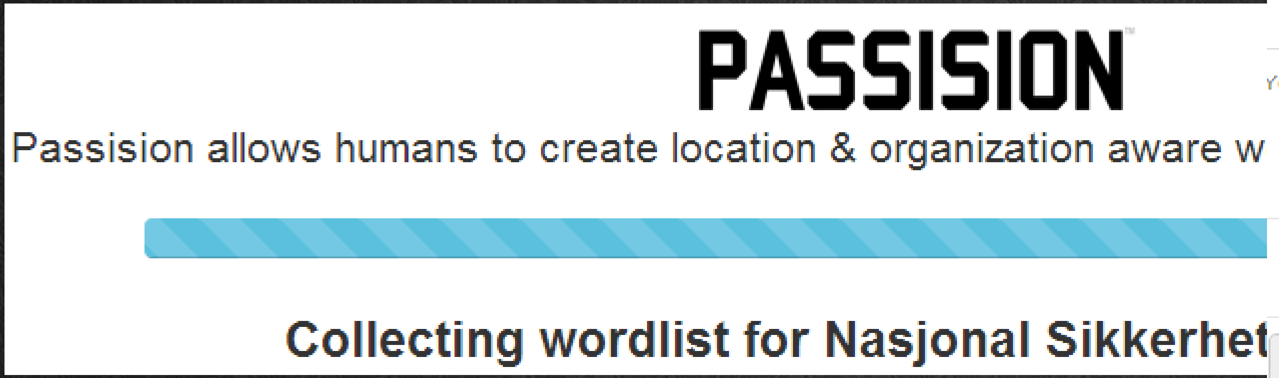
London Stansted airport



Figuring out your next password:

PASSWORD PROFILING

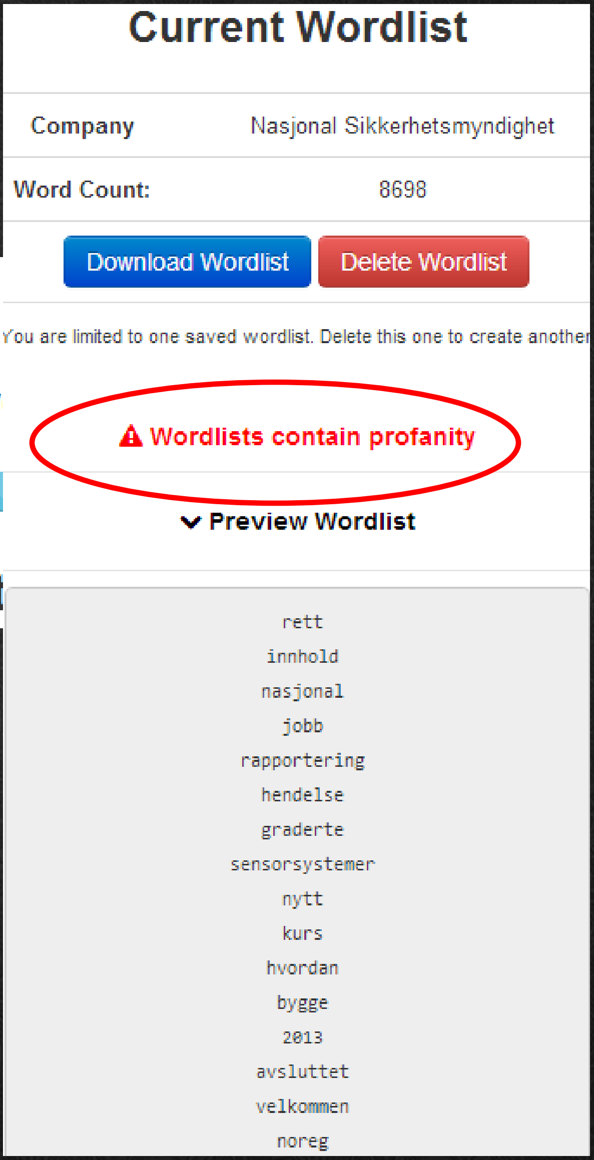
Offensive profiling: Threatagent.com



PASSION™

Passion allows humans to create location & organization aware w

Collecting wordlist for Nasjonal Sikkerhet



Current Wordlist

Company	Nasjonal Sikkerhetsmyndighet
Word Count:	8698

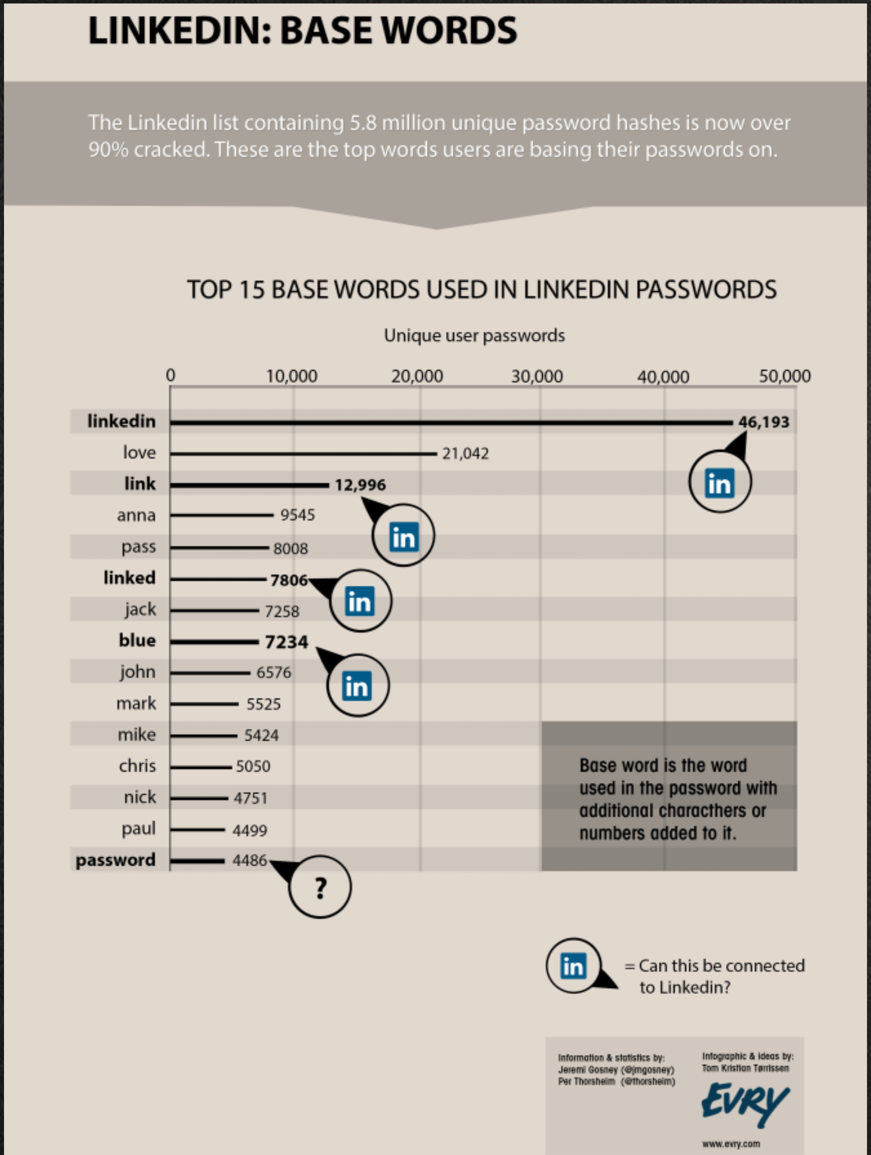
You are limited to one saved wordlist. Delete this one to create another

⚠ Wordlists contain profanity

```
rett
innhold
nasjonal
jobb
rapportering
hendelse
graderte
sensorsystemer
nytt
kurs
hvordan
bygge
2013
avsluttet
velkommen
noreg
```

http://drb0n3z.wordpress.com/2013/04/21/passion-new-wordlist-creation-tool/

Defensive profiling: 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

Unique user passwords

linkedin	**46,193**
love	21,042
link	**12,996**
anna	9545
pass	8008
linked	**7806**
jack	7258
blue	**7234**
john	6576
mark	5525
mike	5424
chris	5050
nick	4751
paul	4499
password	4486

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

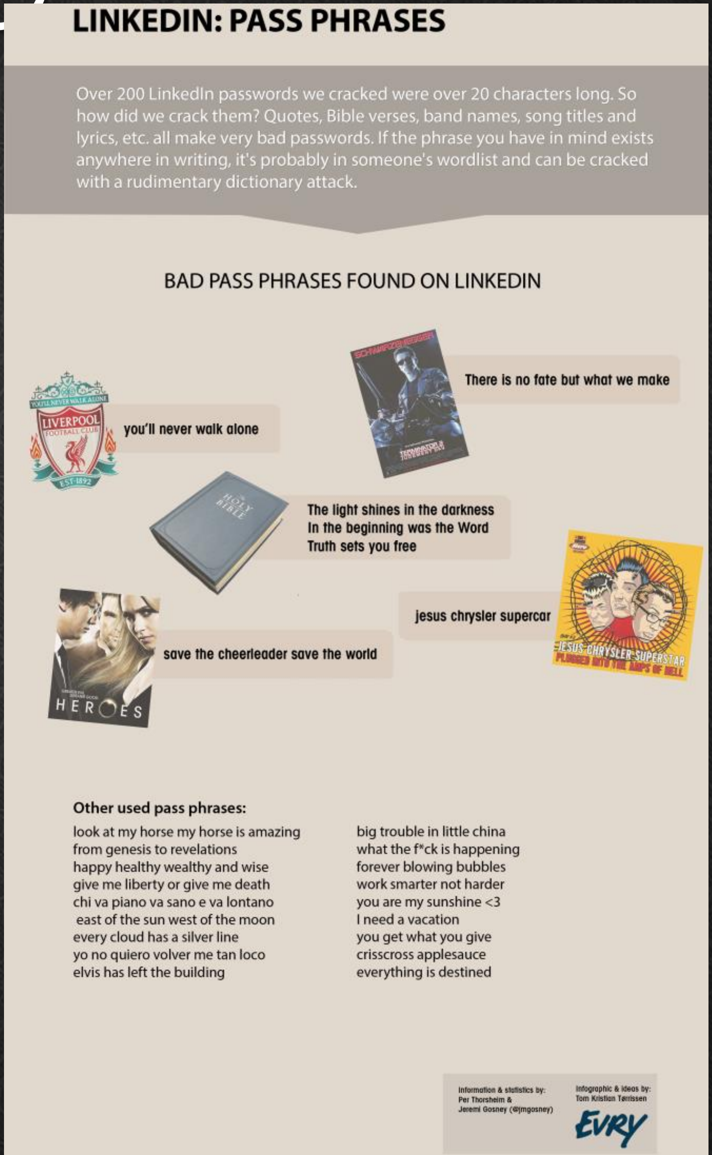
in = Can this be connected to Linkedin?

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

There is no fate but what we make

you'll never walk alone

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

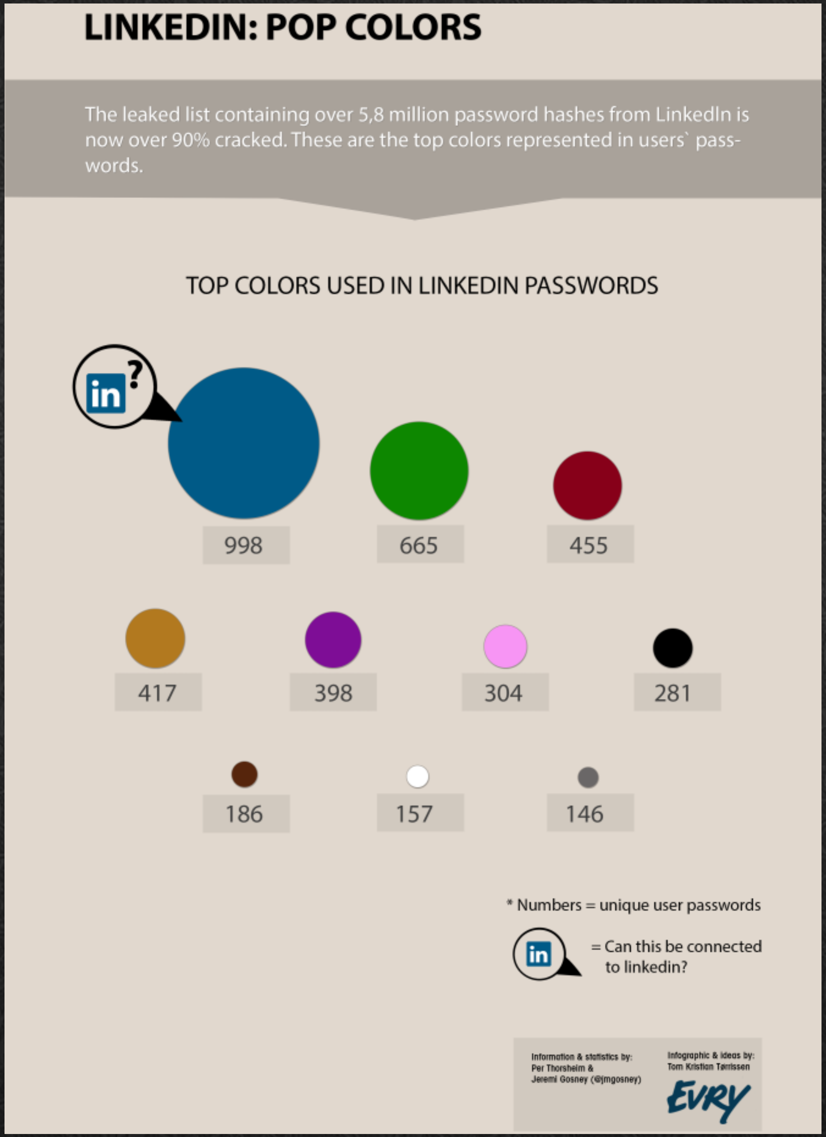
big trouble in little china
what the f*ck is happening
forever blowing bubbles
work smarter not harder
you are my sunshine <3
I need a vacation
you get what you give
crisscross applesauce
everything is destined

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

Infographic & ideas by:
Tom Kristian Tørrissen

EVRY

Color words in Linkedin passwords



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

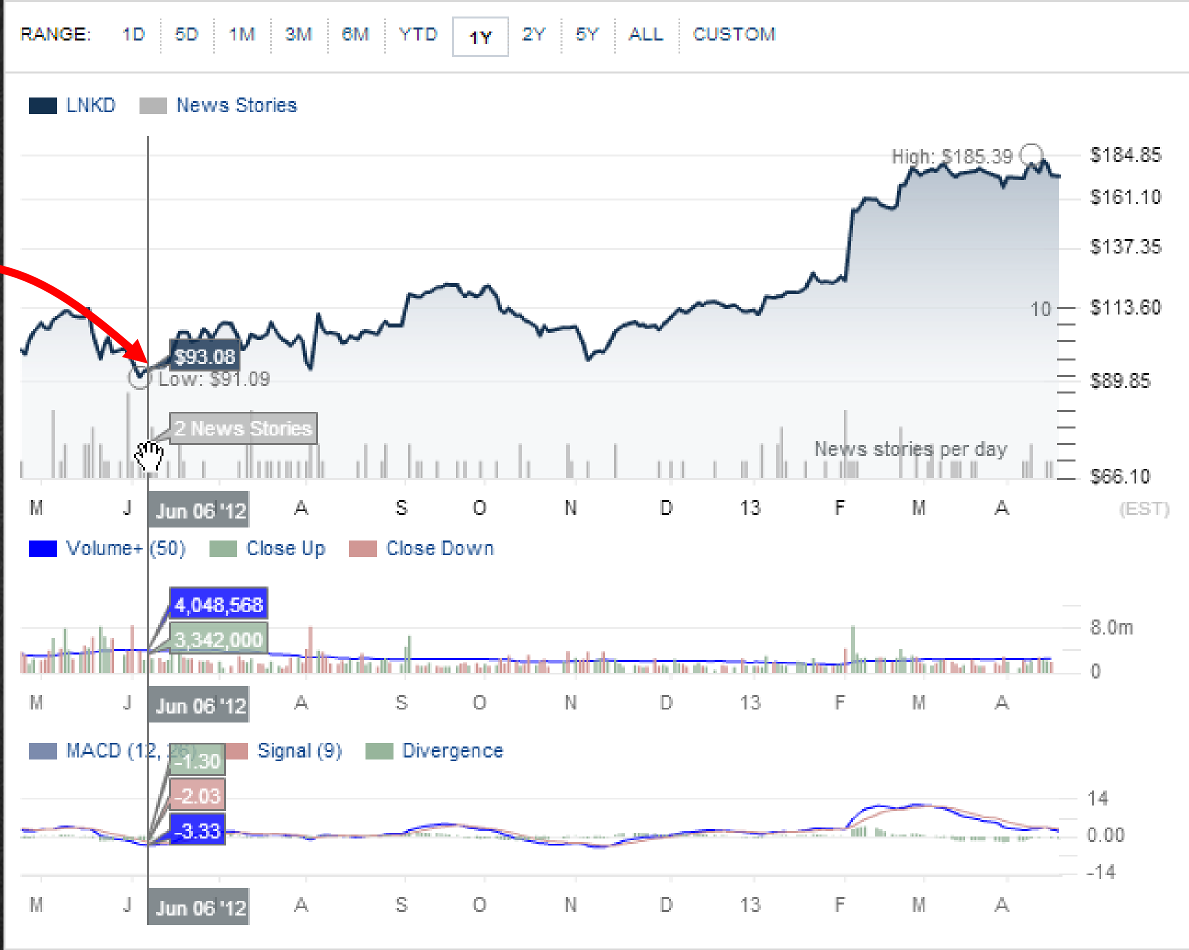
in = Can this be connected to linkedin?

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

Infographic & ideas by:
Tom Kristian Tørrissen
EVRY

Linkedin share price development

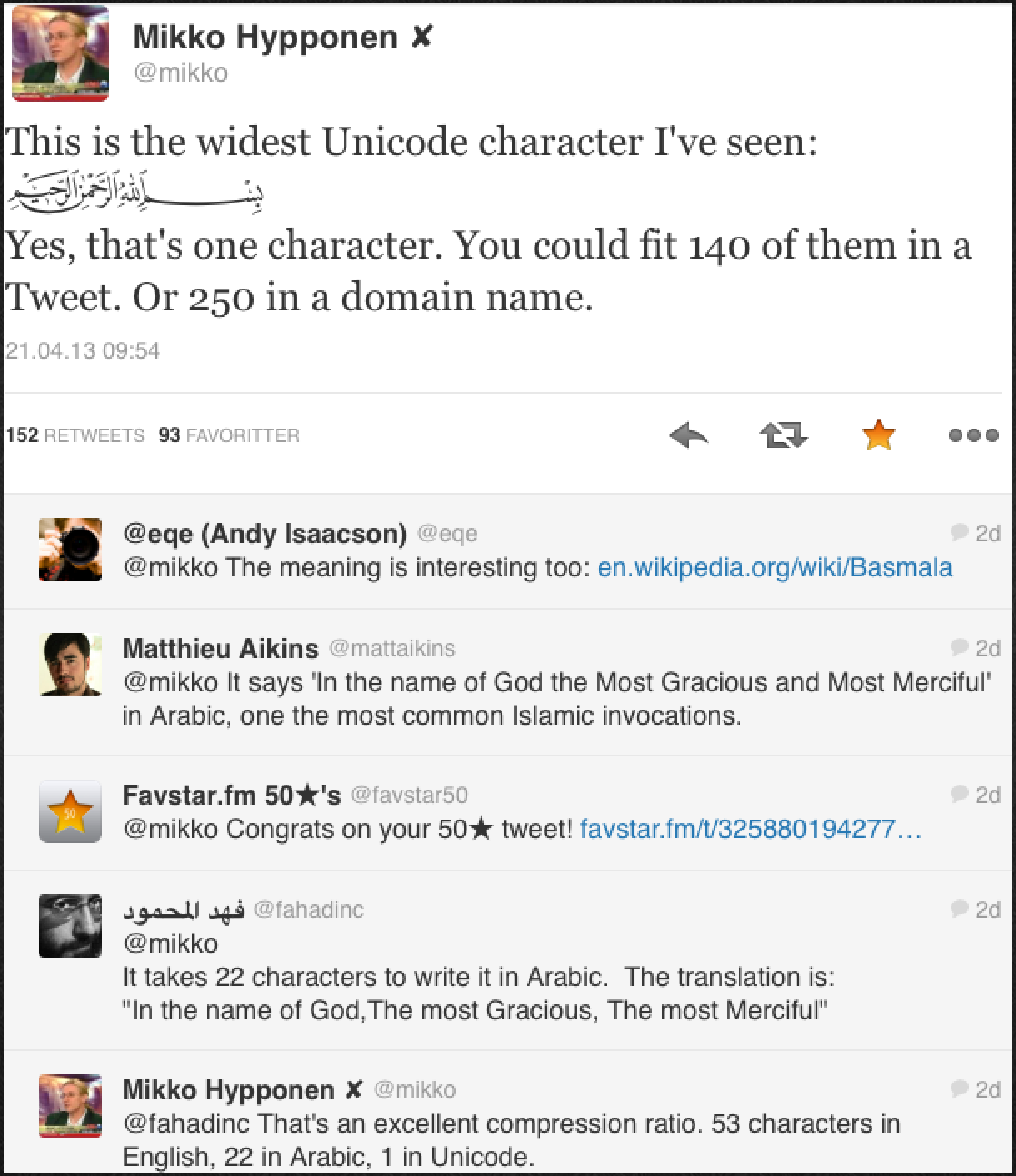
June 6, 2012
Linkedin breach
goes public.



Charsets & Keyspace Calculations

- 4 character groups:
  - lowercase, UPPERCASE, 0-9, !»#%&/()=?`+
- Unicode 6.0 has 109242 characters (!)
  - Video: https://vimeo.com/48858289
- Effect of password policies on keyspace reductions:

  http://openwall.info/wiki/john/policy



Mikko Hypponen ✘
@mikko

This is the widest Unicode character I've seen:
﷽
Yes, that's one character. You could fit 140 of them in a Tweet. Or 250 in a domain name.

21.04.13 09:54

152 RETWEETS **93** FAVORITTER

@eqe (Andy Isaacson) @eqe 2d
@mikko The meaning is interesting too: en.wikipedia.org/wiki/Basmala

Matthieu Aikins @mattaikins 2d
@mikko It says 'In the name of God the Most Gracious and Most Merciful' in Arabic, one the most common Islamic invocations.

Favstar.fm 50★'s @favstar50 2d
@mikko Congrats on your 50★ tweet! favstar.fm/t/325880194277…

فهد المحمود @fahadinc 2d
@mikko
It takes 22 characters to write it in Arabic. The translation is:
"In the name of God,The most Gracious, The most Merciful"

Mikko Hypponen ✘ @mikko 2d
@fahadinc That's an excellent compression ratio. 53 characters in English, 22 in Arabic, 1 in Unicode.

Operation «Face Factor»

- Unique opportunity
- 5000+ headshots
- Passwords, full name etc available
- Analyze!

Categorization

Facial hair

No

Mustache

Little beard

Porn donut

Full beard

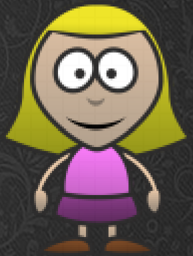
«Unix Guru»

Gender

Glasses (Y/N)

Hair color

Facial hair



Hair color

No hair

«Blond»

Really blond

Brunette

Redhead

Silverfox

… and the result?

Women prefer length.

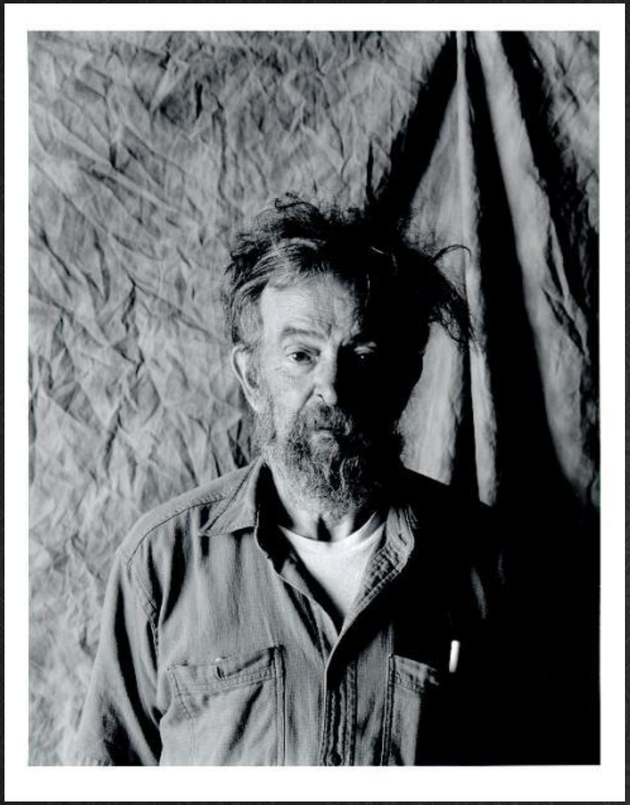
Men prefer variety (entropy).

«Unix gurus» came in last.

The Passwords^ conference

- 2012 archive: Passwords12.at.ifi.uio.no
- Planning 2 conferences this year:
  - Las Vegas, end of July. CFP open until May 17. Operational perspective. See passwordscon.org
  - Bergen, December. FRISC. Academic perspective.

Robert Morris



The three golden rules to ensure computer security are:

1. Do not own a computer;
2. Do not power it on;
3. And do not use it.

"Never underestimate the attention, risk, money and time that an opponent will put into reading traffic."

Thank You!

Per Thorsheim

securitynirvana.blogspot.com

@thorsheim

/GodPraksis

/user/thorsheim

per.thorsheim

+47 90 99 92 59