

Passwords, pins & digital authentication Past, Present and Future?

Per Thorsheim



20:46

Tweet



Per Thorsheim  @thorsheim · 19 m

Got a reputation to maintain.

I have it verbally from [@CormacHerley](#), with a witness present, that he's interested in passwords while I'm obsessed with it.

Cormac: please confirm statement? :-D



Cormac Herley
@CormacHerley

Svar til [@thorsheim](#) og [@spazef0rze](#)

Confirm. I have a healthy curiosity, while [@thorsheim](#) is pathologically obsessed.

[Oversett fra engelsk](#)

02.01.2018, 20:42



Even our government #FAIL?

Anbefaling	NorSIS	Nettvett
Bruk kombinasjon av tall og bokstaver		Y
Passordet må være lett å huske		Y
Passordet må være lett å huske, men vanskelig for andre å gjette		Y
Passordet bør bestå av en kombinasjon av små og store bokstaver, tall og spesialtegn		Y
Vær forsiktig med å bruke det samme passordet på flere tjenester		Y
Unngå bruk av ord som finnes i ordlister eller knyttet til personlig informasjon		Y
Passordet bør ikke inneholde bokstavene Æ, Ø eller Å		Y
Tips: Bruk L33T språk (bokstav <-> tall erstatninger)		Y
Minstelengde	8	8
Bruk store og små bokstaver	Y	Y
Tips: forkortede setninger (5rEftd7M)	Y	Y
Baser ikke passord eller PIN-koder på personlig informasjon	Y	
Unngå ord som finnes i ordbøker (gjelder alle språk)	Y	
Unngå bokstavkombinasjoner som ligner på ord	Y	
Passord bør være så langt som mulig, og minst 8 tegn	Y	
Benytt ulike passord for ulike tilganger	Y	
Bytt passord med jevne mellomrom	Y	
Bruk passfraser (setninger)	Y	
Oppgi aldri passord eller koder til noen – selv ikke banken	Y	
Passord skal være på minimum åtte tegn, og skal inneholde både bokstaver, tall og eventuelt spesialtegn	Y	
Alle standard brukeridenter og passord fra leverandører skal endres før produktet settes i produksjon	Y	

Passwords:

- Won't go away anytime soon
- People don't like to remember them
 - There's no "fun" in remembering passwords
- "How to create..." is not really successful

People forget (or don't know)

- ⦿ An attacker doesn't need your password
- ⦿ Many people have technical access
 - (but very few has legal access to your data)
- ⦿ ... and what about your helpdesk?

We can't..

- Prohibit "weak" passwords
 - Unless, of course, "1984" becomes reality

We should

- Crack our passwords regularly
 - Risk exposure
 - User education / awareness
- Improve our systems
 - Salt, anyone?

You should

- Use a sentence as your password
- If you forget it, use:

I forgot my password.

Password recommendations*

- Make your password a sentence
- Unique account, unique password
 - Write down your passwords
 - Use 2-factor authentication

* As written for the US National Cyber Security Alliance for World Password Day 2016.

And the best news of the day:

Mandatory & frequent change of passwords are stupid!

1. decreases security
2. destroys the user experience
3. Waste of valuable time



';-have i been pwned?

Check if you have an account that has been compromised in a data breach

email address

271
pwned websites

4,949,099,146
pwned accounts


64,696
pastes

71,739,614
paste accounts

Haveibeenpwned.com

What is 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

 Follow

Tweets All / No replies



The Associated Press @AP

2m

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

Expand

Dow



**USD 136.5
BILLION
dollars**

**Window of
Opportunity
= 7 minutes**



الجيش السوري الإلكتروني

SYRIAN ELECTRONIC ARMY

Bedragere lurte norsk bedrift for en halv milliard kroner mot metoden.

EUR 52,000,000

...io bedragere til mot den norske bedriften.
...s gikk politiet ut med en advarsel om metoden som
svindlerne brukte.

ASHLEY MADISON®

Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select ▾

[See Your Matches »](#)

Over **37,565,000** anonymous members!



As seen on: Hannity, Howard Stern, TIME, BusinessWeek, Sports Illustrated, Maxim, USA Today

Ashley Madison is the world's leading married dating service for **discreet** encounters



Trusted Security Award



SSL Secure Site

Change frequencies

A little test of your password guessing capabilities

September1

September2

September3

The problems with forcing regular password expiry

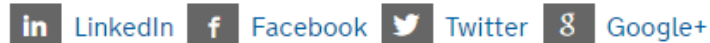
Version: 1

Created: 11 April 2016

Updated: 15 April 2016

Topics: [Passwords](#), [Best Practice](#)

Share this page



Why CESG decided to advise against this long-established security guideline.

Regular password expiry is a common requirement in many security policies. However, in [CESG's Password Guidance](#) published in 2015, we explicitly advised against it. This article explains why we made this (for many) unexpected recommendation, and why we think it's the right way forward.

Let's consider how we might limit the harm that comes from an attacker who knows a user's password. The obvious answer is to make the compromised password useless by forcing the legitimate user to replace it with a new one that the attacker doesn't know. This advice seems straightforward enough.

The problem is that this doesn't take into account the inconvenience to users - the 'usability costs' - of forcing users to frequently change their passwords. The majority of password policies force us to use passwords that we find hard to remember. Our passwords have to be a *handful* of passwords, we can't d

Related Content

[Making security better: Passwords](#)

[Password Guidance: Simplifying Your Approach](#)

[Revealed: the most frequently used passwords of 2015](#)

[Certified Cyber Security Consultancy](#)

[Keeping bulk personal data safe](#)

<https://www.cesg.gov.uk/articles/problems-forcing-regular-password-expiry>

NIST SP800-63B

«Toward better password requirements» – Jim Fenton

#passwords16, BSidesLV

<https://www.youtube.com/watch?v=nXg-kh7fKEE>

NIST SP800-63B

- No more forced & regular password change
- Drop the complexity requirements (length trumps everything!)
- Stop using SMS for sending secrets
- Implement (dynamic) password block lists; 1K-10K most common
 - `OpenPasswordFilter` on GitHub for Windows

Operation «Face Factor»

- Unique opportunity!
- 5000+ photos used on access cards
- ... we knew their passwords
- Analyze all the data!



Categorization

Facial hair

No

Mustache

Small beard

Full beard

«Unix Guru»

«Porn donut»



Gender

Glasses (Y/N)

Hair color

Facial hair



Hair color

No 😊

«Blond»

Superblond

Brunette

Redhead

«Silver fox»

And the results?

Women prefer length.

Men prefer a wider selection (entropy).

«Unix gurus» have the worst passwords.

PINs

1234

Choose your pins (17 year olds, fall 2013)



Girls
1996

Boys
1337
1996

Most common 4-digit PINs:

1234

0000

2580

1111

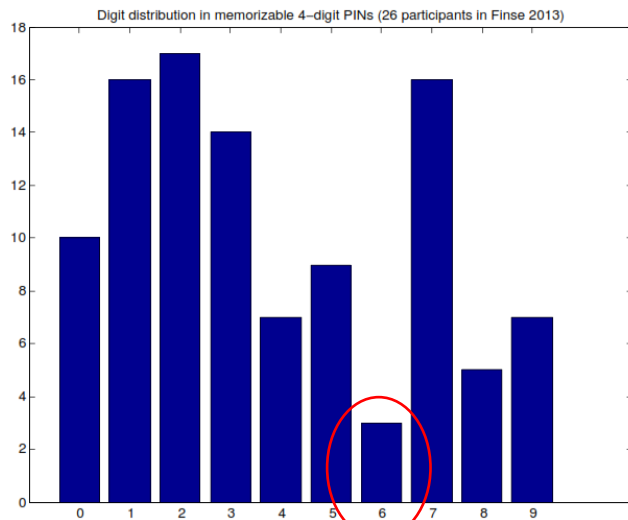
5555

5683

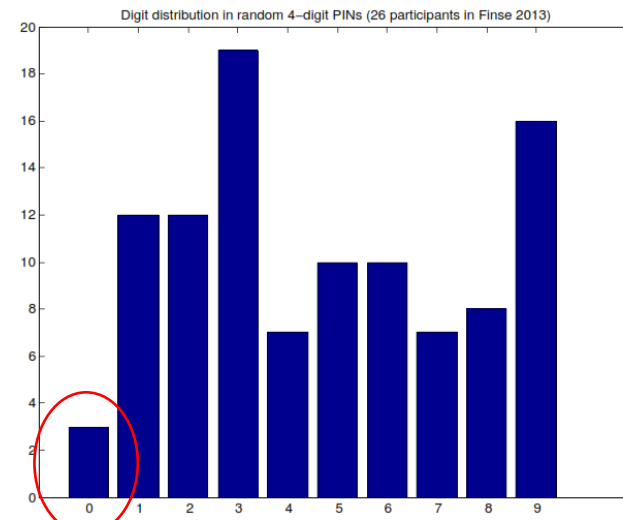
0852

Digit distribution for PINs

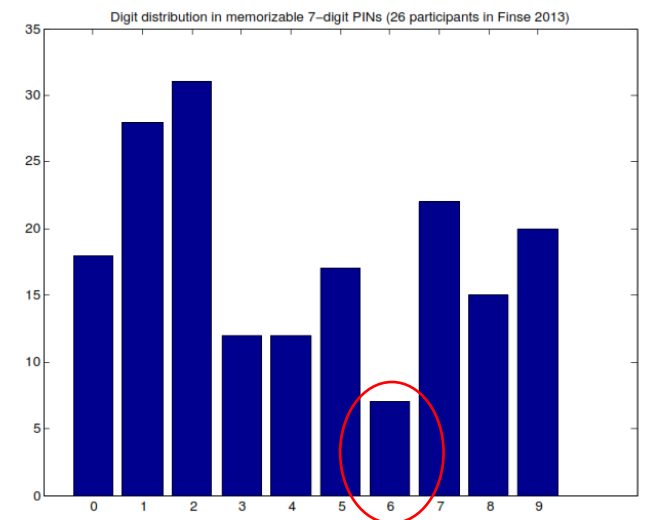
4-digit memorable



4-digit non-memorable



7-digit memorable



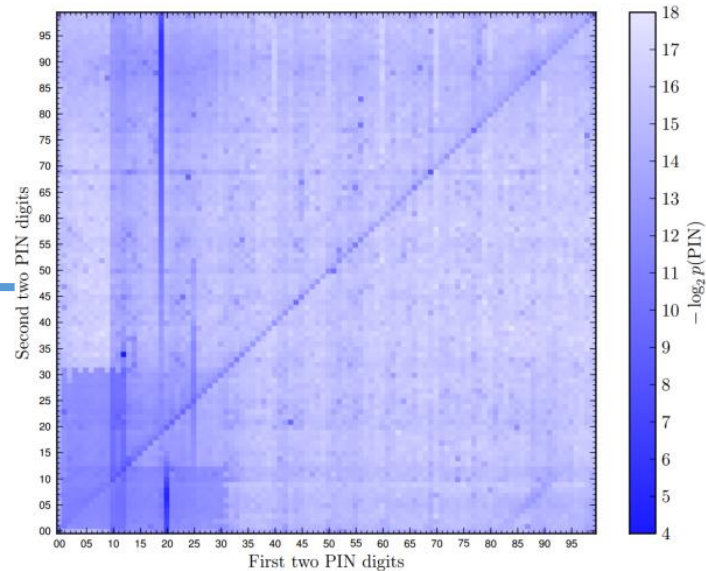
Digit 0 is not «random» enough?

Digit 6 is hard to remember?

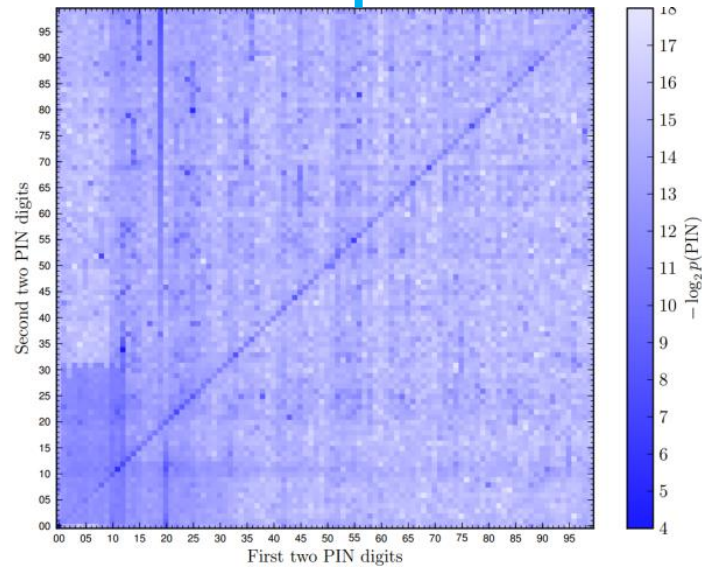
Thank you to Andrey Bogdanov, Sondre Rønjom & Jan Fredrik Leversund for great help!

Heatmapping PINs @Cambridge

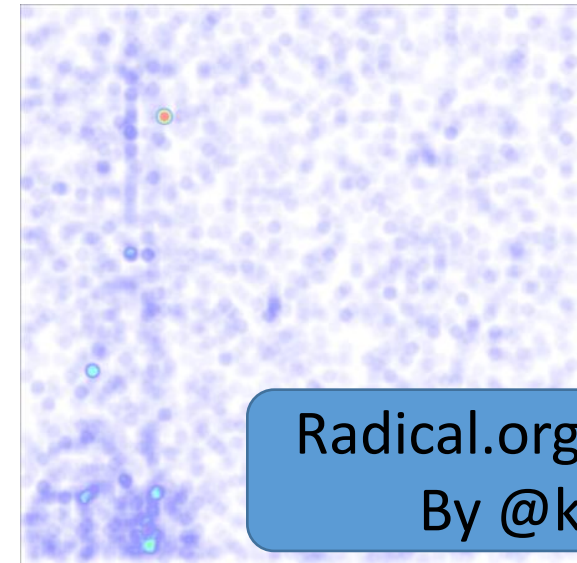
Rockyou



iPhone



Physical access
Control system



Radical.org/pinmap
By @kluzz

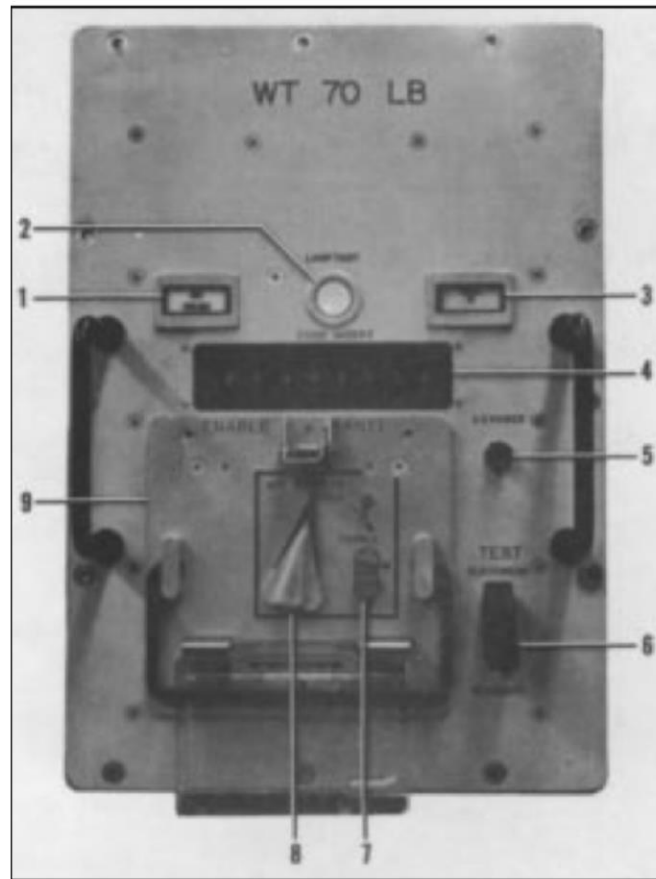
A birthday present every eleven wallets? The security of customer-chosen banking PINs

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

<http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes>

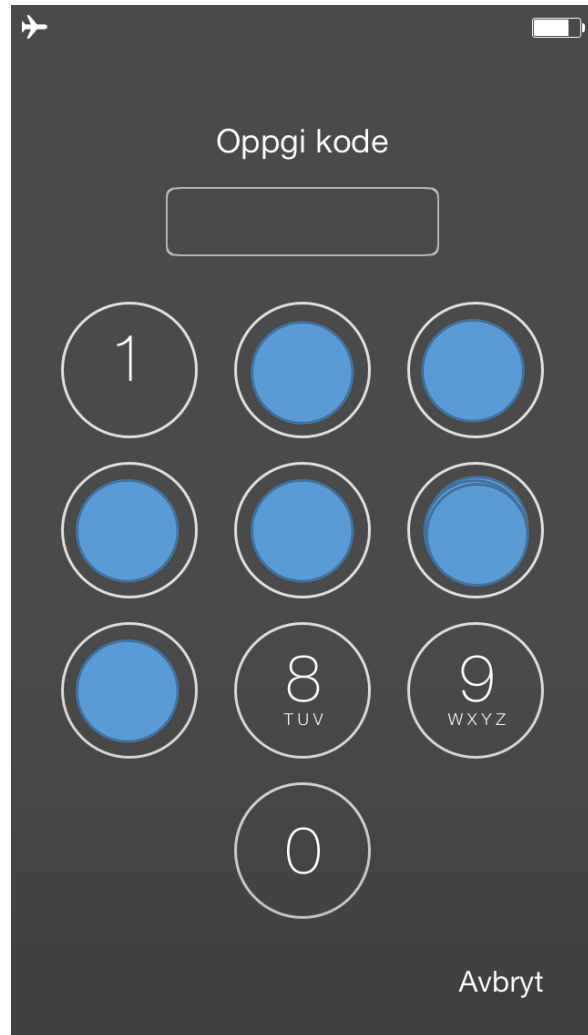
See also: <http://www.datagenetics.com/blog/september32012/index.html>



Bruce Blair, 2015

<https://sgs.princeton.edu/00000000>

Creating a long & memorable PIN:

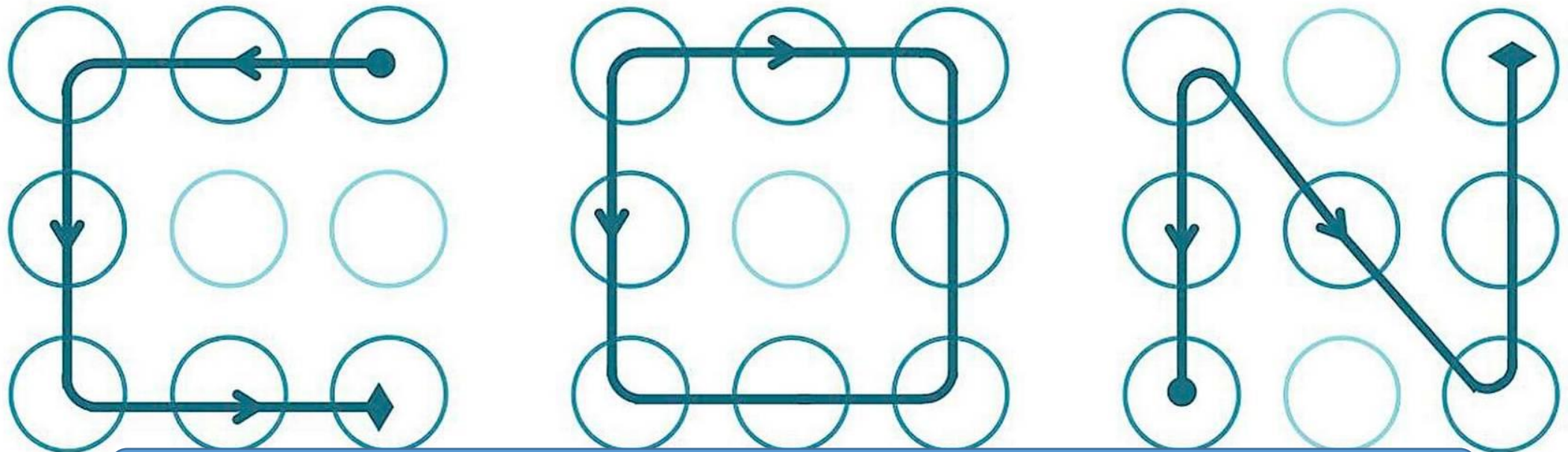


=

Johansen
56426736



(Android) Lock Patterns



10% uses a letter from standard English alphabet



«On User Choice for Android Unlock Patterns»
Loge, Duermuth, Rostad

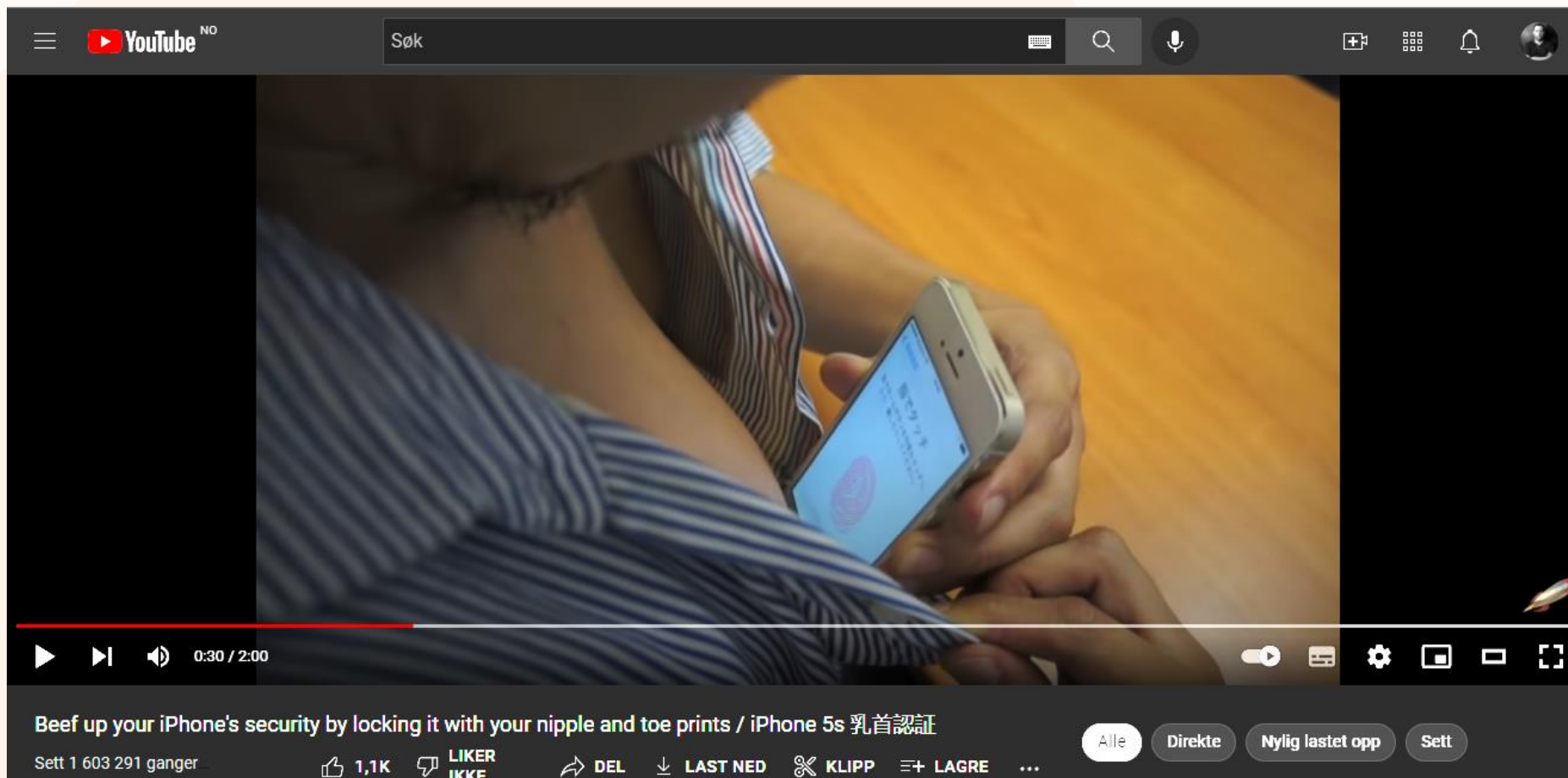
PasswordsCon.org
youtube.com/user/thorsheim

Password alternatives

As in: ADDITIONS to passwords!



HOWTO: Improve your phone biometric protection



The image shows a YouTube video player interface. The video content displays a person's hands holding a white iPhone 5s. The phone's screen shows a biometric security interface with a fingerprint sensor icon. The video player includes a dark grey header with the YouTube logo, a search bar containing the text "Søk", and navigation icons for search, microphone, share, grid, notifications, and profile. The video progress bar is at 0:30 / 2:00. The video title is "Beef up your iPhone's security by locking it with your nipple and toe prints / iPhone 5s 乳首認証". Below the title, it shows "Sett 1 603 291 ganger" and engagement icons for likes (1,1K), dislikes (LIKER IKKE), share (DEL), download (LAST NED), clips (KLIPP), and save (LAGRE). At the bottom right, there are buttons for "Alle", "Direkte", "Nylig lastet opp", and "Sett".

YouTube NO Søk

0:30 / 2:00

Beef up your iPhone's security by locking it with your nipple and toe prints / iPhone 5s 乳首認証

Sett 1 603 291 ganger

1,1K LIKER IKKE DEL LAST NED KLIPP LAGRE

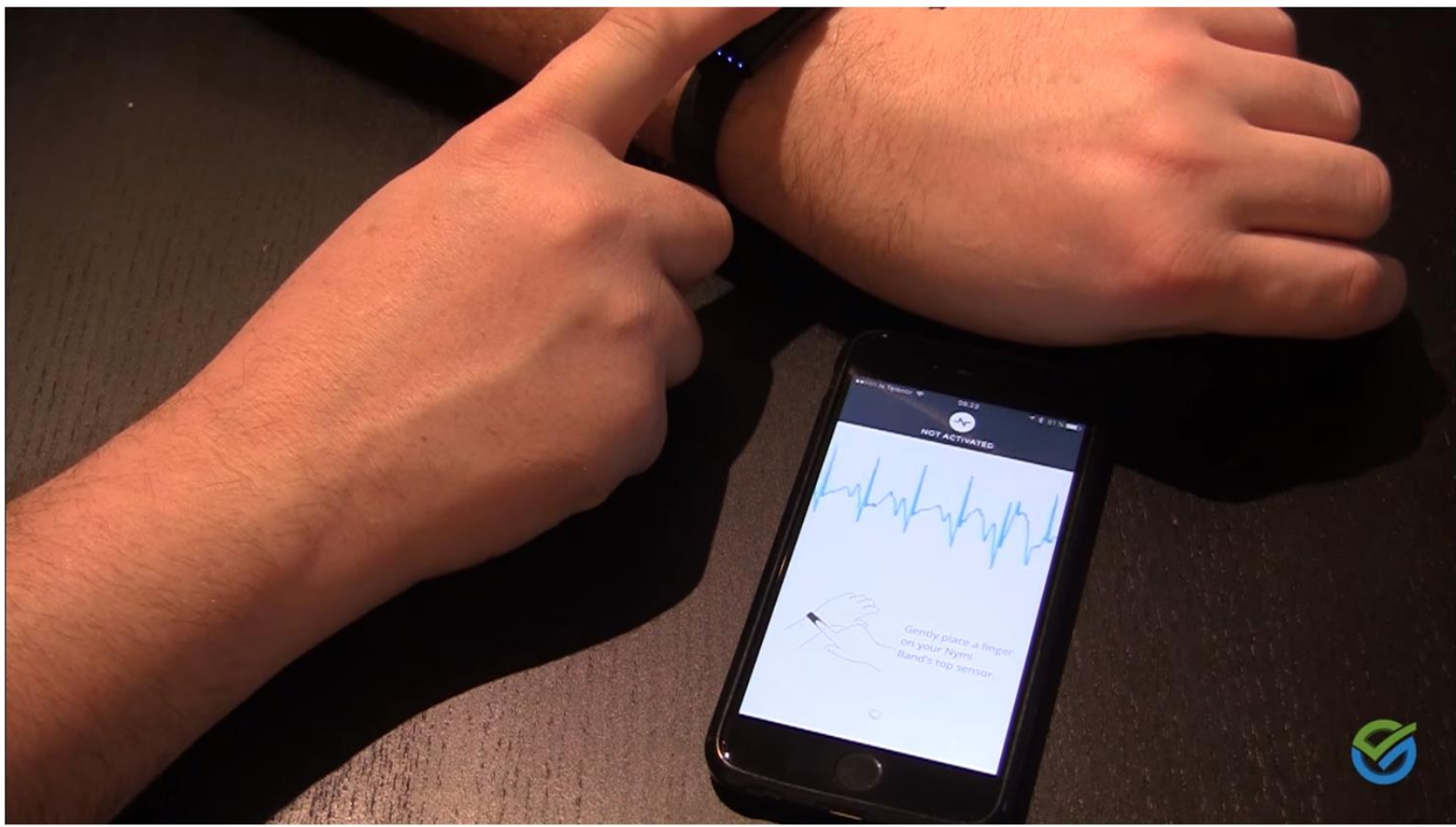
Alle Direkte Nylig lastet opp Sett



ABOUT THE NYMI BAND

Learn more ▶





Insecure Non-Continuous Authentication with Nymi Band

sett 3 887 ganger

15 7 DEL + ...

Neste

AUTOMATISK AVSPILLING



Nymi Band Discovery Kit Unboxing and Demo -
MobileSyrup
sett 3,8k ganger



PENN AND TELLER MOST CONTROVERSIAL MAGICIAN
Ivan Amodei
Anbefalt for deg



GH5 Autofocus FIXED! (2018 Update) | New Tracking Settings
Gerald Undone
Anbefalt for deg



***NEW* GH5 AF FIX | Better than Canon/Sony?**
Matt Krieg
Anbefalt for deg



Making of monotype-prints with plastic bags 3
Rafael Springer
Anbefalt for deg



Keyboard Privacy

tilbudt av Uurity Group

★★★★★ (11)

[Utviklerverktøy](#)

5 115 brukere

LAGT TIL I CHROME



OVERSIKT

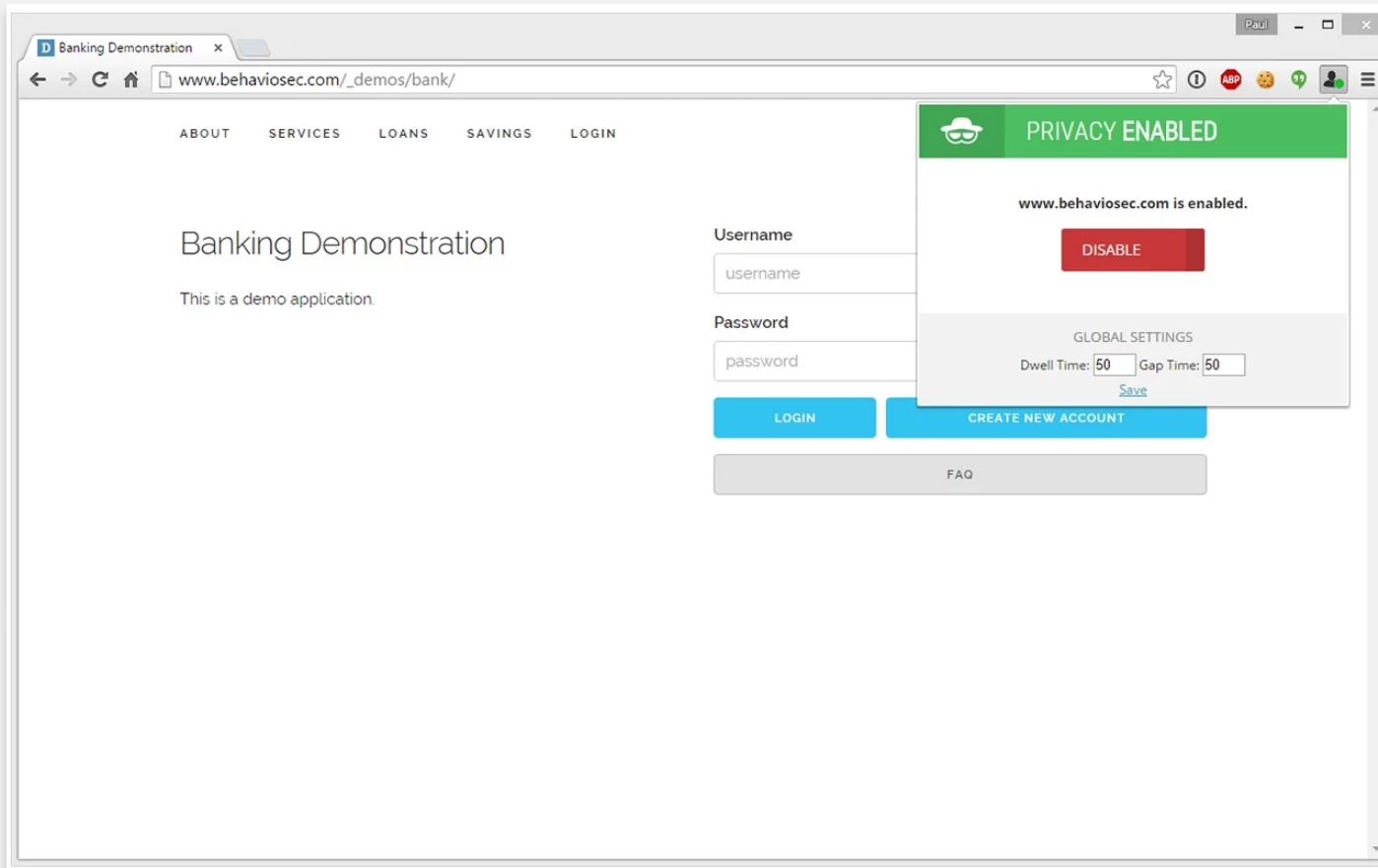
ANMELDELSER

BRUKERSTØTTE

RELATERT

G+1

33



Kompatibel med enheten din

Prevents behavioral profiling by randomizing the rate at which characters reach the DOM.

Prevents behavioral profiling by randomizing the rate at which characters reach the DOM.

Notice:

This is a proof-of-concept plugin, following research by two independent security professionals (Paul Moore & Per Thorsheim). See <https://paul.reviews/behavioral-profiling-the-password-you-cant-change/> for more details.

[Nettsted](#)

[Rapporter misbruk](#)

Versjon: 2.4

Oppdatert: 28. juli 2015

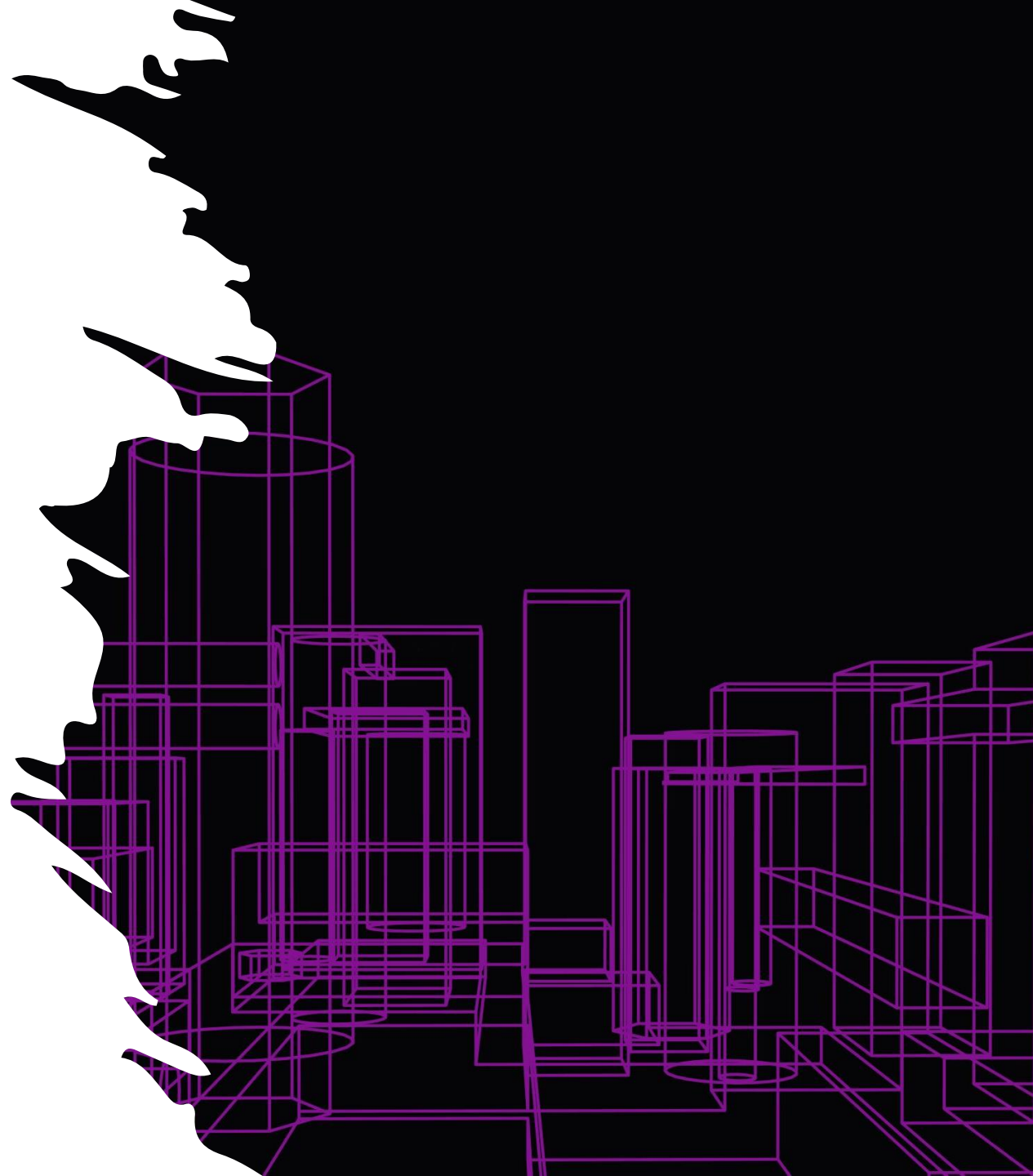
Størrelse: 88.74KiB

Språk: English

Fighting Phone & SMS Spoofing: From Users to Governments

Per Thorsheim

CISA, CRISC



lørdag 10. august 2019



Vi klarte ikke å fakturere ditt medlemskap for inneværende måned. Prøv på nytt, eller oppdater betalingsopplysningene dine for å fortsette å se på Netflix

4pc.xyz/Siste

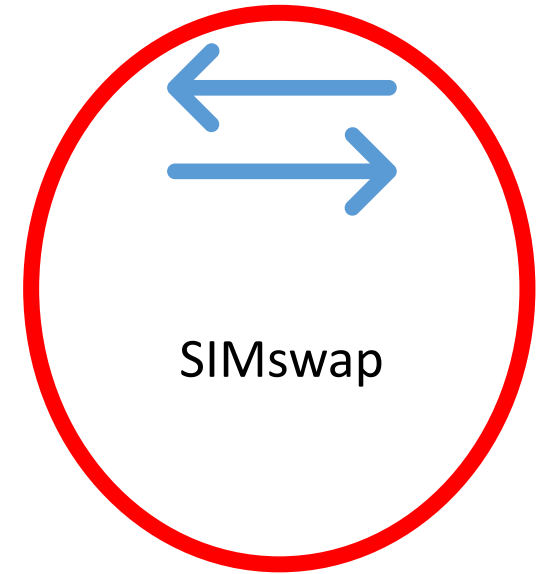
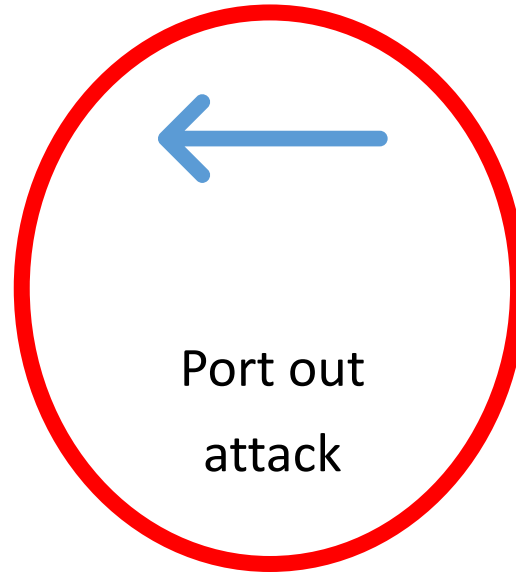
Netflix

<http://4pc.xyz/Siste>

18:31

Mobile Hijacking

2019



Spoofting



«Traditional fraud»



Du er her: [Forsiden](#) • [Aktuelt](#) • [Tiltak for å forhindre mobilkapring](#)

Tiltak for å forhindre mobilkapring

Pressemelding | Dato: 03.09.2019

– Telefonnummeret vårt er i dag knyttet til så mange personlige tjenester, at det er nødvendig å sikre oss be mot at det kan overtas av andre. Vi har sett flere eksempler på at kriminelle har lyktes med å opprette SIM-kort i falskt navn til tross for at loven stiller krav om entydig identifisering. Regjeringen foreslår derfor tydeligere krav til identifisering for å opprette eller endre telefonavtaler, sier digitaliseringsminister Nikolai Astrup.

Kommunal- og moderniseringsdepartementet

Hearing from Norwegian government on September 3, 2019: Actions to prevent mobile hijacking.

RELATERT

- ▶ [Høring om endringer i ekomloven og ekomforskriften med forslag om lovhjemmel for leveringsplikt for bredbånd og tydeligere krav til entydig identifisering av sluttbrukere](#)

#VoiceMailHijacking (spoofing)

Digi.no, version2.dk, nyteknik.se
november/december 2019



Lohans nummer på nett

27 August 2006

Paris Hilton har selv fått smake hvordan det er å lekke hele telefonlisten på nettet. Nå er det Lindsay Lohans tur.

Del

↑ 27.08.06 08:54 ↻ 27.08.06 10:14

Na.

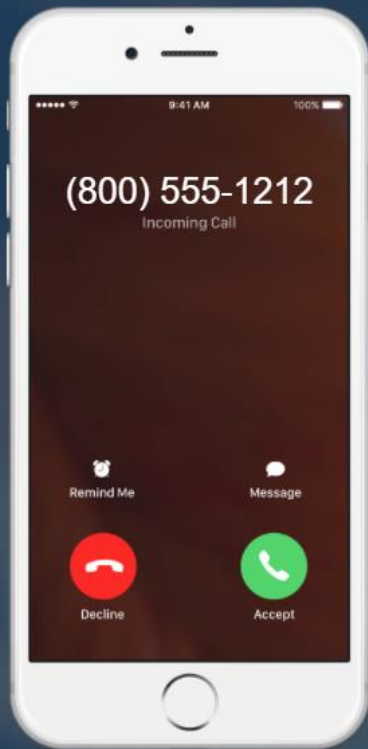
Trine Rasmussen

(SIDE2): Paris Hilton (25) har selv fått sin telefon «hacket», og hennes private nummer ble den gang spredt ut på nettet.

Let's hack!

UEE
NEY

UEE
NEY



Protect Your Privacy

Call and text from a secondary number to protect your personal information and privacy. It's easy to use and works on any phone. Try it for FREE when you sign up on our mobile apps!



Trusted by over 5 Million people who value their privacy.

This website uses cookies to ensure you get the best experience on our website. [Learn more](#)

[Got it!](#)

Scroll to learn more



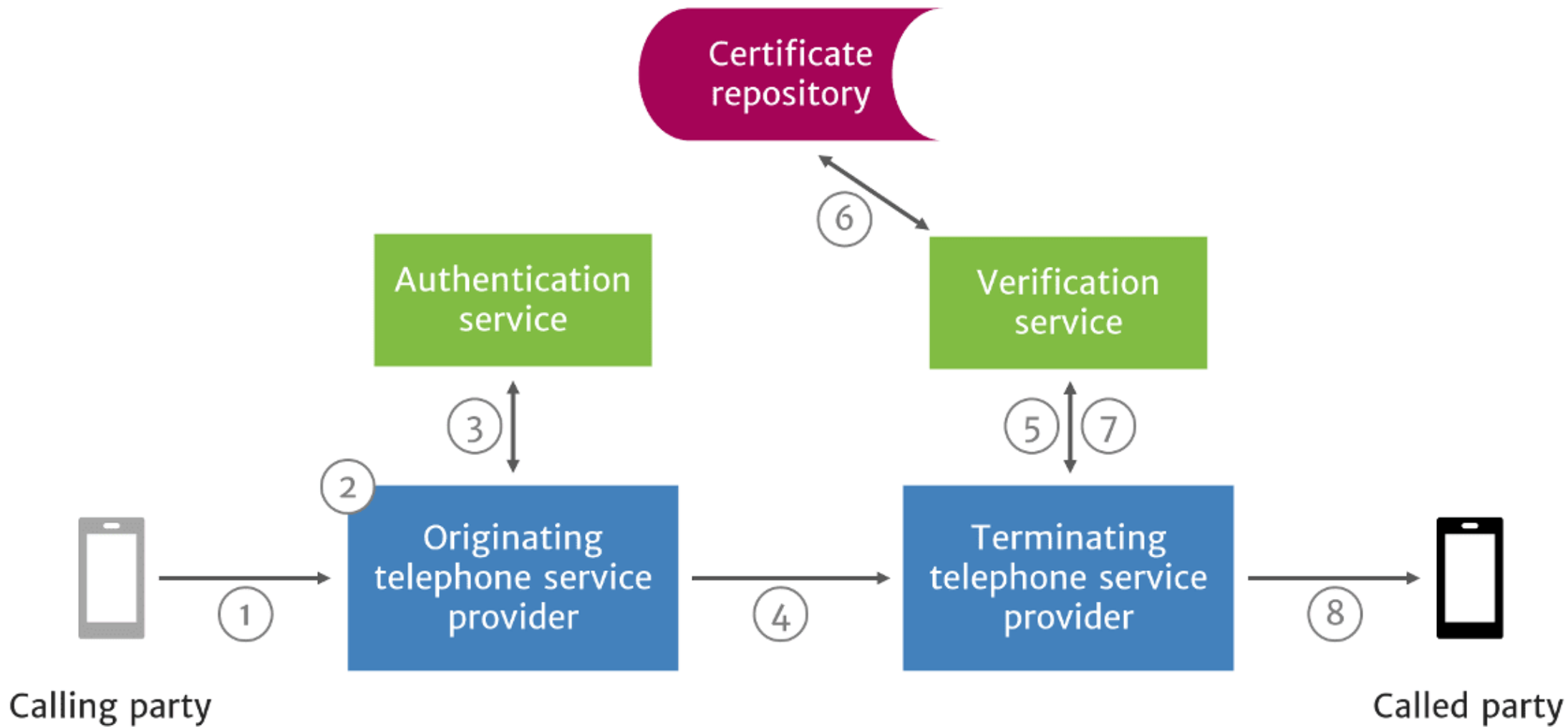
[Hjelp](#)



HOWTO: reduce phone spoofing

STIR/SHAKEN to the people!





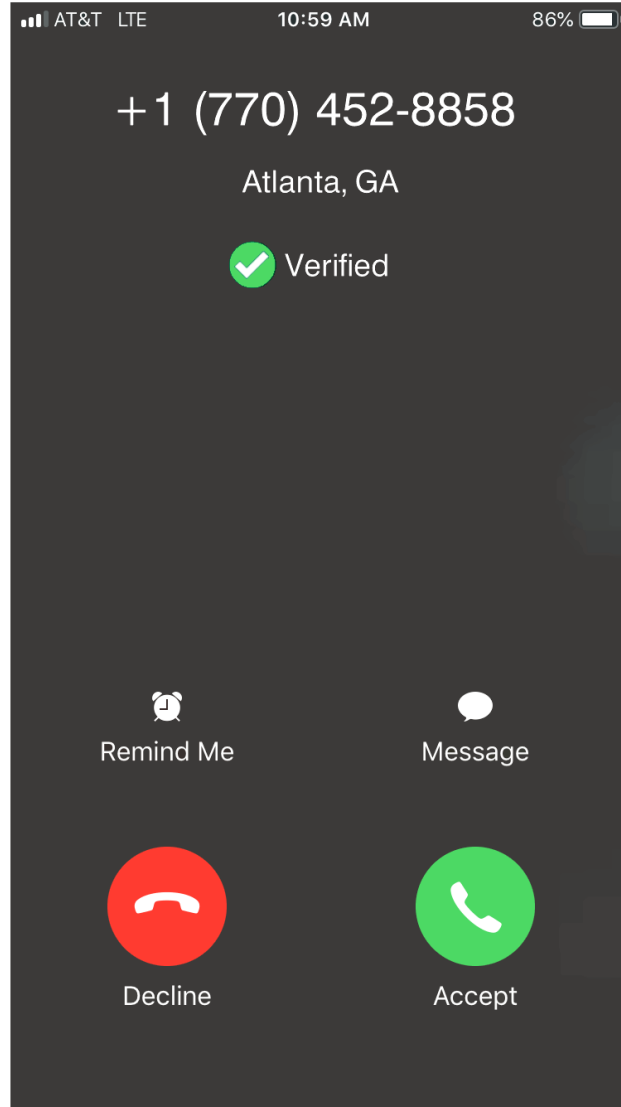
STIR/SHAKEN – Attestation of calls*

- Full attestation
 - The service provider has authenticated the calling party and they are authorized to use the calling number. An example of this case is a subscriber registered with the originating telephone service provider's softswitch.
- Partial attestation
 - The service provider has authenticated the call origination, but cannot verify the call source is authorized to use the calling number. An example of this use case is a telephone number behind an enterprise PBX.
- Gateway attestation
 - The service provider has authenticated from where it received the call, but cannot authenticate the call source. An example of this case would be a call received from an international gateway.

** Text totally ripped from <https://transnexus.com/whitepapers/understanding-stir-shaken/>*

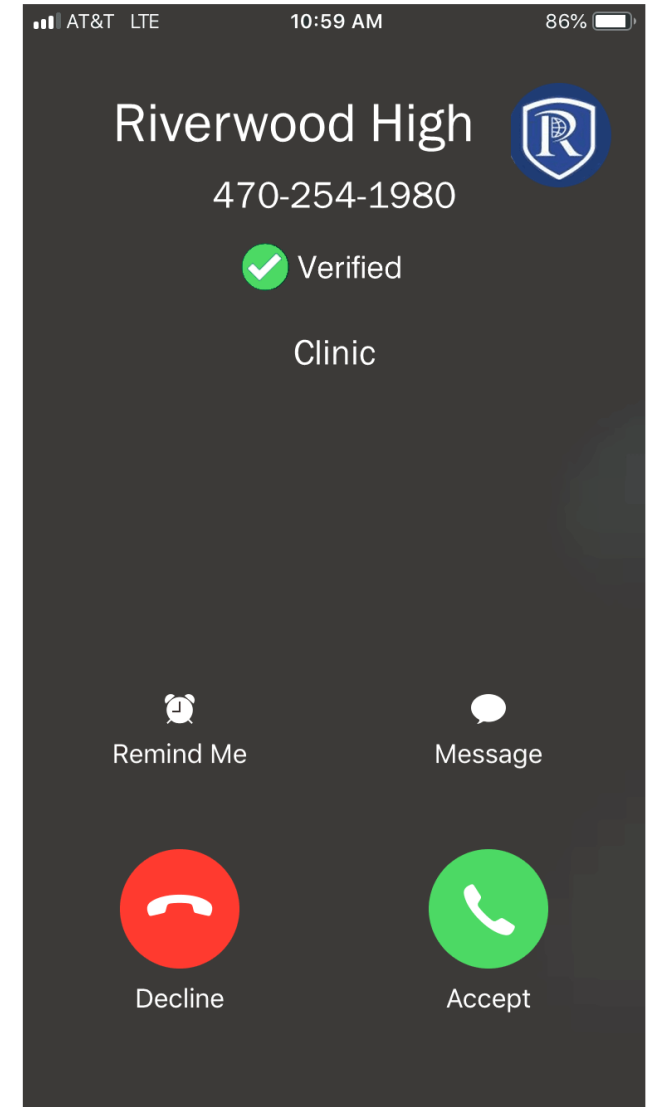
iPhone today

iPhone with STIR/SHAKEN



Cost (?)

iPhone with STIR/SHAKEN & Rich Call Data (RCD)



Business opportunity?

Timelines

USA & Canada

- Jan 2018: Canada expect implementation by March 31, 2019
 - Delayed several times
 - Post-deploy report by May 31, 2022
- DeC 2019: TRACED Act i USA
 - FCC approval March 31, 2020
 - Big providers: June 30 2021
 - Small providers: June 30 2022
- June 30, 2021: T-Mobile USA announce 100% compliance

Norway

- <nothing to report here...>

CEPT ECC Report 338 – CLI Spoofing, June 2022

- Page 34:
- “It is unlikely that all operators in Europe will introduce systems to counteract CLI spoofing on their own initiative, without regulatory intervention. In that sense, the situation is similar to that in the USA where operators only introduced STIR/SHAKEN on a large scale after implementation of corresponding legislation.”
- It is likely that all European operators wishing to terminate calls, where both the called party number and the calling party number are US numbers, will in due course have to implement STIR/SHAKEN. Clearly, this technology has the first mover advantage.



Risk Based Authentication

riskbasedauthentication.org

And the results?

Women prefer length.

Men prefer variety (character entropy).

«Unix gurus» have the absolutely worst passwords.

Omtrent 6 430 resultater (0,46 sekunder)

<https://www.bbc.co.uk> > news > tec... [Oversett denne siden](#)

The gentle art of cracking passwords - BBC News

2. des. 2013 — These studies also reveal that when it comes to **passwords**, **women prefer length** and men diversity. Big data. These facts have come to light ...

<https://www.businessinsider.com> > ... [Oversett denne siden](#)

'Red-Haired Women Tend to Choose the Best Passwords and ...

2. des. 2013 — These studies also reveal that when it comes to **passwords**, **women prefer length** and men diversity.

<https://finance.yahoo.com> > news [Oversett denne siden](#)

'Red-Haired Women Tend To Choose The Best Passwords ...

2. des. 2013 — These studies also reveal that when it comes to **passwords**, **women prefer length** and men diversity. The problem with this amazing claim is that ...

<https://www.businessinsider.in> > art... [Oversett denne siden](#)

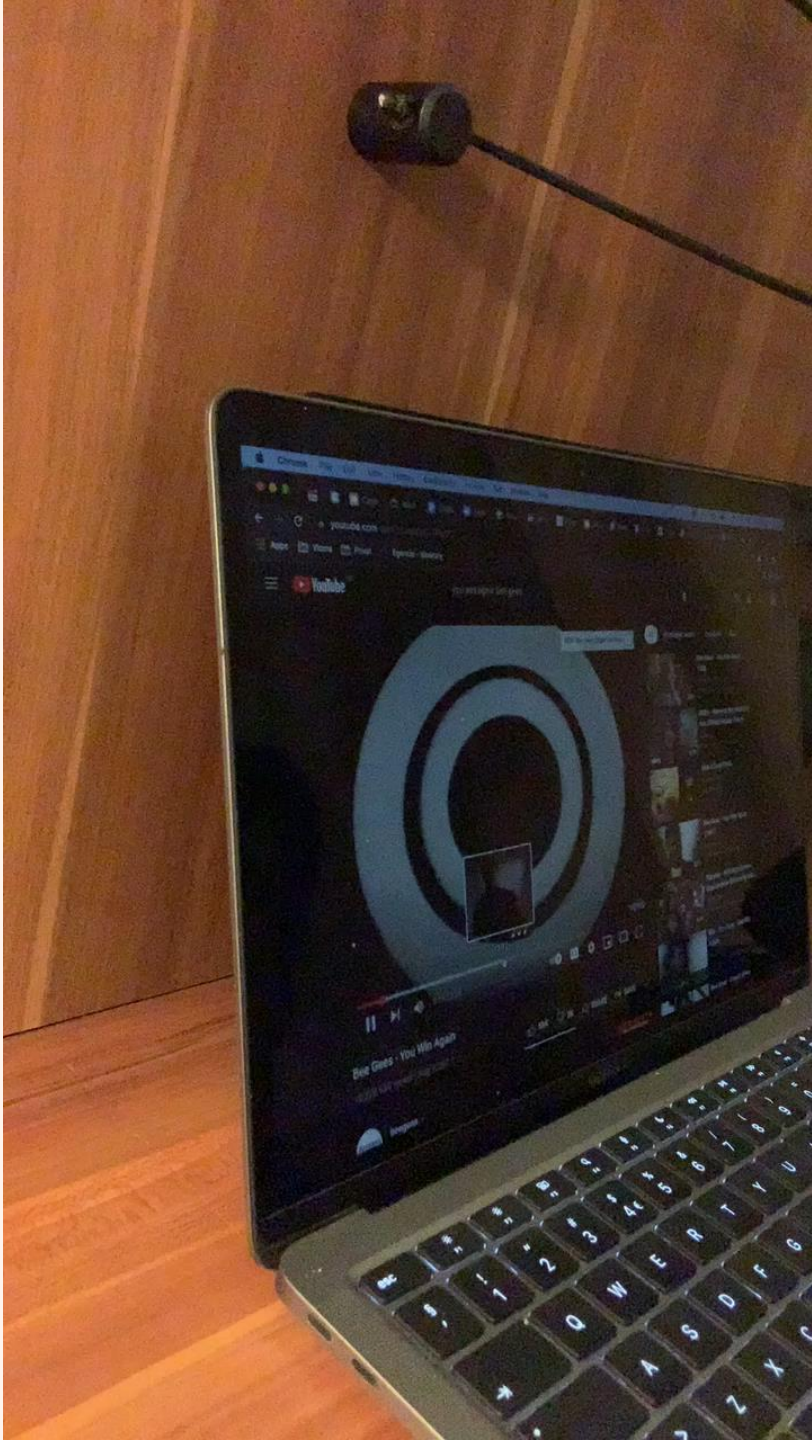
'Red-Haired Women Tend To Choose ... - Business Insider India

2. des. 2013 — studies suggest red-haired **women** tend to **choose** the best **passwords** and men with bushy beards or unkempt hair, the worst.

<https://it.slashdot.org> > story > why... [Oversett denne siden](#)

Why People Are So Bad At Picking Passwords - Slashdot

2. des. 2013 — These studies also reveal that when it comes to **passwords**, **women prefer length** and men diversity. On the internet, the most popular colour ...





[Learn more](#)

Periodic password expiration is an ancient and obsolete mitigation of very low value, and we don't believe it's worthwhile for our baseline to enforce any specific value.

Microsoft is pleased to announce the *draft* release of the security configuration baseline settings for Windows 10 version 1903 (a.k.a., "19H1"), and for Windows Server version 1903. Please evaluate these proposed baselines and send us your feedback via blog comments below.

Download the content here: [Windows-10-1903-Security-Baseline-DRAFT](#). As usual, the content includes GPO backups, GPO reports, scripts to apply settings to local GPO, Policy Analyzer rules files for each baseline and for the full set, and spreadsheets documenting all available GPOs and our recommended settings, settings that are new to this Feature Update, and changes from the previous baselines.

Note that Windows Server version 1903 is Server Core only and does not offer a Desktop Experience (a.k.a., "full") server installation option. In the past we have published baselines only for "full" server releases – Windows Server 2016 and 2019. Beginning with this release we intend to publish baselines for Core-only Windows Server versions as well. However, we do not intend at this time to distinguish settings in the baseline that apply only to Desktop Experience. When applied to Server Core, those settings are inert for all intents and purposes.

This new Windows Feature Update brings very few new Group Policy settings, which we list in the accompanying documentation. The draft baseline recommends configuring only two of those. However, we have made several changes to existing settings, and are considering other changes. Please review the changes carefully and let us know what you think.

[security guide](#)[security baselines](#)[SASC](#)[GRC](#)[DCM](#)[SCCM](#)[SCM update](#)[System Center](#)[malware](#)[customers](#)[Powershell](#)[malware defense](#)

Archives

[April 2019 \(1\)](#)[January 2019 \(1\)](#)[December 2018 \(1\)](#)[November 2018 \(1\)](#)



One IMPORTANT question!



A dark blue, irregularly shaped graphic with a splatter effect, containing white text. The graphic is centered on a white background and has a rough, hand-painted appearance with some lighter blue and white splatters around its edges.

Do I need an
account for that?



Good UX = Good security

IMHO

Onboarding & login process flow

When & why to ask for account creation & login





Creating a new account

(Again I'll ask: WHY do I need an account?)

Create a new account

FOCUS!

Choose a username

This is my beloved passphrase!

Hide



Enter password to confirm

Pros & Cons of «username» vs email?

Religious «EVIL EYE»!

Client-side passphrase generator

Your password cannot contain...
Minimum / maximum length
Any other requirements?

Redundant input field
(Less typing – better UX)

Password strength meter
(Gamification)

«Your password contains invalid characters.»

NO, your startup contains incompetent engineers.

@harribellthomas

About gamification...

HOW SECURE IS YOUR PASSWORD?

Never trust password meters!

Per Thorsheim

computer about

THOUSAND YEARS

to crack your password

not create even stronger passwords with **Dashlane**? It's free!

Tweet Your Result

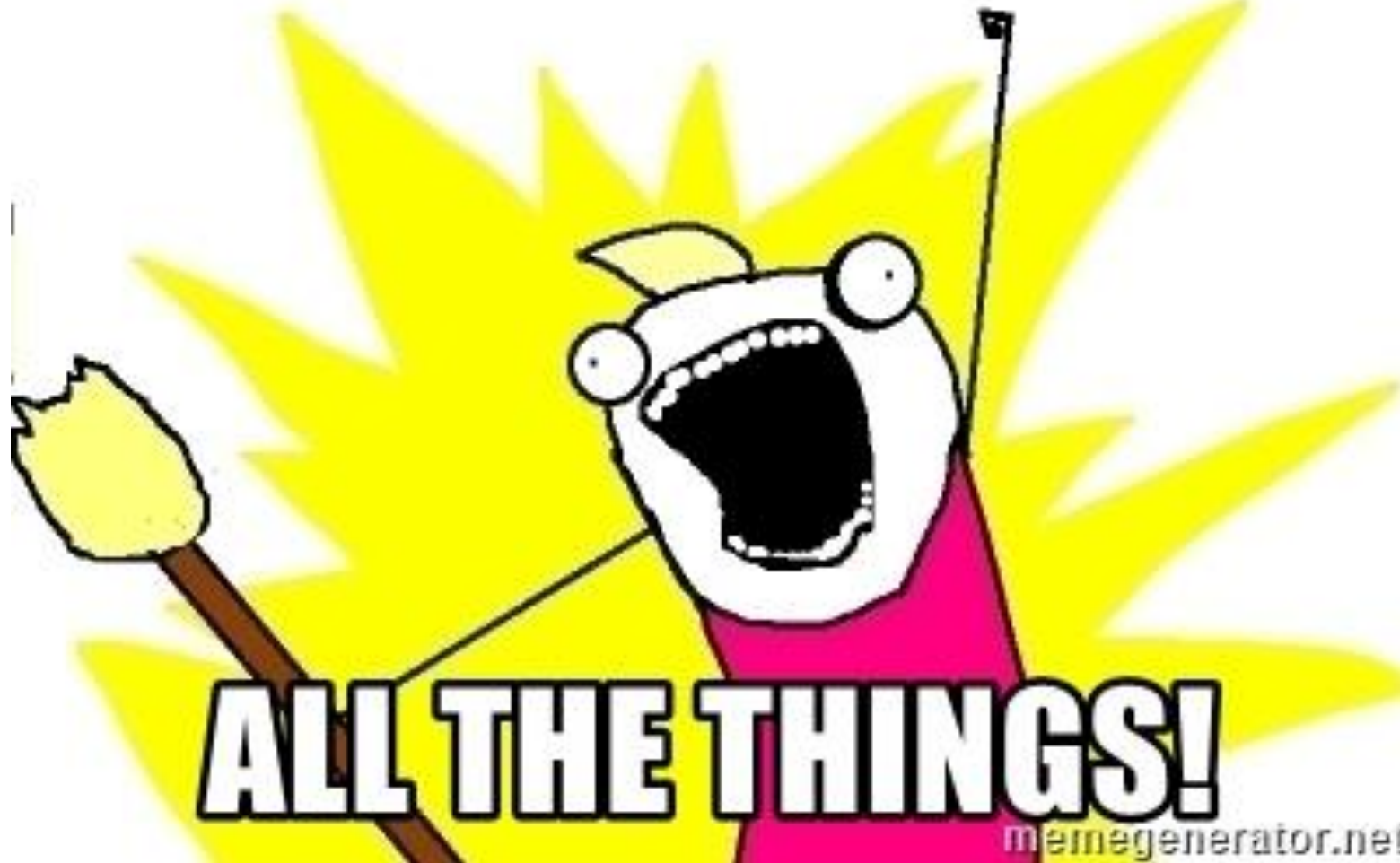


2FA now or later?

Please, don't be annoying!



2-FACTOR AUTH



ALL THE THINGS!

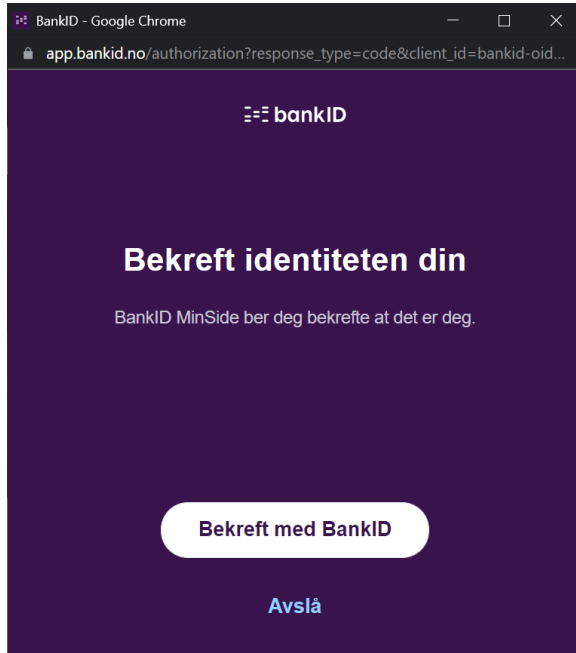
memegenerator.net



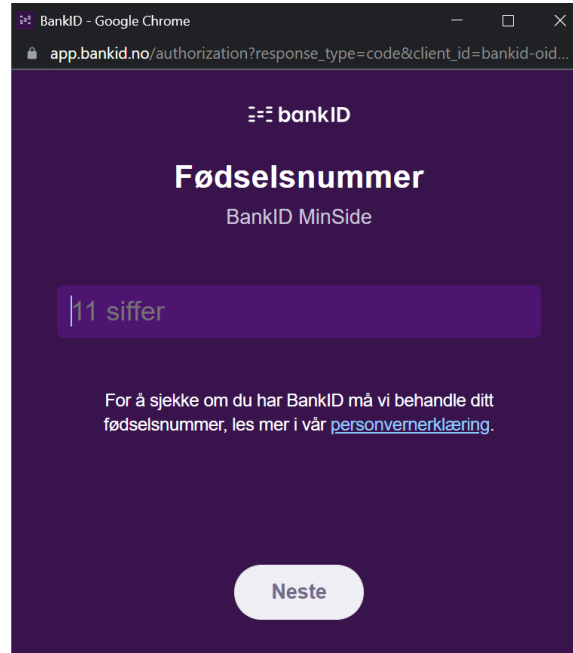
Well, your phone
does that today.

Email. SMS. Voice. In-app push messages.

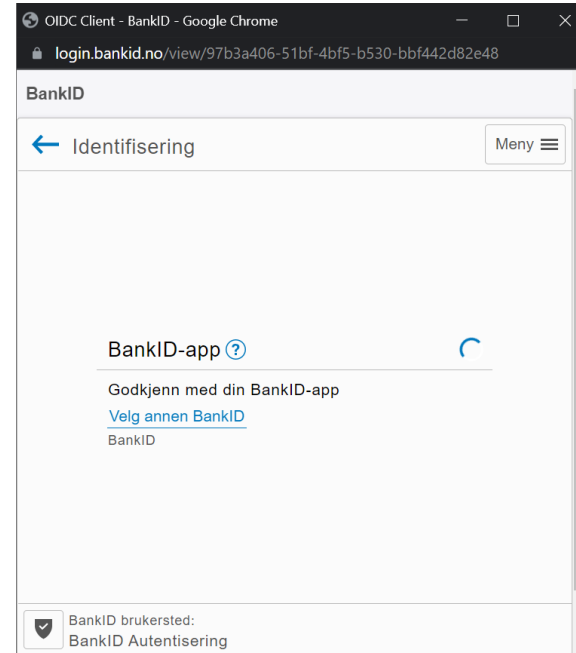
Norwegian BankID login flow



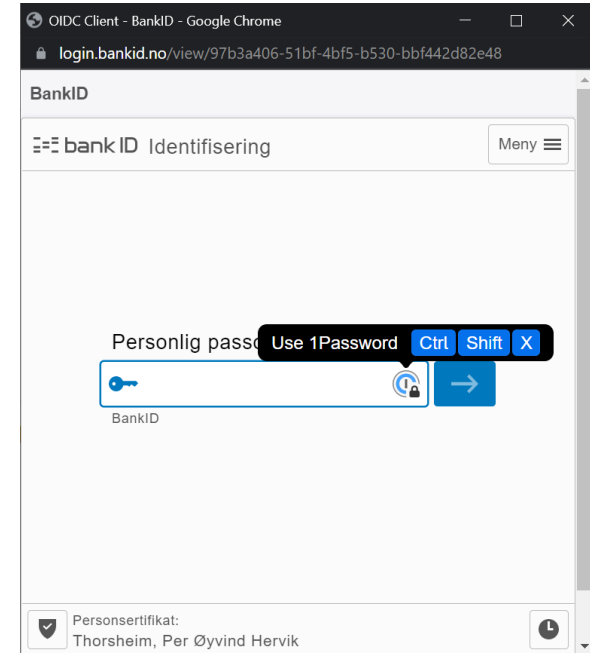
Why?



Username



OTP



Password

HOWTO: Login flow with 2FA

BAD

- Username – Pwd – OTP
- Username + Pwd + OTP

GOOD

- Username – OTP - Pwd



I need to change my password

Tell us why do you want to change your password?

Help users change passwords easily by adding a well-known URL for changing passwords

Redirect a request to `/.well-known/change-password` to the change-passwords URL

Sep 1, 2020 — Updated Sep 24, 2020

Available in: [Español](#), [English](#)

Appears in: [Identity](#)



Eiji Kitamura

[Twitter](#) [GitHub](#) [Homepage](#)

SHARE

SUBSCRIBE

Web.dev/change-password-url/

```
for object to mirror_
mirror_mod.mirror_object

operation == "MIRROR_X":
mirror_mod.use_x = True
mirror_mod.use_y = False
mirror_mod.use_z = False
operation == "MIRROR_Y":
mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True

context.scene.objects.active
obj.select=1
obj.select=1

context.scene.objects.active
mirror_ob.select = 6
bpy.context.selected_objects
data.objects[one.name].select

print("please select exactly

-- OPERATOR CLASSES -----

types.Operator):
X mirror to the selected
object.mirror_mirror_x"
mirror X"
```

Length 15 & No Change.
Implementing NIST SP800-63B for real.

OpenPasswordFilter

- <https://github.com/jephtai/OpenPasswordFilter>
- Cormac Herley says
 - «block Internet top 1K-10K passwords, and you'll be fine.»
- We are a hotel chain. In Scandinavia.
- 18K employees, 6 countries, 210+ locations, and...
- **170+ nationalities working for us**

The background consists of a repeating pattern of speech bubbles in various colors (red, yellow, purple, grey) on a dark teal background. Each speech bubble contains a white question mark. The bubbles are scattered across the entire frame, creating a textured, question-oriented background.

Communicating the Good News

Would you like to never have to change your password again?

And a personal story at the end

Why you should write down your passwords.

per@thorsheim.net

+47 90 99 92 59 Signal

@thorsheim