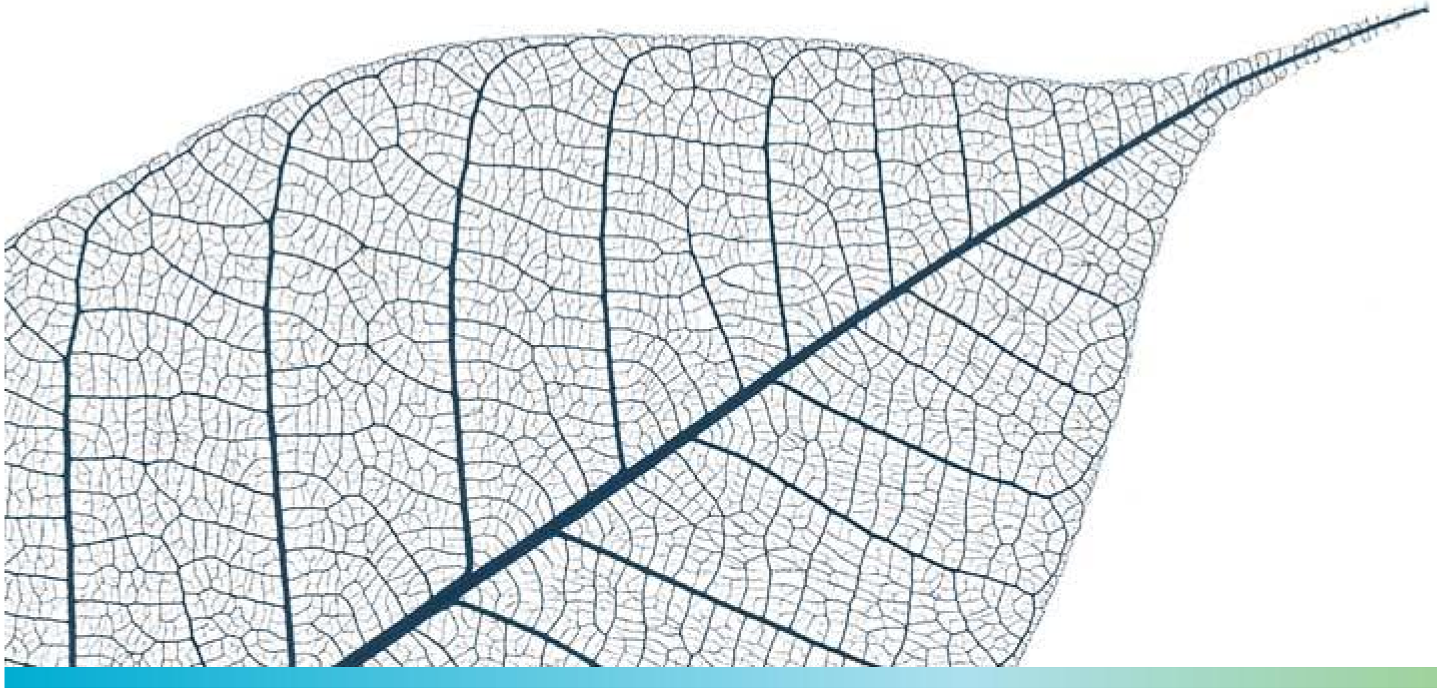
FINSE Winter School

May 8, 212

Passwords: Security vs Usability?

Per Thorsheim
CISA, CISM, CISSP-ISSAP
Security Advisor

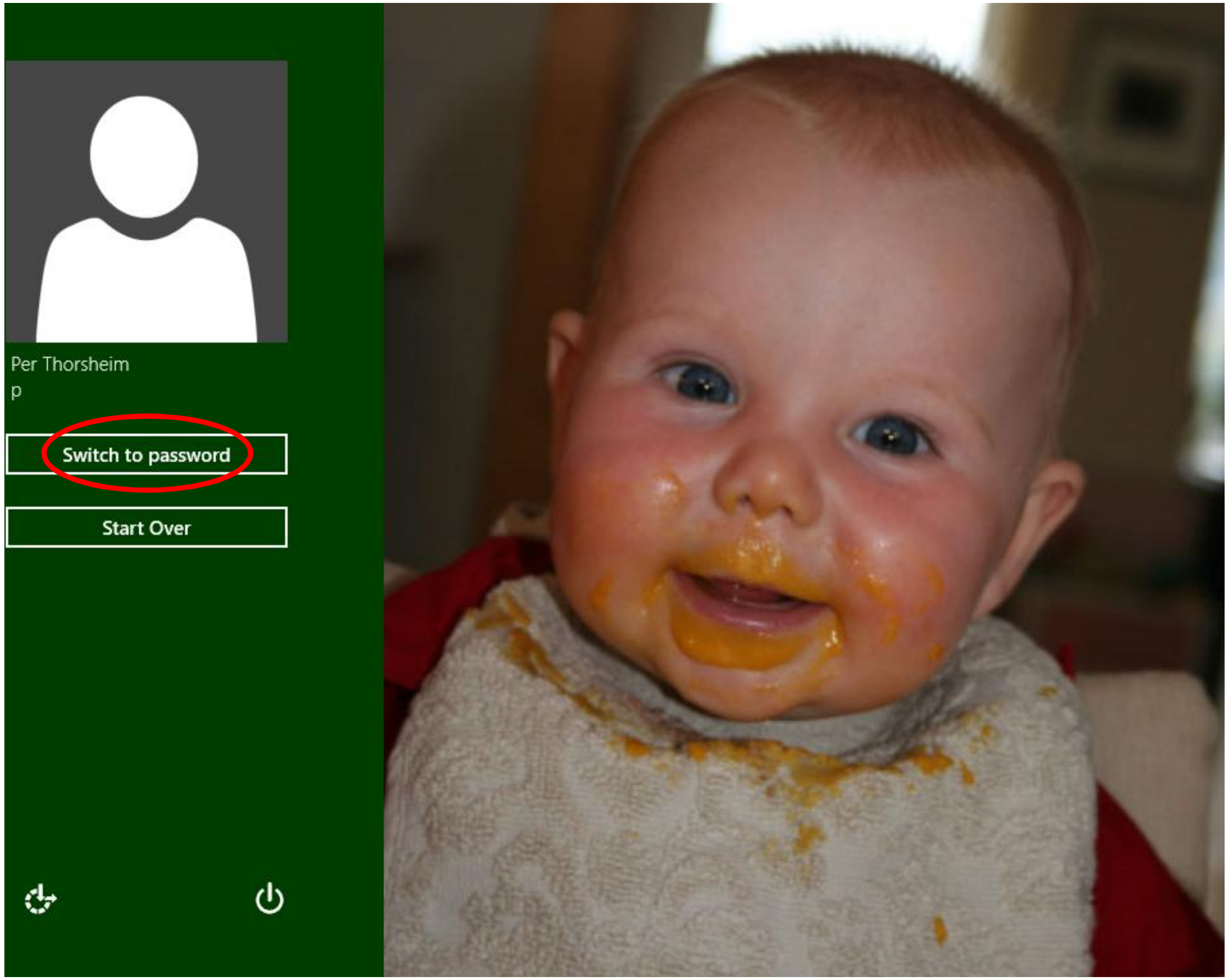
Introduction



About me

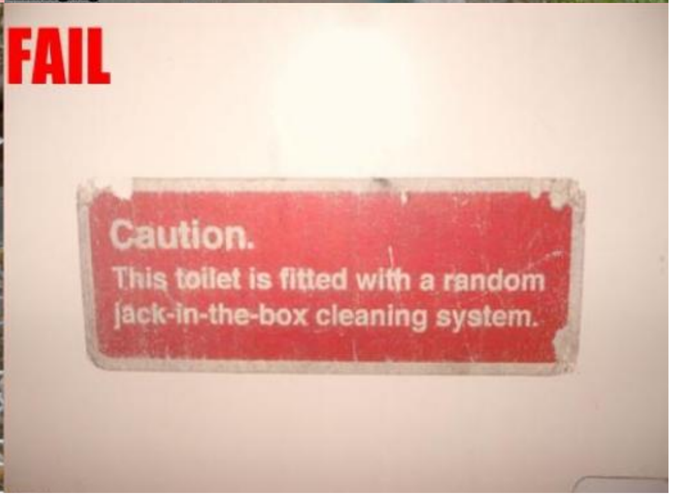
Google picture search

Security should be simple…



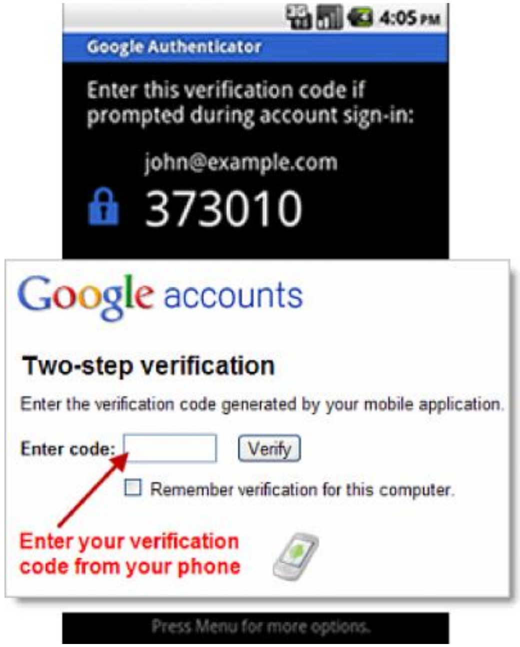
Windows 8 - Picture Password
https://blogs.msdn.com/b/b8/archive/2011/12/16/signing-in-with-a-picture-password.aspx
https://blogs.msdn.com/b/b8/archive/2011/12/19/optimizing-picture-password-security.aspx

…but not stupid…



FAIL
Caution.
This toilet is fitted with a random jack-in-the-box cleaning system.

Good? security usability does exist:


4:05 PM

Google Authenticator

Enter this verification code if prompted during account sign-in:

john@example.com

373010

Google accounts

Two-step verification

Enter the verification code generated by your mobile application.

Enter code: [ ] Verify

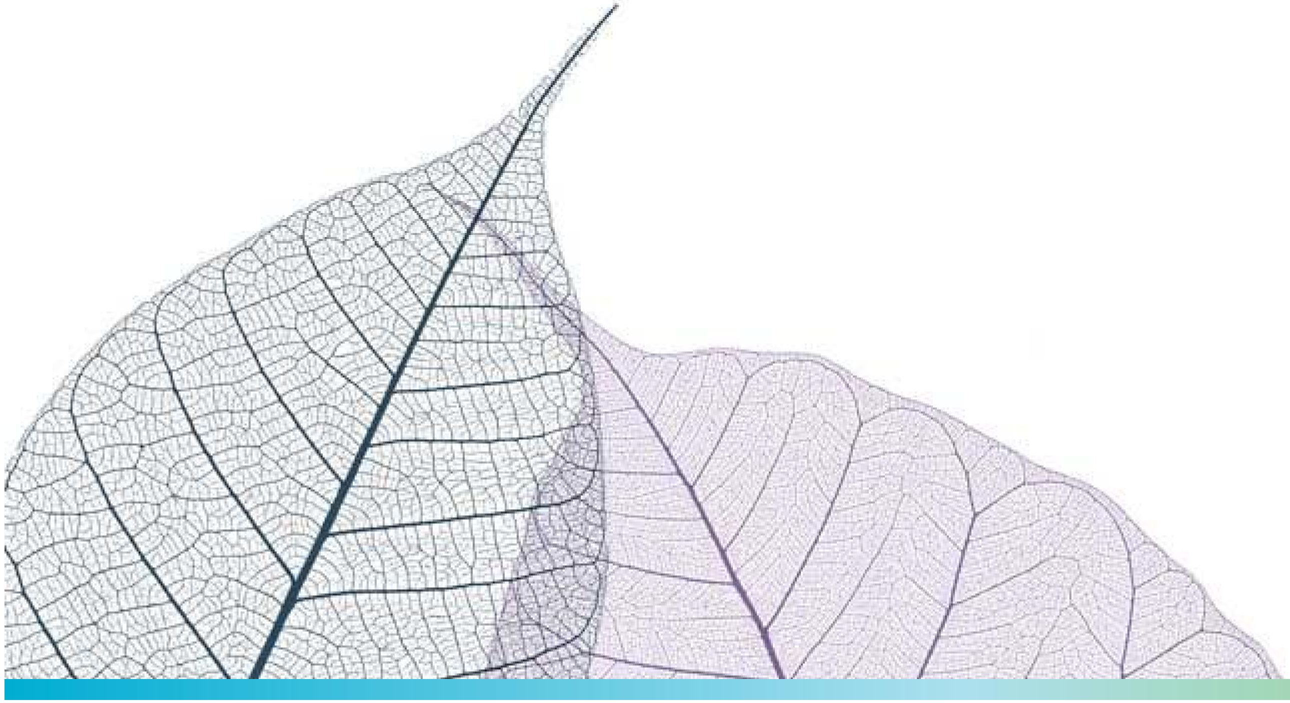
□ Remember verification for this computer.

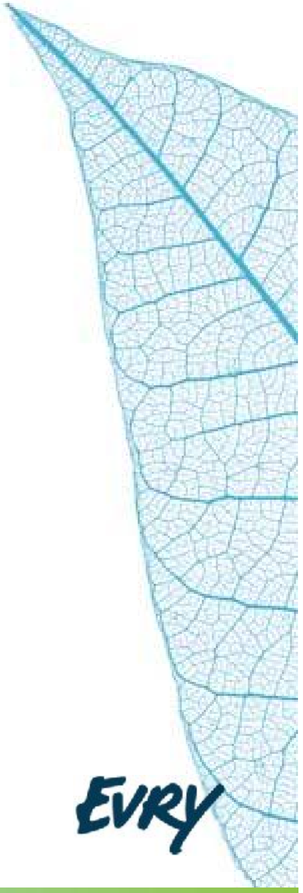
Enter your verification code from your phone

Press Menu for more options.

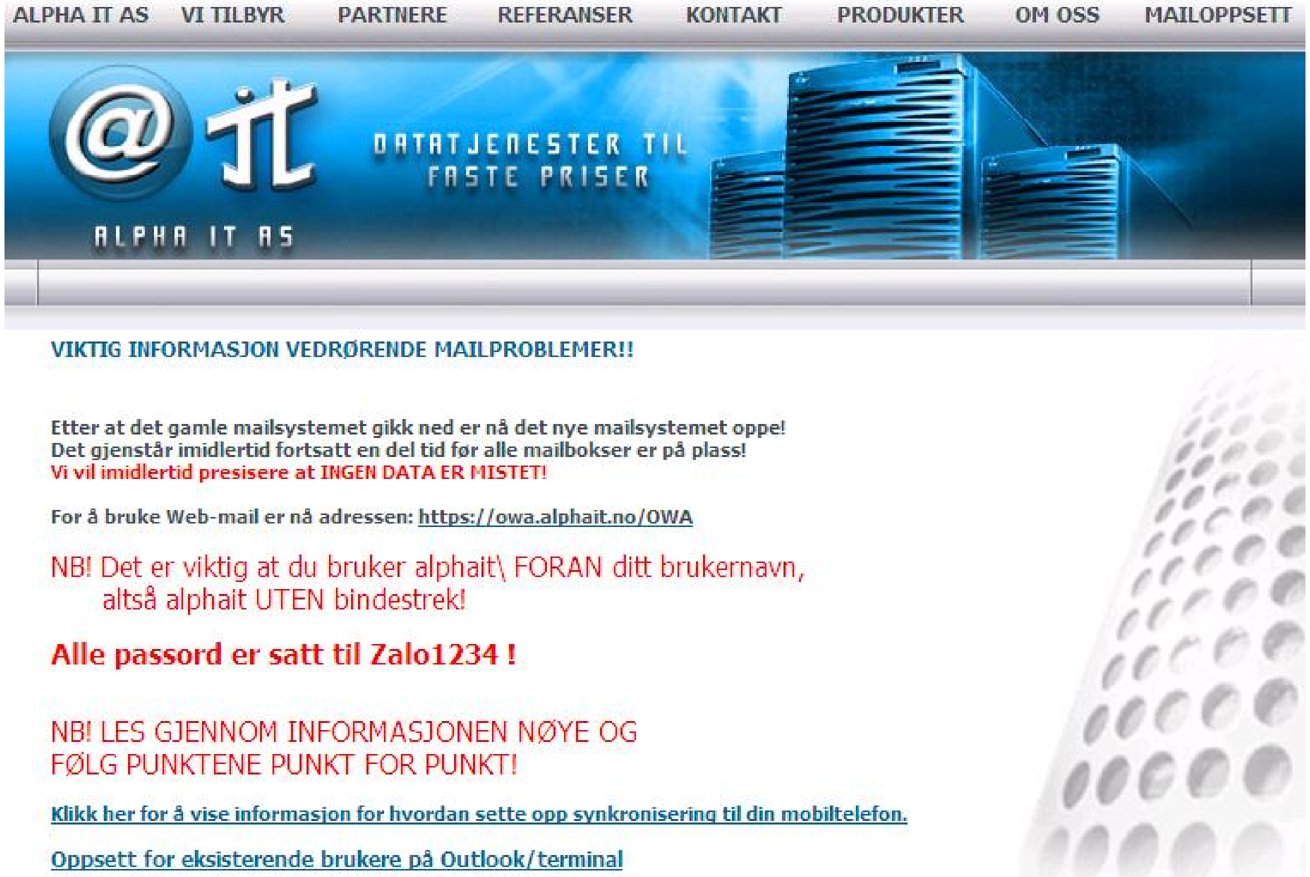
But do remember: In general, 2-factor authentication is one thing you know and one thing you forgot at home.

(Mostly) Bad Examples





Tell everyone their new password in public



VIKTIG INFORMASJON VEDRØRENDE MAILPROBLEMER!!

Etter at det gamle mailsystemet gikk ned er nå det nye mailsystemet oppe!
Det gjenstår imidlertid fortsatt en del tid før alle mailbokser er på plass!
Vi vil imidlertid presisere at INGEN DATA ER MISTET!

For å bruke Web-mail er nå adressen: https://owa.alphait.no/OWA

NB! Det er viktig at du bruker alphait\ FORAN ditt brukernavn,
altså alphait UTEN bindestrek!

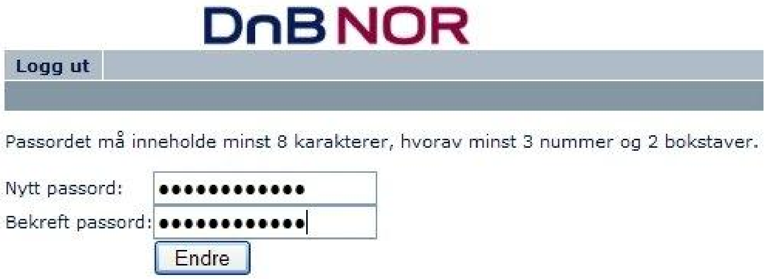
Alle passord er satt til Zalo1234 !

NB! LES GJENNOM INFORMASJONEN NØYE OG
FØLG PUNKTENE PUNKT FOR PUNKT!

Klikk her for å vise informasjon for hvordan sette opp synkronisering til din mobiltelefon.

Oppsett for eksisterende brukere på Outlook/terminal

be careful with your requirements…

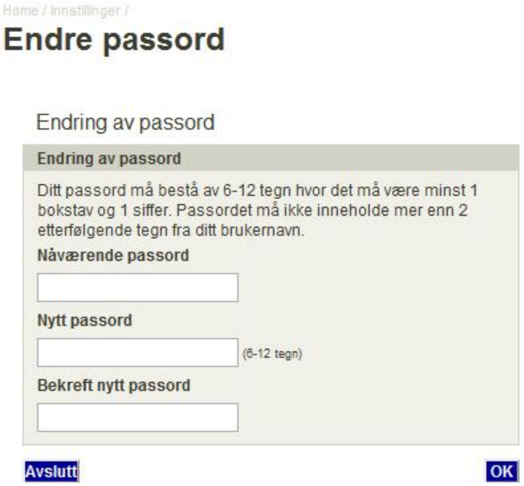


DnB NOR

Passordet må inneholde minst 8 karakterer, hvorav minst 3 nummer og 2 bokstaver.

Nytt passord: ●●●●●●●●●●●●

Bekreft passord: ●●●●●●●●●●●●



Endre passord

Endring av passord

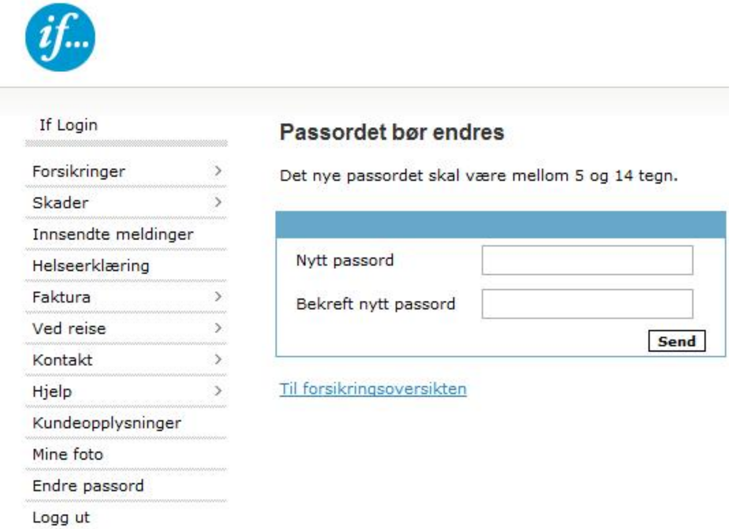
Endring av passord

Ditt passord må bestå av 6-12 tegn hvor det må være minst 1 bokstav og 1 siffer. Passordet må ikke inneholde mer enn 2 etterfølgende tegn fra ditt brukernavn.

Nåværende passord

Nytt passord (6-12 tegn)

Bekreft nytt passord

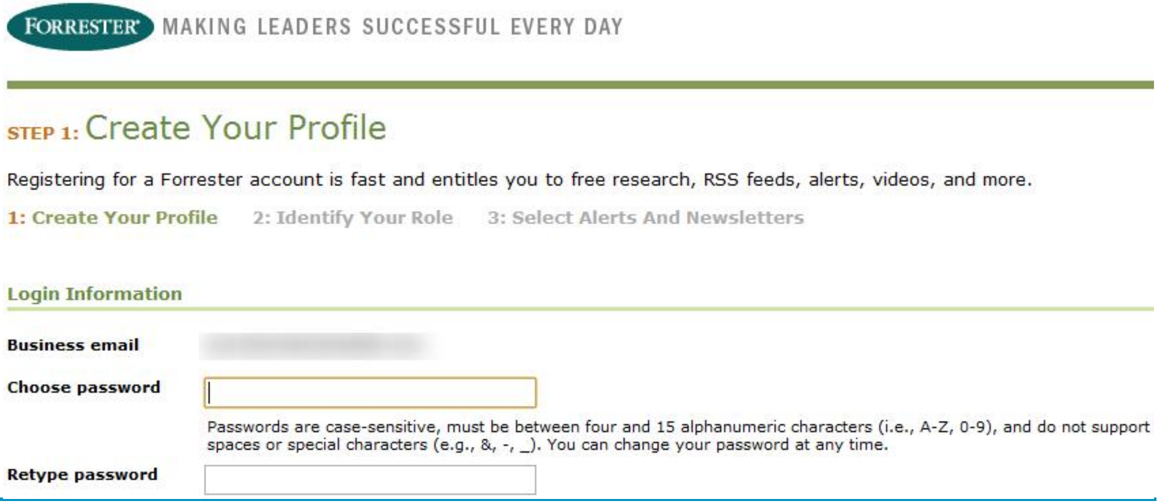


Passordet bør endres

Det nye passordet skal være mellom 5 og 14 tegn.

Nytt passord

Bekreft nytt passord



FORRESTER
MAKING LEADERS SUCCESSFUL EVERY DAY

STEP 1: Create Your Profile

Registering for a Forrester account is fast and entitles you to free research, RSS feeds, alerts, videos, and more.

1: Create Your Profile
2: Identify Your Role
3: Select Alerts And Newsletters

Login Information

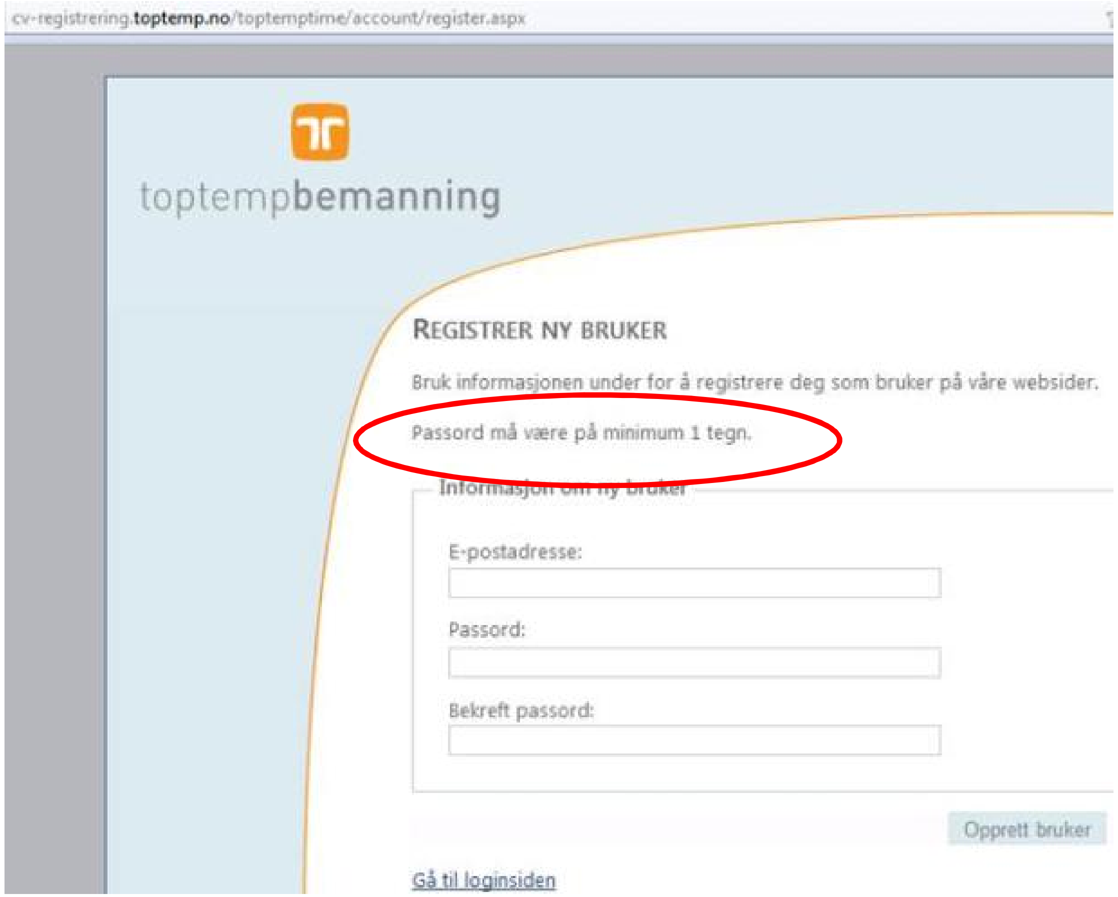
Business email

Choose password

Passwords are case-sensitive, must be between four and 15 alphanumeric characters (i.e., A-Z, 0-9), and do not support spaces or special characters (e.g., &, -, _). You can change your password at any time.

Retype password

…but please do require **something**…



cv-registrering.toptemp.no/toptemptime/account/register.aspx

REGISTRER NY BRUKER

Bruk informasjonen under for å registrere deg som bruker på våre websider.

Passord må være på minimum 1 tegn.

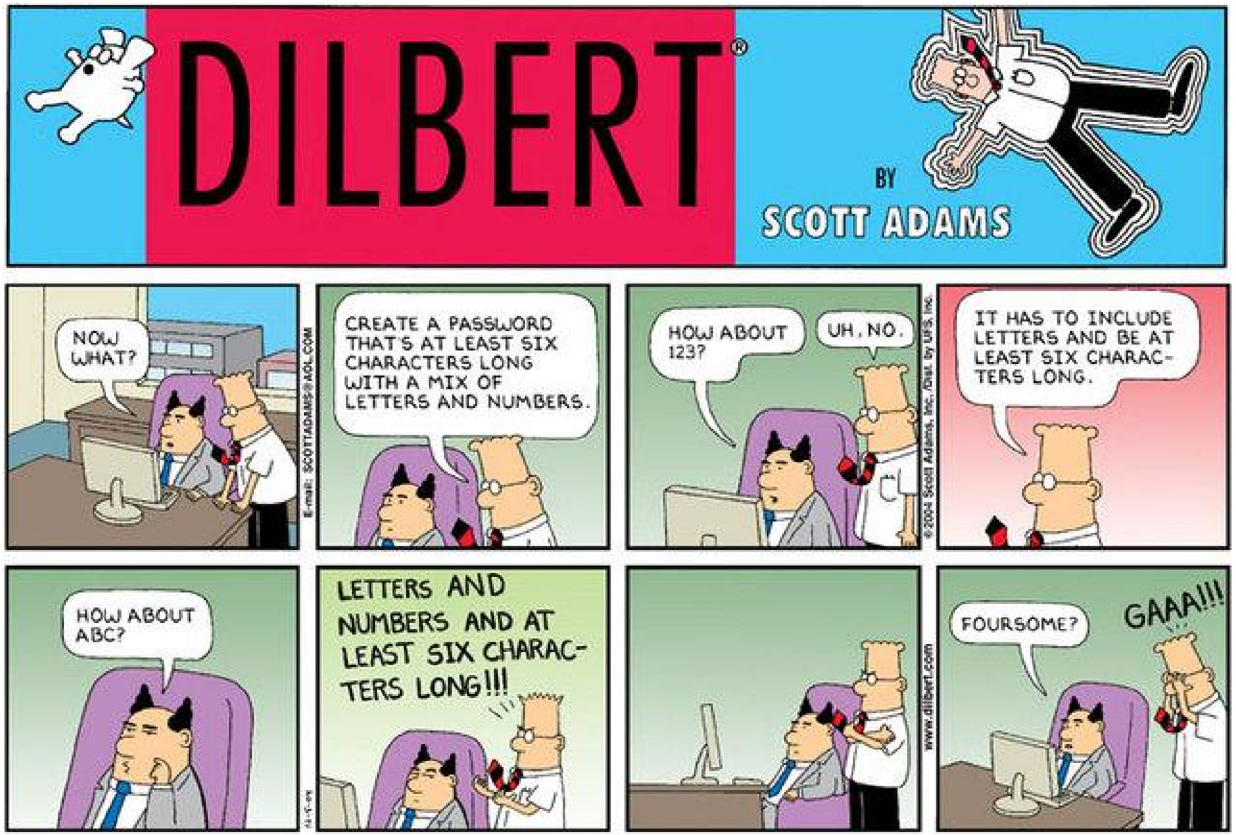
Informasjon om ny bruker

E-postadresse:

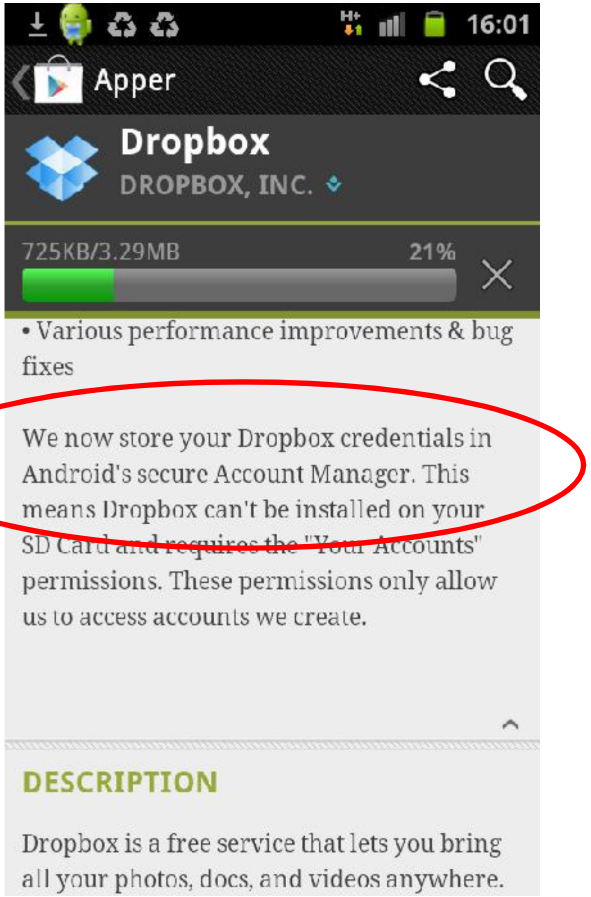
Passord:

Bekreft passord:

…accept end-users for who they are…


DILBERT®
BY
SCOTT ADAMS
NOW WHAT?
E-mail: SCOTTADAMS@AOL.COM
CREATE A PASSWORD THAT'S AT LEAST SIX CHARACTERS LONG WITH A MIX OF LETTERS AND NUMBERS.
HOW ABOUT 123?
UH, NO.
© 2004 Scott Adams, Inc./Dist. by UFS, Inc.
IT HAS TO INCLUDE LETTERS AND BE AT LEAST SIX CHARACTERS LONG.
HOW ABOUT ABC?
LETTERS AND NUMBERS AND AT LEAST SIX CHARACTERS LONG!!!
www.dilbert.com
FOURSOME?
GAAA!!!

Store their credentials safely…

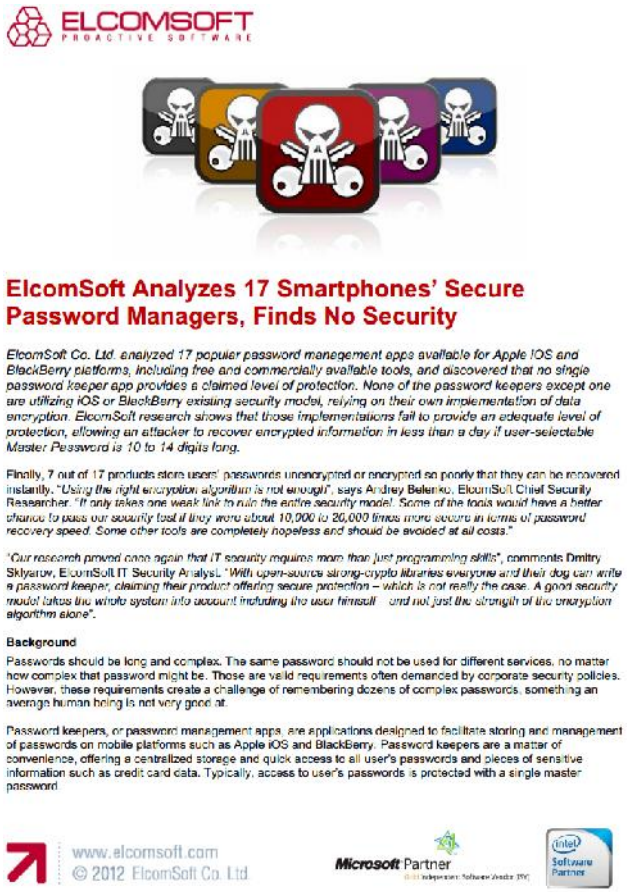


- Various performance improvements & bug fixes

We now store your Dropbox credentials in Android's secure Account Manager. This means Dropbox can't be installed on your SD Card and requires the "Your Accounts" permissions. These permissions only allow us to access accounts we create.

DESCRIPTION

Dropbox is a free service that lets you bring all your photos, docs, and videos anywhere.


ELCOMSOFT
PROACTIVE SOFTWARE

ElcomSoft Analyzes 17 Smartphones' Secure Password Managers, Finds No Security

ElcomSoft Co. Ltd. analyzed 17 popular password management apps available for Apple iOS and BlackBerry platforms, including free and commercially available tools, and discovered that no single password keeper app provides a claimed level of protection. None of the password keepers except one are utilizing iOS or BlackBerry existing security model, relying on their own implementation of data encryption. ElcomSoft research shows that those implementations fail to provide an adequate level of protection, allowing an attacker to recover encrypted information in less than a day if user-selectable Master Password is 10 to 14 digits long.

Finally, 7 out of 17 products store users' passwords unencrypted or encrypted so poorly that they can be recovered instantly. "*Using the right encryption algorithm is not enough*", says Andrey Belenko, ElcomSoft Chief Security Researcher. "*It only takes one weak link to ruin the entire security model. Some of the tools would have a better chance to pass our security test if they were about 10,000 to 20,000 times more secure in terms of password recovery speed. Some other tools are completely hopeless and should be avoided at all costs.*"

"*Our research proved once again that IT security requires more than just programming skills*", comments Dmitry Sklyarov, ElcomSoft IT Security Analyst. "*With open-source strong-crypto libraries everyone and their dog can write a password keeper, claiming their product offering secure protection – which is not really the case. A good security model takes the whole system into account including the user himself – and not just the strength of the encryption algorithm alone*".

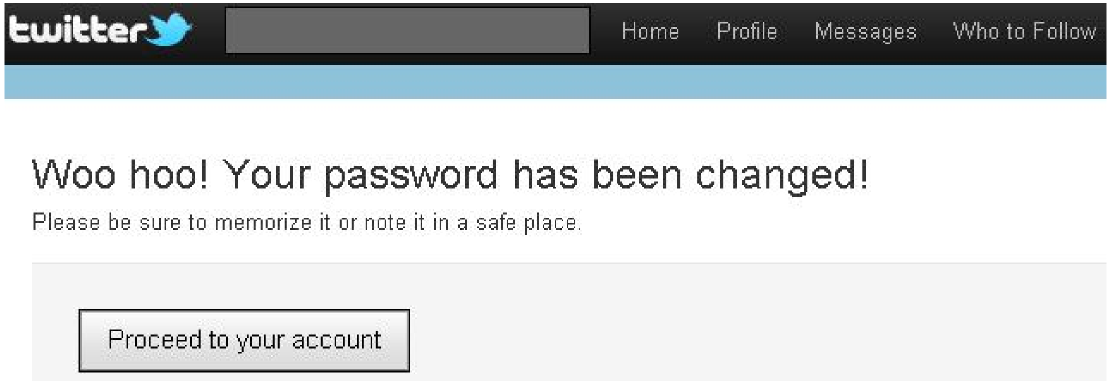
Background

Passwords should be long and complex. The same password should not be used for different services, no matter how complex that password might be. Those are valid requirements often demanded by corporate security policies. However, these requirements create a challenge of remembering dozens of complex passwords, something an average human being is not very good at.

Password keepers, or password management apps, are applications designed to facilitate storing and management of passwords on mobile platforms such as Apple iOS and BlackBerry. Password keepers are a matter of convenience, offering a centralized storage and quick access to all user's passwords and pieces of sensitive information such as credit card data. Typically, access to user's passwords is protected with a single master password.

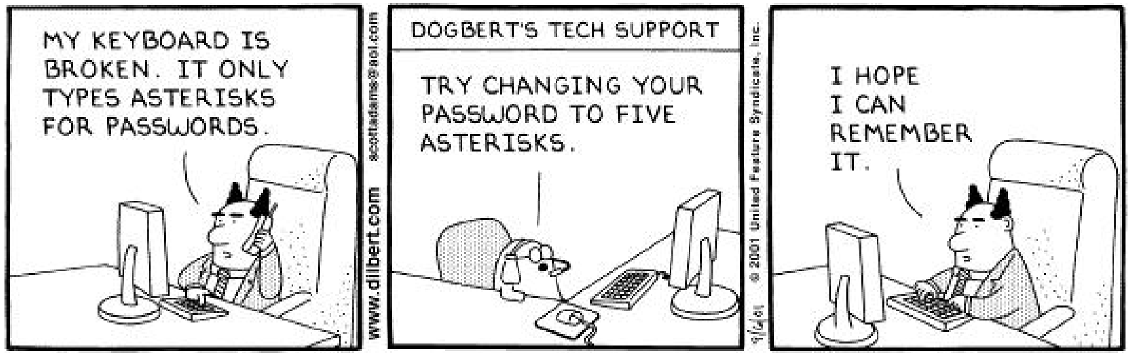
www.elcomsoft.com
© 2012 ElcomSoft Co. Ltd

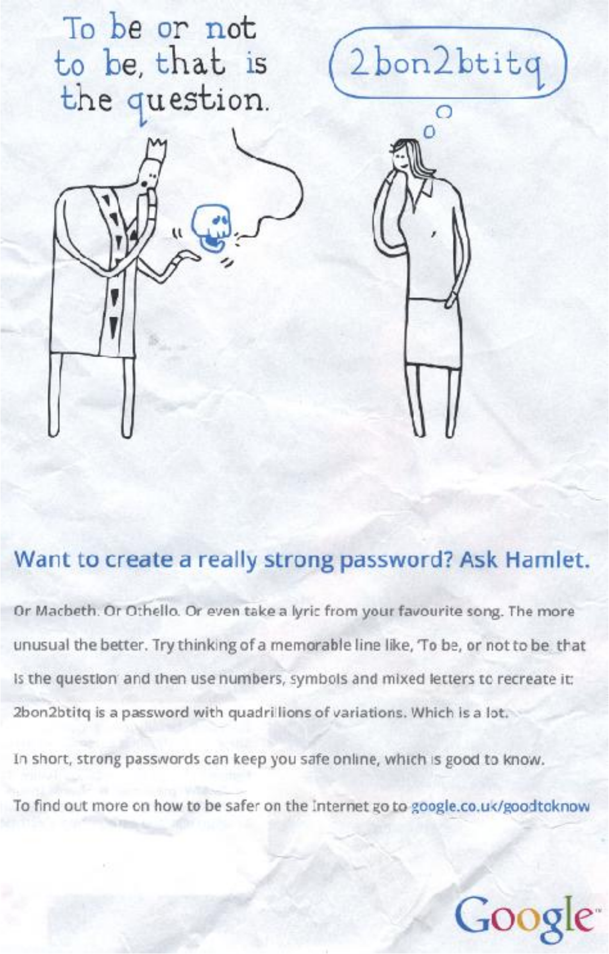
… and give them simple but useful help…



Woo hoo! Your password has been changed!

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


MY KEYBOARD IS BROKEN. IT ONLY TYPES ASTERISKS FOR PASSWORDS.
DOGBERT'S TECH SUPPORT
TRY CHANGING YOUR PASSWORD TO FIVE ASTERISKS.
I HOPE I CAN REMEMBER IT.
www.dilbert.com
scottadams@aol.com
© 2001 United Feature Syndicate, Inc.



Want to create a really strong password? Ask Hamlet.

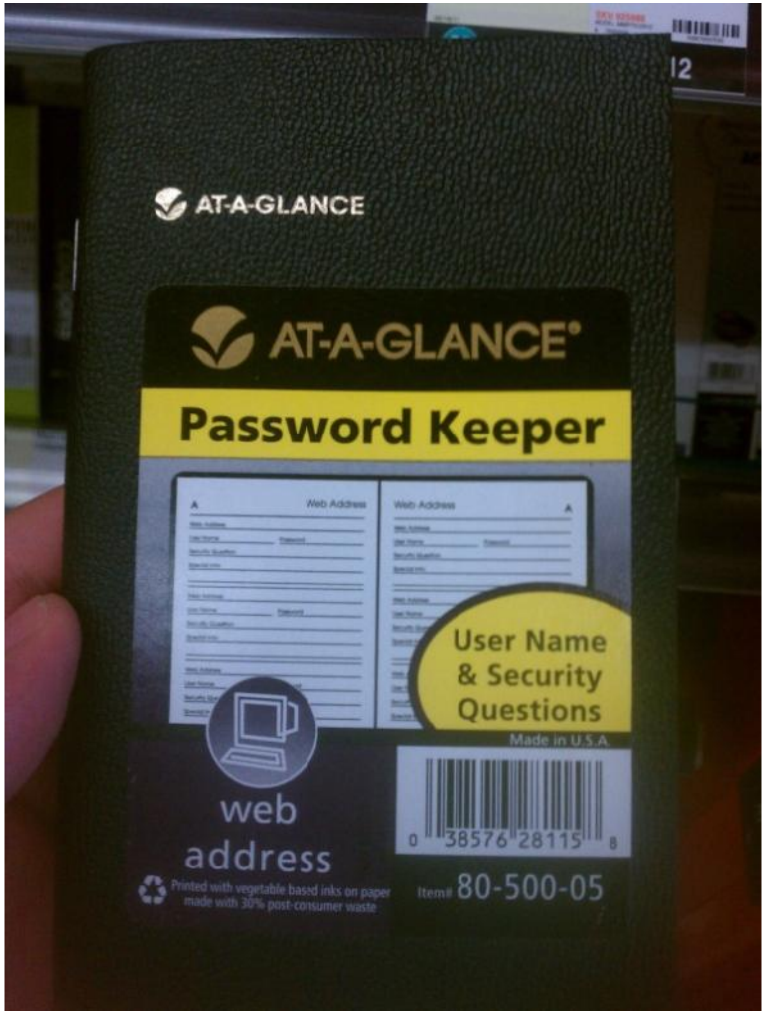
Or Macbeth. Or Othello. Or even take a lyric from your favourite song. The more unusual the better. Try thinking of a memorable line like, 'To be, or not to be, that is the question' and then use numbers, symbols and mixed letters to recreate it: 2bon2btitq is a password with quadrillions of variations. Which is a lot.

In short, strong passwords can keep you safe online, which is good to know.

To find out more on how to be safer on the Internet go to google.co.uk/goodtoknow

Google

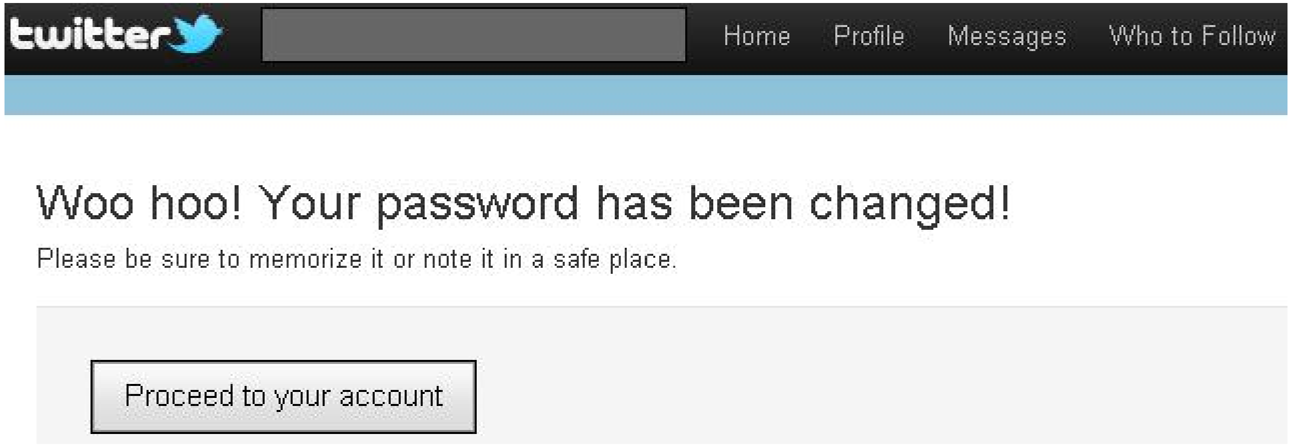
«write down your password» can be smart….


AT-A-GLANCE
AT-A-GLANCE®
Password Keeper
User Name & Security Questions
web address
Made in U.S.A.
Item# 80-500-05
Printed with vegetable based inks on paper made with 30% post-consumer waste

As long as you DO try to hide those POST-IT notes just a little bit!

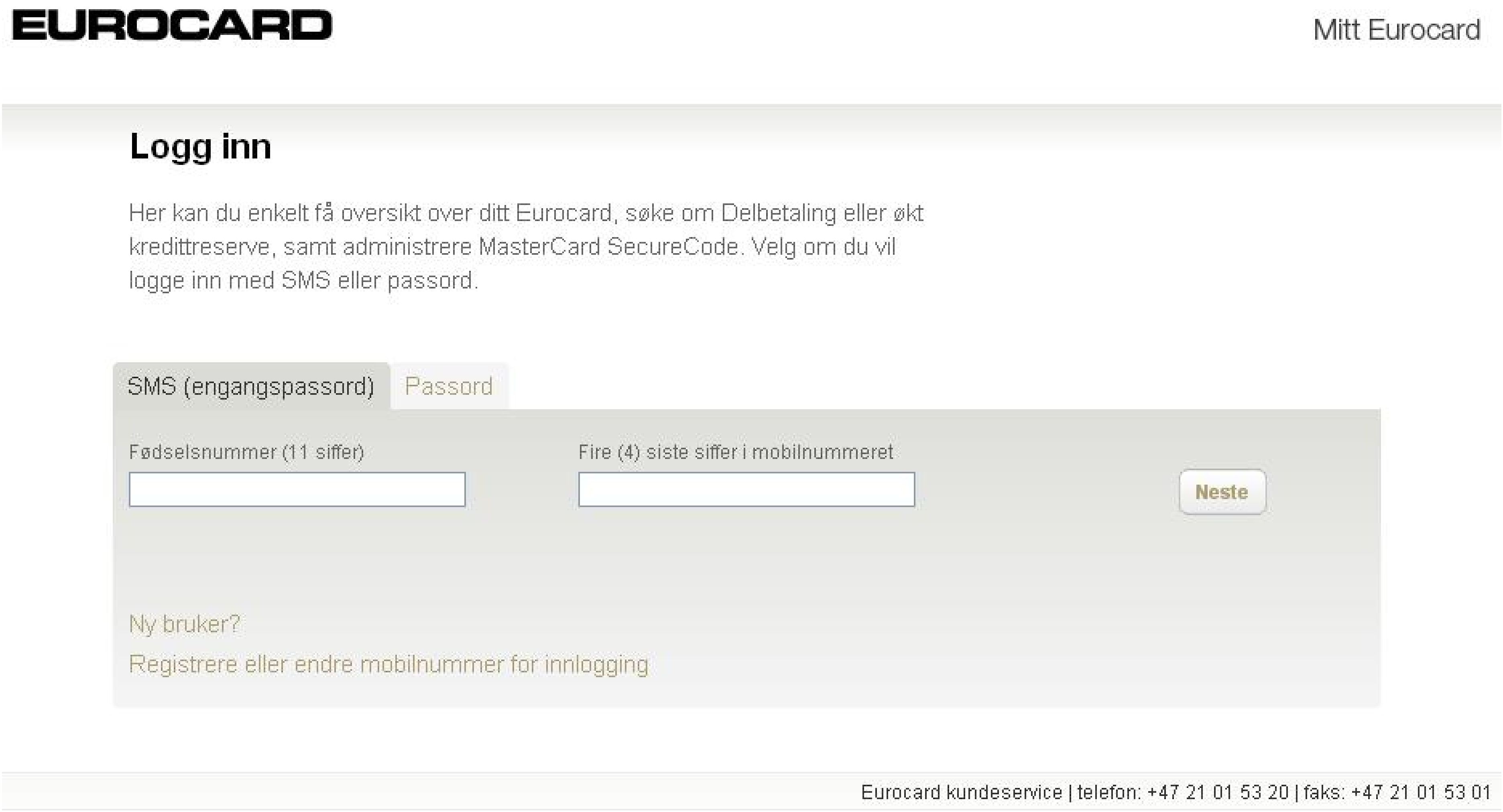
http://securitynirvana.blogspot.com/2010/03/write-down-your-password.html

Hey, some actually do give that advice!



Woo hoo! Your password has been changed!

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



Logg inn

Her kan du enkelt få oversikt over ditt Eurocard, søke om Delbetaling eller økt kredittreserve, samt administrere MasterCard SecureCode. Velg om du vil logge inn med SMS eller passord.

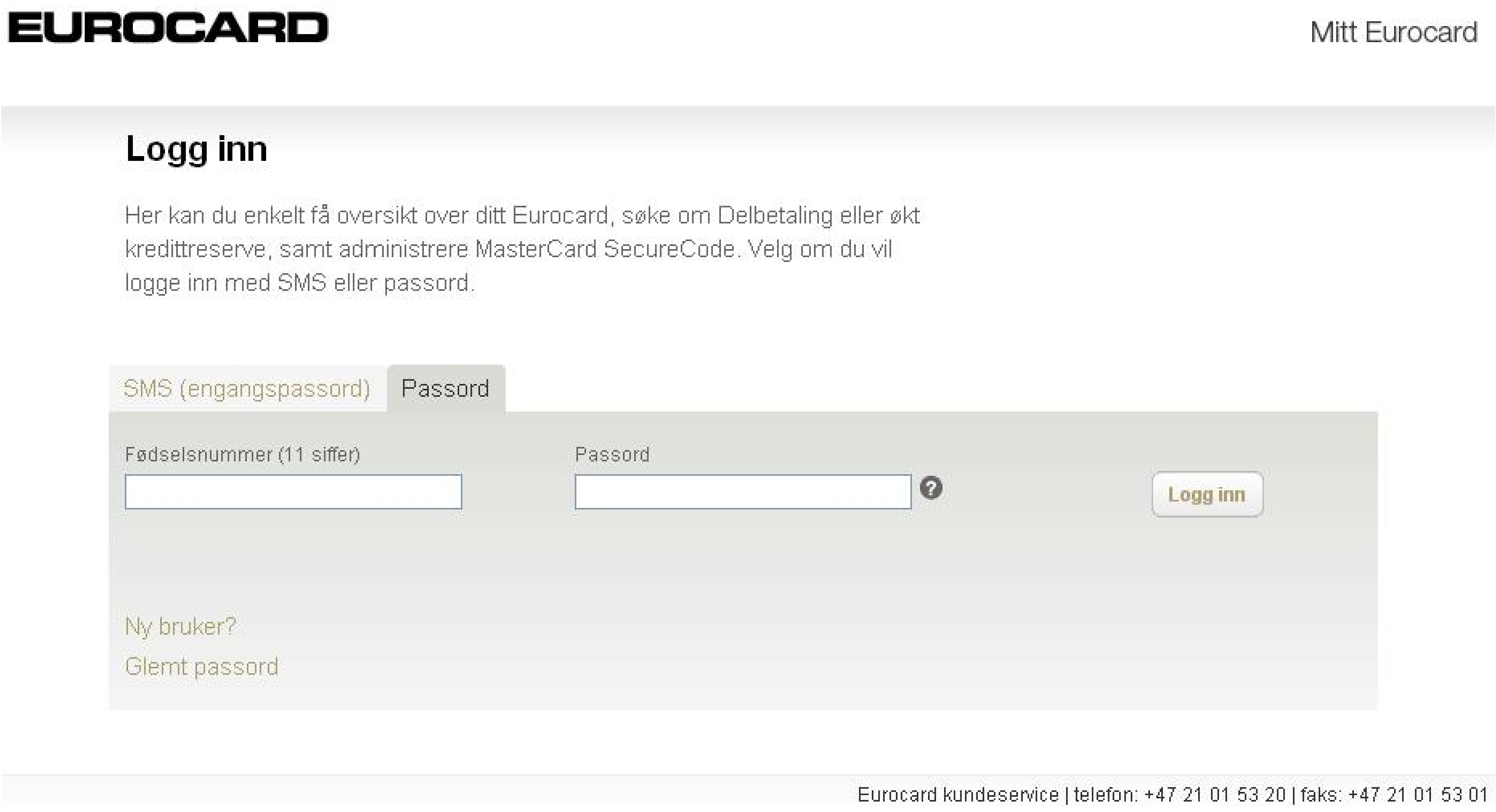
Fødselsnummer (11 siffer)

Fire (4) siste siffer i mobilnummeret

Ny bruker?

Registrere eller endre mobilnummer for innlogging

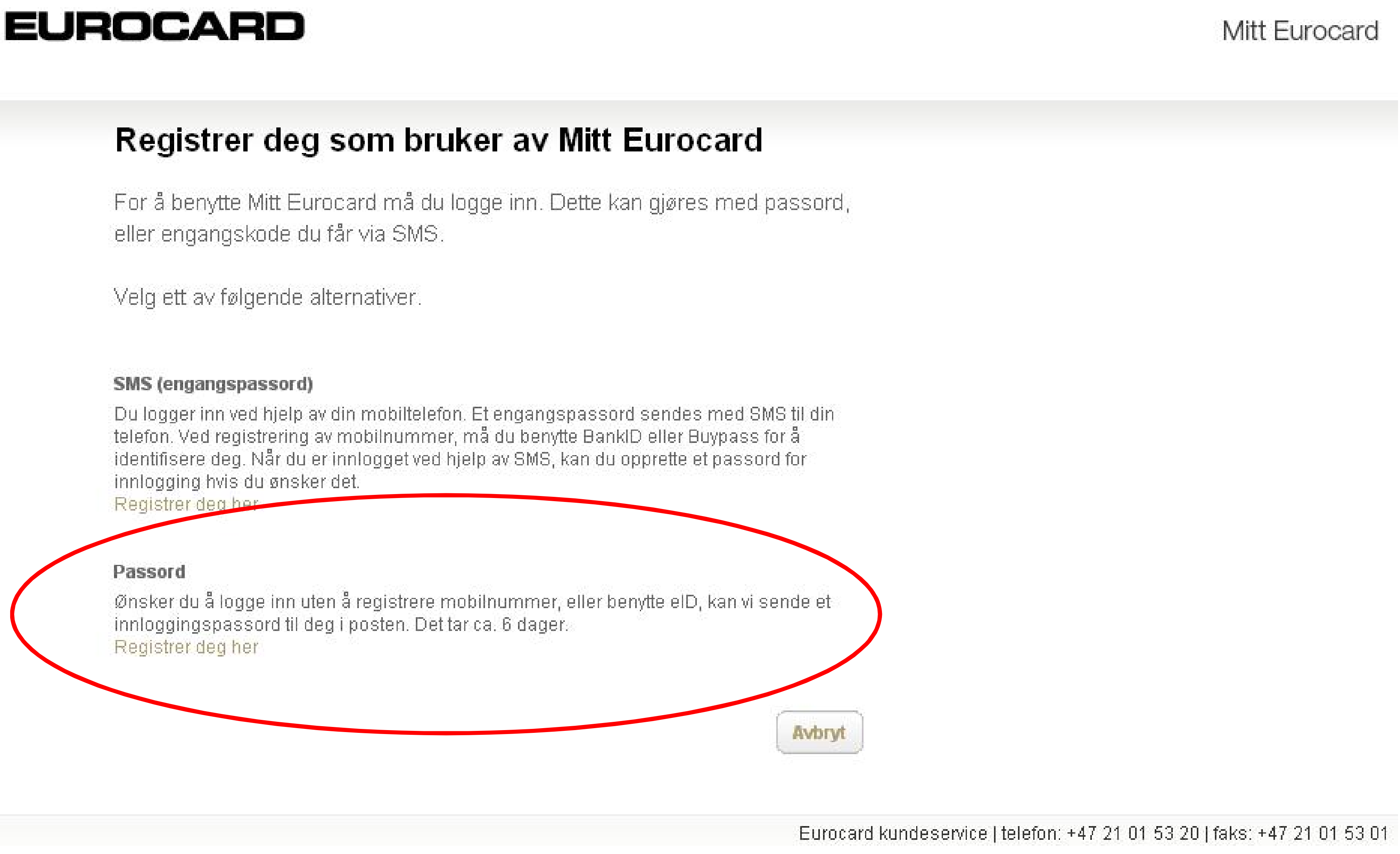
Eurocard kundeservice | telefon: +47 21 01 53 20 | faks: +47 21 01 53 01



Logg inn

Her kan du enkelt få oversikt over ditt Eurocard, søke om Delbetaling eller økt kredittreserve, samt administrere MasterCard SecureCode. Velg om du vil logge inn med SMS eller passord.

Eurocard kundeservice | telefon: +47 21 01 53 20 | faks: +47 21 01 53 01



EUROCARD

Mitt Eurocard

Registrer deg som bruker av Mitt Eurocard

For å benytte Mitt Eurocard må du logge inn. Dette kan gjøres med passord, eller engangskode du får via SMS.

Velg ett av følgende alternativer.

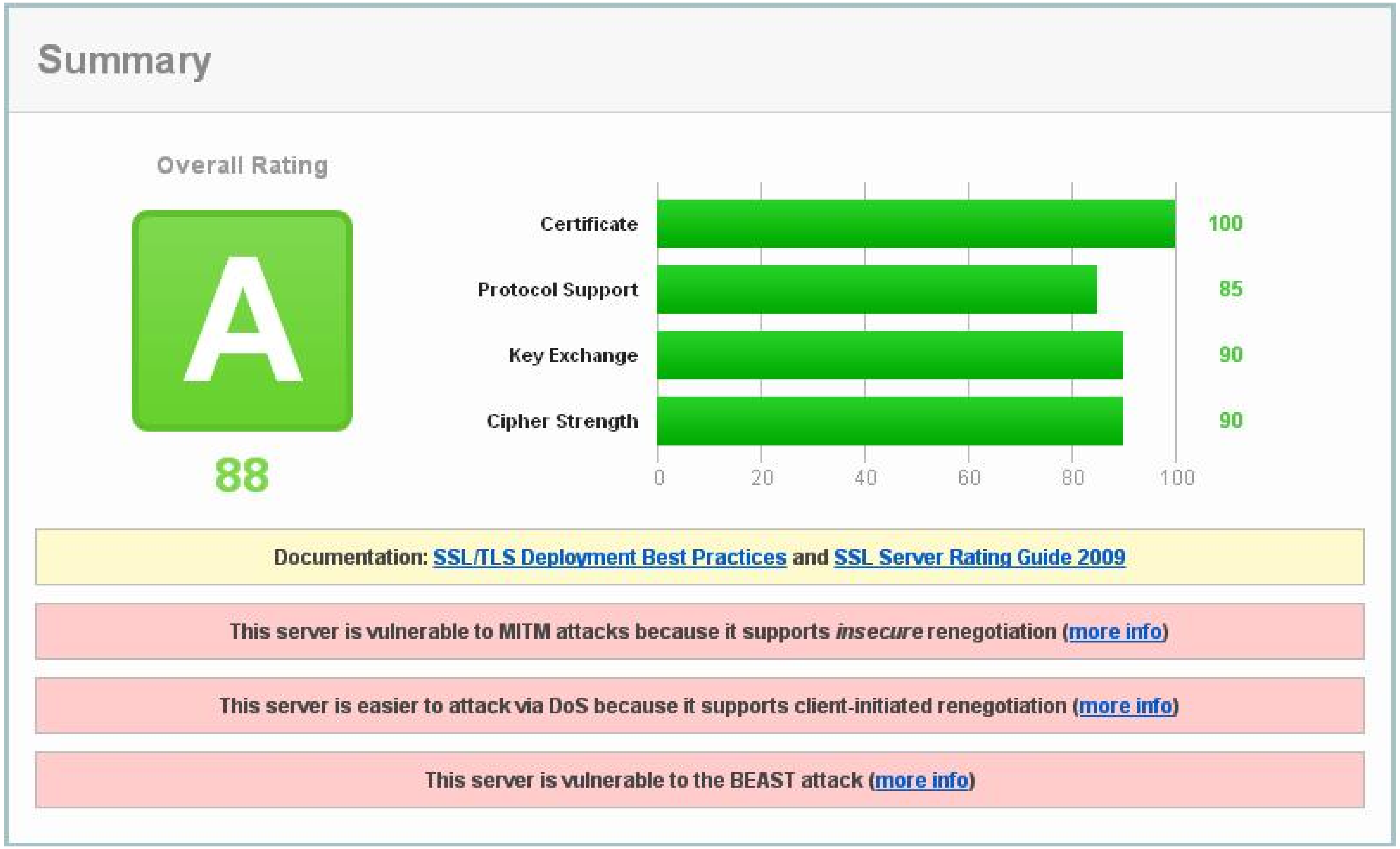
SMS (engangspassord)

Du logger inn ved hjelp av din mobiltelefon. Et engangspassord sendes med SMS til din telefon. Ved registrering av mobilnummer, må du benytte BankID eller Buypass for å identifisere deg. Når du er innlogget ved hjelp av SMS, kan du opprette et passord for innlogging hvis du ønsker det.
Registrer deg her

Passord

Ønsker du å logge inn uten å registrere mobilnummer, eller benytte eID, kan vi sende et innloggingspassord til deg i posten. Det tar ca. 6 dager.
Registrer deg her

Eurocard kundeservice | telefon: +47 21 01 53 20 | faks: +47 21 01 53 01



Documentation: SSL/TLS Deployment Best Practices and SSL Server Rating Guide 2009

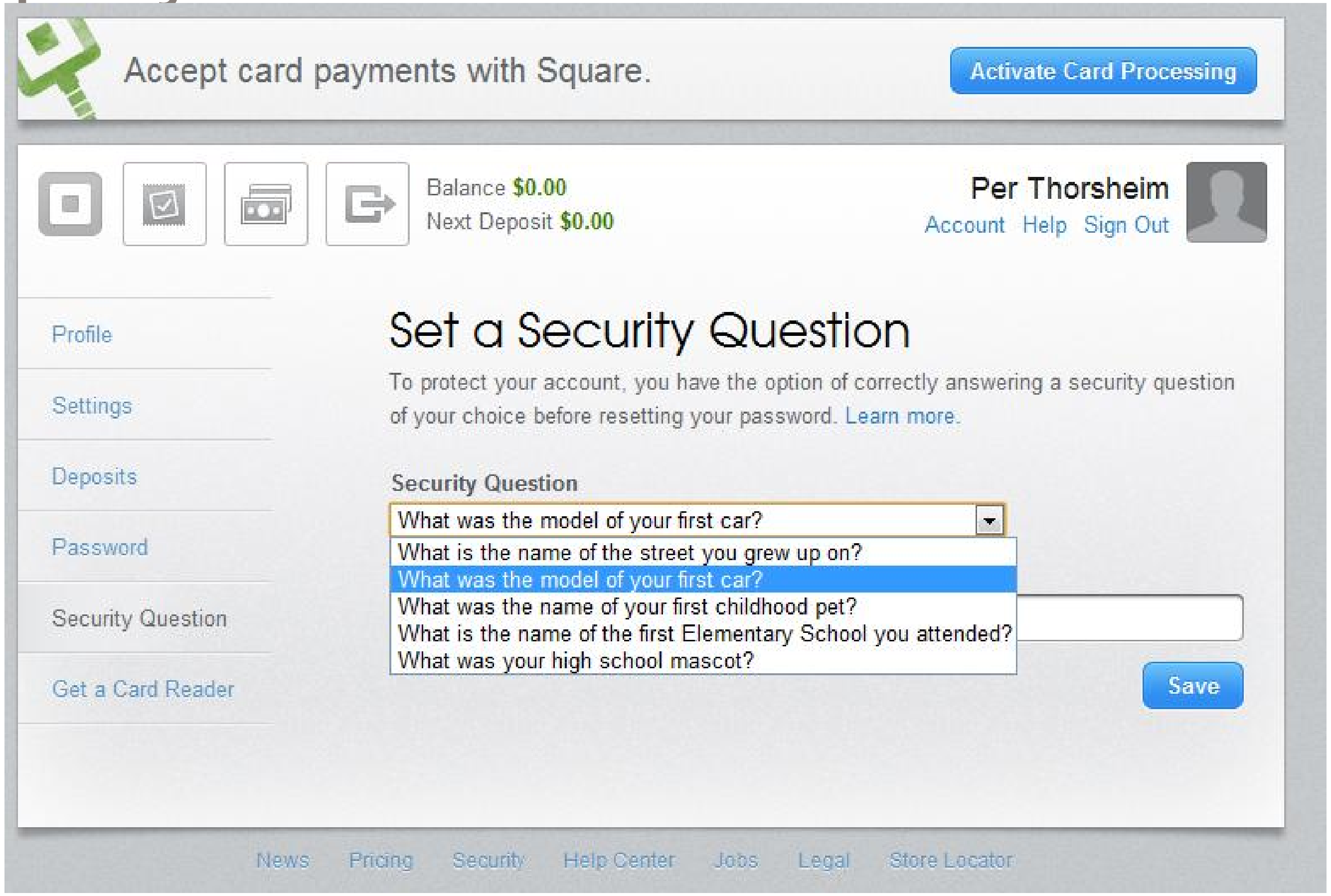
This server is vulnerable to MITM attacks because it supports *insecure* renegotiation (more info)

This server is easier to attack via DoS because it supports client-initiated renegotiation (more info)

This server is vulnerable to the BEAST attack (more info)

www.ssllabs.com

Security questions are *hard* to do properly!



Accept card payments with Square.

Balance $0.00
Next Deposit $0.00

Per Thorsheim

Set a Security Question

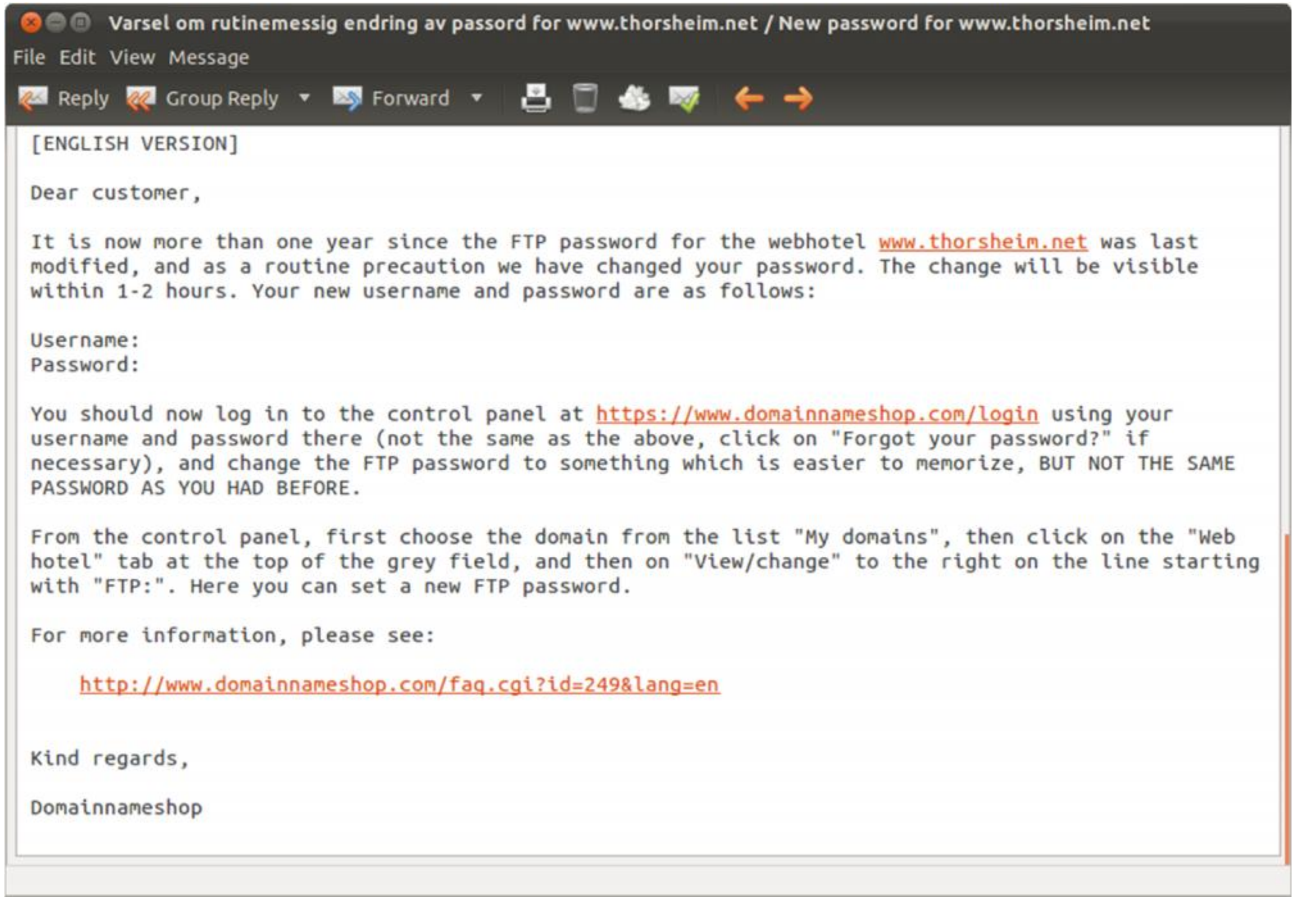
To protect your account, you have the option of correctly answering a security question of your choice before resetting your password. Learn more.

Security Question: What was the model of your first car?

Activate Card Processing
Account
Help
Sign Out
Profile
Settings
Deposits
Password
Security Question
Get a Card Reader
What is the name of the street you grew up on?
What was the model of your first car?
What was the name of your first childhood pet?
What is the name of the first Elementary School you attended?
What was your high school mascot?
Save
News
Pricing
Security
Help Center
Jobs
Legal
Store Locator

www.lightbluetouchpaper.org/2010/03/04/evaluating-statistical-attacks-on-personal-knowledge-questions/

Do NOT e-mail me my password!

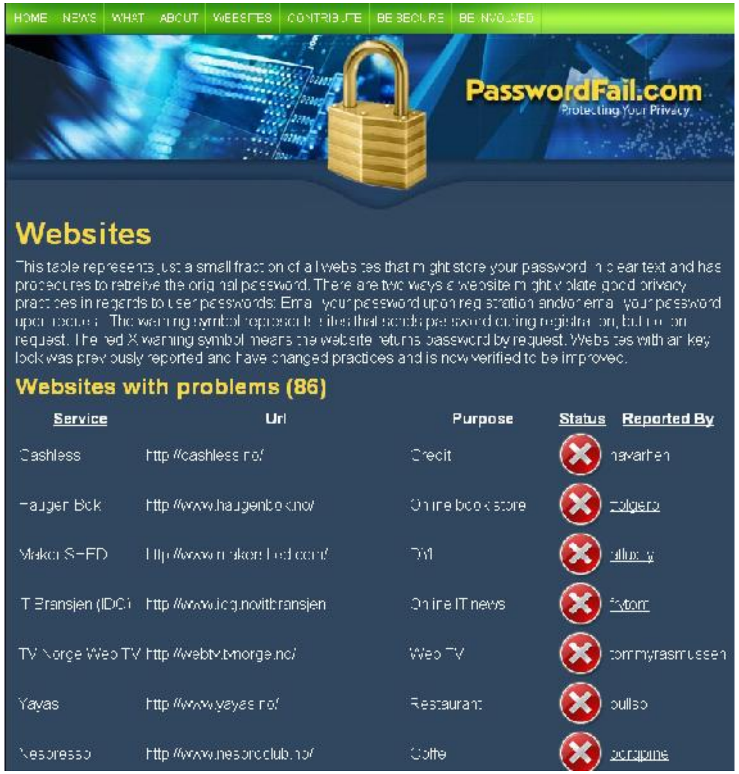


Varsel om rutinemessig endring av passord for www.thorsheim.net / New password for www.thorsheim.net
File Edit View Message
Reply
Group Reply
Forward

```
[ENGLISH VERSION]

Dear customer,

It is now more than one year since the FTP password for the webhotel www.thorsheim.net was last
modified, and as a routine precaution we have changed your password. The change will be visible
within 1-2 hours. Your new username and password are as follows:

Username:
Password:

You should now log in to the control panel at https://www.domainnameshop.com/login using your
username and password there (not the same as the above, click on "Forgot your password?" if
necessary), and change the FTP password to something which is easier to memorize, BUT NOT THE SAME
PASSWORD AS YOU HAD BEFORE.

From the control panel, first choose the domain from the list "My domains", then click on the "Web
hotel" tab at the top of the grey field, and then on "View/change" to the right on the line starting
with "FTP:". Here you can set a new FTP password.

For more information, please see:

    http://www.domainnameshop.com/faq.cgi?id=249&lang=en


Kind regards,

Domainnameshop
```

Or else…..

Hall of shame

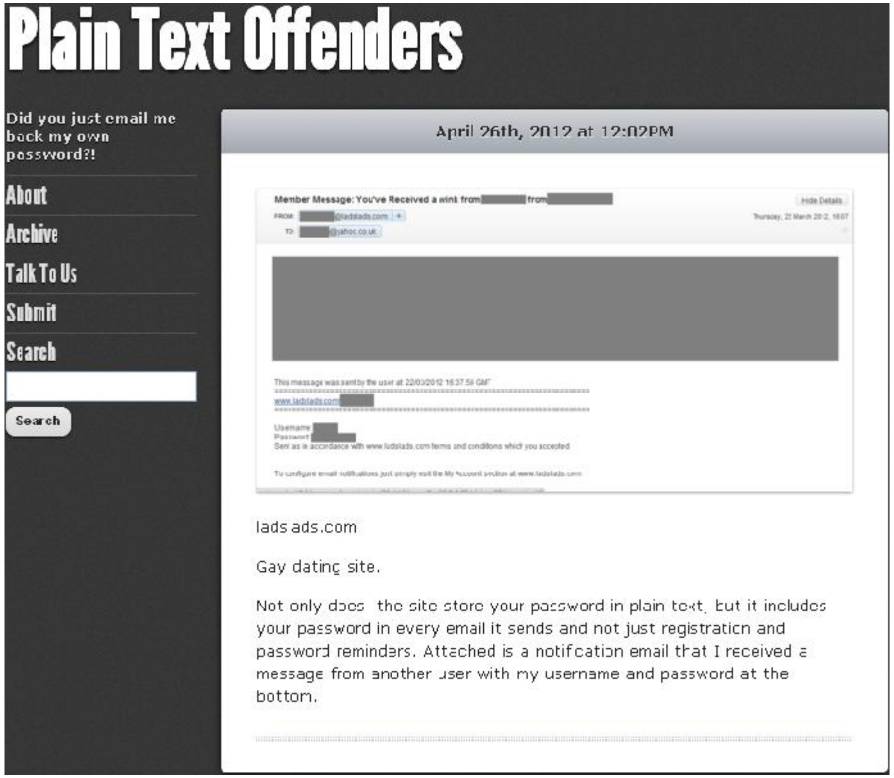


Websites

This table represents just a small fraction of all websites that might store your password in clear text and has procedures to retreive the original password. There are two ways a website might violate good privacy practices in regards to user passwords: Email your password upon registration and/or email your password upon request. The warning symbol represents sites that sends password during registration, but not on request. The red X warning symbol means the website returns password by request. Websites with an key lock was previously reported and have changed practices and is now verified to be improved.

Websites with problems (86)

Service	Url	Purpose	Status	Reported By
Cashless	http://cashless.no/	Credit	☒	navarhen
Haugen Bok	http://www.haugenbok.no/	Online book store	☒	tolgero
Maker SHED	http://www.makershed.com/	DIY	☒	alluxy
IT Bransjen (IDG)	http://www.idg.no/itbransjen	Online IT news	☒	fytom
TV Norge Web TV	http://webtv.tvnorge.no/	Web TV	☒	tommyrasmussen
Yayas	http://www.yayas.no/	Restaurant	☒	pullso
Nespresso	http://www.nespressoclub.no/	Coffe	☒	porcupine



April 26th, 2012 at 12:02PM

Member Message: You've Received a wink from [redacted] **from** [redacted]

Hide Details

FROM: [redacted]@ladslads.com +

TO: [redacted]@yahoo.co.uk

Thursday, 22 March 2012, 16:07

[redacted]

This message was sent by the user at 22/03/2012 16:37:58 GMT

www.ladslads.com[redacted]

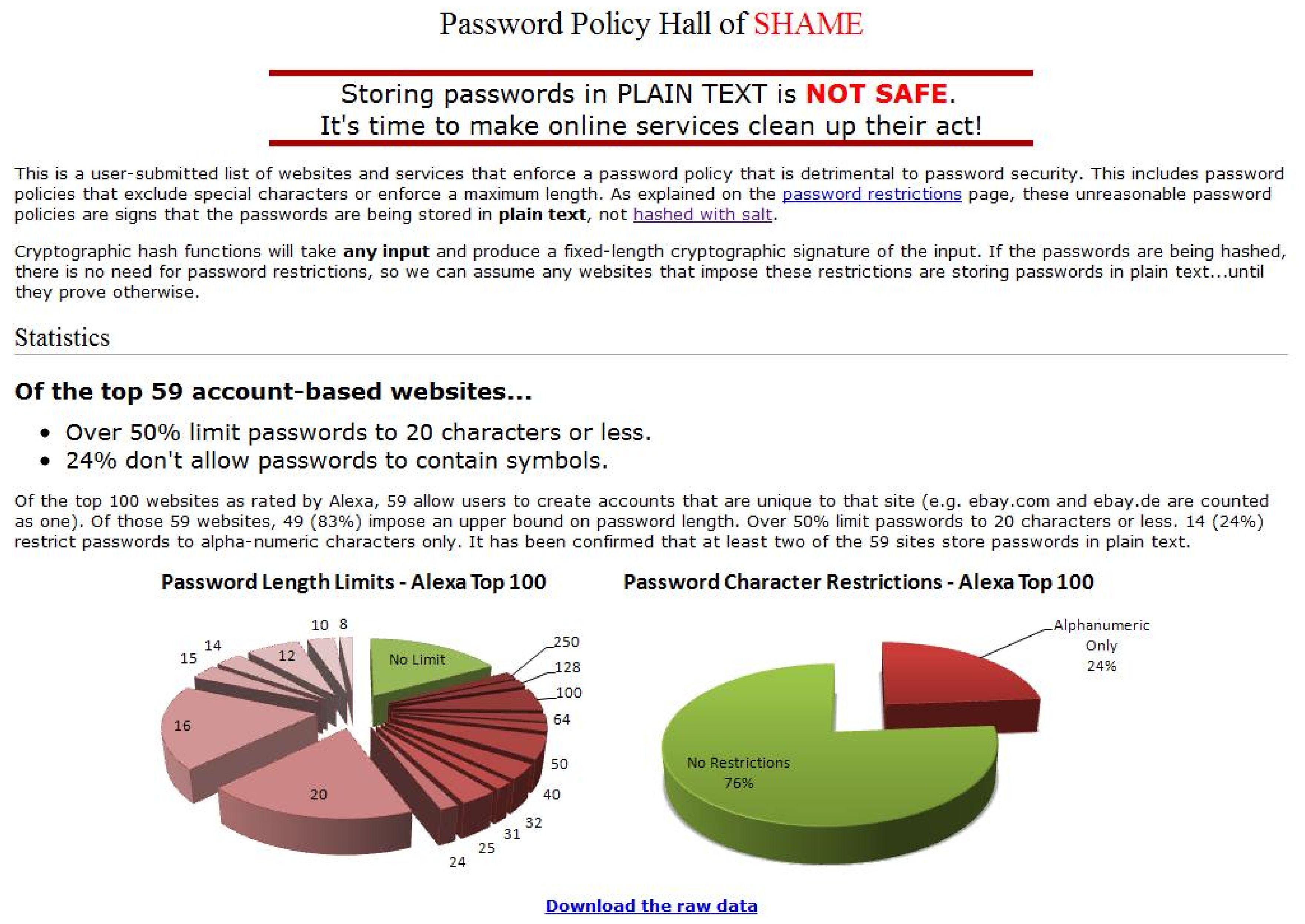
Username: [redacted]
Password: [redacted]
Sent as is accordance with www.ladslads.com terms and conditions which you accepted

To configure email notifications just simply visit the My Account section at www.ladslads.com

ladslads.com

Gay dating site.

Not only does the site store your password in plain text, but it includes your password in every email it sends and not just registration and password reminders. Attached is a notifcation email that I received a message from another user with my username and password at the bottom.



Password Policy Hall of SHAME

Storing passwords in PLAIN TEXT is **NOT SAFE**.
It's time to make online services clean up their act!

This is a user-submitted list of websites and services that enforce a password policy that is detrimental to password security. This includes password policies that exclude special characters or enforce a maximum length. As explained on the password restrictions page, these unreasonable password policies are signs that the passwords are being stored in **plain text**, not hashed with salt.

Cryptographic hash functions will take **any input** and produce a fixed-length cryptographic signature of the input. If the passwords are being hashed, there is no need for password restrictions, so we can assume any websites that impose these restrictions are storing passwords in plain text...until they prove otherwise.

Statistics

Of the top 59 account-based websites...

- Over 50% limit passwords to 20 characters or less.
- 24% don't allow passwords to contain symbols.

Of the top 100 websites as rated by Alexa, 59 allow users to create accounts that are unique to that site (e.g. ebay.com and ebay.de are counted as one). Of those 59 websites, 49 (83%) impose an upper bound on password length. Over 50% limit passwords to 20 characters or less. 14 (24%) restrict passwords to alpha-numeric characters only. It has been confirmed that at least two of the 59 sites store passwords in plain text.

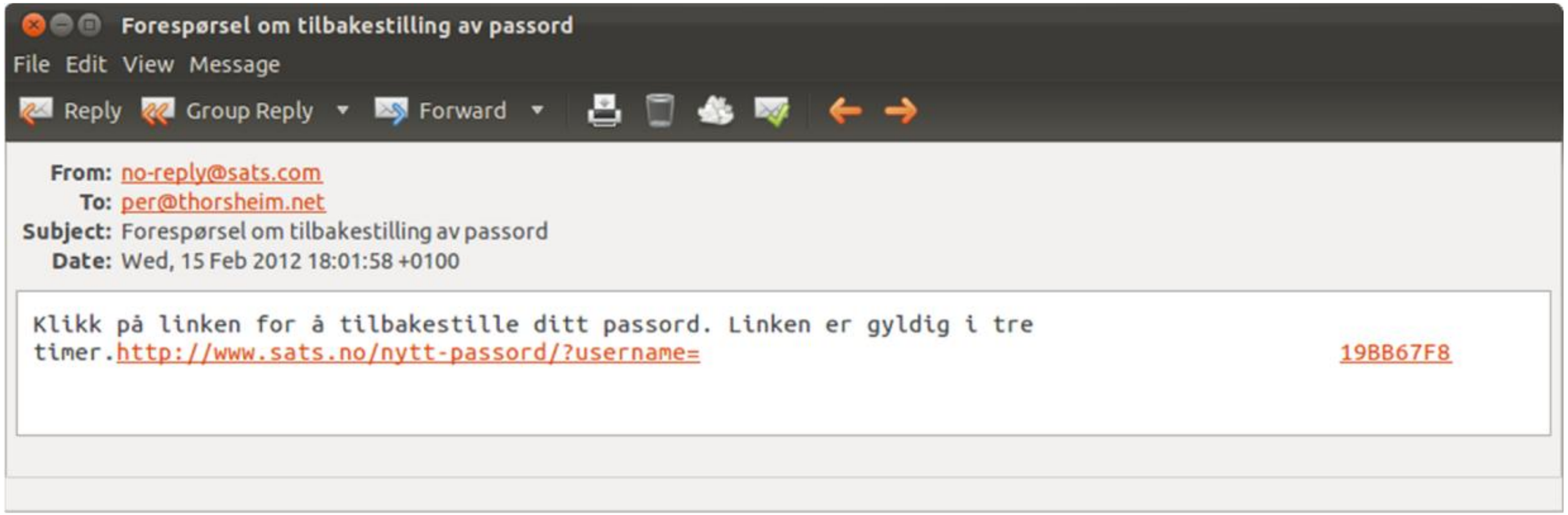
Password Length Limits - Alexa Top 100

Password Character Restrictions - Alexa Top 100

Download the raw data

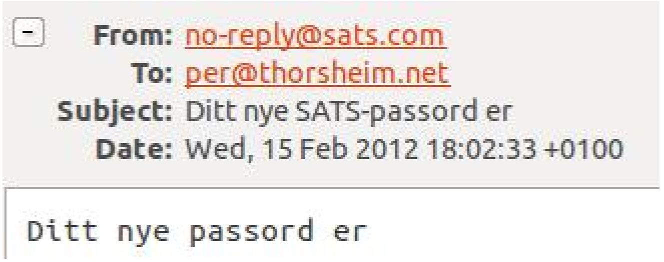
https://defuse.ca/password-policy-hall-of-shame.htm

E-mail can be used for password resets…



From: no-reply@sats.com
To: per@thorsheim.net
Subject: Forespørsel om tilbakestilling av passord
Date: Wed, 15 Feb 2012 18:01:58 +0100

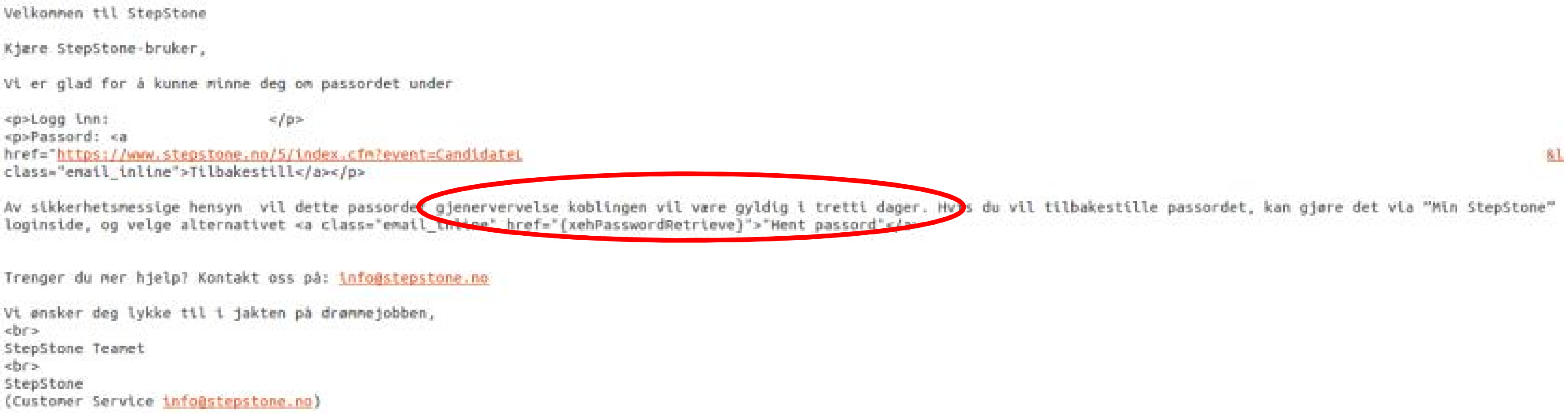
```
Klikk på linken for å tilbakestille ditt passord. Linken er gyldig i tre
timer.http://www.sats.no/nytt-passord/?username=                          19BB67F8
```



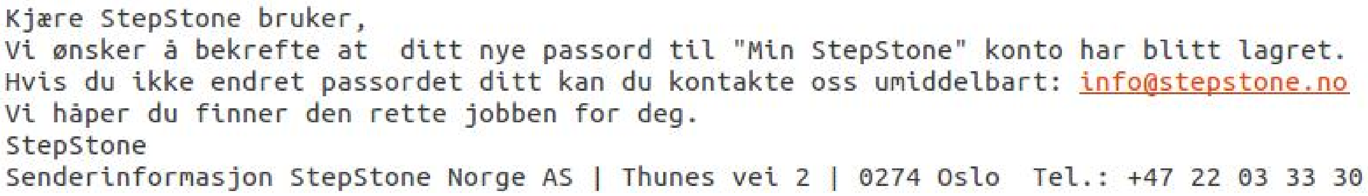
From: no-reply@sats.com
To: per@thorsheim.net
Subject: Ditt nye SATS-passord er
Date: Wed, 15 Feb 2012 18:02:33 +0100

```
Ditt nye passord er
```

…but not everyone does it «correctly»

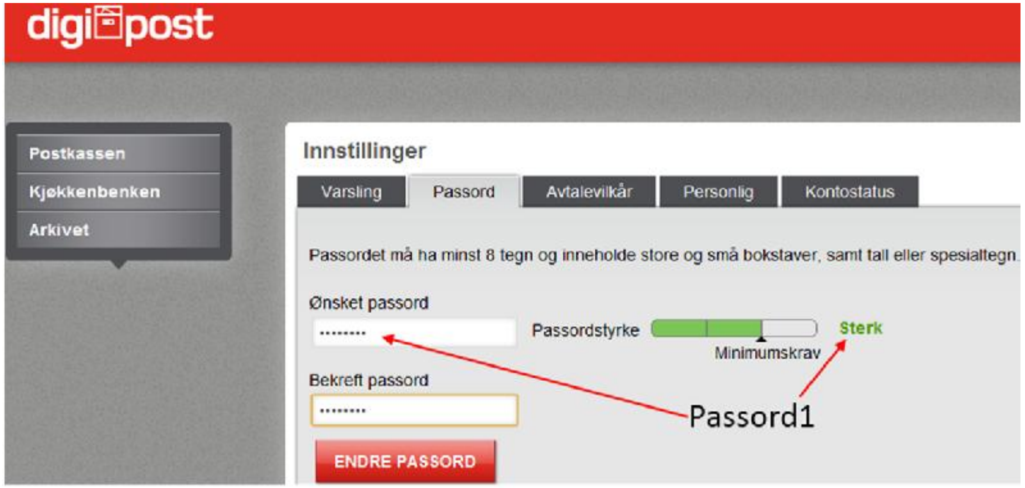


```
Velkommen til StepStone

Kjære StepStone-bruker,

Vi er glad for å kunne minne deg om passordet under

<p>Logg inn:                    </p>
<p>Passord: <a
href="https://www.stepstone.no/5/index.cfm?event=Candidatel                                                      &l
class="email_inline">Tilbakestill</a></p>

Av sikkerhetsmessige hensyn  vil dette passordet gjenervervelse koblingen vil være gyldig i tretti dager. Hvis du vil tilbakestille passordet, kan gjøre det via "Min StepStone"
loginside, og velge alternativet <a class="email_inline" href="{xehPasswordRetrieve}">"Hent passord"</a>


Trenger du mer hjelp? Kontakt oss på: info@stepstone.no

Vi ønsker deg lykke til i jakten på drømmejobben,
<br>
StepStone Teamet
<br>
StepStone
(Customer Service info@stepstone.no)
```



Kjære StepStone bruker,
Vi ønsker å bekrefte at ditt nye passord til "Min StepStone" konto har blitt lagret.
Hvis du ikke endret passordet ditt kan du kontakte oss umiddelbart: info@stepstone.no
Vi håper du finner den rette jobben for deg.
StepStone
Senderinformasjon StepStone Norge AS | Thunes vei 2 | 0274 Oslo Tel.: +47 22 03 33 30

Password meters are dangerous:



Passordet må ha minst 8 tegn og inneholde store og små bokstaver, samt tall eller spesialtegn.

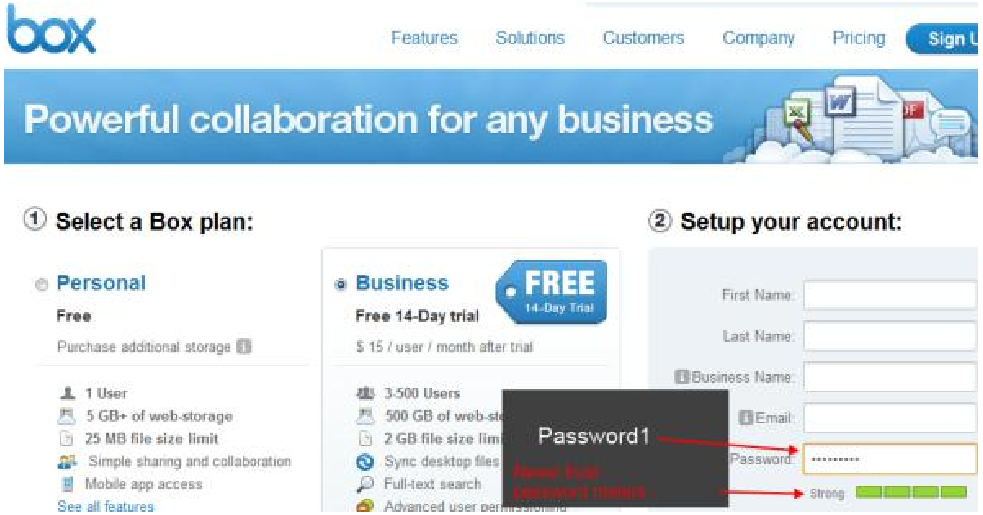
Ønsket passord: ••••••••

Passordstyrke: Sterk

Minimumskrav

Bekreft passord: ••••••••

Passord1



① Select a Box plan:

○ Personal

Free

Purchase additional storage

- 1 User
- 5 GB+ of web-storage
- 25 MB file size limit
- Simple sharing and collaboration
- Mobile app access

● Business

Free 14-Day trial

$ 15 / user / month after trial

- 3-500 Users
- 500 GB of web-st
- 2 GB file size lim
- Sync desktop files
- Full-text search
- Advanced user per

② Setup your account:

First Name:

Last Name:

Business Name:

Email:

Password: ••••••••••

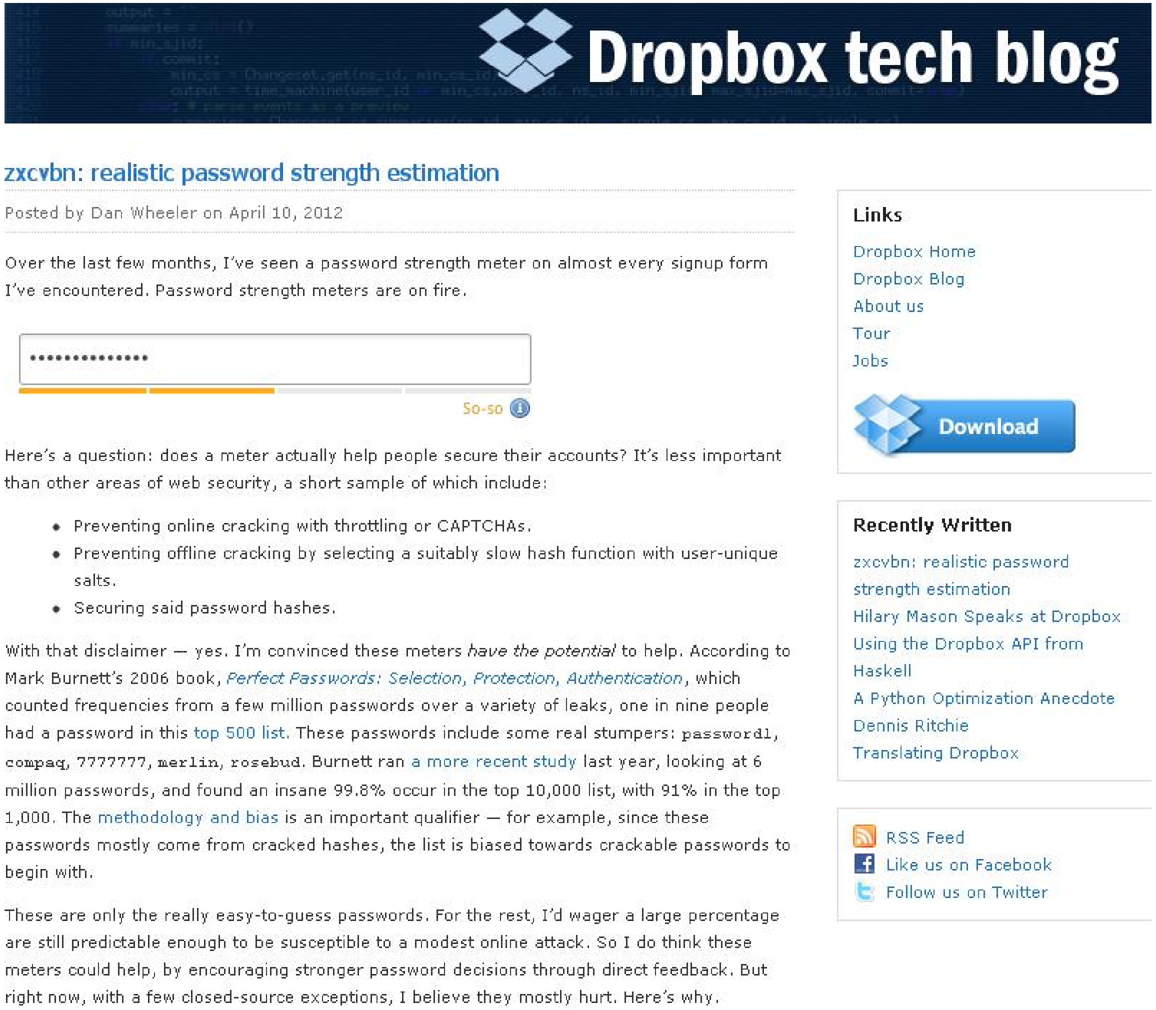
Strong 🟩🟩🟩🟩

Password1

Never trust password meters

http://securitynirvana.blogspot.com/2010/11/revisiting-password-meters.html

…Still want a password meter at your site?



zxcvbn: realistic password strength estimation

Posted by Dan Wheeler on April 10, 2012

Over the last few months, I've seen a password strength meter on almost every signup form I've encountered. Password strength meters are on fire.

Here's a question: does a meter actually help people secure their accounts? It's less important than other areas of web security, a short sample of which include:

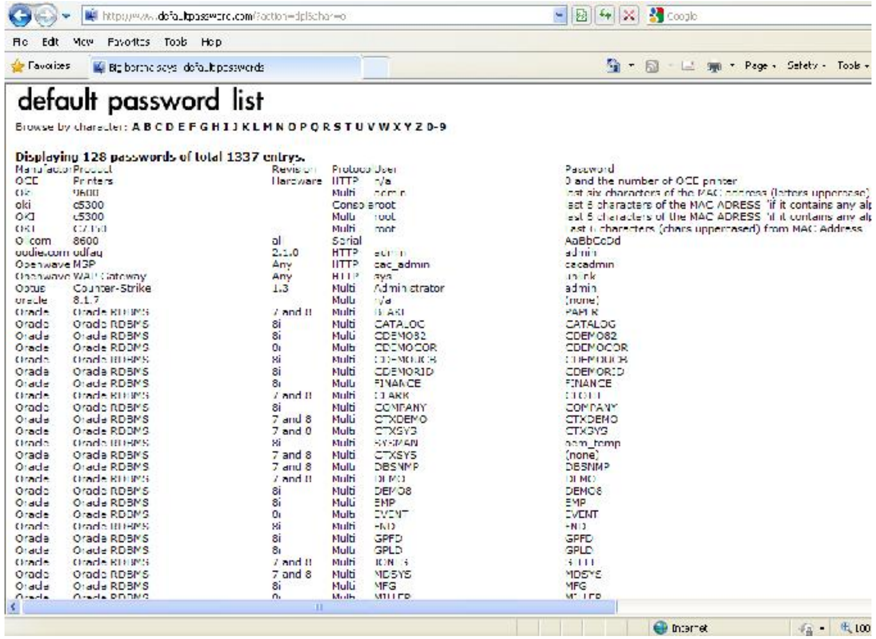
- Preventing online cracking with throttling or CAPTCHAs.
- Preventing offline cracking by selecting a suitably slow hash function with user-unique salts.
- Securing said password hashes.

With that disclaimer — yes. I'm convinced these meters *have the potential* to help. According to Mark Burnett's 2006 book, *Perfect Passwords: Selection, Protection, Authentication*, which counted frequencies from a few million passwords over a variety of leaks, one in nine people had a password in this top 500 list. These passwords include some real stumpers: `password1`, `compaq`, `7777777`, `merlin`, `rosebud`. Burnett ran a more recent study last year, looking at 6 million passwords, and found an insane 99.8% occur in the top 10,000 list, with 91% in the top 1,000. The methodology and bias is an important qualifier — for example, since these passwords mostly come from cracked hashes, the list is biased towards crackable passwords to begin with.

These are only the really easy-to-guess passwords. For the rest, I'd wager a large percentage are still predictable enough to be susceptible to a modest online attack. So I do think these meters could help, by encouraging stronger password decisions through direct feedback. But right now, with a few closed-source exceptions, I believe they mostly hurt. Here's why.

http://tech.dropbox.com/?p=165 & https://github.com/lowe/zxcvbn

No default passwords or backdoors, PLEASE!


http://www.defaultpassword.com/?action=dpl&char=o
File Edit View Favorites Tools Help
Favorites
Big bertha says: default passwords
Page Safety Tools
Internet
100

default password list

Browse by character: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0-9

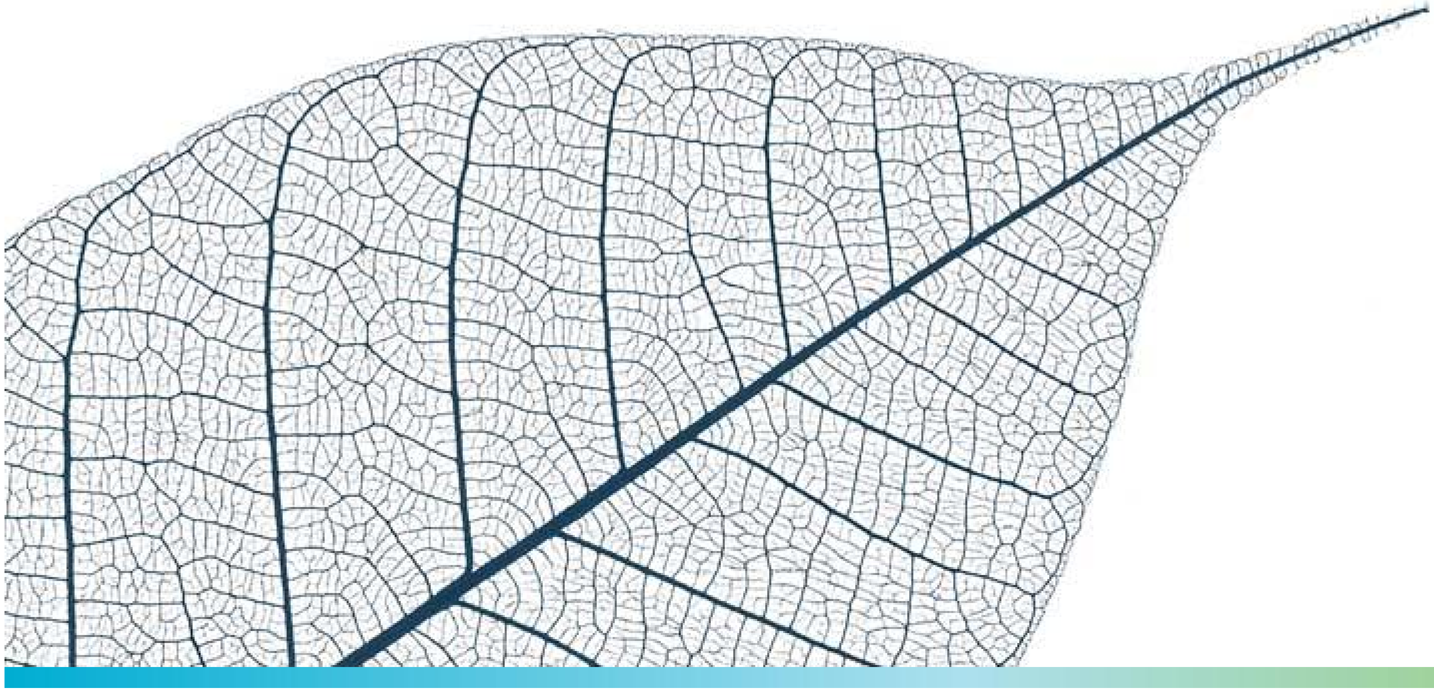
Displaying 128 passwords of total 1337 entrys.

Manufactor	Product	Revision	Protocol	User	Password
OCE	Printers	Hardware	HTTP	n/a	0 and the number of OCE printer
OKI	9600		Multi	admin	last six characters of the MAC address (letters uppercase)
oki	c5300		Console	root	last 6 characters of the MAC ADRESS 'if it contains any alp
OKI	c5300		Multi	root	last 6 characters of the MAC ADRESS 'if it contains any alp
OKI	C7350		Multi	root	Last 6 characters (chars uppercased) from MAC Address
Olicom	8600	all	Serial		AaBbCcDd
oodie.com	odfaq	2.1.0	HTTP	admin	admin
Openwave	MSP	Any	HTTP	cac_admin	cacadmin
Openwave	WAP Gateway	Any	HTTP	sys	uplink
Optus	Counter-Strike	1.3	Multi	Administrator	admin
oracle	8.1.7		Multi	n/a	(none)
Oracle	Oracle RDBMS	7 and 8	Multi	BLAKE	PAPER
Oracle	Oracle RDBMS	8i	Multi	CATALOG	CATALOG
Oracle	Oracle RDBMS	8i	Multi	CDEMO82	CDEMO82
Oracle	Oracle RDBMS	8i	Multi	CDEMOCOR	CDEMOCOR
Oracle	Oracle RDBMS	8i	Multi	CDEMOUCB	CDEMOUCB
Oracle	Oracle RDBMS	8i	Multi	CDEMORID	CDEMORID
Oracle	Oracle RDBMS	8i	Multi	FINANCE	FINANCE
Oracle	Oracle RDBMS	7 and 8	Multi	CLARK	CLOTH
Oracle	Oracle RDBMS	8i	Multi	COMPANY	COMPANY
Oracle	Oracle RDBMS	7 and 8	Multi	CTXDEMO	CTXDEMO
Oracle	Oracle RDBMS	7 and 8	Multi	CTXSYS	CTXSYS
Oracle	Oracle RDBMS	8i	Multi	SYSMAN	oem_temp
Oracle	Oracle RDBMS	7 and 8	Multi	CTXSYS	(none)
Oracle	Oracle RDBMS	7 and 8	Multi	DBSNMP	DBSNMP
Oracle	Oracle RDBMS	7 and 8	Multi	DEMO	DEMO
Oracle	Oracle RDBMS	8i	Multi	DEMO8	DEMO8
Oracle	Oracle RDBMS	8i	Multi	EMP	EMP
Oracle	Oracle RDBMS	8i	Multi	EVENT	EVENT
Oracle	Oracle RDBMS	8i	Multi	FND	FND
Oracle	Oracle RDBMS	8i	Multi	GPFD	GPFD
Oracle	Oracle RDBMS	8i	Multi	GPLD	GPLD
Oracle	Oracle RDBMS	7 and 8	Multi	JONES	STEEL
Oracle	Oracle RDBMS	7 and 8	Multi	MDSYS	MDSYS
Oracle	Oracle RDBMS	8i	Multi	MFG	MFG
Oracle	Oracle RDBMS	8i	Multi	MILLER	MILLER

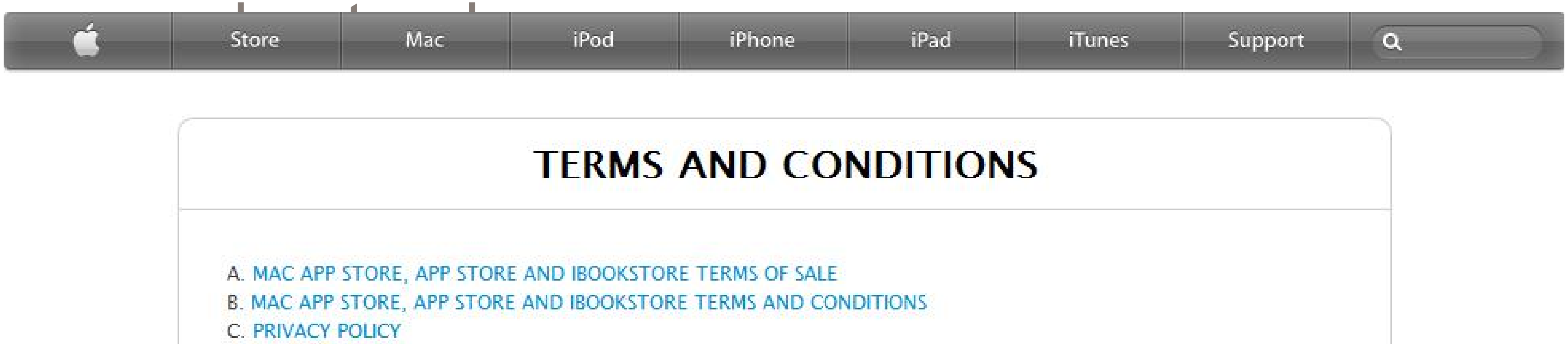
```
Problem:
An undocumented backdoor account exists within all released versions
of RuggedCom's Rugged Operating System (ROS®).  The username for the
account, which cannot be disabled, is "factory" and its password is
dynamically generated based on the device's MAC address.  Multiple
attempts have been made in the past 12 months to have this backdoor
removed and customers notified.
```

http://seclists.org/bugtraq/2012/Apr/185

Written Password Policies

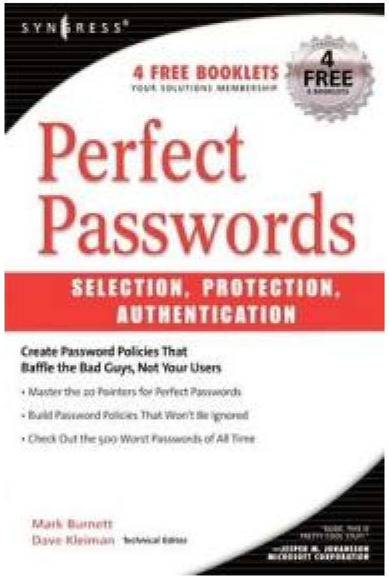


Password policies should be simple to

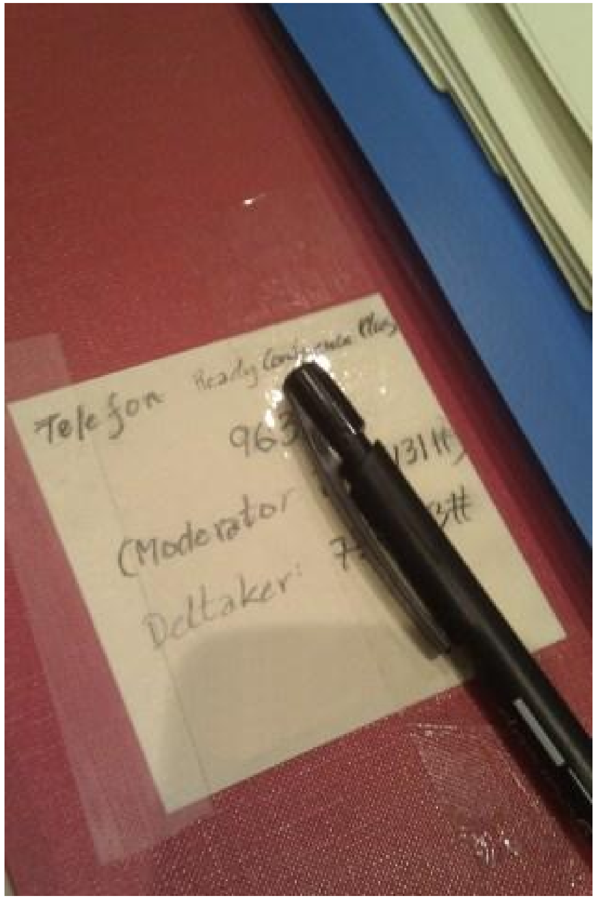


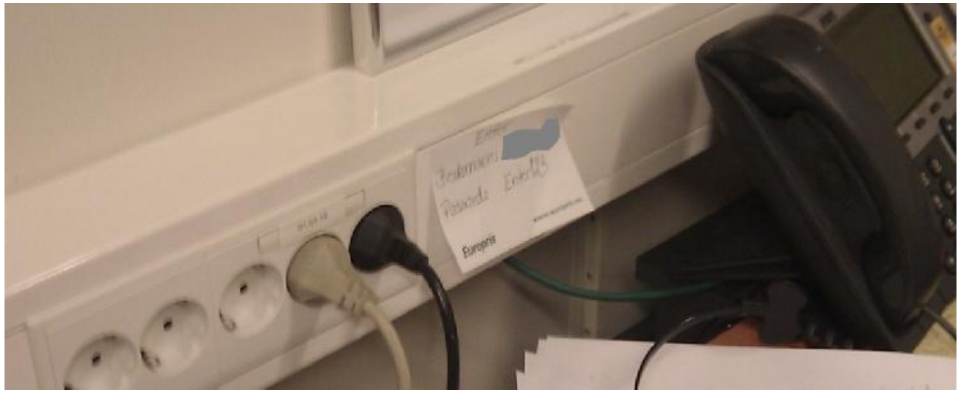
TERMS AND CONDITIONS

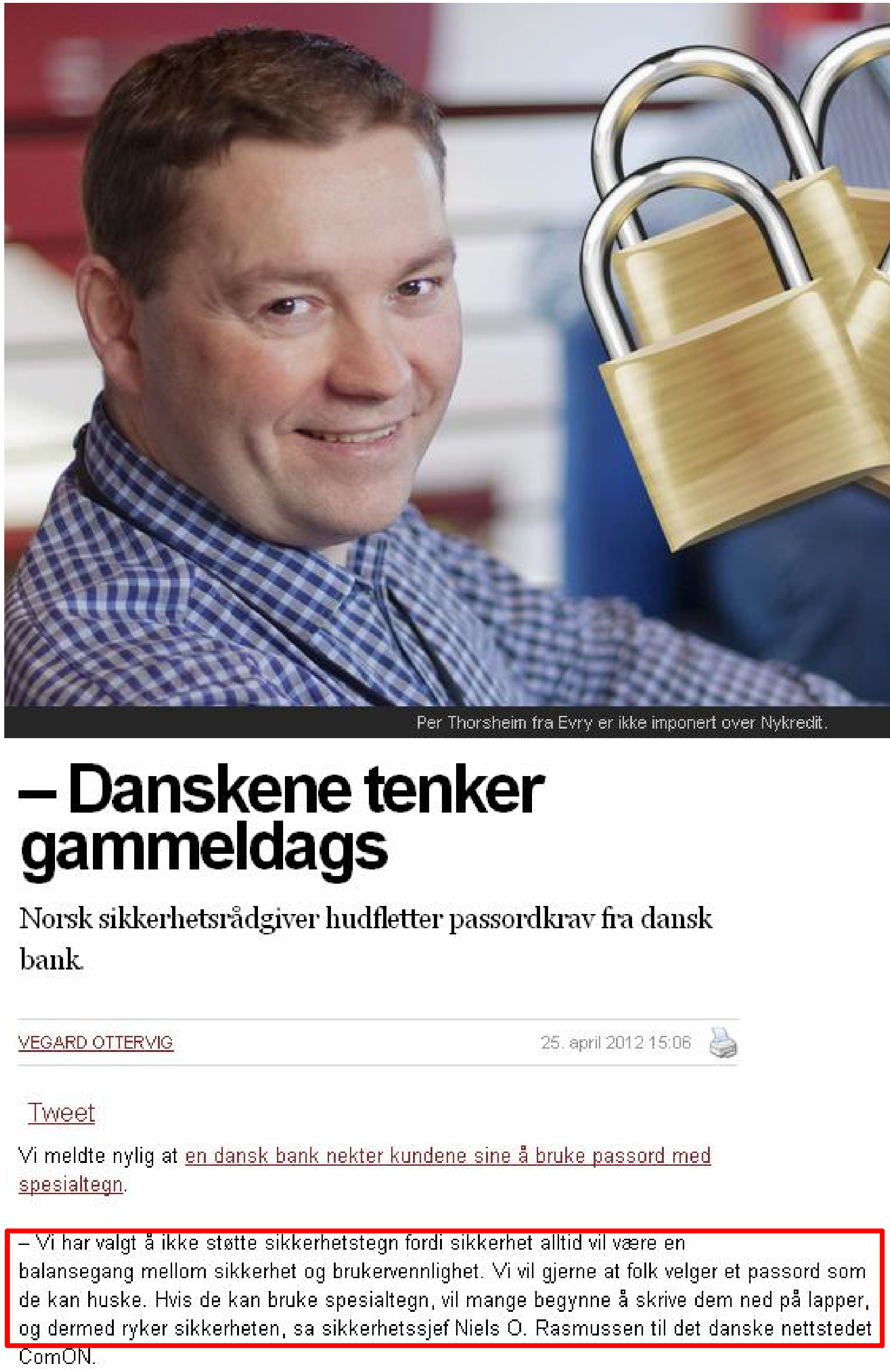
A. MAC APP STORE, APP STORE AND IBOOKSTORE TERMS OF SALE
B. MAC APP STORE, APP STORE AND IBOOKSTORE TERMS AND CONDITIONS
C. PRIVACY POLICY


SYNGRESS®
4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP
4 FREE
Perfect Passwords
SELECTION, PROTECTION, AUTHENTICATION
Create Password Policies That Baffle the Bad Guys, Not Your Users
• Master the 20 Pointers for Perfect Passwords
• Build Password Policies That Won't Be Ignored
• Check Out the 500 Worst Passwords of All Time
Mark Burnett
Dave Kleiman Technical Editor

… or passwords may end up here:







Per Thorsheim fra Evry er ikke imponert over Nykredit.

– Danskene tenker gammeldags

Norsk sikkerhetsrådgiver hudfletter passordkrav fra dansk bank.

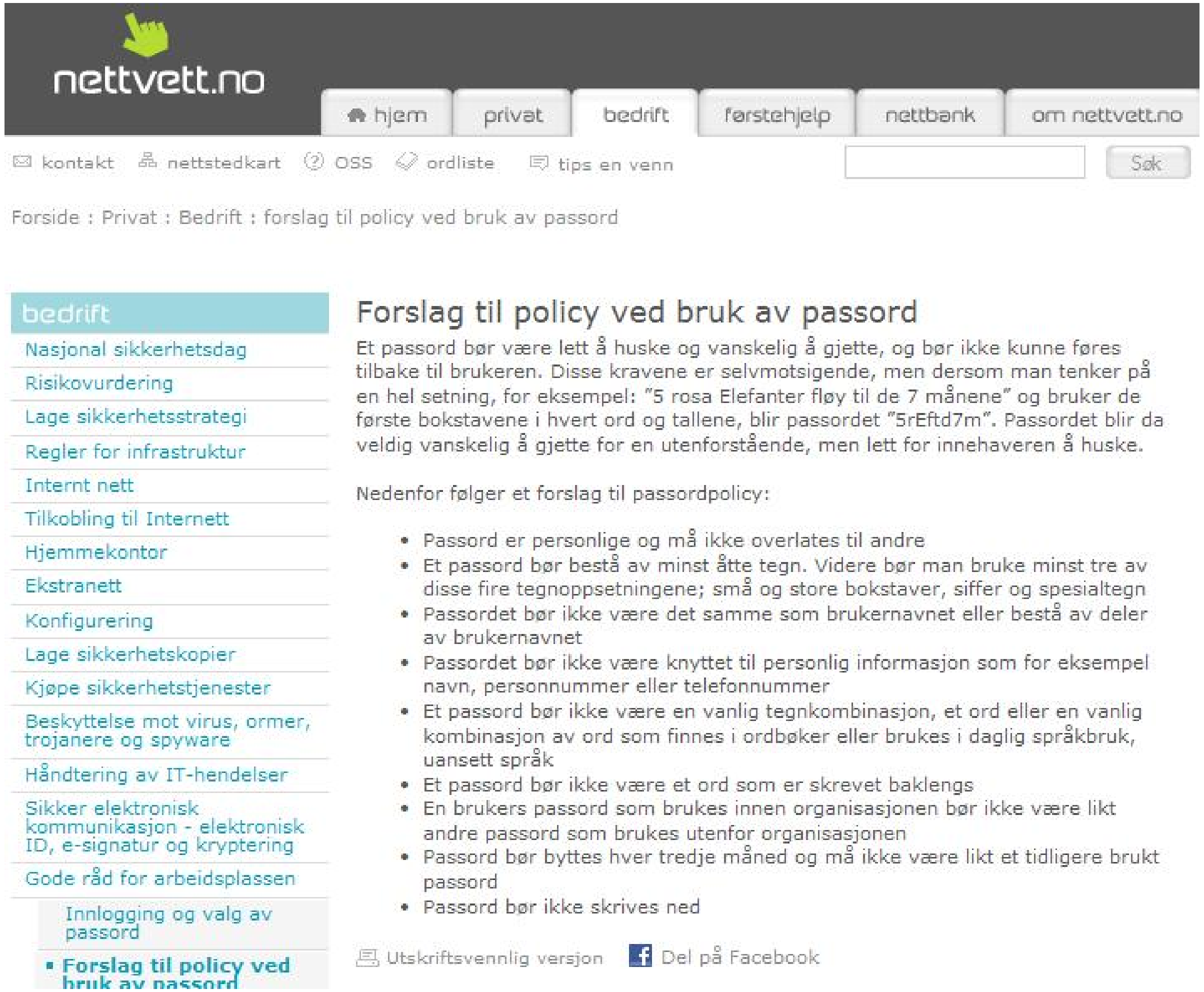
VEGARD OTTERVIG 25. april 2012 15:06

Tweet

Vi meldte nylig at en dansk bank nekter kundene sine å bruke passord med spesialtegn.

– Vi har valgt å ikke støtte sikkerhetstegn fordi sikkerhet alltid vil være en balansegang mellom sikkerhet og brukervennlighet. Vi vil gjerne at folk velger et passord som de kan huske. Hvis de kan bruke spesialtegn, vil mange begynne å skrive dem ned på lapper, og dermed ryker sikkerheten, sa sikkerhetssjef Niels O. Rasmussen til det danske nettstedet ComON.

Our past is paved with bad examples…


nettvett.no
hjem
privat
bedrift
førstehjelp
nettbank
om nettvett.no
kontakt
nettstedkart
OSS
ordliste
tips en venn
Søk
Forside : Privat : Bedrift : forslag til policy ved bruk av passord
bedrift
Nasjonal sikkerhetsdag
Risikovurdering
Lage sikkerhetsstrategi
Regler for infrastruktur
Internt nett
Tilkobling til Internett
Hjemmekontor
Ekstranett
Konfigurering
Lage sikkerhetskopier
Kjøpe sikkerhetstjenester
Beskyttelse mot virus, ormer, trojanere og spyware
Håndtering av IT-hendelser
Sikker elektronisk kommunikasjon - elektronisk ID, e-signatur og kryptering
Gode råd for arbeidsplassen
Innlogging og valg av passord
Forslag til policy ved bruk av passord

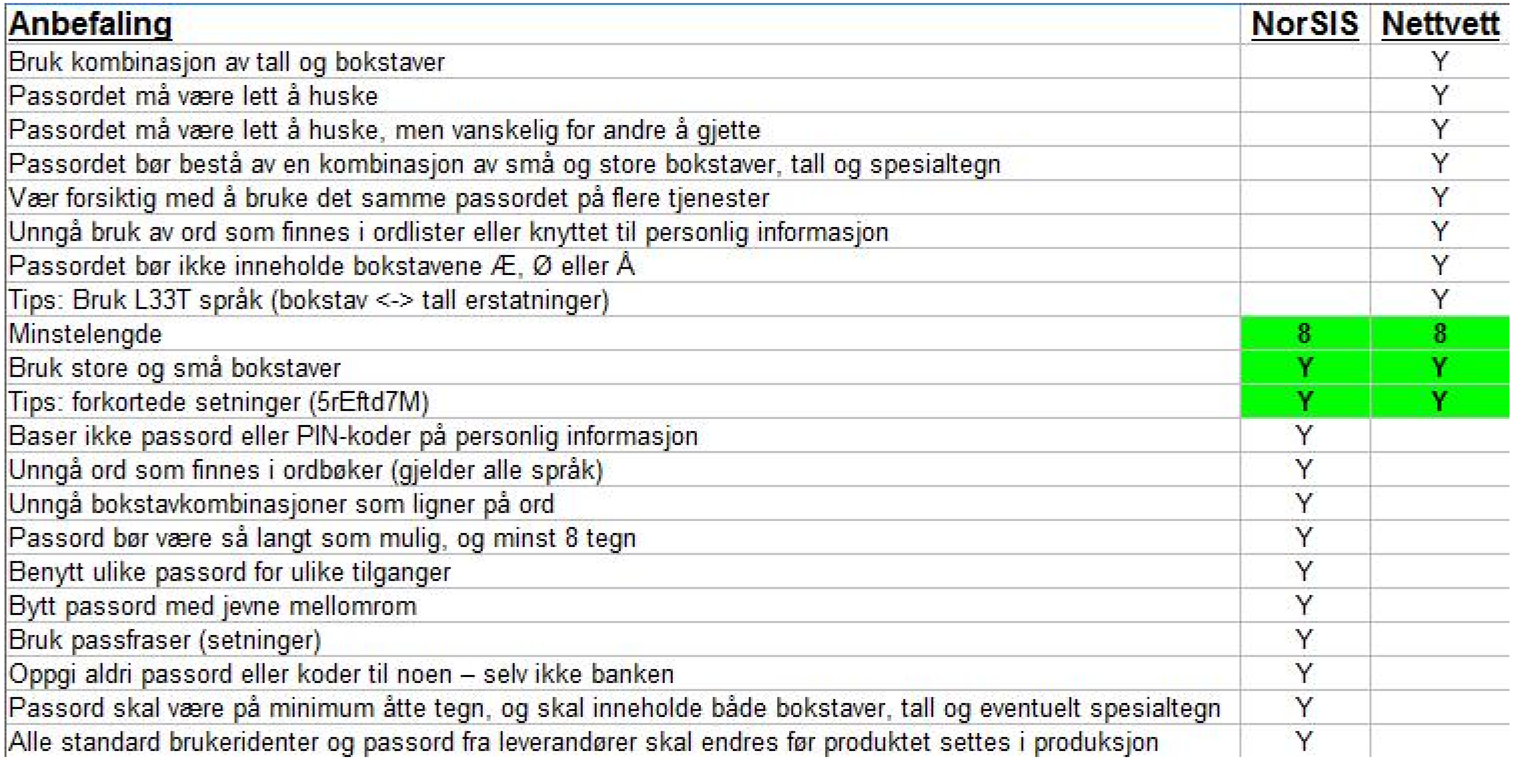
Forslag til policy ved bruk av passord

Et passord bør være lett å huske og vanskelig å gjette, og bør ikke kunne føres tilbake til brukeren. Disse kravene er selvmotsigende, men dersom man tenker på en hel setning, for eksempel: "5 rosa Elefanter fløy til de 7 månene" og bruker de første bokstavene i hvert ord og tallene, blir passordet "5rEftd7m". Passordet blir da veldig vanskelig å gjette for en utenforstående, men lett for innehaveren å huske.

Nedenfor følger et forslag til passordpolicy:

- Passord er personlige og må ikke overlates til andre
- Et passord bør bestå av minst åtte tegn. Videre bør man bruke minst tre av disse fire tegnoppsetningene; små og store bokstaver, siffer og spesialtegn
- Passordet bør ikke være det samme som brukernavnet eller bestå av deler av brukernavnet
- Passordet bør ikke være knyttet til personlig informasjon som for eksempel navn, personnummer eller telefonnummer
- Et passord bør ikke være en vanlig tegnkombinasjon, et ord eller en vanlig kombinasjon av ord som finnes i ordbøker eller brukes i daglig språkbruk, uansett språk
- Et passord bør ikke være et ord som er skrevet baklengs
- En brukers passord som brukes innen organisasjonen bør ikke være likt andre passord som brukes utenfor organisasjonen
- Passord bør byttes hver tredje måned og må ikke være likt et tidligere brukt passord
- Passord bør ikke skrives ned

…. REALLY bad examples in fact.



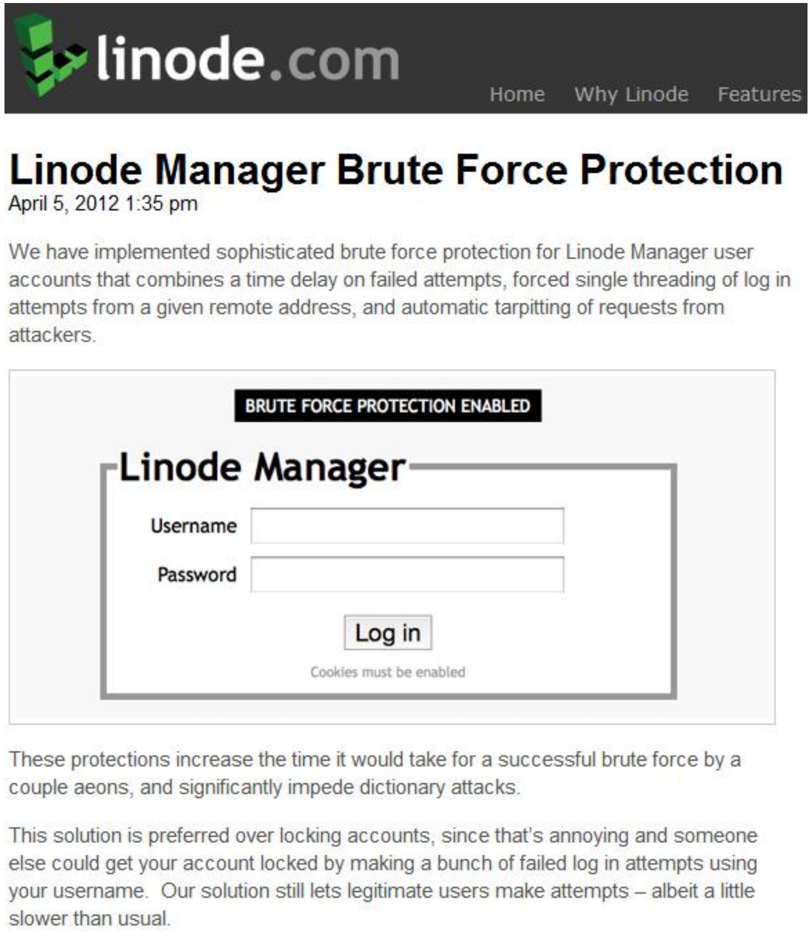
Anbefaling	NorSIS	Nettvett
Bruk kombinasjon av tall og bokstaver		Y
Passordet må være lett å huske		Y
Passordet må være lett å huske, men vanskelig for andre å gjette		Y
Passordet bør bestå av en kombinasjon av små og store bokstaver, tall og spesialtegn		Y
Vær forsiktig med å bruke det samme passordet 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	

Now let me fix that password security for you…

WITHOUT affecting UX **AT ALL**

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

Rate-limiting online bruteforce attacks



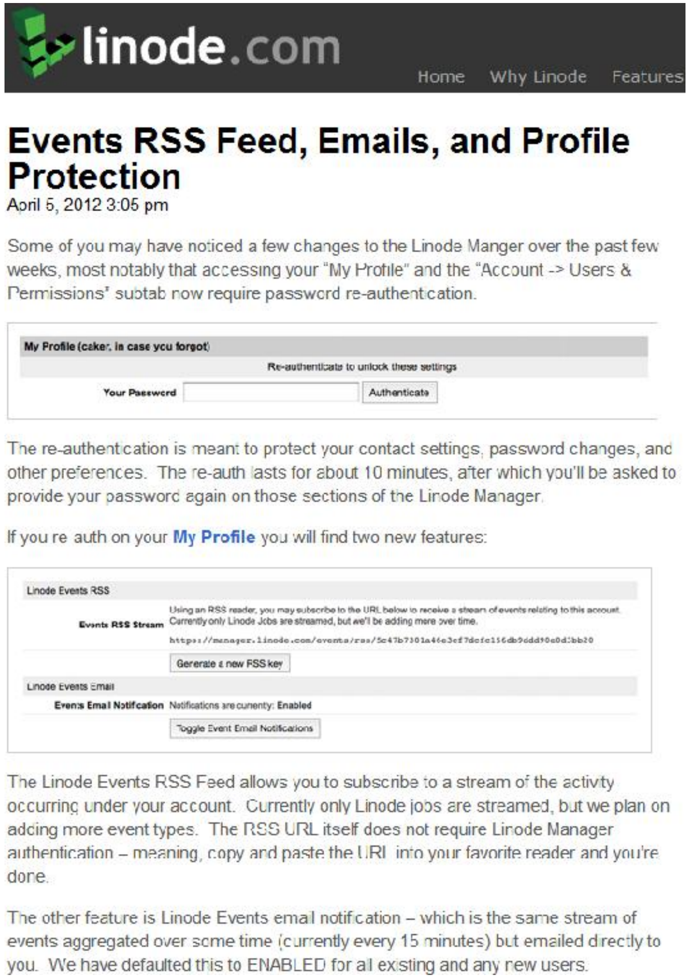
Linode Manager Brute Force Protection

April 5, 2012 1:35 pm

We have implemented sophisticated brute force protection for Linode Manager user accounts that combines a time delay on failed attempts, forced single threading of log in attempts from a given remote address, and automatic tarpitting of requests from attackers.

These protections increase the time it would take for a successful brute force by a couple aeons, and significantly impede dictionary attacks.

This solution is preferred over locking accounts, since that's annoying and someone else could get your account locked by making a bunch of failed log in attempts using your username. Our solution still lets legitimate users make attempts – albeit a little slower than usual.



Events RSS Feed, Emails, and Profile Protection

April 5, 2012 3:05 pm

Some of you may have noticed a few changes to the Linode Manger over the past few weeks, most notably that accessing your "My Profile" and the "Account -> Users & Permissions" subtab now require password re-authentication.

My Profile (caker, in case you forgot)

Re-authenticate to unlock these settings

Your Password

The re-authentication is meant to protect your contact settings, password changes, and other preferences. The re-auth lasts for about 10 minutes, after which you'll be asked to provide your password again on those sections of the Linode Manager.

If you re auth on your **My Profile** you will find two new features:

Linode Events RSS

Events RSS Stream: Using an RSS reader, you may subscribe to the URL below to receive a stream of events relating to this account. Currently only Linode Jobs are streamed, but we'll be adding more over time.

https://manager.linode.com/events/rss/5c47b7301a46e3cf7dcfc156db9ddd90e0d2bb20

Linode Events Email

Events Email Notification: Notifications are currently: **Enabled**

The Linode Events RSS Feed allows you to subscribe to a stream of the activty occurring under your account. Currently only Linode jobs are streamed, but we plan on adding more event types. The RSS URL itself does not require Linode Manager authentication – meaning, copy and paste the URL into your favorite reader and you're done.

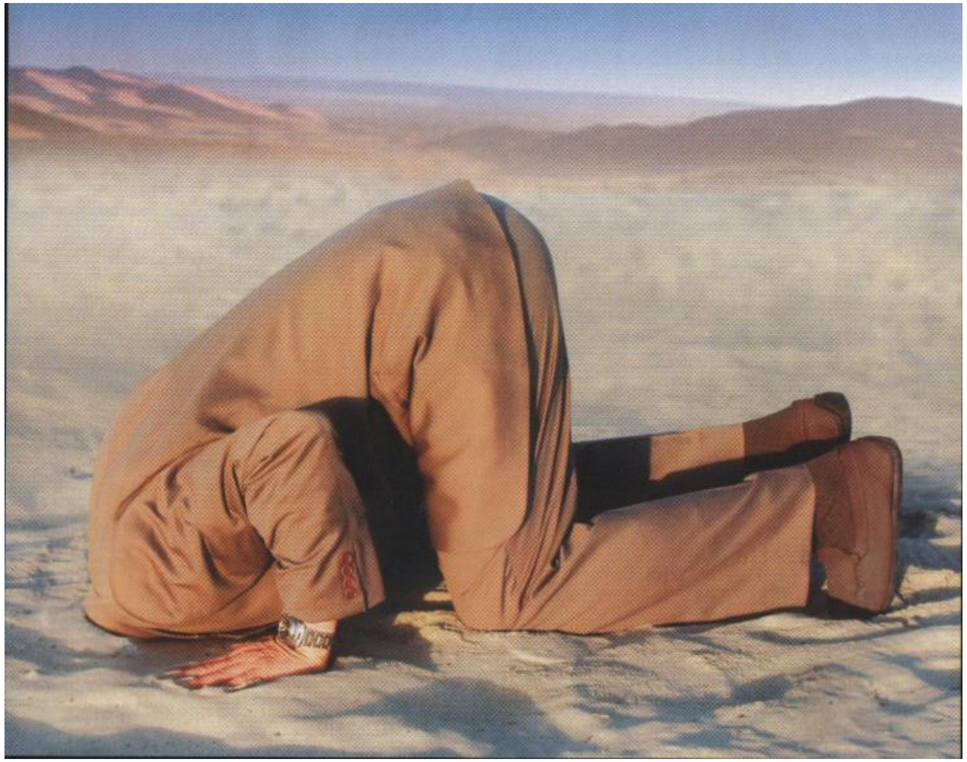
The other feature is Linode Events email notification – which is the same stream of events aggregated over some time (currently every 15 minutes) but emailed directly to you. We have defaulted this to ENABLED for all existing and any new users.

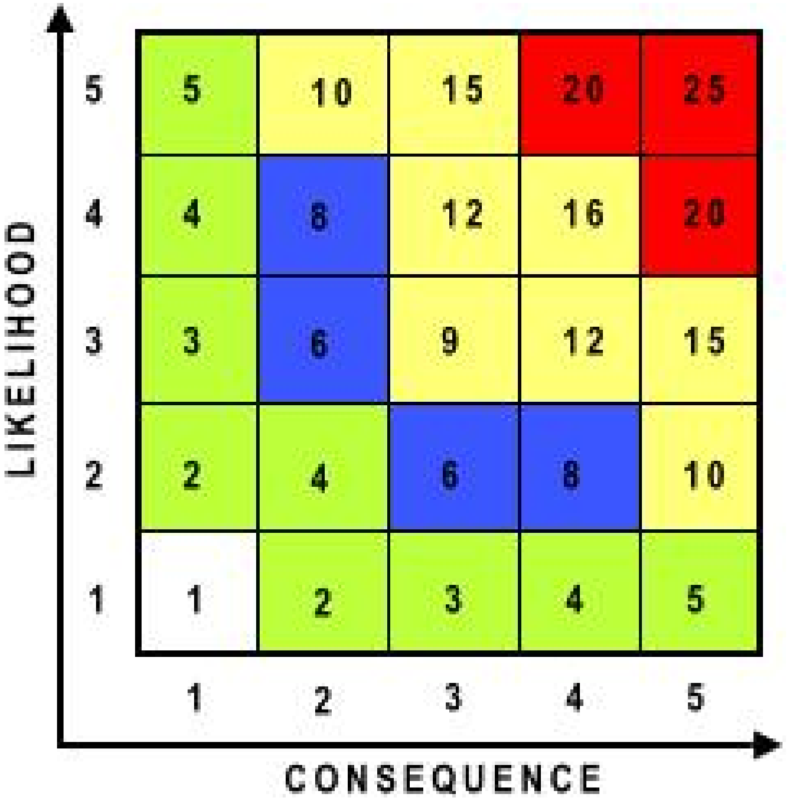
Recommendations

3 Blog posts and 1 academic paper:

1. «Enough with the rainbow tables: what you need to know about secure password schemes»
   http://chargen.matasano.com/chargen/2007/9/7/enough-with-the-rainbow-tables-what-you-need-to-know-about-s.html
2. «Strong password hashing for ASP.NET»
   http://zetetic.net/blog/2012/3/29/strong-password-hashing-for-aspnet.html
3. «Why you should use Bcrypt to hash stored passwords»
   http://phpmaster.com/why-you-should-use-bcrypt-to-hash-stored-passwords/
4. «The quest to replace passwords: a framework for comparative evaluation of web authentication schemes»
   http://www.cl.cam.ac.uk/~fms27/papers/2012-BonneauHerOorSta-password--oakland.pdf

You should do risk analysis…



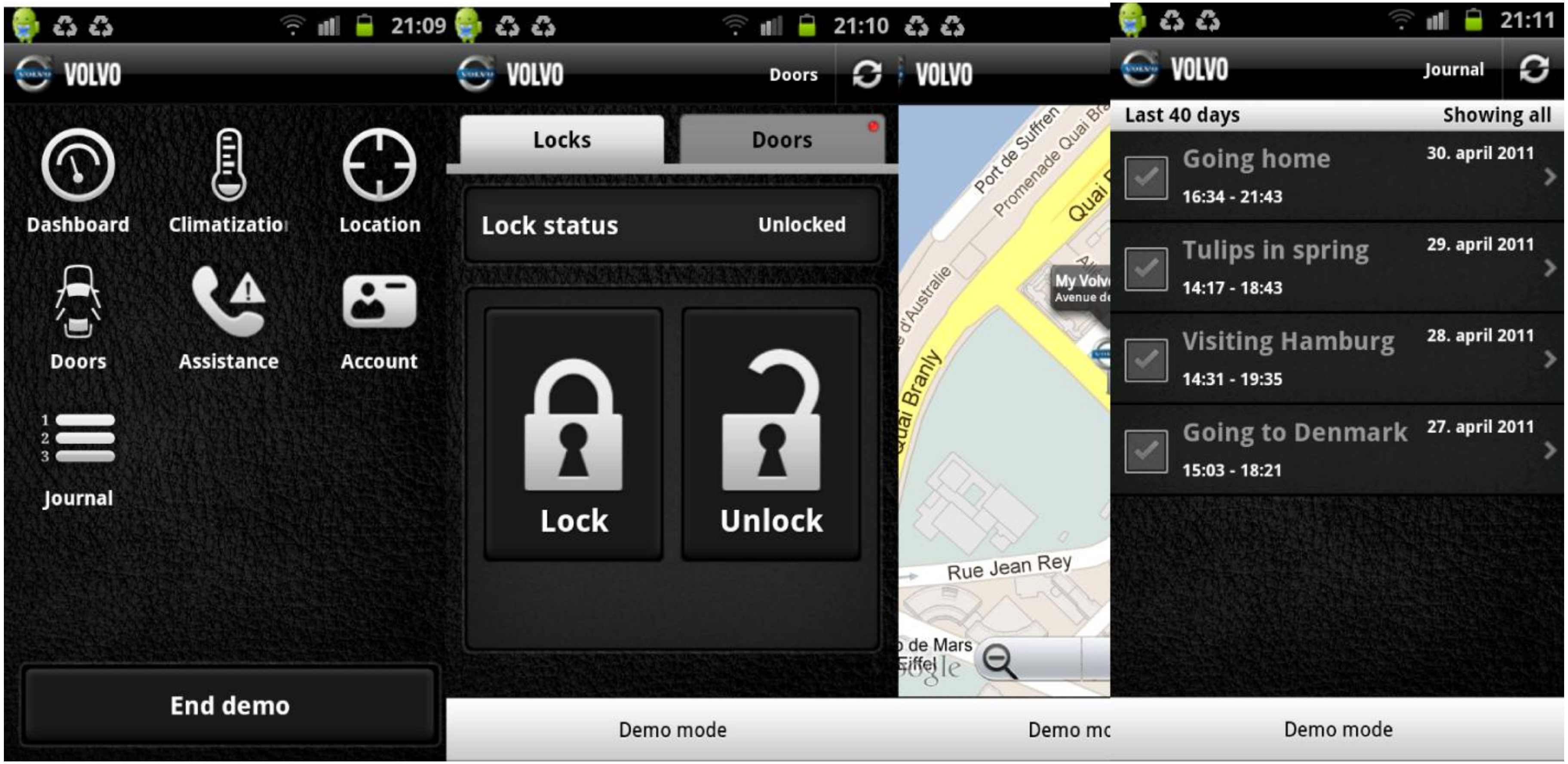


LIKELIHOOD					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

CONSEQUENCE

(Your choice of methodology of course…)

… and accept the real world.



Lock status Unlocked

Last 40 days Showing all

☑	Going home 16:34 - 21:43	30. april 2011
☑	Tulips in spring 14:17 - 18:43	29. april 2011
☑	Visiting Hamburg 14:31 - 19:35	28. april 2011
☑	Going to Denmark 15:03 - 18:21	27. april 2011

Thank you!

in Per Thorsheim

securitynirvana.blogspot.com

@thorsheim

EVRY

EVRY

We bring information to life