

Wachtwoorden een heikel onderwerp.

Onlangs maakte het Nationaal Cyber Security Center (NCSC) bekend dat er bijna anderhalf miljoen Nederlandse e-mail adressen gestolen zijn. Of de wachtwoorden ook gekraakt zijn is niet bekend

Waarschijnlijk gehackt bij bedrijven waarvan de beveiliging van de klantendatabase onvoldoende is.

De gehackte data wordt vaak door verkocht aan spammers of criminelen.

Wachtwoorden een heikel onderwerp.

- Voor veel toepassingen op internet is een gebruikersnaam en een wachtwoord nodig.
- Denk aan DigiD, webwinkels, Marktplaats enzovoort.
- Daarnaast heb je dan ook nog de sociale media waar je een persoonlijk profiel moet aanmaken.
- Werk je met Windows, MAC of Linux dan moet je bij het opstarten inloggen met een wachtwoord.

Wachtwoorden een heikel onderwerp.

- Het belang van **niet** of **moeilijk** te kraken wachtwoorden wordt steeds groter.
- Gebruik voor verschillende diensten ook verschillende wachtwoorden.
- Gebruik geen bestaande woorden of namen.
- Gebruik lange wachtwoorden.

Wachtwoorden een heikel onderwerp.

Het belang van een lang wachtwoord blijkt wel uit de volgende berekeningen.

We gebruiken 26 letters LC en 26 letters UC plus de cijfers 0 tot en met 9. Samen 62 verschillende tekens.

Een wacht woord van 8 tekens levert 62^8 dat is ruim 100 miljoen verschillende combinaties op.

Bij 12 tekens is dit al ruim 1 biljoen combinaties.

Wachtwoorden een heikel onderwerp.

Hackers gebruiken zeer snelle computers om wachtwoorden te kraken.

Daarvoor zetten ze vaak een aantal GPU's (Graphic Processing Unit) in.

Een moderne GPU unit kan wel 2 miljoen set en compare bewerkingen per seconde uitvoeren.

Stel dat de effectieve snelheid 1 miljoen set en compares is, dan kan een wachtwoord van 8 tekens in 100 seconden gevonden worden.

Wachtwoorden een heikel onderwerp.

Een lang wachtwoord is dus belangrijk. In de eerste plaats voor het inloggen op de computer. Want daarmee kan voorkomen worden dat men met malware toegang krijgt tot je computer en het kraken van opgeslagen wachtwoorden een eitje wordt.

Maar hoe onthouden we een moeilijk te kraken wachtwoord. Een veel gebruikte methode is een hulpfrase gebruiken.

Wachtwoorden een heikel onderwerp.

Een paar voorbeelden:

- S ven K ramer w int a ltijd d e 10 k ilometer m aar
h oelang n og?
S K w ad 10 k m h n ?
- M ijn A u to h eeft h et m ooie k enteken 07 V X 38
M A h h m k 07 V X 38

Wachtwoorden van 12 karakters.

Wachtwoorden een heikel onderwerp.

Een ander voorbeeld:

yT4\$Lgcw8kK&rvz4

Een volkomen willekeurig van wachtwoord van 16 karakters.

Als inlog wachtwoord heel veilig!

Helaas voor de gemiddelde gebruiker niet te onthouden.

Wachtwoorden een heikel onderwerp.

Aan een wachtwoordkluis hebben we niets omdat we eerst ingelogd moeten zijn om de kluis te kunnen gebruiken.

De oplossing zit in het gebruik van een USB authenticatie sleutel.

De USB sleutel vult het wachtwoord voor je in zodra de computer in de opstart fase vraagt om het wachtwoord.

Wachtwoorden een heikel onderwerp.

USB authenticatie kunnen we maken met de freeware versie van Rohos.

<http://www.rohos.com/products/rohos-logon-free/>

Installeer het Rohos programma in Win 7 of 8, of MAC.

Start het programma op om de USB key te maken.

Wachtwoorden een heikel onderwerp.

Nadat de vraag of het programma veranderingen aan mag brengen in uw systeem met ja is beantwoord verschijnt het programma om je USB sleutel in te stellen.



Sluit een USB stick aan en klik op configureer USB sleutel.

Wachtwoorden een heikel onderwerp.

Inloggen in Windows en Mac met het Rohos authenticatie programma.

Sluit de usb stick aan op een USB poort, start de computer op en het inloggen verloopt automatisch.

Wachtwoord yT4\$Lgcw8kK&rvz4 is geen probleem. Het wachtwoord heeft 10^{16} combinaties. Kraken kan jaren duren.

Wachtwoorden een heikel onderwerp.

Aan welke eisen moet een wachtwoord voldoen?

Dat kan erg verschillend zijn, sommige sites eisen een combinatie hoofdletters, kleine letters, cijfers en symbolen en een minimum lengte.

Bij anderen zijn symbolen niet toegestaan.

Kijk dus goed aan welke eisen het wachtwoord moet voldoen.

Wachtwoorden een heikel onderwerp.

Maar hoe onthoud je al die andere lange wachtwoorden?

Die onthouden we niet, daarvoor gebruiken we de wachtwoordkluis Keepass of één van de varianten op dit principe.

We kunnen Keepass op de zelfde usb stick installeren als het Rohos log in programma.

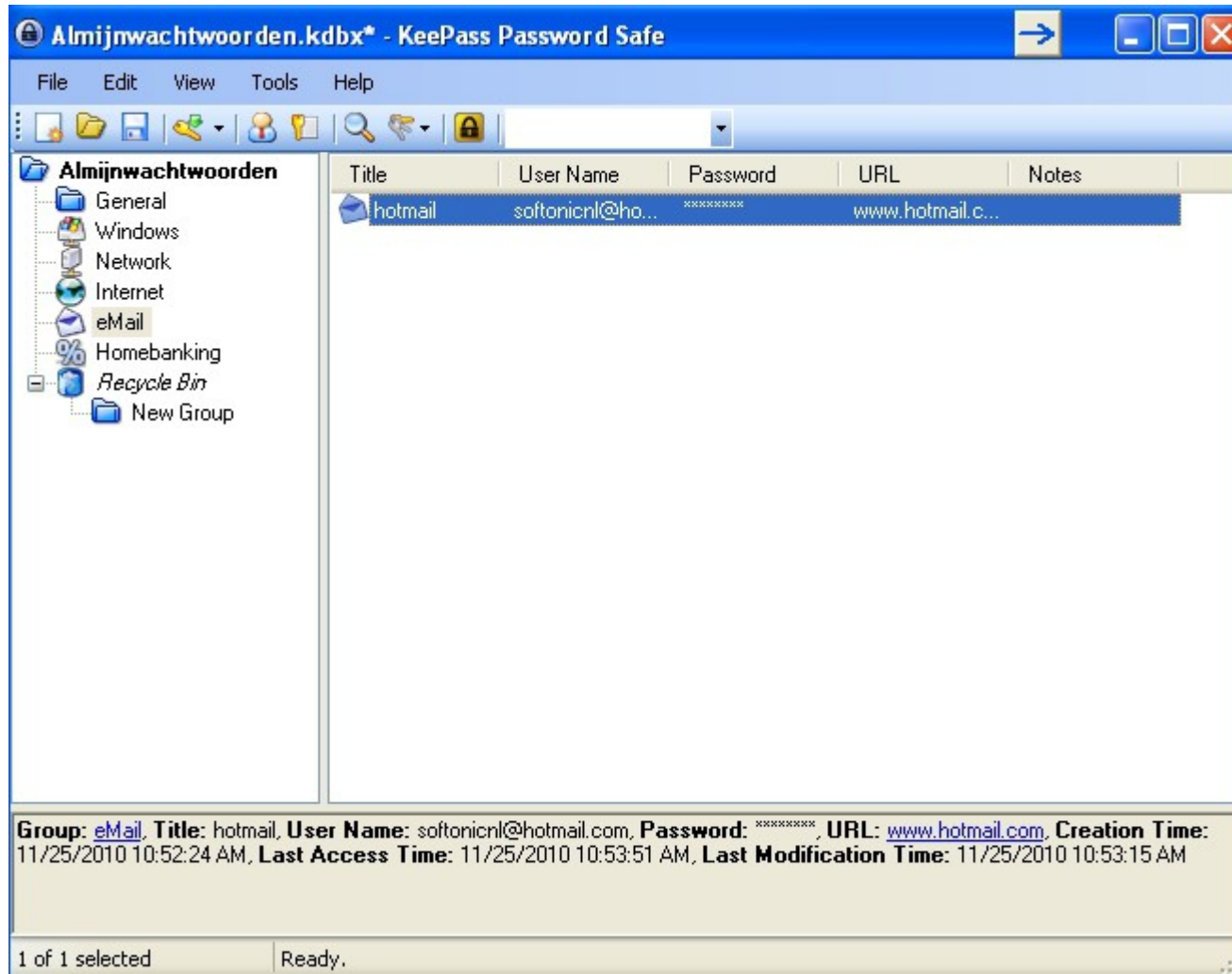
Wachtwoorden een heikel onderwerp.

Keepass kunnen we downloaden van:
<http://sourceforge.net/projects/keepass/>

Voor gebruik met een USB stick kiezen we de portable versie.

We installeren Keepass op de USB stick en maken een snelkoppeling op he bureaublad.

Wachtwoorden een heikel onderwerp.



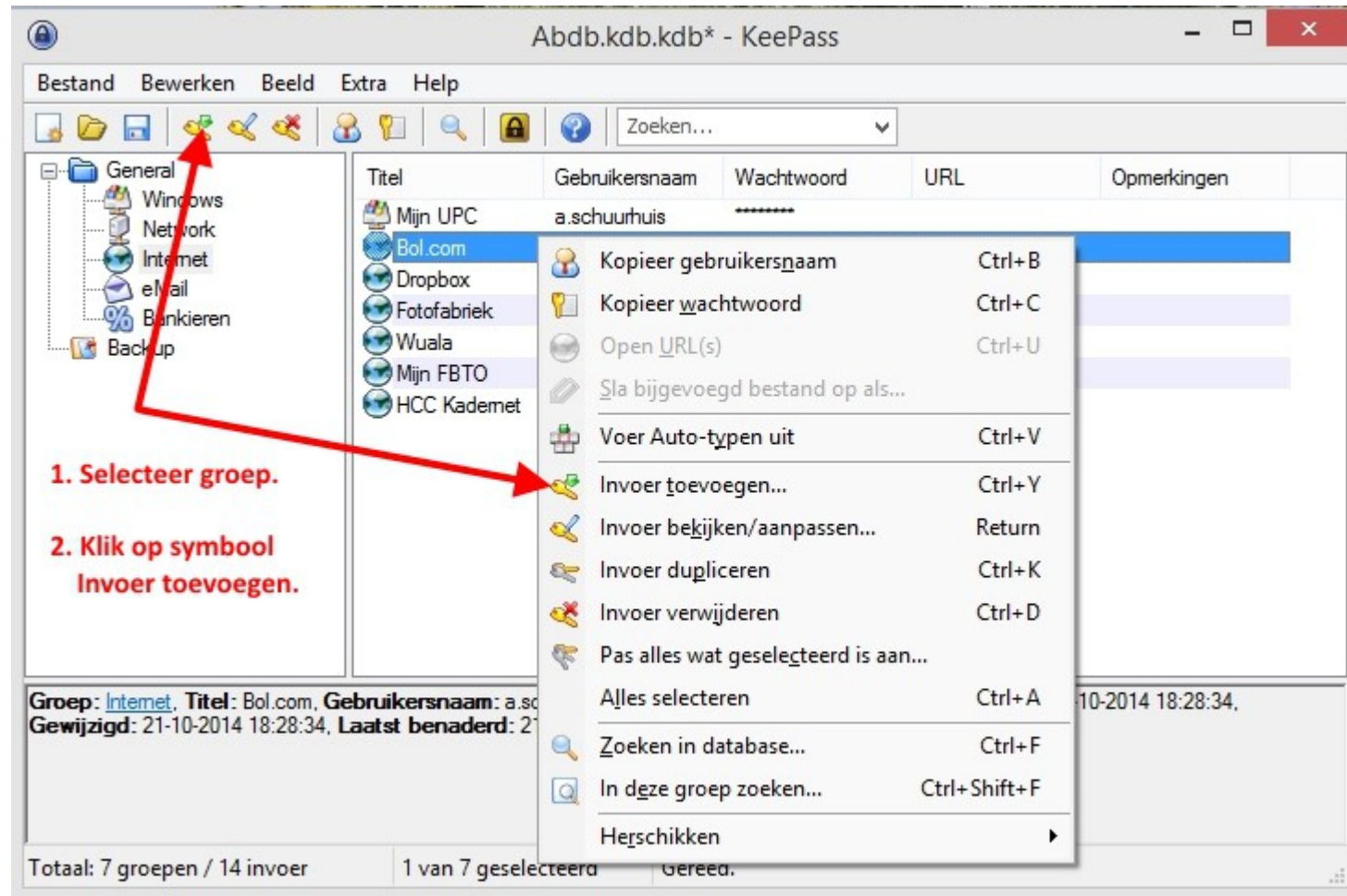
Start het programma en klik op **Nieuw** om een wachtwoorden database aan te maken.

Wachtwoorden een heikel onderwerp.



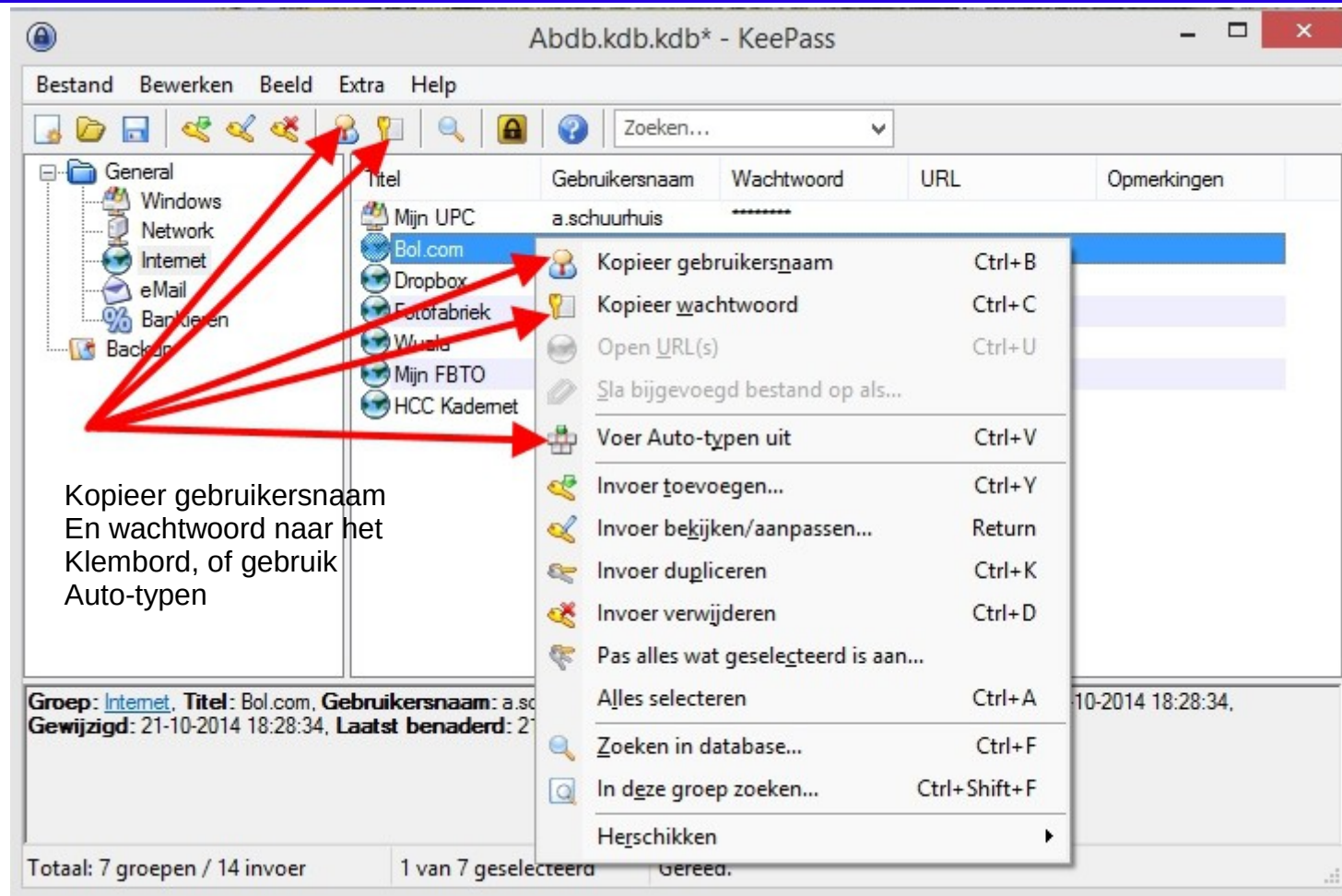
De database moet beveiligd worden met een wachtwoord.
Kies een moeilijk te kraken maar wel te onthouden wachtwoord.

Wachtwoorden een heikel onderwerp.



Na het invoeren het hoofdwachtwoord kunnen we voor de diverse sites de gebruikersnaam en wachtwoord invoeren.

Wachtwoorden een heikel onderwerp.



Inloggen op een website doe je door met je browser naar de website te gaan. Vervolgens open je KeePass. Rechtsklik op de naam van de website in KeePass. Klik in het menu op Auto-typen of gebruik de symbolen gebruikersnaam en ww.

Wachtwoorden een heikel onderwerp.

Keepass kan ook het wachtwoord voor je genereren. Daarbij kun je opgeven uit welke soorten tekens je wachtwoord mag bestaan.

Maar je kunt ook een zelf samengestelde matrix gebruiken zoals voorgesteld in het blad Computer Techniek CT. Een voorbeeld zie je op de volgende dia.

Wachtwoorden matrix.

Wwnr:	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ
1	G2t	8D#	qM6	HS1	Tt7	AB9	Zt&	@42	mZ3	X57	Lk2	ggH	Pv@
2	Dh4	Sk6	S6K	wB7	#3T	bZ&	132	GV8	XpQ	03W	Cf%	\$5P	tTB
3	zS7	AC9	Rt7	G8M	T5#	ANG	Dri	H6%	bZN	K4\$	Jv9	eF0	P1T
4	mc7	nNg	6Ak	P5H	2Uv	Lc7	19k	Y&X	oBz	uR0	WqA	22J	N09
5	rv7	Ts4	6AL	RqZ	YB\$	Zj8	kN7	Cg2	PRv	tF#	SG%	7%T	BCq
6	GvT	oSD	75X	Kt6	Gm4	Wdd	rW6	pT&	aM3	Vg\$	Tt2	8@X	Ld5
7	HJ4	Pn%	Rt7	zD8	MM7	\$F2	Hx6	mU0	Q5L	X62	19R	Bb7	24T
8	KV5	wA9	tR&	CP#	8Dt	&bZ	N6%	tQ#	A!y	bS%	Xt#	nB8	vV3
9	rY7	E5&	Gg2	Uc7	Cu&	LZ4	bU!	0A6	Dv%	43!	B9@	zT&	474
10	lgJ	Vc%	tT#	Lm5	Gg3	Dc%	DD8	Qg&	Tu0	RR3	Ds!	GX&	aT%
11	ZF\$	Ge&	KH0	Cr%	JbY	mG\$	C!T	99S	ZL@	kK5	FY7	cH#	LB4
12	43Y	T9@	md&	Ps6	QN2	xY&	Bb5	KE%	tp2	Pt@	dS7	54H	XP2
13	dF&	Ws8	jJ3	#yS	uU4	Sy%	G77	Pv@	07#	zT&	22X	A4\$	LL3
14	xP5	2@D	rR8	Zu0	vB%	wW#	KF3	gg@	ts!	mN6	DR0	XE7	\$5t
15	Lg8	YB6	47B	WN9	eV6	87d	vR#	fY9	JJ5	AK8	vE#	uS9	21H
16	Zj9	kk4	N6m	Bg#	rV8	rry	3#B	#@!	ZhY	Pd5	Ex6	yy7	09S

Wachtwoorden een heikel onderwerp.

De matrix wordt als volgt gebruikt:

Gebruik voor de naam van de website of dienst waarvoor een wachtwoord gevraagd word een afkorting van 4 of 5 karakters.

Voorbeeld: GMAIL, koppel een rij aan deze dienst. Lees de codes in de rij bij de letters G, M, A, I en L af. Dit is je nieuwe wachtwoord.

Wachtwoorden een heikel onderwerp.

Voor rij 1 levert dit de volgende code op:

HS1Zt&G2tTt7AB9

Deze karaktercombinatie levert 67^{15} verschillende wachtwoorden op. Dat zijn er meer dan 10000000000000000.

Niet eenvoudig om te kraken.

Wachtwoorden een heikel onderwerp.

De wachtwoorden matrix kun je zelf in Excel of Calc samenstellen.

Druk de matrix af of sla hem op, op een USB stick, maar zorg ervoor dat hij niet op je PC staat.

Maak een apart lijstje waarin staat welke dienst met een bepaald rijnummer correspondeert. Je kunt dan altijd je wachtwoord terug vinden.

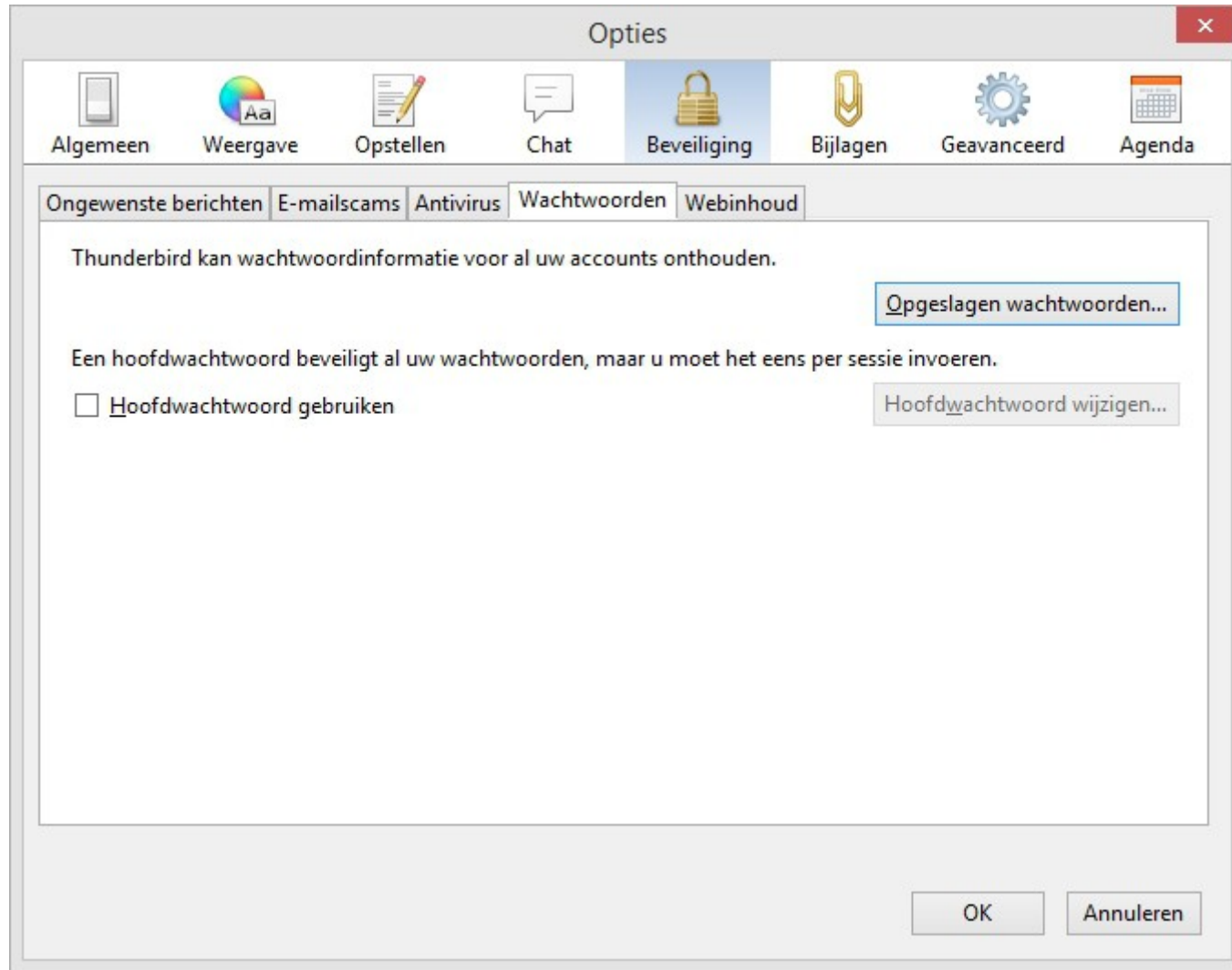
Wachtwoorden een heikel onderwerp.

Tot slot, er valt nog veel meer over de beveiliging van je computer te vertellen.

Belangrijk is zelf attent te zijn op pogingen je gegevens te bemachtigen.

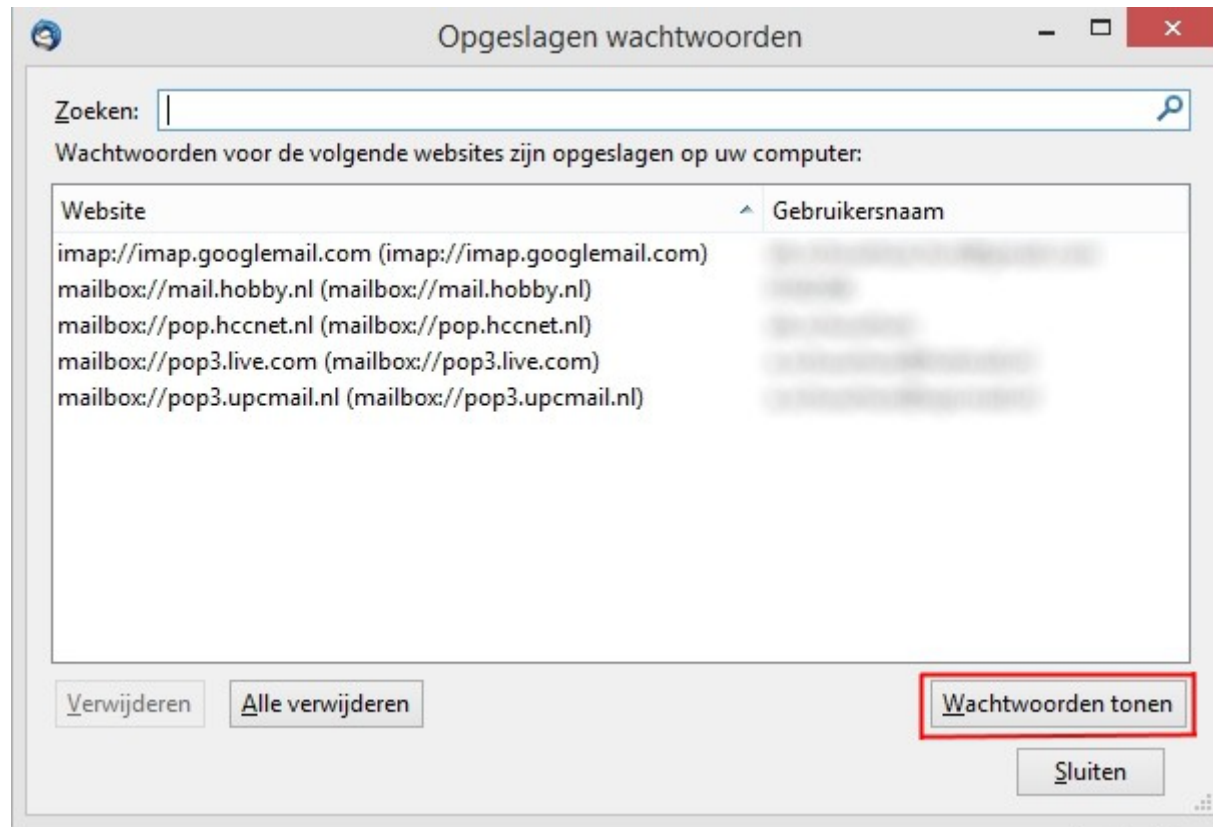
Als een criminele hacker toegang heeft tot je computer is het kwaad geschied, ze weten precies waar ze moeten zijn voor je gegevens.

Wachtwoorden een heikel onderwerp.



Thunderbird e-mail Extra > Beveiliging > Wachtwoorden.

Wachtwoorden een heikel onderwerp.



Klikken op **Wachtwoorden tonen** laat een lijst van wachtwoorden in leesbare tekst zien. Het is niet moeilijk voor te stellen dat een hacker hier wel raad mee weet.

Wachtwoorden een heikel onderwerp.

Twee traps authenticatie.

De beveiliging van je gegevens kan nog verder worden opgevoerd door authenticatie in twee stappen.

Voorbeeld: DigiD met gebruikersnaam en wachtwoord en in stap twee een SMS verificatie code.

Wachtwoorden een heikel onderwerp.

Kenmerk van een goede twee stappen authenticatie is dat er verschillende media gebruikt worden voor de verificatie.

Bij bankieren kennen we al de Random reader
of de TAN codes Transactie Autorisatie Nummer die per
SMS ontvangen worden.

Maar ook authenticatie d.m.v. vingerafdruk, irisscan en
gezichtsherkenning.

Wachtwoorden een heikel onderwerp.

Het al eerder in deze presentatie genoemde Rohos heeft ook een freeware programma dat werkt met gezichtsherkenning.

<http://www.rohos.com/products/rohos-face-logon-free/>

Je computer moet voorzien zijn van een webcam om een aantal foto's van je gezicht te maken en voor de herkenning.

Inloggen doe je door het wachtwoord in te geven en het programma te starten voor de identificatie.

Wachtwoorden een heikel onderwerp.



Wachtwoorden een heikel onderwerp.

Wachtwoorden een heikel onderwerp.
