

De hoeveelheid wachtwoorden in ons leven begint de spuigaten uit te lopen. Steeds hetzelfde wachtwoord gebruiken is niet veilig. In dit artikel vindt u essentiële veiligheidstips en een selectie van de beste wachtwoordmanagers!

Een wachtwoord biedt beveiliging. Maar bent u het kwijt, dan hebt u zélf geen toegang meer tot uw gegevens. De verleiding is dus groot om het aantal verschillende wachtwoorden te beperken en ze zo min mogelijk te wijzigen. Ze zijn dan alleen wel makkelijker te breken. Een betere oplossing is een wachtwoordmanager, die helpt bij het maken en beheren van wachtwoorden. Maar welke managers zijn goed en hoe weet u of uw wachtwoorden wel veilig zijn? De regels in wachtwoordbeveiliging zijn even helder als eenvoudig. Ze staan allemaal in het volgende gedeelte 'Regels in wachtwoordbeveiliging'.



illustratie: SevensHeaven

Orde in wachtwoordchaos

Wachtwoorden maken en bewaren

REGELS IN WACHTWOORDBEVEILIGING

1. Wijzig automatisch gegenereerde en toegewezen wachtwoorden bij het eerste gebruik
Een wachtwoord hoort uniek te zijn, en alleen bekend aan de gebruiker. Krijgt u een wachtwoord toegewezen, dan wijzigt u dit bij het eerste gebruik.

2. Gebruik verschillende wachtwoorden voor al uw accounts
Het is onverstandig voor alle accounts hetzelfde wachtwoord te gebruiken. Raakt het bekend, dan is alle beveiliging verdwenen.

3. Wijzig wachtwoorden minimaal elke paar maanden

Wijzig regelmatig uw wachtwoorden om de kans op inbraak te verkleinen en langdurig misbruik te voorkomen. Slechts een deel van het wachtwoord wijzigen is onvoldoende, zeker als het een volgnummer (zoals de maand of het jaar) betreft.

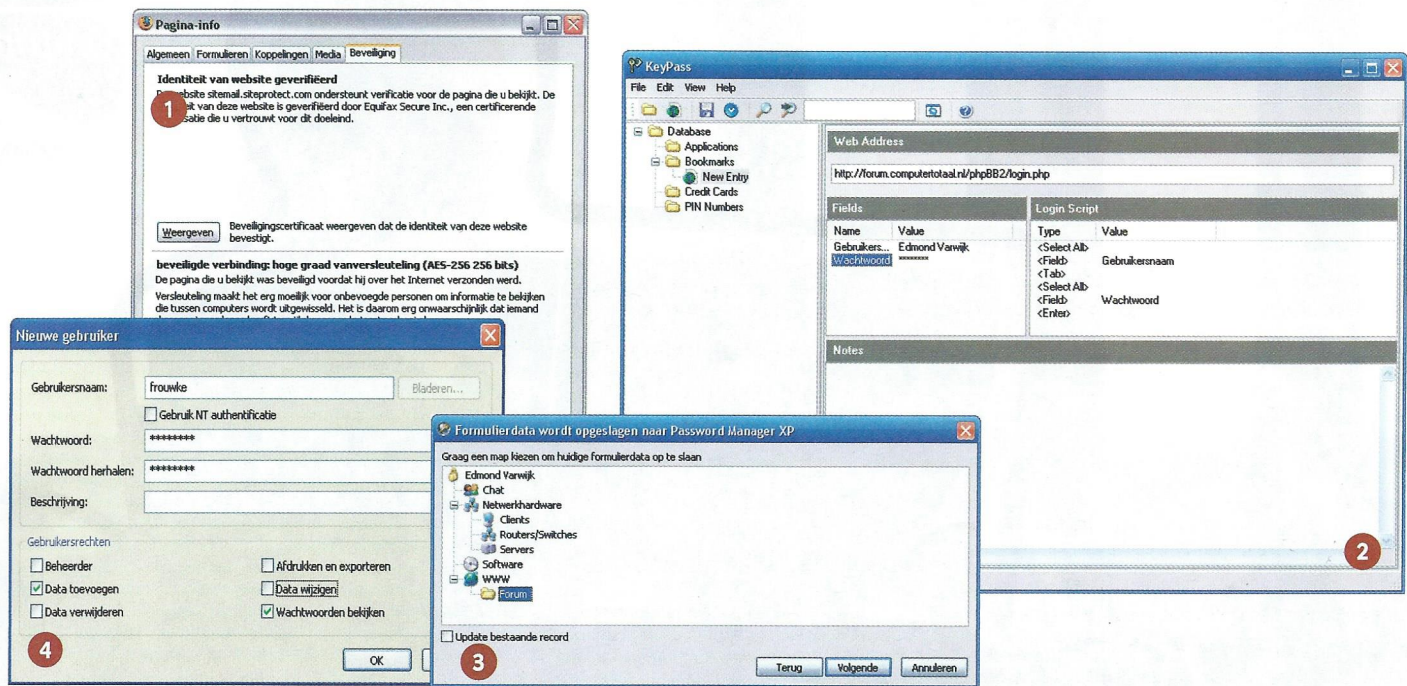
4. Wijzig wachtwoorden na gebruik op publieke computers

Een internetcafé is handig om op vakantie uw e-mail te lezen, maar houd er rekening mee dat u niet weet welke software is geïnstalleerd. Wacht-

woorden zijn met een keylogger of een netwerk-sniffer gemakkelijk te achterhalen.

5. Communiceer veilig

Gebruik wachtwoorden alleen op websites die https gebruiken in plaats van http. Controleer het certificaat en de gebruikte versleuteling via een dubbelklik op het slotje in de statusbalk van de browser (afbeelding 1). En installeer (beveiligings)updates voor uw besturingssysteem en browser, zodat ze op de hoogte zijn van de certificaten die zijn uitgegeven en ingetrokken. Gebruik voor beheer op afstand en verbindingen



over publieke netwerken technieken als SSH en VPN (zie Computer!Totaal februari 2005).

6. Houd wachtwoorden geheim

Veel situaties 'vereisen' dat een wachtwoord aan iemand anders wordt gegeven. Geef hier niet te snel aan toe en wijzig het wachtwoord eerst, zodat u niets verradt over uw andere wachtwoorden. Zet het originele wachtwoord terug zodra het gastgebruik niet meer nodig is.

7. Schrijf wachtwoorden nergens op

Wachtwoorden worden vaak opgeschreven. Een digitale kluis ligt meer voor de hand. Nog beter is het wachtwoorden zo te kiezen dat u ze wel kunt onthouden.

8. Gebruik sterke wachtwoorden

Een wachtwoord mag niet zijn te raden. Namen van kinderen en huisdieren zijn dat wel. Ook mag het wachtwoord niet zijn te kraken met een 'dictionary attack', waarbij gebruik wordt gemaakt van woordenlijsten. Bestaande woorden en begrippen vallen dus eveneens af. Gebruik 'sterke wachtwoorden' die bestaan uit minimaal acht karakters: hoofdletters én kleine letters, cijfers en ook symbolen. Een sterk wachtwoord kan alleen met een 'brute force attack' worden gekraakt, waarbij domweg alle mogelijke combinaties van tekens zijn geprobeerd. Met 26 kleine letters, 26 hoofdletters, 10 cijfers en 32 vreemde tekens op het toetsenbord, in totaal 94 unieke tekens, komt het aantal mogelijk combinaties van 8 tekens op 6095.689.385.410.816. Duurt één kraakpoging een duizendste seconde, dan kost het nog steeds 70.551.960 dagen om zo een wachtwoord met 'brute force' te breken.

WACHTWOORDGEMAK

Overall sterke wachtwoorden gebruiken is niet eenvoudig. U kunt het uzelf wel makkelijker maken zonder de beveiliging te verminderen. Zo is een wachtwoord gemakkelijker te onthouden als het de 'afkorting' van een zin is. Een concreet voorbeeld hiervan is HgV@Dw, dat een afkorting is van 'helemaal gek van al die wachtwoorden', waarbij hoofd- en kleine letters door elkaar gebruikt zijn en letters zijn vervangen door symbolen. Groeien de wachtwoorden u toch boven het hoofd, dan kunt u gebruikmaken van een wachtwoordmanager. Op internet zijn talloze versies beschikbaar en bijna allemaal zijn het programma's die uw wachtwoorden en andere privacygevoelige informatie bewaren in een versleutelde database. Sommige leveren nog aanvullende diensten, zoals het automatisch invullen van webformulieren en wachtwoorden, en de synchronisatie met mobiele apparaten. Computer!Totaal testte voor u dertien wachtwoordmanagers op functionaliteit en bruikbaarheid.

DIGITALE KLUIS

Een wachtwoordmanager is in de eerste plaats een veilige plaats voor gebruikersnamen en wachtwoorden. Uw gegevens horen goed te zijn versleuteld en toch gemakkelijk zijn te gebruiken. Een ingebouwde wachtwoordgenerator is ook handig, mits u geheel op de wachtwoordmanager durft te vertrouwen. Dan is de sterkte van uw wachtwoorden uiteraard ook altijd gegarandeerd. Het enige dat u nog hoeft te onthouden, is het wachtwoord voor de wachtwoordmanager zelf. Opvallend is dat geen van de geteste programma's daar snoeiharde eisen aan stelt. Een enkel programma wil voor de toegang tot de database nog wel het gebruik van een sterk wachtwoord stimuleren, middels een indicatie van de sterkte

van het huidige wachtwoord, maar de meeste doen zelfs dat niet.

WEINIG VERSCHIL

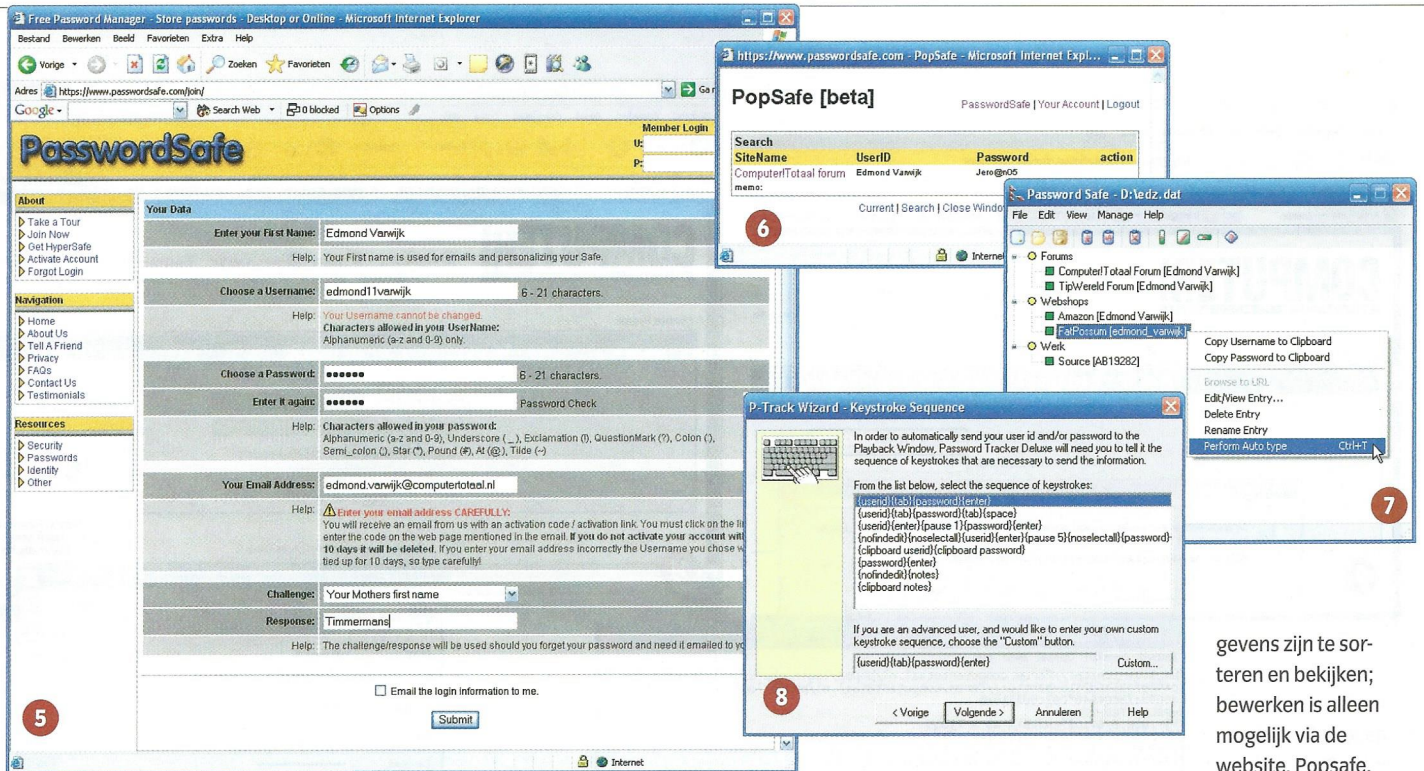
Doordat de noodzakelijke functionaliteit van de wachtwoordmanagers erg beperkt is, lijken de programma's erg veel op elkaar. Zeker programma's die weinig extra's bieden, zoals Password Agent, Access Manager en Keypass (afbeelding 2). Laatstgenoemde biedt nog een Take With Me Wizard, die programma en database op een usb-stick zet, zodat de functionaliteit ook op een andere computer is te gebruiken, maar niet veel meer dan dat. Met sneltoetsen kunt u uw gebruikersnaam en wachtwoord naar een webpagina kopiëren, maar dit gaat wel eens mis en dan verschijnt het (inmiddels niet meer versleutelde) wachtwoord in de adresbalk of het Google-zoekvenster. Niet echt veilig dus. Belangrijk is dat u altijd eerst het goede venster selecteert en de cursor in het juiste lege veld plaatst.

ACCESS MANAGER EN PASSWORD MANAGER XP

Handiger is Access Manager, dat slepen en neerzetten ondersteunt; zo komt u altijd in het goede

FYSIEKE BEVEILIGING

Hoe sterk uw wachtwoord ook is, zonder fysieke beveiliging hebt u er weinig aan. Leg een notebook vast met een ketting en vergrendel de computer als u weggaat. Via Windows-toets+L is het laatste onder Windows XP zo gebeurd. Stel de eigenschappen van de screensaver zo in dat het ontgrendelen een wachtwoord vereist.



gegevens zijn te sorteren en bekijken; bewerken is alleen mogelijk via de website. Popsafe,

venster terecht. Helaas ontbreekt bij dit programma een backupfunctie, wat niet het geval is bij de duurdere Pro-versie, die ook nog bestanden kan versleutelen en veilig van uw systeem kan verwijderen. Ook Password Manager XP is vooral een klassieke kluis waarin inloggegevens in overzichtelijke verzamelingen en mappen worden bewaard (afbeelding 3). Dit programma gebruikt meerdere encryptiemethoden tegelijk en er kunnen extra gebruikersaccounts worden toege-

voegd, met bijvoorbeeld de mogelijkheid om wachtwoorden te mogen bekijken (afbeelding 4).

PASSWORDSAFE.COM

Passwordsafe.com is een digitale kluis op internet waarin u wachtwoorden en andersoortige gegevens kunt bewaren (afbeelding 5). Twee Windows-tooltjes vergemakkelijken het gebruik van Passwordsafe.com. Hypersafe is een programma voor Windows of Mac OS, waarmee accountge-

het andere programma, toont de inloggegevens in een apart browservenster, zodra u een bekende webpagina opent (afbeelding 6). Hoewel Passwordsafe.com niet tegenvalt, krijgt deze site onze wachtwoorden in ieder geval niet. Daarvoor is toch te veel onbekend over deze dienst en wat er met de inloggegevens gebeurt.

PASSWORD SAFE, PASSWORD TRACKER EN SCARABAY

Password Safe (geen relatie met Passwordsafe.com) is de minst uitgebreide van twee opensource

WACHTWOORDMANAGERS

Naam	Website	Omvang	Prijs	Proef-versie	Taal	OS*	Functies **	Encryptie ***	Browser-integratie****	Score
KeePass 0.99b	keepass.sf.net	711kB	Gratis	N.v.t.	NL/EN	W/PPC(3)	A; O; U	A; T	Nee	8
Norton Password Manager 2004	www.symantec.nl	1 cd	€ 35,90	30 dagen (4)	NL	W	A; B; W	Onbekend	Ja	8
RoboForm Portable 6.3.3	www.roboform.com	1,8MB	€ 35,98	Max. 10 accounts	NL/EN	W	A; B; O; U; W	D/3D	Werkbalk IE/M/N/F	8
Scarabay 2.6	www.alnichas.info	828kB	Gratis	N.v.t.	EN	W	A; B; U	Onbekend	Nee	7
Access Manager Pro 2.0.55	www.accessmanager.co.uk	1,7MB	€ 15,95	Max. 10 accounts	EN	W	A; B; O; U; W	B; R	Nee	7
Password Tracker Deluxe 3.63	www.clrpc.com	486kB	€ 14,72	30 dagen	EN	W	A; B; O	RSA	Nee	7
RoboForm 6.3.3	www.roboform.com	1,8MB	€ 24,25	Max. 10 accounts	NL/EN	W/P/PPC	A; B; O; W	D/3D	Werkbalk IE/M/N/F	7
Password Safe 2.09	passwordsafe.sf.net	386kB	Gratis	N.v.t.	EN	W/PPC(1)/L(2)	A; B; O	B	Nee	7
Password Manager XP 2.0	www.cp-lab.com	636kB	€ 24,35	30 dagen	NL/EN	W	A; B; O; U	B; C; 3D; R; RC4; S; T; Tea	Knop in IE	6
Access Manager 2.0.55	www.accessmanager.co.uk	1,7MB	Gratis	N.v.t.	EN	W	A; O; U; W	B; R	Nee	6
Keypass 3.6.5	www.dobysoft.com	2,13MB	\$ 29,95	Max. 10 accounts	EN	W	A; B; O; U	B	Nee	6
Password Agent 2.3.2	www.moonsoftware.com	1,3MB	\$ 24,95	Max. 25 accounts	EN	W	A; B; O; U	A	Nee	6
PasswordSafe	www.passwordsafe.com	N.v.t.	Gratis	N.v.t.	EN	W/L/M/P/PPC/S	B; O	Onbekend	Nee	6

Alle geteste wachtwoordbeheerders gebruiken encryptie om de wachtwoorden en andere gegevens op te slaan. Ook bevatten ze allemaal een wachtwoordgenerator.

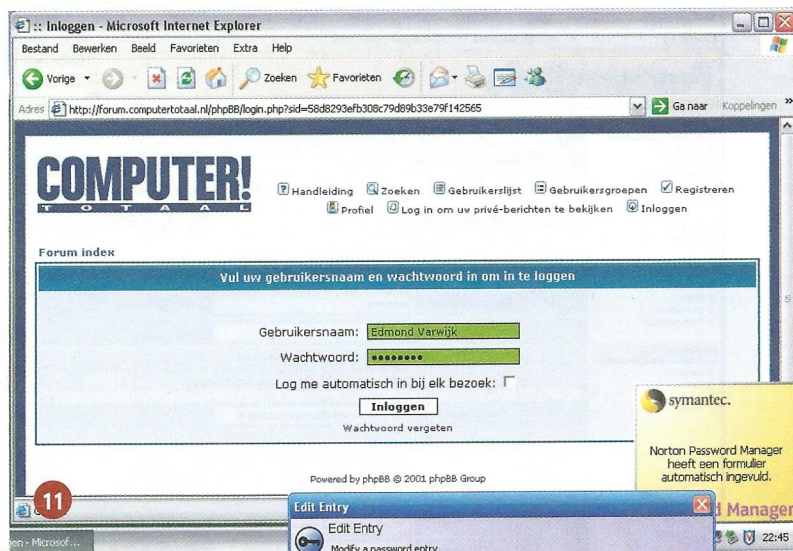
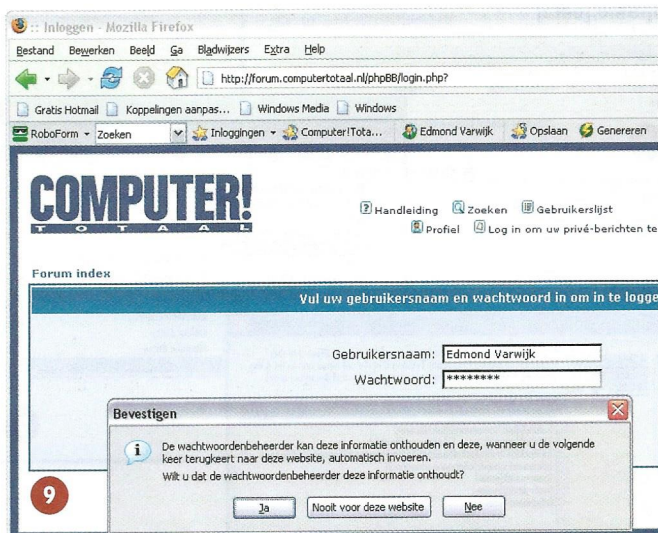
* Besturingssysteem: W = Windows; L = Linux; M = Mac OS; P = Palm OS; PPC = PocketPC; S = Symbian

** Functies: A = Automatisch invullen; B = Backup/restore-wizard; O = Bewaart overige data; U = Opslag USB-stick; W = Webformulieren invullen

*** Encryptie: A = AES (Rijndael); B = Blowfish; C = Cast128; D/3D = DES/3DES; R = Rijndael; RC4 = RC4; RSA = RSA; S = Serpent; T = Twofish; Tea = Tea

**** IE = Internet Explorer, M = Mozilla, N = Netscape, F = Firefox

(1) oudere versie; (2) afgeleid programma gebruikt dezelfde database; (3) via <http://doncho.net/kppc/index.php>; (4) Engelstalige versie via www.symantec.com



wachtwoordmanagers. De andere is KeePass, dat verderop aan bod komt. Password Safe biedt nog wel sneltoetscombinaties om het

inlogscherf te vullen, en ook AutoTyp, dat dit automatisch doet (afbeelding 7). Van Password Safe bestaat nog een oudere versie die compatibel met PocketPC is, en u kunt ook kiezen uit afgeleide programma's die onder Linux dezelfde database gebruiken. Handig in het gebruik zijn Password Tracker de Luxe en Scarabay. Password Tracker de Luxe biedt een handige wizard die helpt de juiste informatie te verzamelen en op de juiste wijze in het inlogscherf te plaatsen (afbeelding 8). Bij het laatste aspect krijgt u nog een aanwijzing voor het kiezen van het juiste veld. Functionaliteit voor gebruik vanaf een usb-stick, ontbreekt helaas. Deze mogelijkheid hebt u weer wel bij Scarabay. Scarabay is geschikt voor een veelvoud van gebruikers en heeft ook een backupfunctie. Wachtwoorden en accountinformatie kunnen met slepen en neerzetten worden gekopieerd. Met veelsoortige informatie voor uitgebreide webformulieren heeft Scarabay weer weinig op, net als de andere eenvoudige wachtwoordmanagers.

ROBOFORM

RoboForm biedt 'Passcards' voor wachtwoorden van websites, 'Identiteiten' om webformulieren in te vullen met persoonlijke gegevens, en 'Safeness' voor overige gegevens. Daaromheen is een woud aan functies gebouwd, wat het gebruiksgemak niet ten goede komt. RoboForm bestaat uit een aantal losse Windows-applicaties, maar de gebruiker zal vooral het snelmenu van de RoboForm-icoon gebruiken, en de RoboForm-werkbalk in de browser (afbeelding 9). Voor PocketPC en Palm zijn aparte versies beschikbaar, en er is

nog een versie die vanaf een usb-stick kan worden gebruikt. Laatstgenoemde is duurder, maar heeft als voordeel dat u RoboForm op elke computer kunt gebruiken; de standaardversie van RoboForm is namelijk beperkt tot één gebruiker en één computer. Opvallend is dat RoboForm niet alle informatie versleutelt. Url's zijn met Notepad nog gewoon te lezen (afbeelding 10).

Norton Password Manager 2004 Norton koppelt wachtwoorden en gebruikersnamen aan profielen, minimaal één per gebruiker. Het verzamelen van informatie (afbeelding 11) en het invullen van de gegevens (afbeelding 12) gaat bijna automatisch doordat Norton vooral goed oplet wanneer u inloggegevens invoert en ze dan direct ook bewaart. Aan deze gebruiksvriendelijkheid dankt Norton zijn hoge notering. Het is een aanrader voor iedereen die vooral geholpen wil worden in het gebruik van wachtwoorden op internet en die niet verlegen zit om een wachtwoordgenerator, draagbaar gebruik vanaf een usb-stick of de mogelijkheid eenmaal ingevoerde wachtwoorden te bekijken.

KEEPASS PASSWORD SAFE

KeePass steekt goed in elkaar. Het is gratis, ondersteunt gebruik vanaf een usb-stick, kopieert wachtwoorden en gebruikersnamen naar websites met sneltoetscombinaties en AutoTyp, heeft een generator voor sterke wachtwoorden en is



in het Nederlands beschikbaar. Bovendien biedt KeePass leuke extra's zoals de mogelijkheid documenten op te nemen in de database (afbeelding 13), die daardoor wel flink kan groeien. Verder biedt het programma expliciete ondersteuning voor gebruik van TAN's, eenmalig te gebruiken codes die vooral door banken nog worden gebruikt. Toch is KeePass niet perfect. Ook hier is het oppassen waar AutoTyp zijn informatie neerzet en is het bijvoorbeeld niet mogelijk vanuit KeePass een telnet te starten.

CONCLUSIE

De verschillen tussen de geteste programma's zijn klein. RoboForm en Norton bieden tegen een hoge prijs ook veel functionaliteit bij formulieren. Norton is daarbij het gebruiksvriendelijkst. Maar de winnaar is KeePass, dat iets meer een echte datakluis is, enkele handige extra's biedt, en tegelijkertijd ook gratis is te gebruiken.

EERDER VERSCHENEN

In onze online shop op ComputerTotaal.nl vindt u de volgende gerelateerde artikelen:
MEER PRIVACY MET PGP
(Computer!Totaal 2, februari 2004)