



## **FPS, wachtwoord & veiligheid**

### **1. Inleiding**

FPS (Fronter, Planning & Scores) wordt door medewerkers van ROC Eindhoven in toenemende mate gebruikt. Naarmate er steeds meer gegevens m.b.t. de student hierin worden opgenomen is het van belang dat deze beschermd worden. Een middel om het systeem te beschermen tegen onbevoegden is het gebruik van een goed wachtwoord. Aan welke criteria een goed wachtwoord moet voldoen en op welke wijze deze bewaard kan worden, wordt uitgelegd in dit schrijven.

Het moge duidelijk zijn dat de beveiliging van een systeem staat of valt bij de wijze waarop de gebruiker hiermee omgaat.

### **2. Websites**

<http://www.waarschuwingsdienst.nl> is een gratis dienst van de Nederlandse overheid. De site is een bron van informatie over veilig internetten en geeft voorlichting en adviezen over computerbeveiliging. Daarnaast waarschuwt deze dienst tegen computervirussen, wormen en beveiligingslekken in software.

Op deze site staan een aantal goede filmpjes over o.a. het omgaan met wachtwoorden, het plaatsen van persoonlijke informatie op het internet, en het onderstaande filmpje over de gevaren van wormen, virussen etc.

### **3. Keepass**

Een handig hulpmiddel is het programma Keepass. Dit is een gratis programma dat je ook Nederlandstalig kunt gebruiken waarin je al je wachtwoorden kunt bewaren. Je hoeft dan nog maar één wachtwoord te onthouden, nl. dat om Keepass te kunnen openen. Bovendien helpt Keepass je om slimme en veilige wachtwoorden te maken. Met Keepass op je USB-stick heb je je wachtwoorden altijd bij de hand. Via de url <http://keepass.info>

### **4. Document beveiligen met wachtwoord in Word**

In Word is het mogelijk om een document aan te maken en vervolgens op te slaan met behulp van een wachtwoord. Om een beveiligd document te kunnen lezen c.q. te bewerken heeft men het wachtwoord nodig.

Hoe je een beveiligd document kunt aanmaken wordt hieronder uitgelegd.

### **5. Een veilig wachtwoord in 5 stappen**

1. Zorg dat uw wachtwoord langer is dan acht tekens. Hoe langer een wachtwoord is des te moeilijker is het te raden. Een lang 'makkelijk' wachtwoord lijkt zelfs beter te zijn dan een kort moeilijk wachtwoord (zie [Wachtwoord wedstrijd bewijst lang is beter theorie](#)).
2. Combineer hoofd- en kleine letters, cijfers en symbolen. Maar kies geen opeenvolgende reeksen zoals '98765432' of '2222222' of bijvoorbeeld lettercombinaties van toetsen die naast elkaar op het toetsenbord staan zoals 'qwerty' of '!@#%\$'.

<b>Hoofd-, kleine letters, cijfers en symbolen</b>
<b>Kleine letters</b>
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
<b>Hoofdletters</b>
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
<b>Cijfers</b>
0 1 2 3 4 5 6 7 8 9
<b>Symbolen</b>
! " # \$ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` {   } ~

3. Bedenk een makkelijk te onthouden zin met minstens één getal en één leesteken (symbool). Bijvoorbeeld: 'Ik hou honderd keer meer van Simon dan van Arnold.' Neem van elk woord daarna de eerste letter en verander de getallen en leestekens. Het veilige wachtwoord luidt dan: lh100kmvSdvA.
4. Wil je het echt goed doen, vervang dan nog enkele tekens door andere tekens die erop lijken. In bovenstaand voorbeeld verving ik de hoofdletter "I" door een "1", de letter "k" (van "keer") door de hoofdletter "X", de "S" door een dollarteken en de hoofdletter "A" door een apenstaartje. Het wachtwoord is dan vrijwel onherkenbaar voor anderen, maar niet voor u en ziet er als volgt uit: 1h100Xmv\$dv@.

<b>Vervang tekens</b>	
<b>Vervang letter ...</b>	<b>door ander teken...</b>
a	@
b	6
c	(
e	&
i	1
j	]
l	!
n	^
o	0
q	9
s	\$
x	*
z	2

5. Verander uw wachtwoorden regelmatig, bijvoorbeeld elke maand.

#### **6. Controleer je wachtwoord**

Via onderstaande link kun je je wachtwoord laten testen:

[http://www.microsoft.com/netherlands/thuisgebruikers/beveiliging/privacy/password\\_checker.aspx](http://www.microsoft.com/netherlands/thuisgebruikers/beveiliging/privacy/password_checker.aspx)