

## **Belang en noodzaak van een goed beheer van het paswoord.**

Elke PC-gebruiker wordt bij het OCMW geïdentificeerd aan de hand van 2 elementen:

1. zijn UID (gebruikersidentificatie), met andere woorden zijn gebruikersnaam;
2. zijn paswoord.

De UID (bijvoorbeeld: jdupont of jvandersteen) wordt bepaald door de systeembeheerder van de informaticadienst om gemakkelijker de toegang van de verschillende gebruikers te beheren.



### **A. Enkele regels inzake de beveiliging van het paswoord:**

- ✓ het paswoord is **strikt persoonlijk**: geef het aan niemand;
- ✓ een paswoord is **uniek voor één bepaald toestel**, gebruik het geen 2 keer. Gebruik het paswoord ook niet opnieuw, maar vernieuw het.
- ✓ een paswoord moet **regelmatig vernieuwd** worden, ten laatste om de drie maanden;
- ✓ het is ideaal om een paswoord te hebben dat **moeilijk te achterhalen is maar wel gemakkelijk te onthouden is** (zie de tips op het einde van de nota);
- ✓ Schrijf uw paswoord nergens op, noch op uw onderlegger of op een Post-it Note dat op uw PC is gekleefd, noch in een elektronisch bestand;
- ✓ Wanneer u on-line bent, vink dan de optie niet aan waarmee uw naam en paswoord worden onthouden (in Internet Explorer, ga naar Tools,

Options, Content, Auto complete, verwijder het vinkje bij User names... en Complete passwords);

- ✓ Gebruik ook geen programma's die worden aangeboden en die u de mogelijkheid bieden om uw paswoord op eender welk moment te herinneren want zulke programma's zijn vaak besturingssoftware die van buitenaf zelf gebruikt kunnen worden om uw paswoord te achterhalen;

NB : het is niet toegelaten om externe programma's zoals Messenger te installeren die aan personen met slechte bedoelingen de mogelijkheid bieden om het paswoord te ontcijferen en alzo van op afstand uw PC binnen te dringen;

Laat dus uw interne en externe toegang niet door een programma noch door een andere persoon dan de systeembeheerder beheren. Indien u twijfelt over de aanwezigheid van een dergelijk programma, aarzel dan niet om contact op te nemen met de informaticadienst.

#### **B. Het regelmatig veranderen van uw paswoord is belangrijk want:**

- Een discrete piraat zou genoeg hebben met het observeren van uw persoonlijke informatie zonder hierbij sporen achter te laten, maar doordat u uw paswoord verandert, zal hij niet meer kunnen binnendringen.

Hier volgen enkele paswoorden die u best niet gebruikt:

- uw **telefoonnummer** ;
- uw naam of voornaam ;
- uw nummerplaat;
- uw socialezekerheidsnummer;
- uw **bijnaam**, zelfs al is die persoonlijk ;
  
- uw **lengte, schoenmaat, gewicht**;
- de naam van uw vriend(in) of van uw echtgeno(o)t(e);
- de naam van uw huisdier: hond, vis, hyena,...

of eender welke combinatie van deze woorden, zelfs in willekeurige volgorde.

### C. Een paswoord komt ook niet voor in:

- **Woordenboeken** (vooral de elektronische zoals technische of spellingwoordenboeken);
- **Tijdschriften;**
- een **boek** over geestige gezegdes;
- een voornamenboek;
- een **bestand** of een **informaticalisting**

### D. Welk paswoord kiezen?

Een paswoord moet per definitie bestaan uit:

- minstens 8 symbolen,
- cijfers, letters of karakters zoals: +, -, ...

Opgelet : het is beter om accenten te vermijden zoals: é, è, ë, ê, enz.



#### **Enkele tips.**

De titel van een film of van een boek.

Bijvoorbeeld : **S**neeuw**w**itje en **d**e **z**even **d**wer**g**en - **A**lice **a**u **p**ays **d**es **m**erveilles.

Door de eerste letter te nemen van elk woord uit de titel bekomt u het volgende paswoord : sedzd- aapdm. Aangezien dit paswoord echter te gemakkelijk te achterhalen is door een piraat en het om de drie maanden veranderd moet worden, kan u een cijfer of een cijferreeks toevoegen. Bijvoorbeeld: sedzd0803 (maand en jaar) – aapdm0803, sedzd3803-aapdm3803 (week en jaar).

U kan natuurlijk het paswoord ingewikkelder maken door de tweede letter of de twee eerste letters van elk woord te nemen.

### Scramblen

Het is ook mogelijk om op een andere, eenvoudiger manier te werk te gaan. U kiest de naam van een film of van een boek, neemt de eerste letter van elk woord en voegt hieraan het aantal letters van elk woord toe. Bijvoorbeeld : Als een jonge hond van Hugo Claus of Voyage autour de ma chambre van Xavier de Maistre geven de volgende paswoorden: a3e3j5h4 – v6a6d2m2c7. Een andere mogelijkheid is aejh3354 of vadmc66227.

Vermijd echter paswoorden met een betekenis aangezien piraten ook vaak een beroep doen op software die gebruik maakt van woordenboeken.

### Associëren

Het associëren van woorden kan eveneens gebruikt worden om een paswoord te vormen, maar het is van belang dat u dan het paswoord moeilijker maakt.

Bijvoorbeeld: lavitaebella zal aangevuld moeten worden met tekens: la+vita-e/bella\*, paswoord waaraan cijfers zullen moeten worden toegevoegd.

Hierbij valt op te merken dat dit paswoord niet volledig betrouwbaar is.

### Vereenvoudigen

Deze techniek bestaat erin alle letters die dubbel zijn in een woord weg te laten. Bijvoorbeeld: “vergelijken” wordt “vergelijk”, waaraan cijfers worden toegevoegd ; “serveur” wordt “servu”, waaraan de volgende cijfers kunnen worden toegevoegd: het aantal letters van het woord “serveur”, het aantal letters van het paswoord en het jaar: servu7503.

### **Besluit.**

Het is aan u om de combinatie te vinden die volgens u gemakkelijk te onthouden is, maar vergeet niet dat geen enkel paswoord onschendbaar is. Indien u deze tips gebruikt, dan zullen piraten er nog langer over doen om een paswoord te kraken.