

## Beveiligingstips voor je laptop

### Paswoord Policy

Om je gegevens ze veilig mogelijk te bewaren zijn er enkele tips:

#### *Verander regelmatig je wachtwoord*

Dit doe je door na het aanmelden op ctrl-alt-del te drukken en dan te kiezen voor Wachtwoord wijzigen... vul eerst je huidig wachtwoord in en vervolgens het nieuwe en bevestig dit nogmaals.

OPGELET:

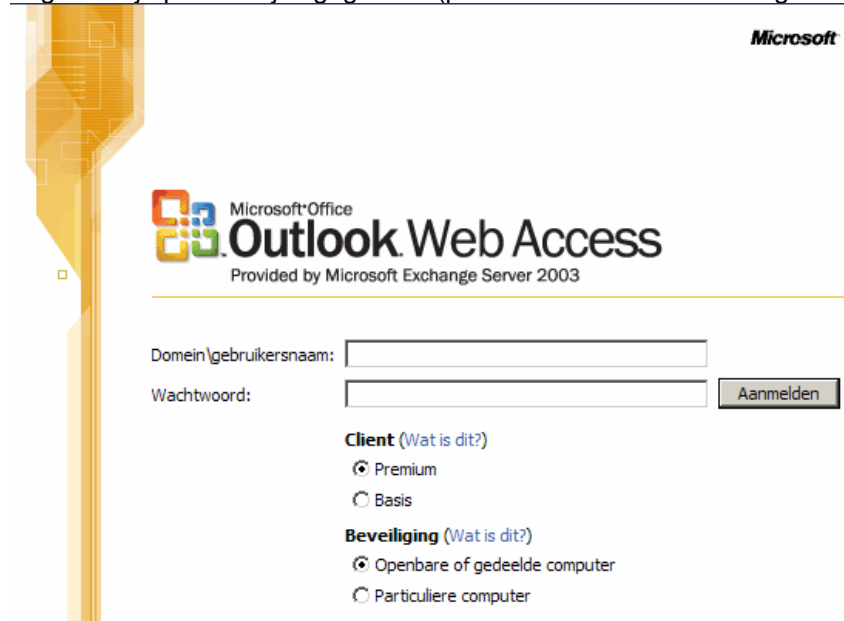
Als je met je personeelsnummer aanmeldt op het domein student voer je dit uit op het moment dat je op het netwerk van school geconnecteerd bent!

Denk er wel aan dat je paswoordwijziging voor alle toepassingen van de PHL geldt (BB, EP, email, enz)

#### *Je wachtwoord wijzigen via de Outlook Web Access*

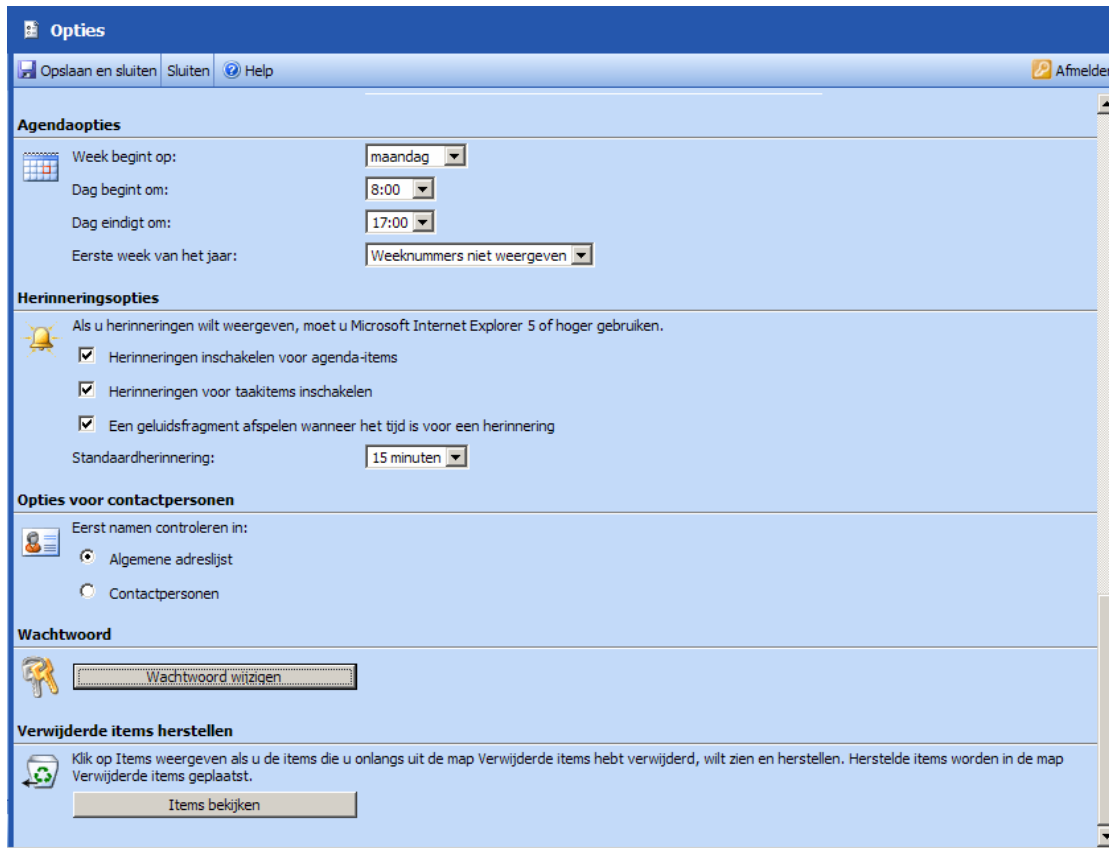
Ga naar de site <http://mail.phl.be>

Log in met je persoonlijke gegevens (personeelsnummer en huidig wachtwoord)



Kies linksonder in het scherm voor de opties van outlook.

De optielijst zal verschijnen en onderaan vind je de functie wachtwoord wijzigen terug



Volgend venster verschijnt

Vul bij domein STUDENT in  
Account = personeelsnummer

Geef je oud paswoord in en geef 2x  
het nieuwe paswoord op dat je wil  
gebruiken.

**OPGELET:**

Als je het wachtwoord via de *Outlook Web Access* wijzigt zal je paswoord voor alle toepassingen onmiddellijk ingaan, dus Blackboard, epos enz.

De controle van je paswoord bij aanmelden op je laptop zal echter pas ingaan op het moment dat je binnen de netwerkgeving van de PHL aanmeldt.

Bv: Je wijzigt thuis via de *Outlook Web Access* je paswoord, je herstart je pc en je wil aanmelden met je nieuwe wachtwoord. Dit zal niet lukken omdat je niet aanmeldt op het netwerk van de PHL, je moet in dit geval je oude paswoord nog gebruiken. Je komt op school aan en pas hier moet je aanmelden met je nieuwe paswoord om toegang te krijgen.

Om niet teveel problemen te krijgen raden we dus aan om je paswoord via de ctrl-alt-del methode te wijzigen wanneer je op het netwerk van de PHL zit, zoals eerder uitgelegd.

#### *Kies een wachtwoord dat complex is*

maak een wachtwoord dat bestaat uit hoofdletters gemengd met kleine letters, cijfers en tekens, minimum 8 tekens lang.

(tip gebruik van vreemde tekens zoals spaties, \_ & %µ£§ enz maken het extra veilig)

Vermijdt ten allen tijd een blanco paswoord, paswoorden met je naam of geboortedatum, naam huisdieren enz. Dit zijn immers de eerste paswoorden die men zal proberen bij een inbraak op het systeem.

#### *Noteer nooit je login en/of paswoord met een sticker/post it enz op je laptop*

De schoolagenda is handig maar absoluut niet de plaats om je logingegevens in te bewaren.

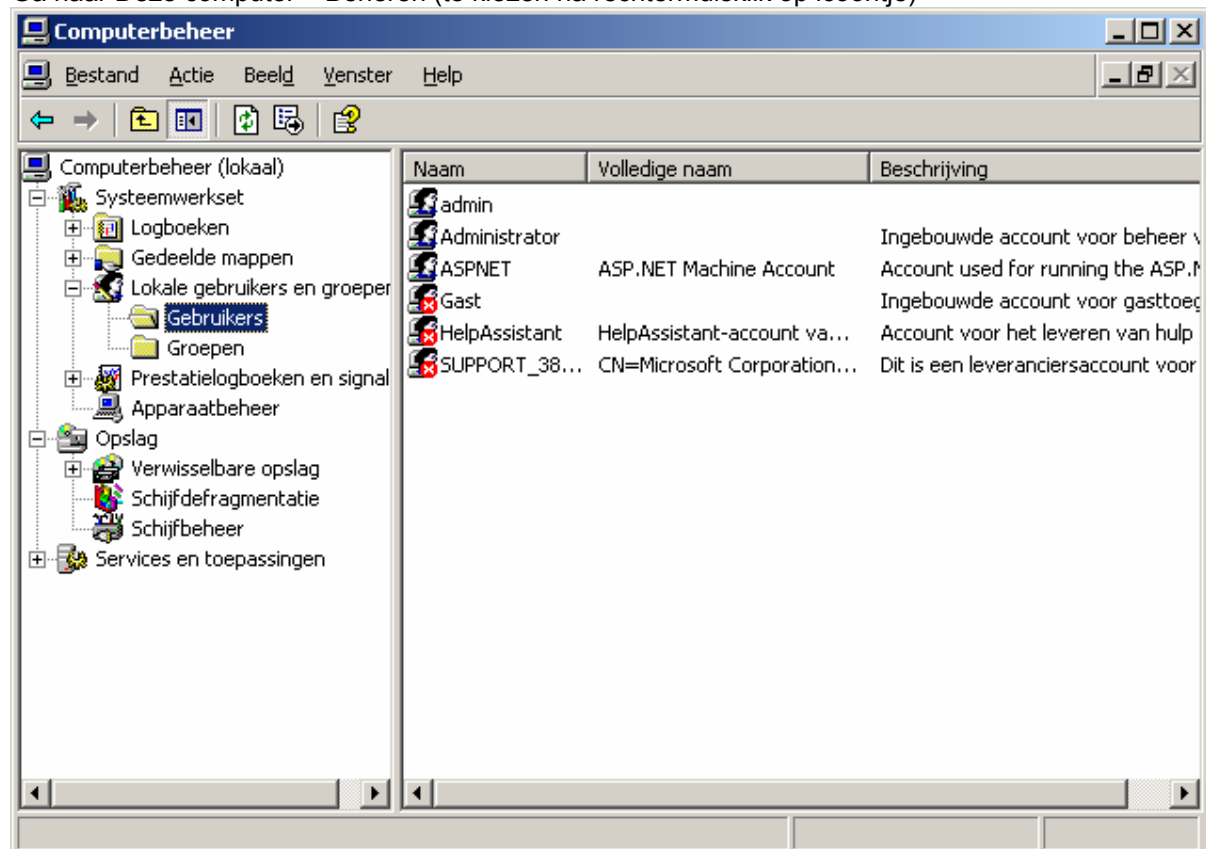
Bewaar ook geen gegevens van login voor de laptop en andere toepassingen op een papier dat bij je laptop zit, ook niet in de laptoptas.

Als je toch je paswoorden wil opschrijven bewaar het papier dan op een veilige plaats thuis

### **Gebruikers uitschakelen en paswoorden van lokale gebruikers wijzigen**

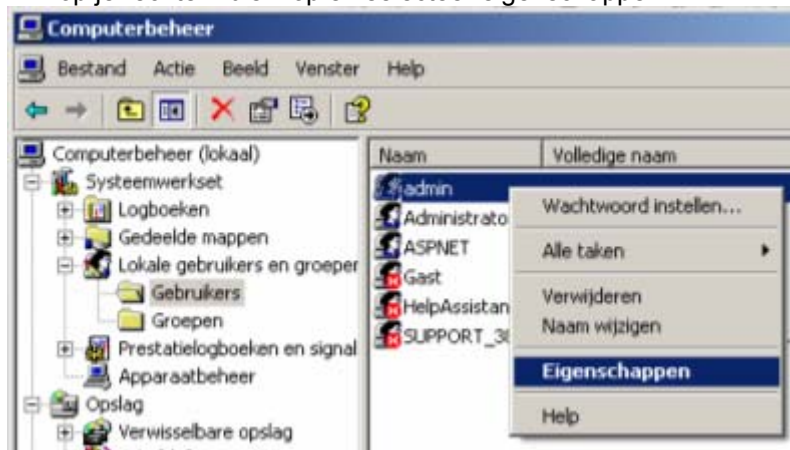
Op je laptop zijn ook lokale users aangemaakt door de laptopdienst of misschien ook door uzelf voor thuisgebruik.

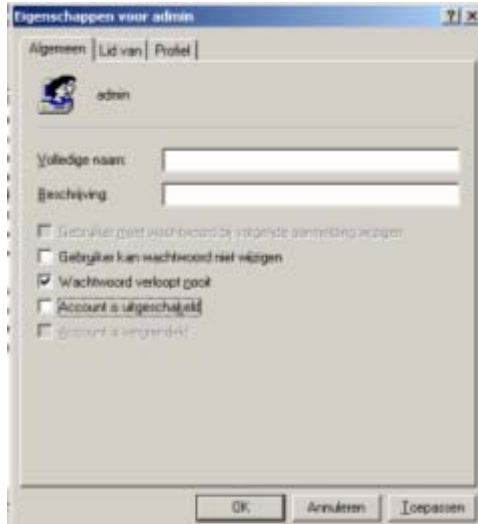
Ga naar Deze computer – Beheren (te kiezen na rechtermuisklik op icoontje)



In de lijst met de lokale gebruikers en groepen kan je zien wie er allemaal toegang heeft tot je laptop. Om je computer extra veilig te maken kan je de namen die je hierin vindt best uitschakelen, met uitzondering van de latitude-account, als er geen latitude-account in het lijstje staat laat je best de administrator account actief.

Account uitschakelen, selecteer de account waarvan je de toegang tot de laptop wil ontzeggen.  
Klik op je rechtermuisknop en selecteer eigenschappen



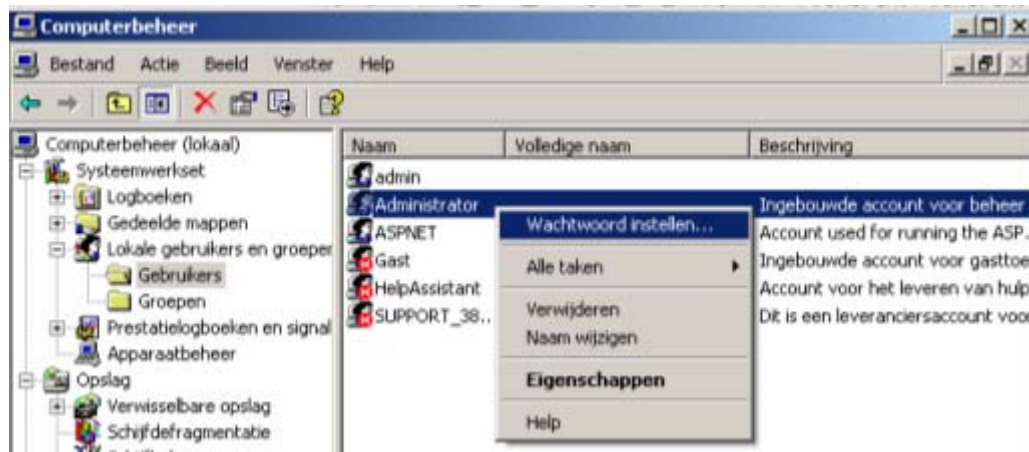


Vink de optie Account is uitgeschakeld aan om ervoor te zorgen dat de user niet meer lokaal kan aanmelden op je laptop

Met lokaal aanmelden bedoelen we aanmelden buiten het domein om. Dus niet op het domein student.

Doe deze stappen voor alle lokale gebruikers **met uitzondering van de latitude (of administrator indien latitude niet bestaat) en ASPNET**

bij twijfel contacteer de IT-dienst voor meer info !!!



De account latitude (administrator indien latitude niet in de lijst staat) schakel je best niet uit, anders kan er bij eventuele problemen met je laptop niet meer aangemeld worden door de mensen van de IT-dienst om support te leveren.

Wat wel raadzaam is om een nieuw paswoord in te stellen (denk er wel aan dat je dit paswoord goed moet onthouden want deze account zal je in principe nooit gebruiken en bij eventuele problemen wel moeten meedelen aan de IT-dienst)

Kies voor de optie Wachtwoord instellen...



Geen nood, aangezien jullie aanmelden met je personeelsnummer op het domein student zal er geen data onbereikbaar worden aangezien je enkel het paswoord van de lokale gebruiker aanpast.

Klik op doorgaan om het paswoord in te stellen



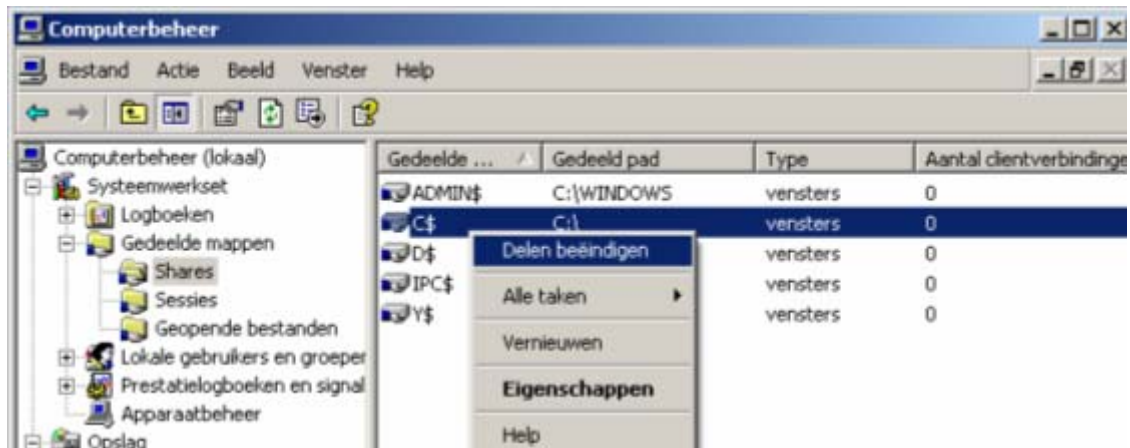
klik op OK om te bevestigen

### Gedeelde mappen uitschakelen (c\$, d\$)

Standaard worden er na een Windows installatie een aantal mappen 'administratief gedeeld' . Dit wil zeggen dat de gegevens van het systeem via deze weg beschikbaar gesteld worden.

Deze gedeelde mappen kunnen er echter voor zorgen dat mensen met minder goede bedoelingen toegang krijgen tot gegevens op je systeem.

Ga opnieuw naar de beheerfunctie van je systeem



In de lijst zie je dat de C: en D: gedeeld worden, schakel deze uit door via de rechtermuisknop te klikken en in de optielijst "Delen beëindigen" te selecteren



Bevestig door op Ja te klikken en doe dit ook voor de D\$

Sommige mensen hebben ook mappen gedeeld voor thuisgebruik, handig om bestanden van je laptop naar een vaste pc of omgekeerd te verplaatsen horen we dan als verklaring.

Denk er echter aan dat je op deze manier andere mensen in veel gevallen vrije toegang verleent tot alle gegevens die in die map zitten. Maw in de schoolomgeving is de kans reëel dat andere gebruikers op het netwerk toegang tot deze map hebben! Uitschakelen is dus de boodschap !

## Bios / opstart paswoord

Er is een mogelijkheid om je laptop nog een stap verder te beveiligen. Dit kan je bereiken door nog voor het opstarten van het besturingsysteem naar een paswoord te laten vragen, het zogenaamde BIOS-paswoord. Zonder dit paswoord zal je systeem niet starten en dus ook geen gegevens van je laptop kunnen verdwijnen.

Het instellen van een BIOS-paswoord heeft wel een paar belangrijke implicaties.

Verliezen van dit wachtwoord kan ertoe leiden dat je systeem niet meer kan opstarten, het is ook niet via 'truckjes' te achterhalen. Bij herstellingen is het soms nodig om instellingen in de BIOS aan te passen, dus bij herstelling steeds het paswoord meedelen.

Persoonlijk ben ik niet echt een voorstander van deze beveiliging maar toch een vermelding waard.

**Voor dit soort ingreep kom je best langs op de laptopdienst, elk systeem is immers anders.**

## Opstartvolgorde

In de BIOS van het systeem kan ingesteld worden wat de opstartvolgorde moet zijn, standaard is deze keuze eerst het cd/dvdstation gevolgd door de harde schijf. Het nadeel van deze opstartvolgorde is dat je via speciale cd's toch het systeem kan laten opstarten en zonder een wachtwoord nodig te hebben de gegevens kan zien. Daarom kan het raadzaam zijn om in de BIOS in te stellen dat altijd van de harde schijf moet opgestart worden. Sommige systemen hebben echter een sneltoets waarmee je manueel toch de opstartvolgorde kan aanpassen...

**Voor dit soort ingreep kom je best langs op de laptopdienst, elk systeem is immers anders.**

## **Activering firewall**

Standaard staat de Windows Firewall niet geactiveerd op de laptops die door de PHL bedield worden, dit omwille van het feit dat we de Firewall van de virusscanner gebruiken. Deze is geavanceerder dan die van Windows en zorgt er ook voor dat vanuit de IT-dienst gecentraliseerd aanpassingen kunnen doorgevoerd worden zonder dat we gebruikers telkens moeten vragen om iets aan te passen.

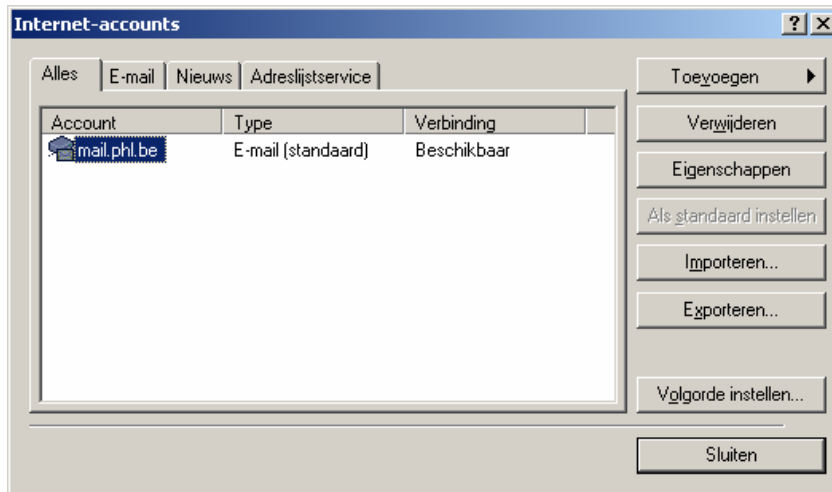
## Configuratie outlook via pop3s / Imaps / smtps (beveiliging tegen pop3 sniffers)

### Outlook Express (Windows XP)

#### POP3

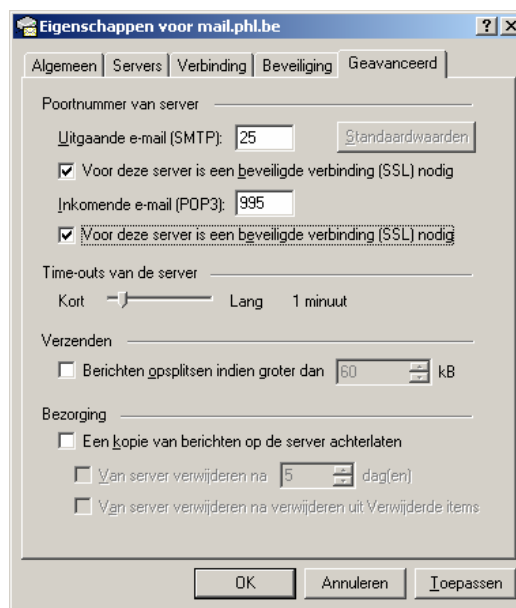
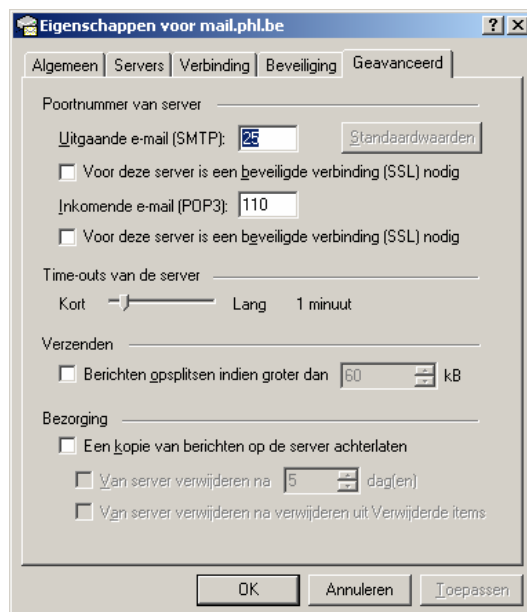
Indien je gebruik maakt van Outlook Express dan kan je best volgende instellingen doen om je mailverkeer te beveiligen tegen diefstal.

Open het programma, ga naar Extra – Accounts



Selecteer je account en kies voor eigenschappen

Ga naar het tabblad geavanceerd en selecteer de SSL beveiligingen, bevestig je keuze.



## IMAP

Voor de beveiliging van een IMAP account ga je eveneens zoals in de vorige stappen naar het tabblad geavanceerd en kies je ook weer voor SSL beveiliging

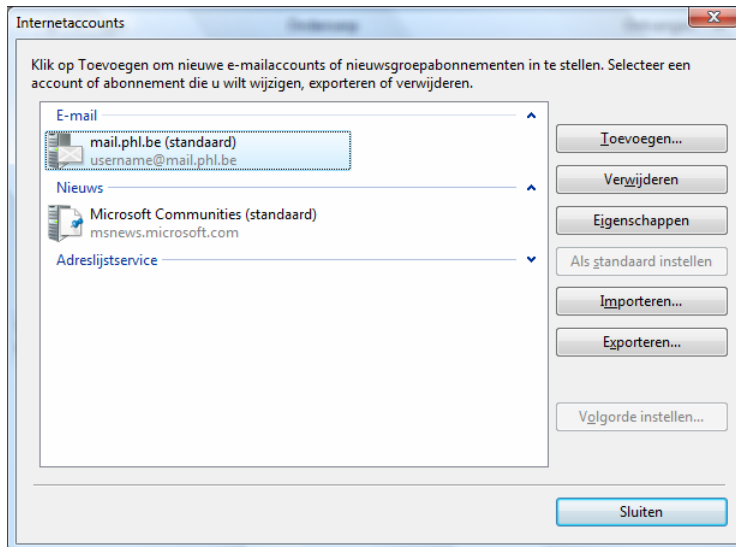


## Windows mail (Windows Vista)

### POP3

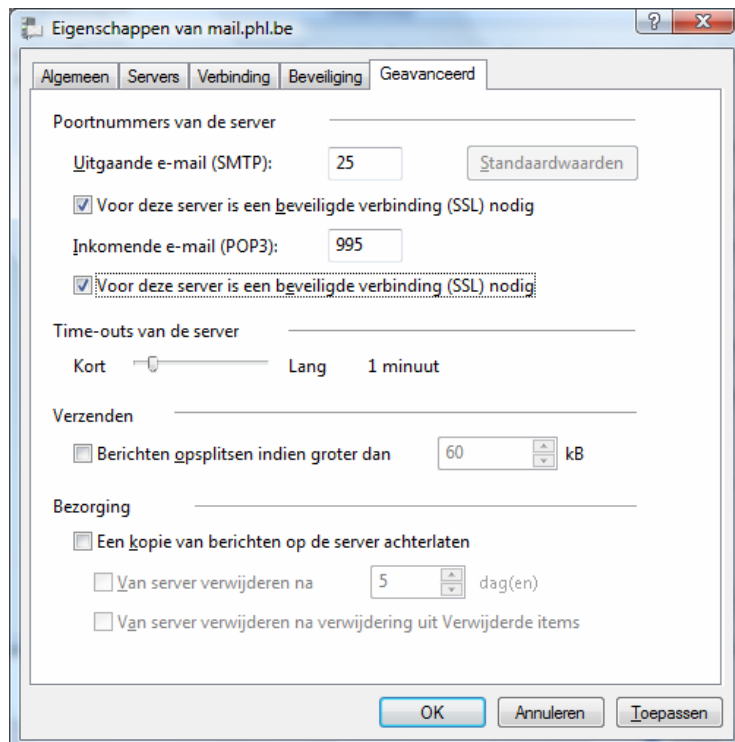
Indien je gebruik maakt van Windows Mail dan kan je best volgende instellingen doen om je mailverkeer te beveiligen tegen diefstal.

Open het programma, ga naar Extra – Internetaccounts



kies voor Eigenschappen

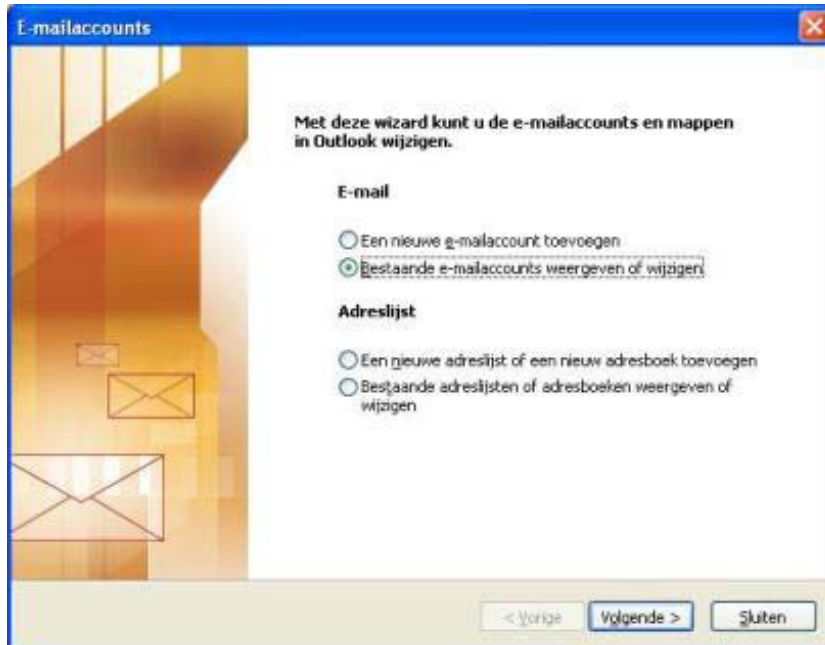
Ga naar het tabblad Geavanceerd en selecteer de SSL beveiligingen, bevestig je keuze.



## Outlook 2003

### POP3

Indien je gebruik maakt van Microsoft Outlook 2003 controleer je best volgende instellingen  
Open outlook – Extra – Accountinstellingen

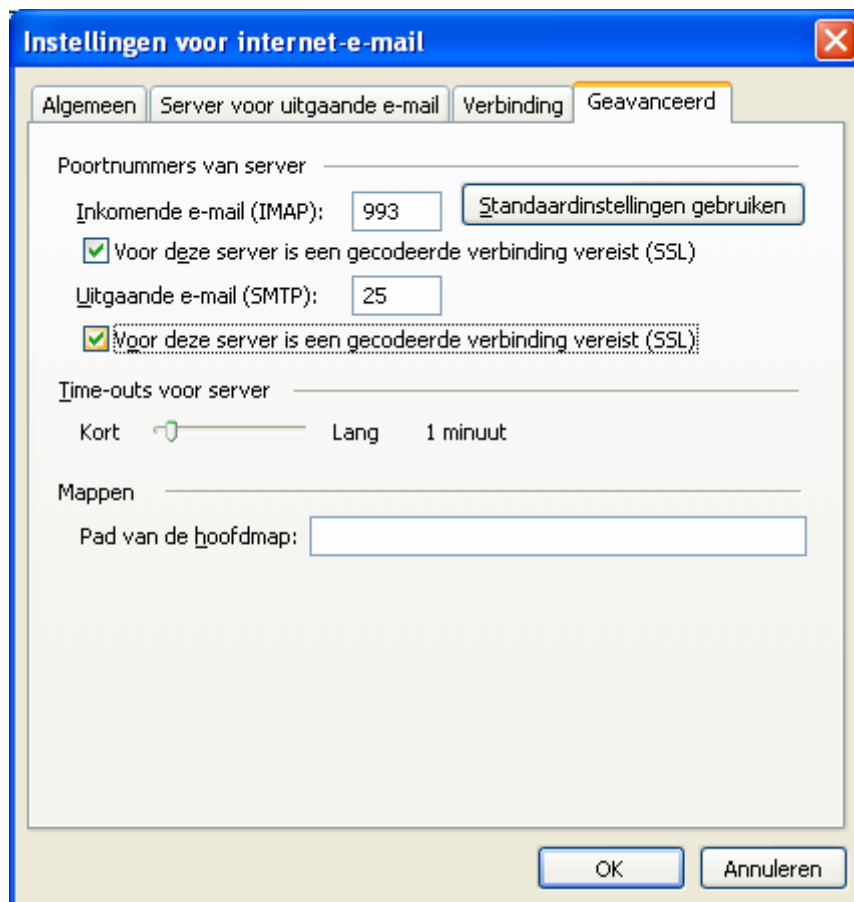


Kies voor Wijzigen en vink in het tabblad Geavanceerd beide SSL opties aan



### IMAP

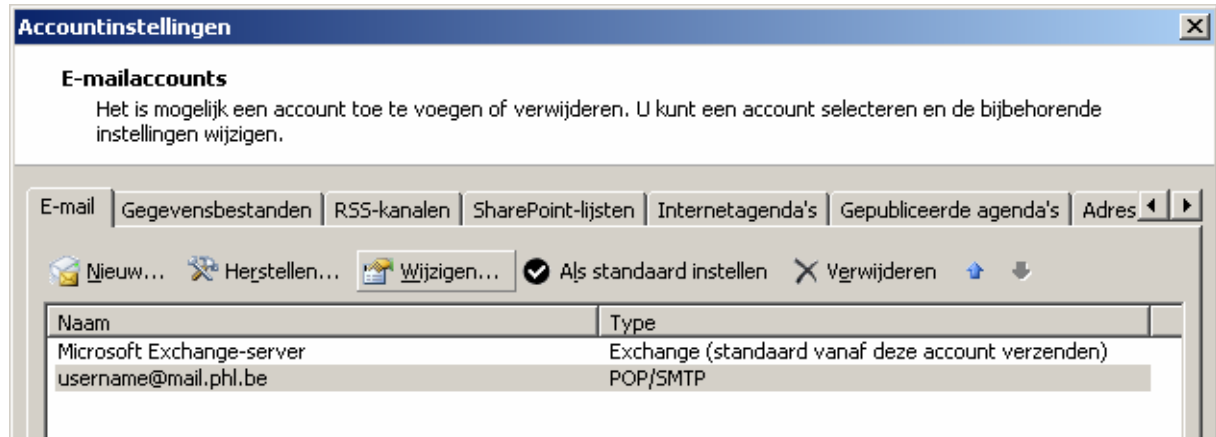
Voor de beveiliging van een IMAP account ga je eveneens zoals in de vorige stappen naar het tabblad geavanceerd en kies je ook weer voor SSL beveiliging



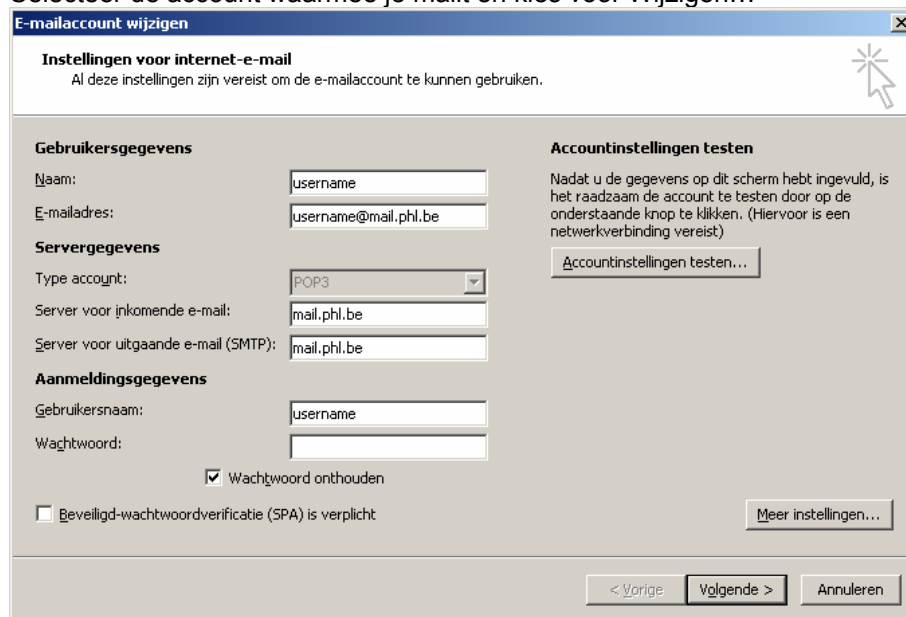
## Outlook 2007

### POP3

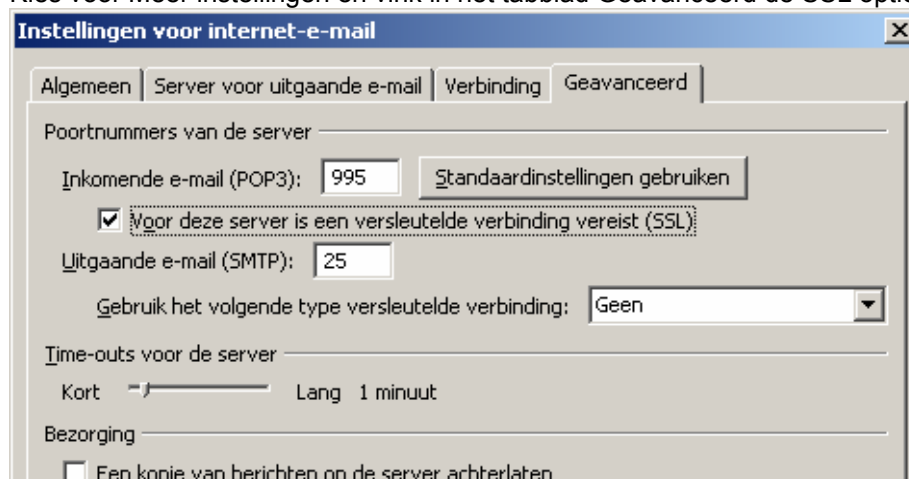
Indien je gebruik maakt van Microsoft Outlook 2007 controleer je best volgende instellingen  
Open outlook – Extra – Accountinstellingen



Selecteer de account waarmee je mailt en kies voor Wijzigen...

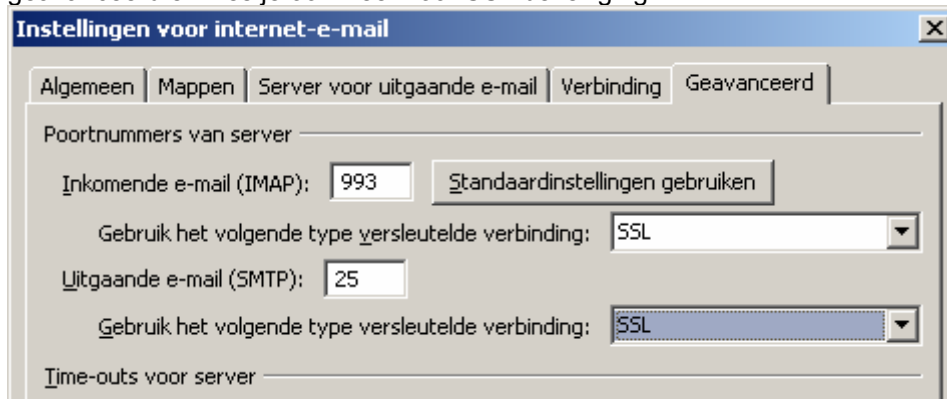


Kies voor Meer instellingen en vink in het tabblad Geavanceerd de SSL optie aan



## IMAP

Voor de beveiliging van een IMAP account ga je eveneens zoals in de vorige stappen naar het tabblad geavanceerd en kies je ook weer voor SSL beveiliging



The image shows a screenshot of the 'Instellingen voor internet-e-mail' (Internet Email Settings) dialog box, specifically the 'Geavanceerd' (Advanced) tab. The dialog has a title bar with a close button (X) and a tabbed interface with the following tabs: 'Algemeen', 'Mappen', 'Server voor uitgaande e-mail', 'Verbinding', and 'Geavanceerd'. The 'Geavanceerd' tab is selected. The settings are as follows:

- Poortnummers van server:**
  - Inkomende e-mail (IMAP): 993 (with a button for 'Standaardinstellingen gebruiken')
  - Gebruik het volgende type versleutelde verbinding: SSL (dropdown menu)
  - Uitgaande e-mail (SMTP): 25
  - Gebruik het volgende type versleutelde verbinding: SSL (dropdown menu)
- Time-outs voor server:** (empty text field)

### **En last but not least...**

Als je je laptop achterlaat, al is het maar voor de spreekwoordelijke 5 seconden, vergrendel je systeem dan altijd !!!

Op die manier kan niemand aan je gegevens zonder je wachtwoord te kennen.

Druk op ctrl-alt-del en kies voor Computer vergrendelen

of

Hou de Windows toets op je toetsenbord ingedrukt en druk daarna op de letter L (Lock)

Als je terug aan je systeem komt moet je enkel je paswoord ingeven en je kan onmiddellijk verder werken waar je gebleven was.

Een nog betere oplossing is je laptop nooit, maar dan ook nooit onbeheerd in een ruimte achterlaten waar studenten zitten of kunnen komen. Voorkomen is immers nog altijd beter dan genezen!