

Mobiel Internet Veiligheidspakket

Gebruikershandleiding Mobiel Internet Veiligheidspakket
voor **Windows Mobile** smartphones

Mobiel IVP Windows Mobile Versie 1.0, d.d. 20-07-2011



Inleiding	3
1 Installatie	4
1.1 Installeren	4
1.2 Activering	4
1.3 Het product starten	5
2 Scannen op virussen	6
2.1 Verwerking geïnfekteerde bestanden	6
3 Ongeautoriseerd netwerkverkeer voorkomen	7
3.1 Een beveiligingsniveau selecteren.....	7
4 Vertrouwelijke gegevens beschermen	8
4.1 Anti-Theft gaan gebruiken	8
4.2 Het toestel op afstand vergrendelen	8
4.3 Uw toestel op afstand wissen	9
4.4 Uw toestel lokaliseren	9
4.5 De SMS-waarschuwing gebruiken.....	9
5 Browserbeveiliging.....	10
5.1 Browserbeveiliging inschakelen:.....	10
6 Het product up-to-date houden	11
6.1 Automatische updates	11
6.2 Handmatige updates.....	11



Inleiding

Met het Mobiel Internet Veiligheidspakket beschermt u uw Windows Mobile smartphone of tablet tegen de bedreigingen van internet. Het Mobiel Internet Veiligheidspakket biedt drie functies: Anti-Theft, Browserbeveiliging en Scannen op Virussen. Het pakket is geschikt voor Windows Mobile versie 5.0 en 6

In deze gebruikershandleiding leest u hoe u het pakket op uw toestel kunt installeren en activeren en krijgt u nadere uitleg over de verschillende mogelijkheden van het pakket. Tot slot vindt u informatie over het up-to-date houden van het Mobiel Internet Veiligheidspakket, zodat u zeker weet dat u altijd beschikt over de meest actuele bescherming.

<p>LET OP: Het Mobiel Internet Veiligheidspakket beschermt uw toestel pas als het geactiveerd is!</p>
--

1 Installatie

Volg de onderstaande instructies voor het installeren en activeren van het Mobiel Internet Veiligheidspakket op uw toestel.

1.1 Installeren

Download het installatiebestand naar uw toestel.

- Open hiervoor de internet browser op uw smartphone of tablet en suft naar: www.kpn.com/downloadmobielivp

- **Of** scan deze QR code met uw mobiele telefoon



Nadat u het product geïnstalleerd heeft, moet u het **activeren**. Als u het product activeert, wordt de beveiliging ingeschakeld.

Opmerking: Als u een upgrade uitvoert van een eerdere versie van het Mobiel Internet Veiligheidspakket, moet u deze versie eerst sluiten. De eerdere versie wordt tijdens de installatie automatisch verwijderd.

1.2 Activering

Nadat u het Mobiel Internet Veiligheidspakket heeft geïnstalleerd. Dient u het uit te schakelen en opnieuw in te schakelen. Op uw scherm verschijnt nu automatisch het activeringsvenster. Volg nu de volgende instructies:

- Selecteer **Ja** in het activeringsvenster.
- Voer uw abonnementscode in en druk op **Activeren**. (Deze abonnementscode vindt u in de bevestigings e-mail die u van KPN heeft ontvangen.)
- Selecteer **Ja** om verbinding te maken met de updateservice. Tijdens deze eerste update wordt de nieuwste virusdefinitie database gedownload.
- Nadat het downloaden is voltooid, verschijnt een bericht dat de registratie is voltooid en dat de toepassing wordt geactiveerd. Selecteer **OK** om de activering te voltooien.
- Scan het apparaat op virussen om te controleren of het geen virussen bevat. (Zie het gedeelte *Scannen op virussen* voor meer informatie).



1.3 Het product starten

Nadat u het Mobiel Internet Veiligheidspakket geactiveerd heeft, wordt de toepassing automatisch gestart als u het apparaat aanzet.

- Als u Windows Mobile Professional of Classic gebruikt, selecteert u **Start > Programma's > KPN**.
- Als u Windows Mobile Standard gebruikt, selecteert u **Start > KPN**.

Selecteer **Ja** als u wordt gevraagd een virusscan uit te voeren.

2 Scannen op virussen

Het Mobiel Internet Veiligheidspakket werkt op de achtergrond en scant uw bestanden automatisch wanneer real-time scannen is ingeschakeld.

- Als tijdens het scannen een virus wordt gevonden, verschijnt een bericht. Selecteer **Ja** om geïnfecteerde bestanden weer te geven of **Nee** om de weergave te sluiten.
- Selecteert u **Ja**, dan verschijnt het scherm **Weergave Infecties** met een lijst van de geïnfecteerde bestanden die op het toestel zijn gevonden. Voor elk item in de lijst wordt de status weergegeven (**geïsoleerd**, **vrijgegeven**) en de naam van het geïnfecteerde bestand.
- Selecteer het geïnfecteerde bestand voor meer details.
 - Als u Windows Mobile Professional of Classic gebruikt, selecteert u **Details weergeven**.
 - Als u Windows Mobile Standard gebruikt, selecteert u **Menu > Details weergeven**.

2.1 Verwerking geïnfecteerde bestanden

- Open **Virusbescherming** in het hoofdvenster.
- Selecteer de optie **Geïnfecteerde bestanden**.
- Selecteer in deze weergave het geïnfecteerde bestand dat u wilt verwerken. En kies een van de volgende acties:
 - **Verwijderen**: het geïnfecteerde bestand wordt verwijderd. U kunt het beste deze optie kiezen. Het bestand wordt definitief van het apparaat verwijderd.
 - **Isolatie**: het geïnfecteerde bestand in isolatie plaatsen als dit nog niet is gebeurd. Een geïsoleerd bestand wordt vergrendeld en kan het apparaat niet beschadigen als het Mobiel Internet Veiligheidspakket is ingeschakeld.
 - **Vrijgeven**: het geïsoleerde bestand wordt vrijgegeven. Als u een bestand vrijgeeft, wordt dit niet meer vergrendeld. U opent het bestand op eigen risico!

Als u Windows Mobile Professional of Classic gebruikt, tikt u op de selectietoets.

Als u Windows Mobile Standard gebruikt, selecteert u **Menu** en vervolgens de gewenste actie.

3 Ongeautoriseerd netwerkverkeer voorkomen

Het Mobiel Internet Veiligheidspakket beschikt over een firewall die het binnenkomende en uitgaande internet- en netwerkverkeer in de gaten houdt. De firewall werkt op de achtergrond en beschermt u tegen inbraakpogingen. Met de vooraf gedefinieerde firewall-niveaus kunt u het beschermingsniveau naar wens instellen.

3.1 Een beveiligingsniveau selecteren

- Open **Firewall** in het hoofdvenster.
- Selecteer **Instellingen** in het menu Firewall.
- Kies een van de volgende firewall-niveaus:
 - **Alles weigeren**: houdt alle netwerkverkeer tegen.
 - **Hoog**: staat de meest voorkomende toepassingen toe en blokkeert al het verkeer dat binnenkomt.
 - **Normaal**: staat alle uitgaande verbindingen toe en blokkeert al het verkeer dat binnenkomt.
 - **Alles toestaan**: staat alle netwerkverkeer toe.
 - **Aangepast**: staat netwerkverkeer toe dat gebaseerd is op uw aangepaste regels. Als u de aangepaste regelset wilt aanpassen, selecteert u **Aangepaste regels bewerken** wanneer het beveiligingsniveau **Aangepast** is geselecteerd.

4 Vertrouwelijke gegevens beschermen

Met de Anti-Theft functie van het Mobiel Internet Veiligheidspakket kunt u uw persoonlijke gegevens beschermen bij verlies of diefstal van uw toestel. Anti-Theft biedt de mogelijkheid om:

- uw toestel op afstand te vergrendelen;
- de gegevens op uw toestel op afstand te wissen;
- uw toestel op afstand te lokaliseren;
- een SMS-waarschuwing te versturen als iemand de SIM-kaart in uw toestel vervangt.

Tip: Aangezien geheugenkaarten eenvoudig verwijderd kunnen worden, kunt u vertrouwelijke informatie het beste in het toestelgeheugen opslaan.

4.1 Anti-Theft gaan gebruiken

Om gebruik te kunnen maken van de verschillende mogelijkheden van Anti-Theft, moet u een beveiligingscode aanmaken. De beveiligingscode moet uit ten minste 8 tekens bestaan. Gebruik een code die eenvoudig te onthouden is, maar moeilijk te raden. Om Anti-Theft te gaan gebruiken volgt u de volgende aanwijzingen:

- Open **Anti-Theft** in het hoofdvenster.
- Selecteer **Instellingen** in het menu Anti-Theft.
- Selecteer welke functies u wilt inschakelen:
 - Selecteer **Blokkeren op afstand inschakelen** als u het apparaat op afstand wilt kunnen vergrendelen.
 - Selecteer **Wissen op afstand inschakelen** als u het apparaat op afstand wilt kunnen wissen.
 - Selecteer **Locator inschakelen** als u het apparaat op afstand wilt kunnen lokaliseren.
- Geef uw **Beveiligingscode** op en typ de code nogmaals om deze te bevestigen.

4.2 Het toestel op afstand vergrendelen

Als u het toestel op afstand vergrendelt, kan het niet worden gebruikt zonder uw toestemming. Het toestel kan alleen weer worden ontgrendeld met het eerder door u ingevoerde ontgrendelingspatroon.

Om uw verloren of gestolen toestel te vergrendelen stuurt u het volgende SMS-bericht naar uw toestel:

#LOCK#<wachtwoord>

(Bijvoorbeeld: #LOCK#abcd1234)

Opmerking: U kunt de externe vergrendeling alleen inschakelen wanneer de apparaatvergrendeling is ingeschakeld.

4.3 Uw toestel op afstand wissen

Met Anti-Theft kunt u op afstand alle persoonlijke gegevens wissen die zijn opgeslagen op uw toestel. Het Mobiel Internet Veiligheidspakket verwijdert de informatie van de geplaatste SD-kaart, SMS- en MMS berichten, contactpersonen en agendagegevens.

Om het verloren of gestolen toestel te wissen stuurt u het volgende SMS-bericht naar uw toestel:

#WIPE#<wachtwoord> (Bijvoorbeeld: #WIPE#abcd1234)

4.4 Uw toestel lokaliseren

Om uw verloren of gestolen toestel te lokaliseren stuurt u een SMS-bericht naar uw eigen nummer. Anti-Theft stuurt een SMS-bericht terug met de laatste locatie van het toestel. De locatie wordt weergegeven in de vorm van GPS-coördinaten. Anti-Theft slaat zelf geen locatiegegevens op. De enige locatiegegevens staan in het SMS-bericht dat naar u wordt verzonden.

Stuur het volgende SMS bericht naar uw toestel om het toestel te lokaliseren:

#LOCATE#<wachtwoord> (Bijvoorbeeld: #LOCATE#abcd1234)

Tip: Verzend het lokalisatiebericht naar uw toestel nadat u het toestel hebt ingesteld om te controleren of dit correct functioneert.

LET OP: Om gebruik te kunnen maken van deze mogelijkheid dient GPS ingeschakeld te zijn op uw toestel.

4.5 De SMS-waarschuwing gebruiken

U kunt instellen dat Anti-Theft u een SMS bericht stuurt als iemand de SIM-kaart in uw toestel vervangt. Volg hiervoor de volgende instructies:

1. Open **Anti-Theft** in het hoofdvenster.
2. Selecteer **SMS waarschuwingsnummer**. Het dialoogvenster SMS waarschuwingsnummer wordt geopend.
3. Geef het telefoonnummer op waarnaar het SMS-bericht moet worden verzonden als de SIM-kaart in het toestel wordt vervangen.

5 Browserbeveiliging

Browserbeveiliging beschermt u tegen websites die persoonlijke gegevens, zoals creditcardnummers, gebruikers accountgegevens en wachtwoorden van u kunnen stelen.

Browserbeveiliging controleert de websites waarnaar u surft met Internet Explorer. Browserbeveiliging wordt automatisch ingeschakeld nadat u het Mobiel Internet Veiligheidspakket hebt geactiveerd en als Internet Explorer is ingesteld als uw standaard browser. Als u een andere browser gebruikt, wordt het browsen niet beveiligd door Browserbeveiliging.

5.1 Browserbeveiliging inschakelen:

- Open **Browserbeveiliging** in het hoofdvenster.
- Selecteer **Instellingen** in het menu Browserbeveiliging.
- Selecteer **Browserbeveiliging inschakelen**.
- In **Netwerk** selecteert u of u Browserbeveiliging altijd wilt gebruiken, of alleen als u via het netwerk van uw eigen provider gebruikmaakt van internet:
 - Selecteer **Alleen mijn provider** om Browserbeveiliging alleen te gebruiken als u het netwerk van uw eigen provider gebruikt. (Nationaal)
 - Selecteer de instelling **Alle providers** op de bescherming aan te laten staan als u zich buiten het bereik van het netwerk van uw eigen provider bevindt. (Internationaal)

6 Het product up-to-date houden

6.1 Automatische updates

Het Mobiel Internet Veiligheidspakket bevat een service voor automatische updates. Hiermee wordt de virusdefinitie-database in de toepassing regelmatig bijgewerkt, zodat u altijd beveiligd bent tegen de nieuwste virussen. Automatische updates worden ingeschakeld nadat u het product hebt geactiveerd. Het Mobiel Internet Veiligheidspakket moet verbinding maken met internet om te kunnen controleren op de nieuwste updates.

6.2 Handmatige updates

U kunt er ook voor kiezen om het Mobiel Internet Veiligheidspakket niet automatisch, maar handmatig bij te werken. Dit kan bijvoorbeeld handig zijn als u naar het buitenland reist (om roaming-kosten te vermijden).

Volg deze aanwijzingen als u het Mobiel Internet Veiligheidspakket handmatig wilt bijwerken:

- Selecteer **Menu > Update** in de hoofdweergave
- Selecteer **Ja** om te bevestigen dat u de nieuwste update wilt ophalen.
- Selecteer **Ja** wanneer u wordt gevraagd een nieuwe toepassingsupdate te downloaden.
- Nadat het bijwerken is voltooid, selecteert u **Ja** om het apparaat te scannen op virussen. (Zie het gedeelte *Scannen op virussen* voor meer informatie.)