

Mobiel Internet Veiligheidspakket

Gebruikershandleiding Mobiel Internet Veiligheidspakket
voor **Symbian** (Nokia) smartphones

Mobiel IVP Symbian Versie 1.0, d.d. 20-07-2011



1	Inleiding	3
2	Installatie.....	4
2.1	Installeren	4
2.2	Activeren.....	4
3	Scannen op virussen	6
3.1	Geïnfecteerde bestanden verwerken:	6
4	Ongeautoriseerd netwerkverkeer voorkomen	7
4.1	Het beveiligingsniveau selecteren	7
5	Vertrouwelijke gegevens beschermen met Anti-Theft.....	8
5.1	Het toestel op afstand vergrendelen	8
5.2	Toestel-vergrendeling bij vervanging SIM-kaart.....	9
5.3	Uw toestel op afstand wissen	9
5.4	Uw toestel lokaliseren	10
6	Internet browsen beveiligen	11
6.1	Browserbeveiliging inschakelen.....	11
6.2	Privacymodus	11
7	Het Mobiel Internet Veiligheidspakket up-to-date houden	13
7.1	Automatische updates	13
7.2	Handmatige updates.....	13
7.3	Versie updates.....	13
8	Technische ondersteuning.....	14



1 Inleiding

Met het Mobiel Internet Veiligheidspakket beschermt u uw Nokia smartphone of tablet tegen de bedreigingen van internet. Het Mobiel Internet Veiligheidspakket biedt drie functies: Anti-Theft, Browserbeveiliging en Scannen op Virussen. voor Nokia is geschikt voor modellen met Symbian versies S60 3rd Edition & 5th Edition en Symbian^3.

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>
--

2 Installatie

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

2.1 Installeren

Selecteer een van de volgende methoden om het Mobiel Internet Veiligheidspakket op uw toestel te installeren:

- Download het installatiebestand naar de computer en verplaats het naar het toestel.
- Download het installatiebestand naar de computer en installeer het Mobiel Internet Veiligheidspakket via Nokia PC Suite.

Of download het installatiebestand rechtstreeks naar uw toestel.

- Open hiervoor in uw internet browser op uw mobiele telefoon of tablet de volgende link: www.kpn.com/downloadmobielivp

- Of scan de QR code met uw mobiele telefoon



Nadat u het Mobiel Internet Veiligheidspakket geïnstalleerd heeft, moet u het activeren. Als u het Mobiel Internet Veiligheidspakket activeert, wordt de beveiliging ingeschakeld.

Opmerking: Als u een upgrade uitvoert van een eerdere versie van het Mobiel Internet Veiligheidspakket, hoeft u de vorige versie niet te verwijderen, maar moet u de Mobiel Internet Veiligheids pakket instellingen controleren nadat u de nieuwe versie hebt geïnstalleerd.

2.2 Activeren

- Open de toepassing. Het welkomstschermb wordt weergegeven.
- Druk op **Doorgaan**.
- Selecteer **Abonnementsnummer** als activeringstype en kies **Doorgaan**. Geef uw abonnementsnummer op en druk op **OK**. (Deze abonnementscode vindt u in de bevestigings-e-mail die u van KPN heeft ontvangen.)



- Druk op **Ja** en selecteer het internet toegangspunt waarmee u verbinding wilt maken met de updateservice. Tijdens deze eerste update wordt de nieuwste virusdefinitie database gedownload en worden uw gegevens geregistreerd.
- Druk vervolgens op **Doorgaan** om de activering te voltooien. Nadat de activering is voltooid, scant u het toestel op virussen om er zeker van te zijn dat het toestel geen virussen bevat. (Zie hiervoor het gedeelte *Scannen op virussen*.)

LET OP: Scan het toestel altijd als u hierom wordt gevraagd!

3 Scannen op virussen

Het Mobiel Internet Veiligheidspakket wordt op de achtergrond uitgevoerd en bestanden worden automatisch gescand

- Het Mobiel Internet Veiligheidspakket geeft een melding als tijdens de real-time scan een virus wordt gevonden. Druk op **Ja** om geïnfecteerde bestanden meteen weer te geven of **Nee** om de bestanden later te bekijken.
- Selecteert u **Ja**, dan verschijnt het scherm een lijst van de geïnfecteerde bestanden die op het toestel zijn gevonden. Voor elk item in de lijst wordt de status weergegeven (**geïsoleerd**, **vrijgegeven**).
- Voor meer informatie over een geïnfecteerd bestand bladert u naar het geïnfecteerde bestand. Selecteer **Weergave**.
- In de weergave met infectiegegevens worden het pad en de bestandsnaam van het geïnfecteerde bestand weergegeven en de naam van het virus.

3.1 Geïnfecteerde bestanden verwerken:

- Blader in de infectieweergave naar het geïnfecteerde bestand dat u wilt verwerken.
- Druk op de selectietoets.
- 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 toestel verwijderd.
 - **Isoleren**: het geïnfecteerde bestand in isolatie plaatsen als dit nog niet is gebeurd. Een geïsoleerd bestand wordt vergrendeld en kan het toestel 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!

4 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.

4.1 Het beveiligingsniveau selecteren

- Blader naar **Instellingen** en druk op de selectietoets.
- Selecteer **Firewall** in de selectielijst met instellingen.
- 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.

5 Vertrouwelijke gegevens beschermen met Anti-Theft

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;
- uw toestel automatisch te laten vergrendelen wanneer de SIM kaart wordt vervangen;
- de gegevens op uw toestel op afstand te wissen;
- uw toestel op afstand te lokaliseren;

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

5.1 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.

Volg de volgende aanwijzingen om de externe vergrendeling in te stellen:

- Blader naar **Instellingen** en druk op de selectietoets.
- Selecteer **Anti-Theft** in de selectielijst met instellingen.
- Voer een **vergrendelings code** in als u deze nog niet hebt gemaakt.
- Schakel **vergrendeling op afstand** in. Het vergrendelde toestel kan worden ontgrendeld met de vergrendelings code.

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.

5.2 Toestel-vergrendeling bij vervanging SIM-kaart

Anti-Theft kan uw toestel automatisch ook vergrendelen wanneer er een andere SIM-kaart in het toestel wordt geplaatst. Het vergrendelde toestel kan dan alleen weer worden ontgrendeld met een vergrendelings code. Volg onderstaande aanwijzingen voor het instellen van de toestelvergrendeling:

- Blader naar **Instellingen** en druk op de selectietoets
- Selecteer **Anti-Theft** in de selectielijst met instellingen.
- Voer een **Vergrendelings code** in. De vergrendelings code moet uit minstens 5 tekens bestaan. **Bewaar deze code op een veilige plek!**
- Als u uw toestel wilt vergrendelen als de SIM-kaart wordt vervangen, selecteert u **Ja** bij **Blok. bij gew. SIM**.

5.3 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.

Volg de volgende aanwijzingen om uw toestel op afstand te kunnen wissen:

- Blader naar **Instellingen voor Anti-Theft** en druk op de selectietoets
- Selecteer **Anti-Theft** in de selectielijst met instellingen.
- Schakel **Wissen op afstand** in
- Voer een **Wiscode** in. De wiscode moet uit minstens 8 tekens bestaan. **Bewaar deze code op een veilige plek!**

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

#WIPE#<wachtwoord>

(Bijvoorbeeld: #WIPE#abcd1234)

LET OP: Wanneer het toestel wordt gewist, worden alle gegevens op het toestel verwijderd!
--

5.4 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.

6 Internet browsen beveiligen

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

Browserbeveiliging controleert websites die u via de standaard browser van uw toestel bezoekt. Als u een browser van derden gebruikt, biedt Browserbeveiliging geen bescherming tijdens het browsen op internet.

TIP: Schakel de internet browser uit en maak de cache leeg voordat u Browserbeveiliging gebruikt.

6.1 Browserbeveiliging inschakelen

- Blader naar **Instellingen** en druk op de selectietoets.
- Selecteer **Browserbeveiliging** in de selectielijst met instellingen.
- Zet **Browserbeveiliging** aan.
- In **Te gebruiken 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 Browsing protection 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)

6.2 Privacymodus

Browserbeveiliging kan informatie over schadelijke websites automatisch naar de analyse sturen om de kwaliteit van de service te behouden. De verstuurd informatie wordt gebruikt om de beschermingsmogelijkheden van diensten en producten te verbeteren. U kunt zelf kiezen welke informatie naar de analyse wordt verstuurd, door het instellen van de privacymodus. Dit gaat als volgt:

- Blader naar **Instellingen** en druk op de selectietoets.
- Selecteer **Overige instellingen** in de selectielijst met instellingen.
- In de Privacymodus selecteert u:
 - **Alleen statistieken** om alleen de statistieken van Browserbeveiliging en gegevens over de server verbinding te versturen.
 - **Alles toestaan** om statistieken en informatie over websites te versturen die niet zijn geanalyseerd of schadelijk materiaal bevatten.



TIP: Voor de beste service, raden wij u aan de privacymodus in de stand **Alles toestaan** te laten staan.

Privacy-verklaring

Door informatie te versturen, wordt uw privacy niet in gevaar gebracht. Hoewel de verzonden informatie in sommige rechtsgebieden als persoonsgegevens kan worden beschouwd, wordt uw privacy tijdens het proces beschermd. De informatie wordt op beveiligde wijze verstuurd, overbodige persoonsgegevens worden verwijderd en de informatie wordt anoniem verwerkt in een bulkbestand. Hierdoor kan de informatie op geen enkele wijze met u in verband worden gebracht. In de informatie die u verstuurt, zijn geen gebruikers accountgegevens, IP-adressen of licentiegegevens opgenomen. Wij beschermen uw privacy bovendien door bij het verzenden van de informatie gebruik te maken van codering.

7 Het Mobiel Internet Veiligheidspakket up-to-date houden

7.1 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.

7.2 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:

- Blader naar **Virusbeveiliging** en druk op de selectietoets.
- Selecteer **Nu bijwerken**.
- Selecteer het internet toegangspunt voor verbinding met de update server. De nieuwste virusdefinitie database wordt gedownload en direct gebruikt.
- Als de update is voltooid, drukt u op **Ja** om het toestel te scannen op virussen als dit wordt gevraagd. Zie het gedeelte **Scannen op virussen** hierboven.

7.3 Versie updates

Als er een nieuwe versie van het Mobiel Internet Veiligheidspakket beschikbaar is, wordt u gevraagd deze te downloaden. Zodra de update is voltooid, start de toepassing automatisch opnieuw op.

8 Technische ondersteuning

In het hoofdvenster van de gebruikersinterface wordt het beveiligingsoverzicht en de huidige status weergegeven. Als wordt aangegeven dat uw toestel niet is beschermd, doet u het volgende:

- Blader naar **Beveiligingsoverzicht** en druk op de selectietoets.
- Selecteer het item met een rood of geel statuspictogram en druk op de selectietoets om het probleem op te lossen.