

1. Uw tablet beveiligen



Het risico op virussen of andere schadelijke software (*malware* genoemd) is bekend van pc's. Minder bekend is dat u ook op een tablet met malware geconfronteerd kan worden als uw tablet verbinding maakt met internet.

Door de manier waarop een tablet werkt, zijn de gevolgen van een besmetting met schadelijke software niet zo groot als op een pc. Zo werken apps vooral afgeschermd van elkaar, waardoor een besmetting van alle apps en bestanden op een tablet niet snel kan voorkomen. Toch kan een met malware besmet tablet frustrerend zijn. Bijvoorbeeld omdat al uw gegevens stiekem worden doorgegeven via internet of uw tablet slechter gaat werken.

Malware komt voornamelijk op een tablet terecht via besmette apps. Het is dus zaak goed op te letten waar vandaan u apps downloadt. De officiële app stores *Play Store* voor *Android*-tablets en *App Store* van Apple zijn in ieder geval veilig.

Voor extra veiligheid kunt u een *antivirusapp* op uw tablet installeren. Voor *Android*-tablets zijn diverse apps beschikbaar, zowel betaald als gratis. In de *App Store* van Apple zijn geen antivirusapps te downloaden. Dit omdat Apple vindt dat de beveiliging op een iPad en bij de *App Store* voldoende bescherming vormen tegen schadelijke apps. Er zijn wel apps voor de iPad verkrijgbaar die onder *mobile security* (mobiele veiligheid) vallen, maar deze zijn dan onder andere gericht op de bescherming tegen diefstal.

Ter beveiliging van uw tablet is het belangrijk dat u het besturingssysteem en de apps regelmatig *update*. Dit houdt in dat een nieuwe, verbeterde versie van de software wordt geïnstalleerd. Hiermee worden ook recent ontdekte veiligheidsproblemen opgelost.

Ook is het belangrijk dat de beveiligingsopties van internetbrowsers als *Internet* en *Chrome* op een *Android*-tablet en *Safari* op de iPad ingeschakeld zijn. Hiermee voorkomt u onder andere dat u het slachtoffer wordt van *phishingwebsites*. Dit zijn websites waarop met behulp van valse informatie wordt geprobeerd belangrijke gegevens te stelen, zoals uw toegangscode voor internetbankieren.

Bij het gebruik van draadloos internet via Wi-Fi is het belangrijk dat u erop let dat u een veilig netwerk gebruikt. In dit hoofdstuk leest u hier meer over.

In dit hoofdstuk leert u:

- wat malware is;
- uw tablet updaten;
- apps updaten;
- een antivirusapp installeren en gebruiken op uw *Android*-tablet;
- welke beveiliging nodig is op uw iPad;
- wat phishing is en welke beveiligingsinstellingen u kunt opgeven in uw browser;
- uw apparaat beveiligen met een wachtwoord of code;
- veilig met Wi-Fi werken.

1.1 Wat is malware?

De term *malware* is een samentrekking van *malicious software*, ofwel kwaadaardige of schadelijke software. Het is een verzamelnaam voor software die schade kan aanrichten op uw tablet.

Voor een deel worden deze apps (programma's) gemaakt door personen die het leuk vinden om in te breken in computers (ook wel *hacken* genoemd) of vervelende apps te verspreiden. Maar vooral professionele criminelen houden zich tegenwoordig bezig met deze vorm van misdaad. Met computercriminaliteit, ofwel cybercrime, zijn namelijk miljoenen te verdienen.

Lange tijd hebben criminelen zich alleen gericht op pc's. Maar door de enorme populariteit van tablets, zijn dit ook steeds populairdere doelen voor malware geworden. Vooral *Android*-tablets zijn een gewild doel.

Tablets zijn door de manier waarop apps gewoonlijk gedownload worden, moeilijker te besmetten met malware. Wanneer u een app uit de *Play Store* op een *Android*-tablet of *App Store* op een iPad downloadt, zal deze al gecontroleerd zijn op malware. Het is echter mogelijk op andere manieren alsnog een besmetting op te lopen. Het gaat hier dan vooral om *Android*-tablets.

Schadelijke apps kunnen niet direct alle apps en bestanden op een tablet besmetten. Dit is iets wat bijvoorbeeld wel eenvoudig kan met malware op een computer. Apps op een tablet werken in een beschermde eigen ruimte, waardoor brede besmetting niet snel mogelijk is. Toch kan ook een beperkte besmetting met malware op uw tablet vervelende gevolgen hebben.

Malware is onder te verdelen in verschillende soorten:

- *Virus* is een verzamelnaam voor apps die zelfstandig kunnen functioneren, maar vaak meeliften in een andere app. Als de besmette app wordt geopend, wordt automatisch het virus geactiveerd. Sommige virussen richten weinig schade aan. Ze laten bijvoorbeeld een bepaalde boodschap op uw beeldscherm zien op een bepaalde datum, maar doen niet meer dan dat. Andere, meer agressieve virussen zorgen ervoor dat u op een gegeven moment niet meer kunt werken op uw tablet. Een belangrijke eigenschap van virussen is dat ze zich makkelijk kunnen vermenigvuldigen en zichzelf zelfstandig kunnen verspreiden, bijvoorbeeld door zichzelf te versturen via e-mails aan mensen in uw contactenlijst.
- *Wormen* en *Trojaanse paarden* zijn varianten van virussen. Dit zijn apps die net zo schadelijk kunnen zijn als virussen, maar los van andere apps functioneren. Ze worden vaak gebruikt door *hackers* (computerinbrekers) om uw tablet over te nemen voor criminele activiteiten, zoals voor het inbreken op tablets of computers of versturen van *spam* (ongewenste reclamemails). Ze creëren vaak een zogenoemde *backdoor* (achterdeur) waardoor hackers makkelijk op uw tablet naar binnen kunnen.
- *Spyware* is geen virus, maar een schadelijke app die stiekem op uw tablet wordt geplaatst wanneer u een besmette app installeert of een schadelijke website bezoekt. Spyware wordt gebruikt om uw tablet te bespioneren en uw gegevens via

internet door te geven aan malafide organisaties en criminelen. Die gebruiken uw gegevens bijvoorbeeld om u ongewenste reclamemails te sturen.

- *Adware* plaatst tijdens het surfen advertenties in een venster van uw browser.
- De laatste jaren is de zogenaamde *ransomware* (gijzelvirus) in opkomst. Hierbij wordt met malware uw tablet lamgelegd. U krijgt de mededeling dat u door geld te storten uw tablet weer 'terugkrijgt'. Een variant hierop is een valse mededeling van ransomware dat u zogenaamd illegale activiteiten met uw tablet heeft uitgevoerd en dat u door geld te storten, arrestatie door de politie kunt voorkomen. U moet nooit op dit soort afpersing ingaan en aangifte doen bij de politie.

1.2 Uw tablet updaten

De besturingssystemen *Android* en *iOS* (voor de iPad) worden continu aangepast, uitgebreid en verder beveiligd. De toevoegingen en verbeteringen worden in de vorm van *updates* verspreid. Hierin worden problemen opgelost of nieuwe functies toegevoegd. Het is belangrijk dat uw besturingssysteem zo snel mogelijk van de laatste updates wordt voorzien. Zo voorkomt u dat beveiligingsfouten kunnen worden misbruikt of uw tablet niet optimaal werkt.

U kunt handmatig zoeken op updates en op sommige tablets ook instellen dat automatisch wordt gezocht naar updates en dat deze ook automatisch worden geïnstalleerd. Als automatisch updaten kan worden ingesteld, wordt aangeraden dit te doen. Zo zorgt u ervoor dat altijd de laatste versie van *Android* of *iOS* is geïnstalleerd op uw tablet.



Let op!

Als u in het buitenland bent en internet gebruikt via het mobiele datanetwerk, is het verstandig om automatisch updaten juist uit te zetten. Het gebruik van internet in het buitenland kan extra kosten met zich meebrengen en het is verstandig uw datagebruik beperkt te houden. Zorg er dan voor dat u voor uw reis al de laatste versie van *Android* of *iOS* geïnstalleerd heeft of gebruikmaakt van Wi-Fi.



Op een *Android*-tablet controleert u als volgt op updates:

 **Open de app *Instellingen*** 

Mogelijk vindt u de software-updates op de pagina Algemeen:

 **Tik, indien nodig, op** **Algemeen**

U gaat op zoek naar de informatie over uw tablet:

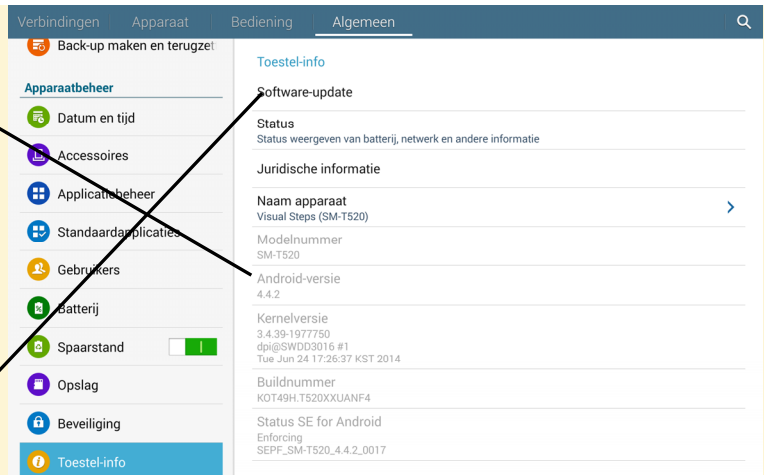
 **Sleep, indien nodig, omhoog over het linkerdeel van het scherm**

 **Tik op**  **Toestel-info** **of**  **Over tablet**

Waarschijnlijk ziet u nu al de huidige versie van *Android*:

U laat controleren op updates:

 **Tik op Software-update of Systeemupdates**

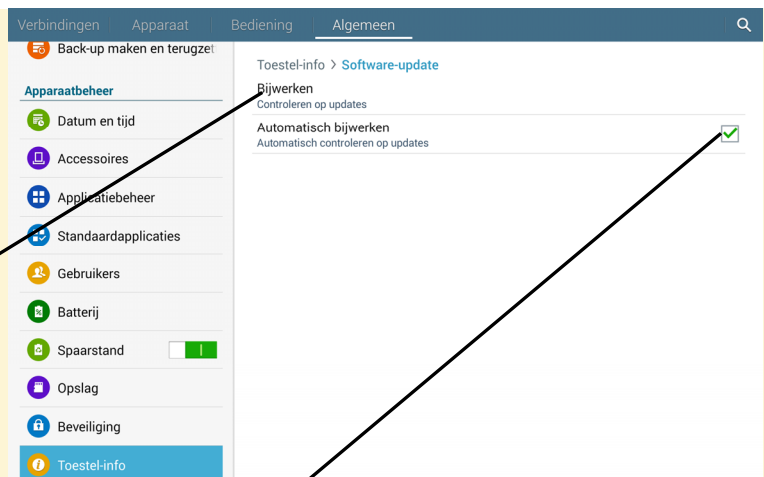


Mogelijk moet u op uw tablet nog op een opdracht geven:

 **Tik op Bijwerken**
Controleren op updates

Op sommige tablets heeft u ook de mogelijkheid automatisch te zoeken naar updates en deze ook automatisch te installeren. In dat geval raden wij u aan deze optie in te schakelen:

 **Tik, indien nodig, een vinkje  bij Automatisch bijwerken**
Automatisch controleren op updates



Als er bij handmatig zoeken op updates een nieuwere versie wordt gevonden, wordt hiervan een melding getoond en kunt u de updates installeren. In dat geval:

 **Volg, indien nodig, de aanwijzingen op het scherm**

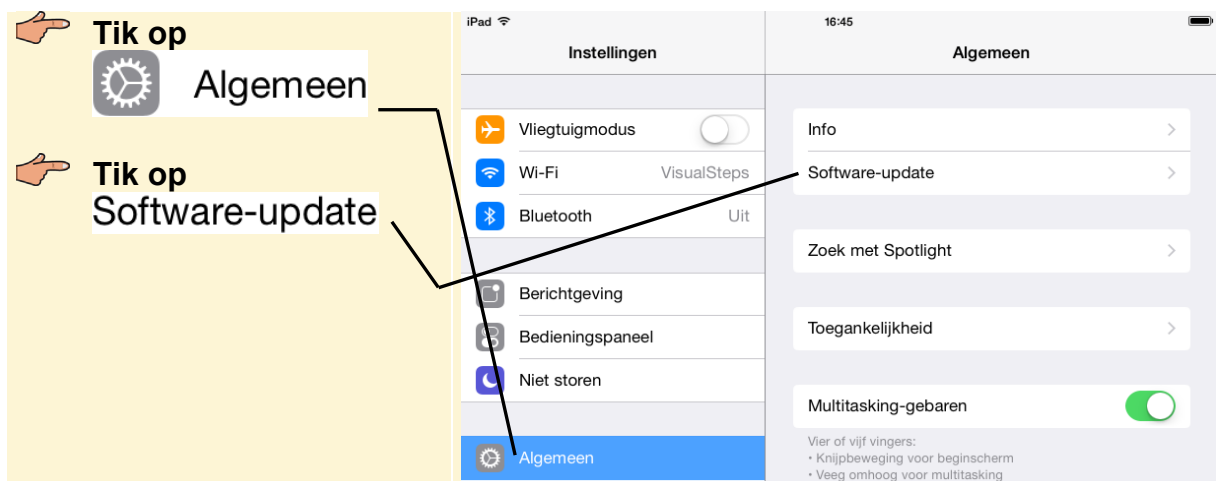
 **Ga, indien nodig, terug naar het beginscherm van de app *Instellingen*** 

 **Ga terug naar het beginscherm van de tablet** 

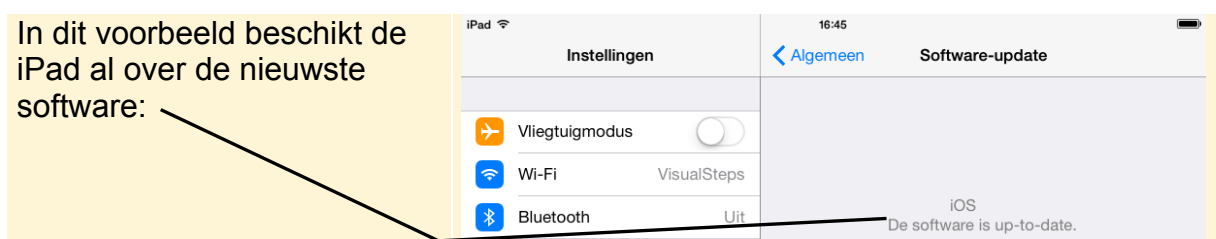
Op een iPad controleert u als volgt op updates:



 **Open de app *Instellingen*** 



Er wordt gecontroleerd of er nieuwe software voor de iPad beschikbaar is:



Als er wel een nieuwere versie gevonden wordt, ziet u hiervan een melding en kunt u de aanwijzingen op het scherm volgen om de update te installeren.

Volg de aanwijzingen op het scherm

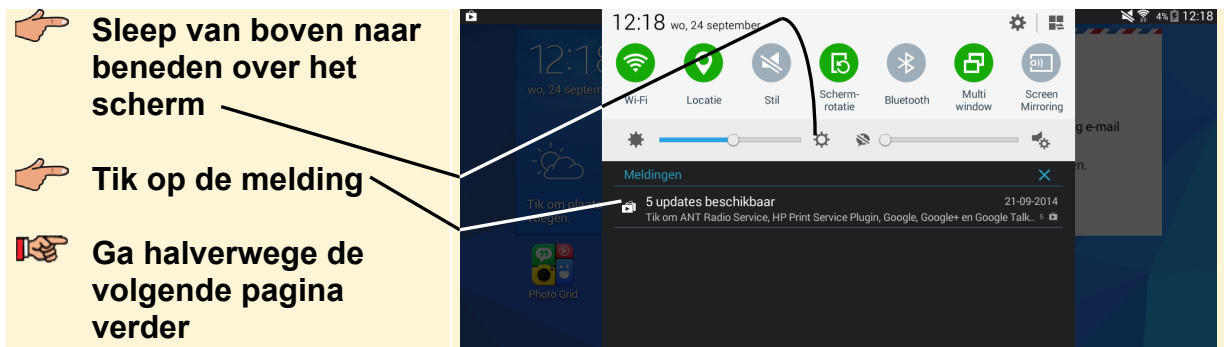
Ga, indien nodig, terug naar het beginscherm van de app *Instellingen* 7

Ga terug naar het beginscherm van de tablet 2

1.3 Apps updaten

De apps die u op uw tablet installeert, zullen na verloop van tijd een gratis update krijgen. Deze updates kunnen nodig zijn om problemen te verhelpen. Het is ook mogelijk dat er met een update nieuwe functionaliteiten worden toegevoegd, zoals nieuwe levels (niveaus) bij een spel.

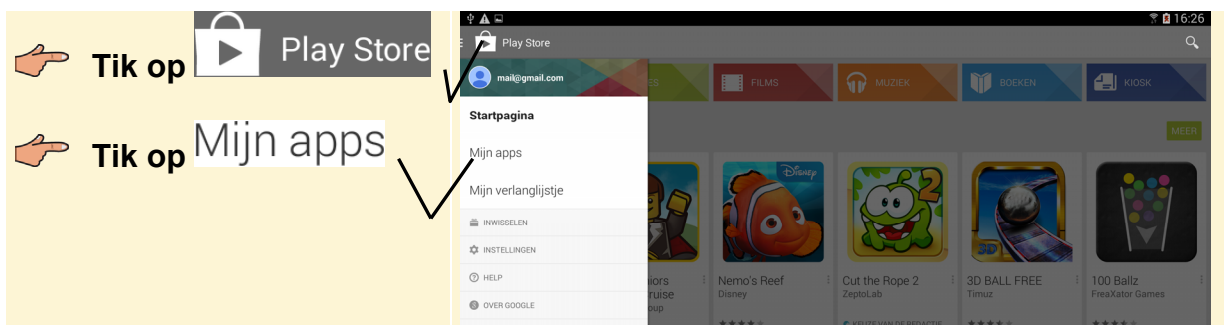
Op een *Android*-tablet ziet u vaak een melding in de statusbalk of in het *Meldingenpaneel* als er updates beschikbaar zijn:



Daarnaast kunt u ook handmatig controleren of er updates voor de apps beschikbaar zijn:

Open de *Play Store*

U bekijkt een overzicht van alle apps op uw tablet:



In dit voorbeeld zijn meerdere updates gevonden. Zo installeert u alle updates:

