Veilig werken met je tablet

De enorme populariteit van tablets heeft een vervelende bijkomstigheid. Het maakt ze erg interessant voor makers van virussen en andere schadelijke software. Daarom is het belangrijk uw tablet veilig te houden.

Virussen, spyware, phishing zijn helaas al jaren bekende termen van de pc. Wie werkt met een pc weet inmiddels wel dat het belangrijk is om een antivirusprogramma te gebruiken en voorzichtig te zijn met wat hij allemaal downloadt en installeert op zijn computer.
Veel mensen weten niet dat tablets en ook smartphones tegenwoordig ook steeds meer risico lopen op bezoeken van schadelijke software.
De reden daarvoor ligt onder andere in de grote populariteit van tablets. Hoe meer tablets er zijn, des te meer potentiële slachtoffers en des te meer resultaat voor criminelen.
Daarnaast zijn tablets echte internetapparaten: ze zijn bijna continue verbonden met internet en daardoor eenvoudig te bereiken.
Hoewel tablets ook computers zijn met een besturingssysteem, werken ze niet helemaal hetzelfde als pc's. Zo werken apps, in tegenstelling tot programma's op de pc, in een afgeschermde ruimte in het geheugen zonder andere processen te verstoren, de z.g. sandbox. Dat maakt het moeilijk voor virussen om op de traditionele manier andere programma's, bestanden of het besturingssysteem te besmetten.
Desondanks blijven er nog voldoende mogelijkheden over om malware (schadelijke software) op een tablet te installeren zonder dat de gebruiker iets doorheeft.
Waar virussen vooral gericht zijn op vernielen, ligt de voorkeur van criminelen tegenwoordig veel meer bij het verzamelen van informatie. Dus is het stiekem installeren van spyware erg populair. Deze spyware houdt dan onder andere bij welke websites je bezoekt en welke gegevens je intypt in formulieren, zoals bij internetbankieren. Ook populair op tablets is software die je bij het surfen op internet ongevraagd doorstuurt naar een andere website, zoals sites met illegale medicijnen of seksuele inhoud.

Beveiliging voor Android tablets

Van de twee grote spelers op de tabletmarkt, **Apple** en **Android**, loopt u met een **Android tablet** het meeste risico. Dat komt niet alleen door de populariteit van Android tablets, maar vooral doordat dit besturingssysteem en de bijbehorende apps ***minder streng*** gecontroleerd worden dan bij Apple.
Google staat toe dat Android apps ook geïnstalleerd kunnen worden buiten Google Play. Op deze manier heeft Google geen controle op de geïnstalleerde app.
Maar Google heeft ook andere procedures voor het toelaten van apps tot Google Play.
Google controleert met het programma Bouncer pas achteraf, nadat een app al is toegelaten tot Google Play, of apps schadelijk zijn. Dit programma kijkt naar bekende malware en *verdacht gedrag*.
Beveiligingssoftwaremaker Trend Micro scande in februari 1,9 miljoen apps binnen en buiten Google Play. Bij 286.000 apps (15 procent van het totaal!) werd een vorm van malware geconstateerd. Daarvan stond bijna een kwart apps (66.000 apps, is 23 procent) in Google Play.
Google heeft ook ingezien dat malware een groot gevaar is voor het platform en heeft daarom sinds Jelly Bean (Android 4.2) een ingebouwde virusscanner toegevoegd aan Android. Echter uit een recent onderzoek van de North Carolina State University blijkt dat deze slechts 20 procent van de malware tegenhoudt.
Malware kan je ook krijgen door op een verkeerde link te klikken op internet. De link verwijst dan naar een website waar een code of programma op staat dat gebruik maakt van een lek in een browser of plug-in (bijv. de Flash plug-in).
Android is regelmatig in het nieuws omdat er een nieuwe malware-uitbraak heeft plaatsgevonden.
Het gaat dan bijvoorbeeld om programma's die zich voordoen als bv. een spel maar ondertussen schadelijke software bevatten.
Je kunt zelf al veel problemen voorkomen door voorzichtig te zijn met welke apps je installeert op je tablet.
Installeer alleen apps uit de officiële Google Play Store. Download dus geen apps uit andere bronnen, want dat verhoogt het risico op het binnenhalen van malware aanzienlijk.
Alleen als het om een app gaat die door een bekende producent via de eigen website wordt aangeboden, zoals een antivirus-app, is het betrouwbaar. Overigens wordt u in deze gevallen toch vaak weer via een link doorverwezen naar de Google Play Store.

Installeren van een Android app

Bij het installeren van een app moet u bij Android altijd aangeven tot welke gegevens deze app toegang mag krijgen. Je hebt het dus in eigen hand of je dit wel of niet wilt. Let hierbij in het bijzonder op het verlenen van toegang tot je persoonlijke gegevens.
Vertrouwt je het niet? Probeer dan eerst via internet meer informatie over de app te vinden of kijk in de Google Play Store bij de reacties van andere gebruikers.
Er zijn overigens ook legitieme apps die graag jouw persoonlijke informatie

verzamelen en gebruiken voor reclamedoeleinden. Dit is legaal als je daar toestemming voor hebt gegeven.
Let hierop vooral bij gratis apps, want voor niets gaat de zon op, maar de regen is ook gratis.

Installeren van virusscanners

Als je het bovenstaande goed gelezen hebt hangt de veiligheid bij het gebruik van de tablet voor een groot deel van jezelf af, maar dat is met al het computergebruik zo.
Er zijn programma's die je daarbij een beetje kunnen helpen. Zo kan je ook op een Android tablet of telefoon een virusscanner installeren.
Het is echter goed om te beseffen dat deze apps niet hetzelfde werken als een virusscanner op je pc.
Er zijn namelijk ook beveiligingsproblemen waar die apps helemaal niets aan kunnen doen. Als er een lek in het besturingssysteem zelf blijkt te zitten, kan een app daar hooguit voor waarschuwen. Google of je telecomprovider zullen dan zelf echter een patch voor het systeem moeten publiceren, want de app kan zelf niet voorkomen dat het lek wordt misbruikt. Ook kunnen antivirusapps niet voorkomen dat malafide apps worden geïnstalleerd. De antivirusapp kan pas waarschuwen voor een virus als het al is geïnstalleerd. Mogelijk is het dan al te laat.
Toch is het belangrijk om zo'n app te installeren. Wil je b.v. veilig kunnen internetbankieren dan moet je dat altijd doen.
Download deze virusscanners altijd via de Google Play Store.
Er zijn inmiddels aardig wat aanbieders van antivirus of antimalware apps voor de tablet of smartphone.
Veel bekende antivirus software producenten, zoals Norton en Bitdefender, bieden deze apps aan voor een relatief lage prijs: soms in een voordeel combinatie met antimalware software voor de pc.
Er zijn ook goede gratis antivirussoftware apps voor de tablet of mobiel. Een aantal vertrouwde virusscanners zijn:

- AVG - Gratis
- Avast Antivirus & Security - Gratis
- Norton Mobile Security - Gedeeltelijk gratis
- McAfee Mobile Security - Gratis
- TrustGo Antivirus & Mobile Security - Gratis
- Trend Micro Mobile Securi ty & Antivirus – Gratis

Waakzaamheid is toch de beste manier om te voorkomen dat je gegevens worden gestolen.
Download alleen bekende apps uit de Play Store.
Zoek via Google zonodig of een applicatie betrouwbaar is.
Apps kunnen ook helpen om te zien of software op je Android-toestel veilig is.
Bovendien bieden veel apps andere handige functies, zoals een overzicht van apps die toegang hebben tot privédata en de mogelijkheid om je telefoon door middel van gps terug te vinden als je deze kwijt bent.
Anti-malware voor de smartphone bevat gewoonlijk meer functies dan alleen bescherming tegen schadelijke programma's, zoals bescherming van privacy tijdens het surfen, een back-up functie voor jouw gegevens en anti-diefstal opties voor wanneer je smartphone is gestolen.

Beveiliging voor de iPad

De iPad is, net als de Macbooks en iMacs van Apple, al van nature goed beveiligd tegen malware. Het besturingssysteem zit zodanig in elkaar dat malware-besmettingen bijna niet mogelijk zijn.
Daarnaast kan je met je iPad alleen de goed gecontroleerde apps uit de iTunes store downloaden. Dat heeft tot gevolg dat je als gebruiker weinig rommel krijgt voorgeschoteld en relatief veilig bent ten opzichte van andere mobiele besturingssystemen. Dit gaat goed tenzij je de iPad hebt laten **jailbreaken**. Het uitvoeren van een jailbreak betekent dat je de beveiliging doorbreekt, waardoor je ook software buiten Apple's App Store om kunt installeren. In dat geval mis je de strenge controle van Apple op veiligheid en loop je veel risico.

Dit is een uitgave van de DigiBar Schagen