

# OUCH!

## IN DEZE EDITIE...

- Jouw tablet beveiligen
- Veilig blijven

## Jouw Nieuwe Tablet Beveiligen

### Overview

Proficiat met jouw nieuwe tablet! Deze technologie is een eenvoudig en krachtig middel om te communiceren met anderen, online te winkelen, films te kijken, games te spelen en een reeks van andere activiteiten uit te voeren. Omdat jouw tablet een belangrijk deel van jouw leven zal uitmaken, misschien vervangt het zelfs jouw computer, geven we je een aantal belangrijke maatregelen die je kan nemen om jouw tablet en gegevens te beveiligen.

### Gast redacteur

Lori Rosenberg heeft een uitgebreide ervaring in het ontwikkelen van trainingen en trainingsmateriaal rond informatiebeveiliging voor medewerkers en klanten. Verder is ze gepassioneerd door het ontwikkelen van nieuwe en inspirerende leermethodes. Je kan haar vinden op Twitter als [@InfoSecLori](#).

### Jouw Tablet Beveiligen

Het zal je verbazen dat niet hackers het grootste risico zijn voor de veiligheid van jouw tablet, maar dat jij dit eigenlijk bent. De kans is groter dat jouw tablet verloren raakt of gestolen wordt dan dat de tablet wordt gehackt. De belangrijkste stap om jouw tablet te beveiligen is het voorzien van automatische schermvergrendeling. Hierdoor dien je iedere keer als je de tablet wenst te gebruiken, dat je het scherm moet ontgrendelen met een PIN-code, een swipe patroon of met jouw vingerafdruk. Dit zorgt ervoor dat wanneer jouw tablet wordt gestolen of verloren raakt, dat niemand anders toegang kan krijgen. Deze maatregel beschermt al jouw persoonlijke gegevens, mobiele apps en alle andere gegevens op het toestel. Eens je de automatische vergrendeling hebt ingeschakeld, zijn er nog bijkomende maatregelen die je kan treffen om jouw toestel te beveiligen:

1. Installeer of schakel software in waarmee je jouw toestel vanop afstand kunt volgen. Zo kan je als jouw toestel gestolen of verloren raakt, het volgen vanaf het Internet om de locatie te vinden of om in het slechtste geval de gegevens op jouw toestel volledig te wissen.
2. Update jouw toestel en schakel automatische updates in zodat het altijd de laatste nieuwe versie van het besturingssysteem heeft. Hackers zoeken altijd naar nieuwe zwakke plekken in software en softwareleveranciers voorzien continu nieuwe updates en patches om deze te dichten. Door de laatste versie van het besturingssysteem en de meest recente softwareversies te draaien, maak je het hackers veel moeilijker om jouw tablet aan te vallen.

## Jouw Nieuwe Tablet Beveiligen

3. Wees voorzichtig wanneer je de tablet voor het eerste gebruik instelt, besteed hier extra aandacht aan de privacy instellingen. Een van de grootste privacy issues is de mogelijkheid dat anderen jouw locatie kunnen weten en volgen. We raden aan om deze functie standaard uit te schakelen en slechts in te schakelen voor die apps waarvan je denkt dat ze dit echt nodig hebben. Voor bepaalde apps is het belangrijk dat jouw locatie gekend is, zoals bij kaart apps of bij het vinden van een restaurant in de buurt, maar de meeste apps hebben deze locatiegegevens niet continu nodig.
4. De meeste tablets en apps bewaren jouw gegevens in de Cloud. Daarom begrijp je best op welke manier jouw gegevens worden beveiligd. Het laatste wat je wil is dat er bijvoorbeeld jouw privé foto's worden gedeeld met de hele wereld via het Internet inclusief de GPS-locatie gegevens die in de foto's zitten. Net daarom schakel je standaard het delen van gegevens uit via de Cloud en schakel je het in voor als je specifieke zaken wilt delen.
5. Tablets zorgen ervoor dat je gegevens kunt synchroniseren met andere toestellen zoals jouw smartphone of laptop. Synchronisatie is een handig middel maar wees voorzichtig met de apps en functies die dit mogelijk maken. Indien je synchronisatie hebt ingeschakeld, wees dan niet verrast als je eerder bezochte websites en tabbladen ziet verschijnen in jouw browser die je op het werk gebruikt.



*De beste manier om jouw tablet te beveiligen is door automatische schermvergrendeling in te schakelen, privacy instellingen aan te passen en jouw tablet te blijven updaten.*

## Veilig Blijven

Eens je de tablet hebt beveiligd, wil je er zeker van zijn dat dit zo blijft. Hier zijn enkele belangrijke stappen die je kan nemen om jouw tablet veilig te houden:

- Jailbreak of hack jouw tablet niet. Dit zorgt ervoor dat een groot aantal security maatregelen worden omzeild en maken het toestel extra kwetsbaar voor hackpogingen.
- Download enkel apps van vertrouwde bronnen. Voor iPads download je enkel apps van iTunes. Deze apps worden gescreend door Apple vooraleer ze worden uitgegeven. Voor Google raden we aan om enkel Google Play te gebruiken. Voor Amazon tablets blijf je best bij de Amazon App Store. Je kan ook apps downloaden van andere sites, maar deze zijn niet officieel en kunnen mogelijk besmet zijn. Ten slotte, ongeacht de plaats vanwaar je de app haalt, eens je de app niet meer gebruikt, kan je deze best verwijderen.

## Jouw Nieuwe Tablet Beveiligen

- Wanneer je een nieuwe app installeert, kijk dan de privacy instellingen na, zoals je ook deed wanneer je de tablet voor het eerste gebruik instelde. Wees voorzichtig met de toegang per app. Heeft de app wel werkelijk een behoefte aan toegang tot gegevens van al jouw vrienden en contactpersonen? Indien je het niet eens bent met een bepaalde toegangsvereiste voor een app, ga dan op zoek naar een andere app die wel voldoet aan jouw vereisten. Bovendien kan je best regelmatig nagaan of de toegangen niet zijn veranderd.

Jouw tablet is een krachtig hulpmiddel, waarvan we willen dat je ze gebruikt en er plezier aan beleeft. Door deze stappen te onthouden kan je jouw tablet al heel veilig houden.

### Meer Weten?

Ga naar <http://www.securingthehuman.org> om je te abonneren op de maandelijkse OUCH! Security awareness nieuwsbrief, toegang te krijgen tot het OUCH! archief en kom meer te weten over SANS security awareness oplossingen.

### Over Cegeka Groep

Cegeka Groep is een onafhankelijke ICT-dienstverlener opgericht in 1992. Cegeka heeft zijn hoofdkantoor in België en heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Tsjechië en Slowakije. Het bedrijf levert diensten aan klanten in heel Europa: enterprise cloud- en securitydiensten, applicatiediensten, agile coaching en outsourcingdiensten. Cegeka stelt 3.200 mensen tewerk en haalde in 2013 een omzet van 330 miljoen euro. Bezoek [www.cegeka.com](http://www.cegeka.com) voor meer informatie.

### Bronnen (Engels)

Securely Using Mobile Apps: <https://www.securingthehuman.org/ouch/2015#january2015>

10 tips voor een veilig gebruik van je tablet: <https://www.safeonweb.be/nl/tips/10-tips-voor-een-veilig-gebruik-van-je-smartphone-tablet-0>

Using the Cloud Securely: <https://www.securingthehuman.org/ouch/2014#september2014>

Disposing of Your Mobile Device: <https://www.securingthehuman.org/ouch/2014#june2014>

SANS Security Tip of the Day: [https://www.sans.org/tip\\_of\\_the\\_day.php](https://www.sans.org/tip_of_the_day.php)

OUCH! Is een publicatie van SANS Securing The Human en wordt verdeeld onder de [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). Deze nieuwsbrief mag verder verdeeld worden en gebruikt worden in uw eigen security awareness programma, zolang u de inhoud niet wijzigt. Stuur een bericht naar [ouch@securingthehuman.org](mailto:ouch@securingthehuman.org) voor meer informatie en voor vertalingen.

Redactie: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis  
Vertaald door: Sven Jacobs, Tom Palmaers



[securingthehuman.org/blog](http://securingthehuman.org/blog)



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



[securingthehuman.org/gplus](https://securingthehuman.org/gplus)