Nationaal Cyber Security Centrum
*Ministerie van Veiligheid en Justitie*

# *Veilig gebruik van smartphones en tablets*

## *Risico's en maatregelen*

Factsheet FS-2011-03
versie 1.2 | 24 mei 2014

**Naast bellen en sms'en kan men met een smartphone of tablet internetten, e-mailen en applicaties (zogenaamde apps) downloaden en gebruiken. Smartphones en tablets zijn populair en worden gebruikt voor zowel privé als zakelijke doeleinden. Hierdoor kunnen deze apparaten toegang bieden tot vertrouwelijke of persoonlijke data.**

**Veel apps verwerken vertrouwelijke en/of persoonlijke informatie. Deze apps kunnen uw informatie vrijgeven aan derde partijen. Denk hierbij aan uw contacten, locatie, e-mails, agenda-afspraken en documenten. Dit brengt beveiligingsrisico's met zich mee.**

**In deze factsheet leest u wat belangrijke beveiligingsrisico's zijn van het gebruik van een smartphone en/of tablet en hoe u op een verstandige manier met deze beveiligingsrisico's om kunt gaan en mogelijke schade kan voorkomen of beperken.**

**De belangrijkste feiten op een rij:**

- De grens tussen privé- en zakelijk gebruik van de smartphone vervaagt. Eén voorbeeld hiervan is de BYOD-trend.
- Het 'op straat' komen te liggen van vertrouwelijke of persoonlijke informatie is een groot beveiligingsrisico.
- Sommige apps geven vertrouwelijke of persoonlijke informatie door aan derde partijen.
- De dreiging van malware op smartphones neemt toe.
- Door een aantal handelingen is de beveiliging van uw smartphone en/of tablet te vergroten.

### Risico's van integratie smartphones met bedrijfsnetwerken

In de afgelopen jaren is de grens tussen privé- en zakelijk gebruik van smartphones vervaagd. Werkgevers staan het toe aan werknemers om hun eigen privétoestellen te gebruiken voor zakelijke activiteiten. Deze zogenoemde 'Bring-Your-Own-Device' (BYOD)-trend zorgt ervoor dat meer vertrouwelijke informatie op privésmartphones en tablets komt te staan. Het 'op straat' komen te liggen van vertrouwelijke informatie is één van de grootste beveiligingsrisico's.

Als uw werkgever een smartphone aan u verstrekt, zijn daarop mogelijk al diverse beveiligingsmaatregelen ingesteld. Het advies is dan ook om tijdens uw werkzaamheden alleen gebruik te maken van de door uw werkgever verstrekte smartphone of, in het geval van uw privétoestel, de BYOD-richtlijnen van uw werkgever na te leven.

### Risico's van het lekken van persoonlijke informatie

Naast het zakelijke gebruik worden smartphones en tablets ook voor privédoeleinden gebruikt. Hierdoor wordt persoonlijke informatie opgeslagen op deze apparaten. Denk hierbij aan uw contacten, locatie, e-mails, agenda-afspraken en documenten. Deze gegevens worden door sommige apps verzameld, verwerkt en wellicht beschikbaar gesteld aan (kwaadwillende) derde partijen.[1,2] Het 'lekken' van persoonlijke informatie is ook één van de grootste beveiligingsrisico's.

Deze factsheet is tot stand gekomen in samenwerking met Ronald Kingma (SecureLabs), Brenno de Winter en de Betaalvereniging.

[1] http://www.nu.nl/tech/3665758/snapchat-lekt-gebruikersnamen-en-telefoonnummers.html
[2] https://www.security.nl/posting/41811/

## Drie belangrijke beveiligingsmaatregelen:

Door deze drie maatregelen toe te passen, kunt u grote risico's voorkomen.

- *Authenticatie van de gebruiker*: gebruik een pincode of wachtwoord om uw apparaat te vergrendelen.
- *Versleuteling van vertrouwelijke of persoonlijke informatie*: indien mogelijk, stel uw apparaat zo in om alle informatie te versleutelen (inclusief eventuele backups).
- *Wissen van data*: in sommige gevallen kan het wissen van data (eventueel op afstand) voorkomen dat uw data gelekt wordt.

### Lever uw smartphone 'schoon' in

Op het moment dat u uw smartphone verkoopt of weggeeft aan iemand anders adviseren wij de fabrieksinstellingen te herstellen en alle informatie te wissen.[3] Denk hierbij aan uw contactgegevens, sms'jes, e-mails, de door u geïnstalleerde apps en instellingen. Het wissen voorkomt dat de nieuwe eigenaar toegang heeft tot de achtergebleven informatie op de smartphone.

### Voorkom malware op uw smartphone

De dreiging van malware op smartphones neemt toe.[4] Criminelen maken misbruik van kwetsbaarheden van uw smartphone of u downloadt een 'onschuldig' lijkende app, die - zonder dat u dat door heeft - geheime, kwaadaardige functies bevat. In sommige gevallen is een app zelf niet kwaadaardig maar bevat deze wel enkele kwetsbaarheden die door een derde partij voor kwaadaardige doeleinden kan worden misbruikt.[1]

Als uw smartphone is geïnfecteerd met kwaadaardige software (malware) kunnen criminelen bijvoorbeeld:

- Zien wat u intypt om zo gebruikersnamen, wachtwoorden of andere (vertrouwelijke) informatie te achterhalen.
- Sms'jes versturen naar (dure) servicenummers of een abonnement afsluiten zonder dat u daarvan op de hoogte bent.
- Uw inloggegevens voor mobiel bankieren onderscheppen en gebruiken om uw rekening te plunderen.[5]

Om de kans op een malware-besmetting te verminderen, adviseren wij u het volgende:

- Wees terughoudend met het installeren van onbekende apps op uw smartphone. Controleer vooraf de betrouwbaarheid van zowel de app als de leveranciers.[6]
- Ga bewust om met de instellingen van de apps.
- Wees, indien mogelijk, terughoudend met het verlenen van rechten aan apps. Stel altijd de vraag of een app bijzondere rechten per se nodig heeft om zijn diensten uit te voeren. Bijv. heeft een foto app per se toegang tot uw contactenlijst nodig?
- Voorzie uw smartphone en/of tablet altijd van de laatste versie van het besturingssysteem.
- Zorg ervoor dat de apps op uw apparaat altijd voorzien zijn van de laatste updates. Bij enkele besturingssystemen valt dit te automatiseren.
- Installeer indien mogelijk een virusscanner op uw smartphone.[7]

### Pas op voor onbetrouwbare netwerken

Smartphones en tablets beschikken over een breed scala aan draadloze netwerken zoals WiFi en Bluetooth. Deze draadloze netwerken zijn kwetsbaar voor afluisteren, waardoor informatie kan worden onderschept, zelfs wanneer verbindingen versleuteld zijn. Daarnaast kan gevoelige informatie langs andere weg uitlekken. Door zwakheden in de beveiliging van gsm-communicatie, bijvoorbeeld, kunnen telefoongesprekken en sms-berichten worden afgeluisterd en ook is gebleken dat voicemails door derden af te luisteren kunnen zijn.[8]

Wij adviseren u om de volgende maatregelen in acht te nemen:

- Schakel WiFi en Bluetooth uit wanneer u daar geen gebruik van maakt.
- Wees kritisch waar en wanneer u van een publiek (niet versleuteld) WiFi-netwerk gebruik maakt. Het is af te raden om op openbare plaatsen van een publiek WiFi-netwerk gebruik te maken. Doet u dat toch, vermijd dan werk of financiële activiteiten. Stel uw smartphone zo in dat het niet automatisch verbinding maakt met een WiFi-netwerk.
- Weest bewust dat zelfs als de naam van het netwerk klopt u niet automatisch met het juiste netwerk bent verbonden. Aanvallers gebruiken soms de naam van uw vertrouwde netwerk. Dit kan omdat uw apparaat zelf zoekt naar netwerken door de naam uit te zenden. Aanvallers kunnen dit opvangen en dan met deze naam uw netwerk imiteren; uw apparaat zal automatisch verbinding maken met dit netwerk.

### Functionaliteit op afstand

Er zijn programma's voor smartphones die een functionaliteit bieden die op afstand kan worden uitgevoerd[3], bijvoorbeeld in het geval dat u uw telefoon bent verloren. Hieronder enkele voorbeelden van een dergelijke functionaliteit.

- Het wissen van informatie en het resetten naar de standaard fabrieksinstellingen.
- Het lokaliseren van uw smartphone zodat u op een kaart ziet waar uw smartphone zich bevindt.
- Een bericht op het display weergeven zodat de vinder weet waar de smartphone kan worden terugbezorgd.
- Een nieuwe toegangscode instellen om uw smartphone te beveiligen.

[3] Raadpleeg de leverancier van uw apparaat voor meer informatie over hoe dergelijke maatregelen worden toegepast.

[4] http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-malware-high-risk-apps-hit-1m-mark/ en http://www.infosecurity-magazine.com/view/36686/mobile-malware-infects-millions-lte-spurs-growth/

[5] https://www.security.nl/posting/368902/

[6] Bronnen die hierbij geraadpleegd kunnen worden zijn reviews van de app in de 'app store' (bijv. Apple App Store, Google Play, etc.) of de ICT-afdeling van uw organisatie.

[7] http://www.av-comparatives.org/mobile-security-review-august-2013/

[8] Op de website: https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling vindt u o.a. het whitepaper 'Beveiliging van mobiele apparatuur en datadragers' en de factsheets 'Tips voor veilig gebruik van mobiele telefoons', 'Afluisteren van GSM-communicatie' en 'Kwetsbaarheden in voicemaildiensten'.

## Weest alert bij het gebruik van gevoelige diensten zoals internet bankieren

Aanvallers kunnen internetverkeer onderscheppen en de versleuteling van verbindingen met websites ongedaan maken als zij het netwerk beheersen waar u gebruik van maakt. Dat is bijvoorbeeld het geval wanneer zij een malafide draadloos netwerk opzetten met een voor uw apparaat bekende naam, zodat uw apparaat daar automatisch verbinding mee maakt (zie eerder). Een aanvaller is dan in staat om zogenaamde 'SSL-stripping' uit te voeren waardoor de verbinding met een website niet meer beveiligd is en daardoor kan worden gemanipuleerd.

Bij zo'n aanval kan een aanvaller bijvoorbeeld financiële transacties aan te passen die over het netwerk gaan, ook als deze versleuteld zijn. Zo kan het bankrekeningnummer van de ontvanger worden aangepast. Daarbij kunnen aanvallers ook de gegevens aanpassen die in uw scherm worden getoond, om de manipulatie te verbergen. U ziet dan niet dat geld bijvoorbeeld naar een andere rekening dan bedoeld wordt overgemaakt.

Het verwijderen van de beveiliging van de verbinding is te zien doordat het slotje dat hoort bij de beveiligde verbinding ontbreekt. Aanvallers proberen u echter te misleiden door bijvoorbeeld het icoon van de website (het 'favicon') in een slotje te veranderen, zodat er toch een slotje zichtbaar is.

Om de risico's van manipulatie van transacties te verminderen adviseren wij het volgende:

- Gebruik geen gevoelige diensten, zoals internet bankieren wanneer u gebruikt maakt van WiFi op een openbare plaats. Doet u dit toch, controleer dan of u echt met het door u vertrouwde netwerk verbonden bent. Vermijd het gebruik van internetbankieren via publieke hotspots.
- Gebruik bij internet bankieren in openbare plaatsen bij voorkeur bancaire apps in plaats van websites, daarbij werkt de aanval via SSL-stripping niet.
- Controleer bij internetbankieren via websites van banken goed of u daadwerkelijk een versleutelde verbinding heeft (het internetadres moet beginnen met https) en of het slotje op de goede plek staat.
- Volg de adviezen op die worden gegeven op www.veiligbankieren.nl

Nederlandse banken hebben een nieuwe technologie ingevoerd (of zijn daar mee bezig) genaamd *HTTP Strict Transport Security* (afgekort HSTS), waardoor het niet meer mogelijk is de beveiliging van verbindingen ongedaan te maken via SSL-stripping.

## Geef geen informatie via uw smartphone vrij

Uit onderzoek blijkt dat een deel van de apps voor smartphones data van individuele gebruikers (bijvoorbeeld persoons- en locatiegegevens) verzamelt en deze op de achtergrond doorstuurt naar derden (bijv. externe servers, ontwikkelaars of adverteerders), zonder de gebruiker te informeren[9]. Apps worden door u geïnstalleerd, vaak zonder dat u weet wie de ontwikkelaar is en wat de programmacode is. Hierbij geeft u soms toestemming voor toegang tot informatie zonder te weten wat hiermee wordt gedaan.

Om onbewust vrijgeven van informatie te voorkomen of dit zoveel mogelijk te beperken adviseren wij u het volgende:

- Lees de factsheet "Veilig op sociale netwerken"[10] aandachtig door. Hierin wordt een overzicht gegeven van de beveiliging- en privacyrisico's verbonden aan sociale netwerken.
- Kijk kritisch naar de standaardinstellingen van uw toestel ten aanzien van beveiliging, privacy en connectiviteit. Beperk het delen van of de toegang tot informatie (zoals locatiegegevens) wanneer dit niet nodig is.
- Lees voordat u een app installeert de voorwaarden en privacybeleid van de aanbieder door, zodat u op de hoogte bent van hoe er met uw gegevens wordt omgegaan.

## Wees voorzichtig bij het gebruik van onlinediensten

Er zijn veel leveranciers die online opslag van foto's, documenten of back-ups aanbieden. Deze online opslag vindt meestal in de Cloud plaats[11]. De beveiliging van dergelijke diensten heeft u niet zelf in de hand en is niet altijd afdoende, wees dus voorzichtig bij online opslag vanaf uw smartphone. U moet altijd voorzichtig zijn met het online opslaan van uw vertrouwelijke gegevens. De online bestanden zijn direct toegankelijk voor iedereen die uw inloggegevens (vaak gebaseerd op e-mailadres en wachtwoord) weet te achterhalen.

Om op een veilige manier gebruik te maken van online opslag adviseren wij u het volgende:

- Schrijf uw inloggegevens niet op. Als u dat toch doet, bewaar ze dan op een veilige plek en gescheiden van uw smartphone.
- Versleutel uw bestanden vóórdat deze online worden gezet.
- Wijzig regelmatig uw wachtwoord.

### Overige tips:

- Informeer binnen uw organisatie of er beleid en/of richtlijnen zijn met betrekking tot het gebruik van smartphones.
- Schaf nieuwe apps voor uw smartphone altijd aan via officiële distributiekanalen van leveranciers, zogenaamde 'app stores'.
- Wees ervan bewust dat u extra risico loopt als u uw smartphone en/of tablet 'jailbreakt' omdat de officiële 'app stores' op deze manier worden omzeild waardoor de kans groter is om kwaadaardige apps te installeren.

[9] http://www.nuzakelijk.nl/e-business/2302373/veel-gratis-applicaties-sturen-gevoelige-data-door.html, http://webwereld.nl/nieuws/67335/meeste-android-apps-lekken-priv--gegevens.html en http://webwereld.nl/nieuws/67365/meerderheid-iphone-apps-lekt-priv--gegevens.html,

[10] https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/factsheet-veilig-op-sociale-netwerken.html

[11] Voorbeelden hiervan zijn Apple iCloud en Google Drive.

**Tot slot: Uw smartphone kwijt of gestolen?**

Neem maatregelen zodat bij verlies of diefstal geen vertrouwelijke of persoonlijke informatie op straat komt te liggen.[3]

- Beveilig de toegang tot uw smartphone door middel van een toegangscode die door derden niet makkelijk te raden is en wijzig deze regelmatig. De SIM-kaart heeft een eigen toegangscode en wij adviseren om deze toegangscode ook regelmatig te wijzigen.
  Let op: De toegangscode beveiligt alleen de smartphone en niet de losse verwijderbare media zoals de (micro-)SD-kaart. Op het moment dat een kwaadwillende dergelijke media uit uw smartphone heeft verwijderd, heeft deze toegang tot alle niet-versleutelde gegevens die hierop zijn opgeslagen.
- Stel uw smartphone zo in dat na een tijdsperiode (bijv. 1 minuut) de smartphone automatisch wordt vergrendeld.
- Activeer de functionaliteit waarmee informatie op uw smartphone standaard versleuteld opgeslagen wordt.
- Overweeg om uw smartphone zo in te stellen dat na een aantal mislukte inlogpogingen (bijv. 10) de smartphone wordt gereset naar de standaard fabrieksinstellingen en uw informatie op de smartphone wordt gewist.
- Maak gebruik van een toepassing die het beheren van uw smartphone op afstand ondersteunt, zodat u bij vermissing controle houdt over uw smartphone, zie het kader “Functionaliteit op afstand”.
- Maak regelmatig een reservekopie/back-up van uw smartphone zodat u bij vermissing of het defect raken van uw smartphone niet uw informatie kwijt bent.
- Bewaar de International Mobile Equipment Identity (IMEI)-code op een veilige plek en gescheiden van uw smartphone. De IMEI-code is een 15-cijferig nummer en is de unieke identificatie (serienummer) van uw smartphone. Deze IMEI-code heeft u nodig om bij verlies of diefstal aangifte te doen bij de politie.
- Doe altijd aangifte bij de politie als u merkt dat uw smartphone is verdwenen. Wanneer u uw smartphone gebruikt voor werk, meldt het dan ook bij de hiervoor aangewezen instantie binnen uw organisatie (bijvoorbeeld beveiliging of facilitaire zaken). Daarnaast kunt u het ook registreren in het telefooncheckregister.

Uitgave van **Nationaal Cyber Security Centrum**
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
www.ncsc.nl | info@ncsc.nl
T 070-888 75 55 | F 070-888 75 50
Publicatienr: FS-2011- 3