APPS

MAAR EEN SPELLETJE?

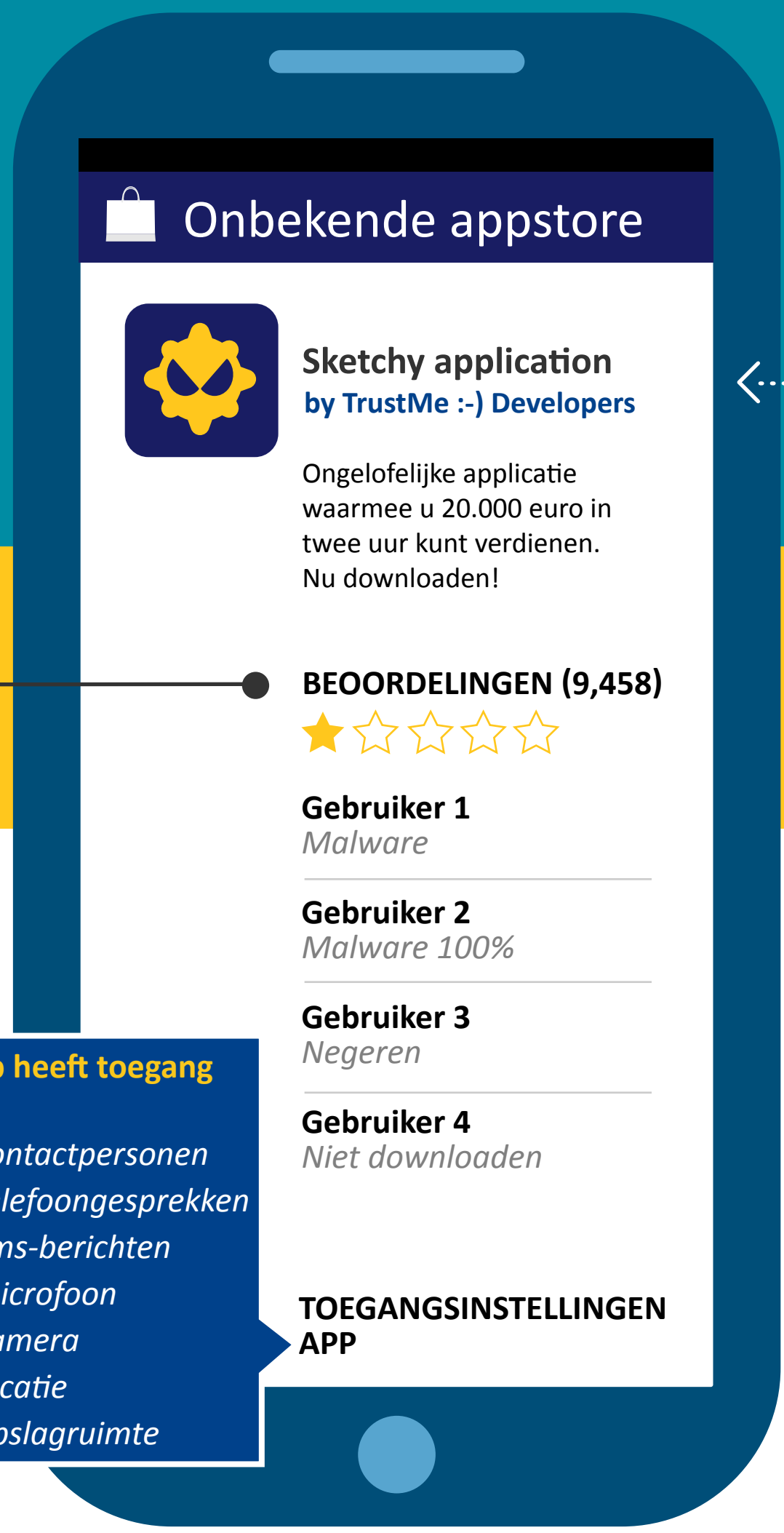
Installeer alleen apps van officiële appstores.

Als u een app wilt installeren, doe dan eerst onderzoek naar de uitgever en de app zelf. Pas op voor e-mails of sms-berichten met links erin. Via dit soort links kunnen er onbedoeld apps van derde partijen of onbekende bronnen geïnstalleerd worden.

LEES DE RECENSIES EN BEOORDELINGEN VAN ANDERE GEBRUIKERS.

NEEM DE TOEGANGSINSTELLINGEN VAN DE APP ZORGVULDIG DOOR

Controleer tot welke gegevens de app toegang heeft en of deze gegevens gedeeld kunnen worden met externe partijen. Heeft de app al deze toegangsinstellingen nodig? Zo niet, download deze dan niet.



INSTALLEER EEN MOBIELE-BEVEILIGINGSAPP

Een mobiele-beveiligingsapp controleert alle apps die u op uw apparaat heeft geïnstalleerd en gaat installeren op kwaadwillende software.

EUROPOL EC3 European Cybercrime Centre | POLITIE | ALERT online | Betaalvereniging Nederland

#MobileMalware

MALWARE VOOR
MOBIEL BANKIEREN

MALWARE KAN U GELD GAAN KOSTEN

Malware voor mobiel is speciaal ontwikkeld om uw financiële gegevens te stelen.

HOE RAAKT UW APPARAAT BESMET?

Door kwaadwillende websites te bezoeken

Door kwaadwillende apps te downloaden

Phishing

WAT ZIJN DE RISICO'S?

Cybercriminelen krijgen toegang tot uw inloggegevens

Onbevoegde transacties

WAT KUNT U DOEN?

https://

Download de officiële app van uw bank en let er altijd op dat u de echte website van uw bank bezoekt.

Zorg ervoor dat u niet automatisch wordt ingelogd op de app of website van uw bank.

Houd uw betaalpasnummer en wachtwoord geheim en deel ze niet met anderen.

Schakel automatische updates in. Installeer, indien mogelijk, een mobiele-beveiligingsapp die u op de hoogte stelt van verdachte activiteiten.

Als u een mobiele telefoon kwijtraakt of een nieuw nummer heeft gekregen, neem dan contact op met uw bank, zodat zij uw gegevens kunnen bijwerken.

Verstuur geen bankgegevens via sms-berichten of e-mail.

Gebruik bij voorkeur een beveiligd Wi-Fi-netwerk als u verbinding maakt met de mobiele website of app van uw bank.

Controleer uw rekeningoverzicht regelmatig.

EUROPOL EC3 European Cybercrime Centre | POLITIE | ALERT online | Betaalvereniging Nederland

#MobileMalware

MOBIELE
RANSOMWARE

LET GOED OP UW PERSOONLIJKE BESTANDEN

Ransomware houdt uw mobiele apparaat en alle gegevens die erop staan gevangen en laat ze pas weer vrij als u betaald heeft. Deze variant van malware vergrendelt het scherm van uw mobiele telefoon of voorkomt dat u bepaalde bestanden of functies kunt gebruiken.

HOE WORDT UW APPARAAT BESMET?

Door geïnfecteerde websites te bezoeken.

Door imitaties van legitieme apps te downloaden.

Door te klikken op kwaadwillende links en bijlagen in phishing-mails.

WAT ZIJN DE RISICO'S?

Verlies van al uw gegevens doordat u de fabrieksinstellingen op uw apparaat moet terugzetten.

Cybercriminelen kunnen volledige toegang tot uw apparaat krijgen en uw gegevens delen met derde partijen.

WAT KUNT U DOEN?

Maak regelmatig een back-up van uw gegevens en zorg ervoor dat al uw apps en uw besturingssysteem up-to-date zijn.

Download geen apps van onbekende appstores.

Schakel automatische updates in. Installeer, indien mogelijk, een mobiele-beveiligingsapp die u laat weten wanneer u het slachtoffer bent geworden van ransomware.

Let goed op bij verdachte e-mails en websites die u een onwaarschijnlijk aantrekkelijk aanbod doen of om andere redenen verdacht lijken.

Geef niemand anders beheerderstoegang tot uw apparaat.

Betaal het losgeld niet. U financiert hiermee criminelen en moedigt ze aan om hun criminele activiteiten voort te zetten.

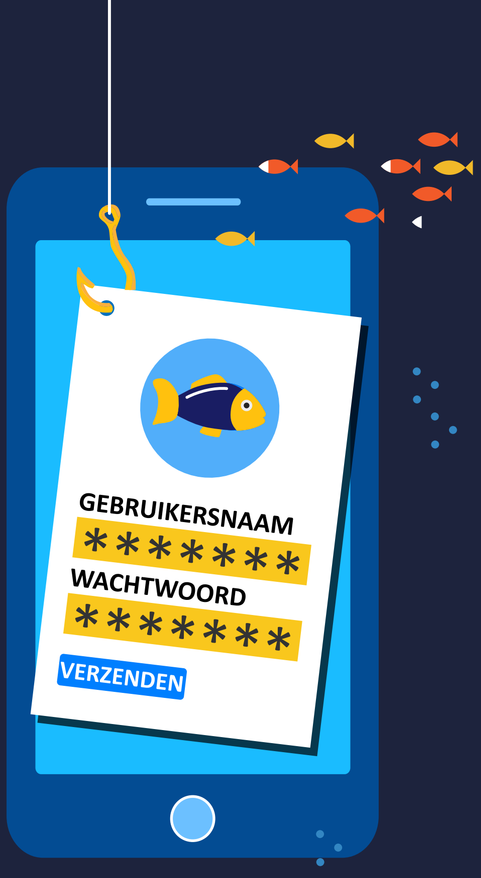
EUROPOL EC3 European Cybercrime Centre | POLITIE | ALERT online | Betaalvereniging Nederland

#MobileMalware

WEBGEBASEERDE RISICO'S

GOED OPLETTEN VOORDAT U KLIKT.

U kunt uw geld, persoonlijke gegevens en zelfs uw opgeslagen gegevens kwijtraken als het apparaat niet meer werkt.



WAT ZIJN DE RISICO'S?

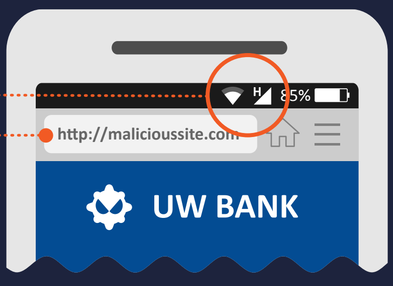
PHISHING-AANVALLEN: Tijdens een phishing-aanval proberen cybercriminelen achter de persoonlijke gegevens van internetgebruikers te komen door zich voor te doen als een betrouwbare partij. Zij zijn actief via e-mail, sms-berichten en sociale-mediaplatformen.

SURFEN OP INTERNET: Uw mobiele apparaat kan geïnfecteerd raken wanneer u een onveilige website bezoekt.

BESTANDEN DOWNLOADEN: E-mails kunnen kwaadwillende links of bijlagen bevatten.

WAAROM KAN HET GEBEUREN?

Mobiele apparaten zijn **ALTIJD VERBONDEN** met het internet.



Mobiele browsers geven de url's weer op een klein scherm. Op het **COMPACTE SCHERMFORMAAT** is het vaak moeilijk om te beoordelen of het domein betrouwbaar is.

Vanwege het persoonlijke karakter van een mobiele telefoon, zijn gebruikers geneigd om **ANDERE GEBRUIKERS AUTOMATISCH TE VERTROUWEN.**

WAT KUNT U DOEN?

Wees alert als een bedrijf u telefonisch of via sms vraagt om uw persoonlijke gegevens. Om te verifiëren of het bericht/telefoongesprek legitiem is, kunt u direct contact opnemen met het bedrijf door het officiële telefoonnummer te bellen.

Als u op internet surft met uw mobiele apparaat, let er dan op dat u websites bezoekt via HTTPS. U kunt dit altijd controleren door te kijken naar het begin van de url.

Klik nooit op een link of bijlage in een ongewenste e-mail of sms, maar verwijder de berichten direct.

Let ook goed op bij websites met grammaticale fouten, spelfouten en een lage resolutie.

Schakel automatische updates in. Installeer, indien mogelijk, een mobiele-beveiligingsapp die u op de hoogte stelt van verdachte activiteiten.

EUROPOL EC3 European Cybercrime Centre | POLITIE | ALERT online | Betaalvereniging Nederland

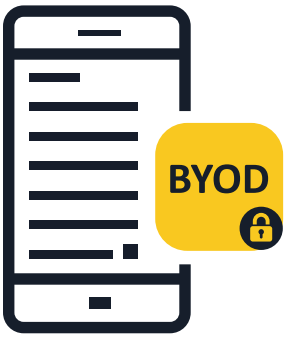
#MobileMalware

MOBIELE MALWARE

TIPS EN ADVIEZEN VOOR BEDRIJVEN

1 Informeer uw personeel over de risico's van mobiele apparaten

- Door 'mobiel werken' vervagen de grenzen tussen zakelijk en persoonlijk gebruik. Bedrijven kunnen schade oplopen als gevolg van een aanval die in eerste instantie gericht was op het mobiele apparaat van een individu. Een mobiel apparaat is een computer en moet ook beveiligd zijn.



2 Voer een bring-your-own-device-beleid (BYOD) in binnen uw bedrijf

- Medewerkers die hun eigen apparaten gebruiken om toegang te krijgen tot de gegevens en systemen van hun bedrijf moeten de bedrijfsrichtlijnen volgen – ook als ze slechts hun e-mail, kalender of contactpersonen gebruiken. Selecteer de technologieën die u gebruikt om mobiele apparaten te beheren en beveiligen zorgvuldig en zorg ervoor dat uw medewerkers voorzichtig te werk gaan.

3 Zorg ervoor dat uw veiligheidsarchitectuur ook een mobiele-beveiligingsbeleid bevat

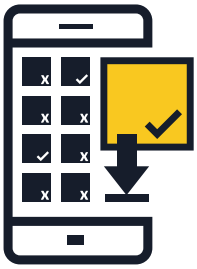
- Als een apparaat niet voldoet aan de beveiligingseisen, mag het niet gebruikt worden om verbinding te maken met het bedrijfsnetwerk of om bedrijfsgegevens te openen. Bedrijven moeten hun eigen Mobile Device Management- (MDM) of Enterprise Mobility Management-oplossingen (EMM) implementeren.
- Daarnaast is het verstandig ze ook een Mobile Threat Defence-oplossing (MTD) installeren. Dit verhoogt de zichtbaarheid en contextuele bewustwording van de risico's die apps, netwerken en besturingssystemen met zich meebrengen.

4 Let op bij het openen van bedrijfsgegevens via openbare Wi-Fi-netwerken

- De meeste openbare Wi-Fi-netwerken zijn niet beveiligd. Als een medewerker bedrijfsgegevens opent via een onbeveiligd Wi-Fi-netwerk op een vliegveld of in een café, kunnen deze gegevens ingezien worden door onbevoegde personen. Om dit te voorkomen, kunnen bedrijven een beleid voor 'effectief gebruik' implementeren.

5 Zorg ervoor dat uw besturingssystemen en apps actueel zijn

- Adviseer uw medewerkers om software-updates voor het besturingssysteem van hun mobiele apparaten te downloaden zodra deze beschikbaar zijn. Met name voor Android-systemen is het verstandig om onderzoek te doen naar het updatebeleid van mobiele providers en de fabrikanten van mobiele telefoons. Door de meest recente updates te installeren, zorgt u er niet alleen voor dat uw apparaat beter beveiligd is, maar ook dat het beter werkt.



6 Installeer alleen apps van betrouwbare bronnen

- Bedrijven moeten ervoor zorgen dat er alleen apps van officiële bronnen zijn geïnstalleerd op mobiele apparaten die verbinding maken met het bedrijfsnetwerk. Zo kunnen zij bijvoorbeeld een bedrijfs-appstore oprichten, waar eindgebruikers alleen door het bedrijf goedgekeurde apps kunnen openen, downloaden en installeren. Neem contact op met uw beveiligingsleverancier voor hulp met de installatie of het opzetten van uw eigen appstore.

7 Jailbreaking tegengaan

- Bij een jailbreak worden de veiligheidsbeperkingen van het besturingssysteem verwijderd, waardoor gebruikers volledige toegang krijgen tot het besturingssysteem en alle hieraan gekoppelde functies. Door uw mobiele apparaat te jailbreaken, kunt u verborgen beveiligingsproblemen blootleggen, waardoor u een verhoogd veiligheidsrisico loopt. Het gebruik van apparaten met root-functionaliteit moet binnen de bedrijfsomgeving verboden zijn.

8 Overweeg cloudgebaseerde opslagsystemen

- Mobiele gebruikers hebben vaak toegang nodig tot belangrijke documenten; niet alleen via hun werkcomputer, maar ook buiten het kantoor met hun eigen telefoon of tablet. Bedrijven kunnen een beveiligd, centrale opslag - en synchronisatiesysteem opzetten om op een veilige manier aan deze behoefte tegemoet te komen.

9 Motiveer uw medewerkers om een mobiele-beveiligingsapp te installeren

- Alle besturingssystemen kunnen geïnfecteerd raken met een virus. Zorg er, indien mogelijk, voor dat uw medewerkers een mobiele-beveiligingsoplossing gebruiken die malware, spyware en kwaadwillende apps opspoort en elimineert, en daarnaast beschikt over andere privacygerelateerde en antidiefstalfuncties.

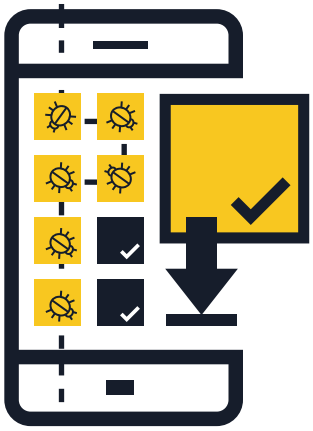
EUROPOL EC3 European Cybercrime Centre | POLITIE | ALERT online | Betaalvereniging Nederland

#MobileMalware

MOBIELE MALWARE

TIPS EN ADVIEZEN DIE U HELPEN OM UZELF TE BESCHERMEN

1 Installeer alleen apps van betrouwbare bronnen



- **Koop uw apps alleen bij bekende appstores** — als u een app wilt installeren, doe dan eerst onderzoek naar de uitgever en de app zelf. Pas op voor e-mails of sms-berichten met links erin. Via dit soort links kunnen er onbedoeld apps van derde partijen of onbekende bronnen geïnstalleerd worden.
- **Lees de recensies en beoordelingen,** als die er zijn, van andere gebruikers.
- **Neem de toegangsinstellingen van de app zorgvuldig door** — controleer tot welke gegevens de app toegang heeft en of deze gegevens gedeeld kunnen worden met externe partijen. Download de app niet als u de gebruiksvoorwaarden verdacht vindt of niet vertrouwt.

2 Klik niet op links of bijlagen in ongewenste e-mails of sms-berichten

- **Klik niet op links in ongewenste e-mails of sms-berichten** (sms en mms) — maar verwijder ze direct na ontvangst.
- **Controleer ingekorte url's of QR-codes** — Deze kunnen u namelijk doorsturen naar schadelijke websites of direct malware installeren op uw apparaat. Gebruik een url-previewsite om te zien of het webadres betrouwbaar is voordat u erop klikt. Als u een QR-code wilt scannen, gebruik dan een QR-reader die een preview geeft van het gekoppelde webadres en beveiligingssoftware die u waarschuwt bij risicovolle links.

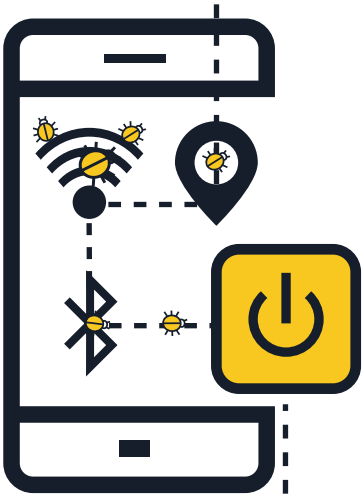
3 Log uit van websites nadat u een betaling heeft gedaan

- **Sla uw gebruikersnamen en wachtwoorden nooit op in uw mobiele browser of apps** — als uw telefoon of tablet verloren raakt of gestolen wordt, kan iedereen inloggen op uw accounts. Zodra de internetbetaling voltooid is, moet u uitloggen van de website en niet alleen maar uw browser sluiten.
- **Kijk uit met online bankzaken of aankopen via een openbaar Wi-Fi-netwerk** — gebruik hiervoor uitsluitend bekende en betrouwbare netwerken.
- **Controleer de url van de website** — let erop dat het webadres klopt voordat u inlogt of gevoelige informatie invoert. Download de officiële app van uw bank om ervoor te zorgen dat u altijd verbonden bent met de juiste website.

4 Zorg ervoor dat uw besturingssysteem en apps actueel zijn

- **Zorg ervoor dat u de meest recente updates installeert voor het besturingssysteem van uw mobiele apparaat** — deze updates zorgen er niet alleen voor dat uw apparaat beter beveiligd is, maar ook dat het beter werkt.

5 Schakel uw Wi-Fi, locatievoorzieningen en Bluetooth uit als u ze niet gebruikt



- **Schakel Wi-Fi uit als u het niet gebruikt** — als de verbinding niet goed beveiligd is, kunnen cybercriminelen toegang krijgen tot uw gegevens. Gebruik, indien mogelijk, een 3G- of 4G-verbinding in plaats van hotspots. U kunt uw gegevens ook beveiligen door middel van een virtual private network (VPN).
- **Geef uw apps geen onnodige toegang tot uw locatievoorzieningen** — deze informatie kan gedeeld of gelekt worden, of gebruikt worden om u push-ads te sturen op basis van uw locatie.
- **Schakel Bluetooth uit als u het niet gebruikt** — controleer of het volledig uitgeschakeld is en niet slechts in 'onzichtbare' modus staat. Bluetooth staat standaard vaak zo ingesteld dat anderen zonder uw toestemming verbinding kunnen maken met uw apparaat. Kwaadwillende gebruikers zouden op deze manier uw bestanden kunnen kopiëren of toegang kunnen krijgen tot andere apparaten die verbonden zijn met uw Bluetooth. Ook zouden ze toegang kunnen krijgen tot uw telefoon, zodat ze kunnen bellen of sms-berichten kunnen sturen, wat kan leiden tot torenhoge rekeningen.

6 Houd uw persoonlijke gegevens geheim

- **Geef uw persoonlijke gegevens nooit door** als u daarom gevraagd wordt in sms-berichten of e-mails die van uw bank of een ander gerenommeerd bedrijf lijken te zijn. In deze gevallen kunt u contact opnemen met de betreffende instantie om het verzoek om informatie te verifiëren.
- **Controleer uw mobiele-rekeningoverzichten regelmatig op verdachte afschrijvingen** — als u bepaalde transacties niet herkent, neem dan direct contact op met uw bank.

7 Jailbreak uw apparaat niet

- Bij een jailbreak worden de veiligheidsbeperkingen van het besturingssysteem verwijderd, waardoor gebruikers volledige toegang krijgen tot het besturingssysteem en alle hieraan gekoppelde functies — **Door uw mobiele apparaat te jailbreaken** kunt u verborgen beveiligingsproblemen blootleggen, waardoor u een verhoogd veiligheidsrisico loopt.

8 Maak back-ups van uw gegevens

- **Veel smartphones en tablets bieden u de mogelijkheid om draadloos back-ups te maken van uw gegevens** — bekijk de opties die uw besturingssysteem biedt. Als u een back-up van uw smartphone of tablet heeft gemaakt, kunt u uw persoonlijke gegevens heel eenvoudig herstellen als uw apparaat verloren is geraakt, of als het gestolen of beschadigd is.

9 Installeer een mobiele-beveiligingsapp

- Alle besturingssystemen kunnen geïnfecteerd raken met een virus. Gebruik, indien mogelijk, **een mobiele-beveiligingsoplossing** die malware, spyware en kwaadwillige apps opspoort en elimineert, en daarnaast beschikt over andere privacygerelateerde en antidiefstalfunctie.