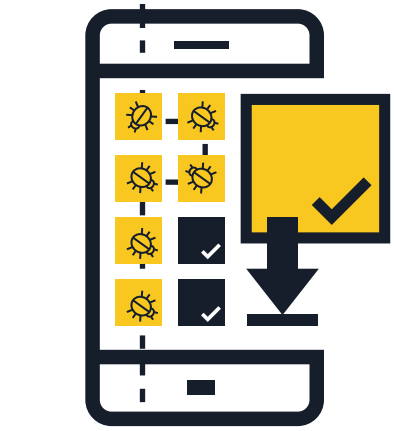
MOBIELE MALWARE

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.

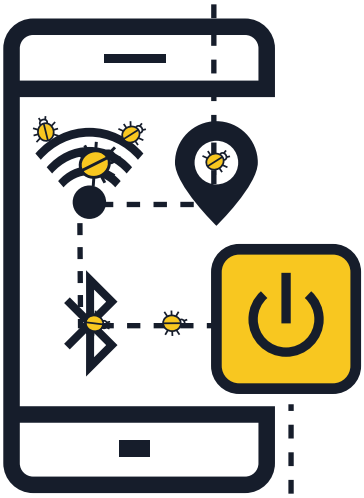
3 Log uit van websites nadat u een betaling heeft gedaan

- **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.
- **Doe geen 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).

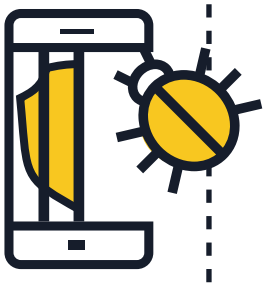
■ **Geef uw apps geen onnodige toegang tot uw locatievoorzieningen** — deze informatie kan gedeeld of gelekt worden, of gebruikt worden om u push-ads te sturen op basis van uw locatie.

■ **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. Kwaadwillige 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 serviceprovider.



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 antidiefstalfuncties.

EUROPOL EC3 European Cybercrime Centre

Police Politie

#MobileMalware