DIRKJAN VAN ITTERSUM

VEILIG ONLINE

MET JE SMARTPHONE

consumentenbond

1e druk, juli 2019

Auteur: Dirkjan van Ittersum
Verder werkten mee: Ronald Kamp (Consumentenbond), Mediaeval Tekst en Vorm, Nijmegen
Eindredactie: Lisa van Rens
Grafische verzorging: PUUR Publishers
Beeld omslag: PUUR Publishers

ISBN 978 905951 4416
NUR 988

INHOUD

INLEIDING

In korte tijd heeft de smartphone een grote plek in ons leven gekregen. Het kleine apparaat bewaart een schat aan (persoonlijke) informatie. Die mag niet zomaar in vreemde handen vallen.
Toch is de kans op digitale ongelukken aanwezig, al was het maar omdat het toestel overal mee naartoe gaat. Je kunt het apparaat kwijtraken of het kan gestolen worden. Ook bestaat het gevaar slachtoffer te worden van een digitale inbraak, bijvoorbeeld via een wifihotspot.
Eenmaal 'binnen' op de smartphone kan een crimineel voor flink wat ellende zorgen. Veel mensen gebruiken een bankapp. Als de hacker daarop inbreekt, is er risico op forse financiële schade. En met toegang tot je e-mail kan een crimineel ook bij alle gekoppelde diensten, en zo je hele digitale leven overnemen.

Neem maatregelen om digitale risico's zo klein mogelijk te maken

Gelukkig zijn er eenvoudige maatregelen mogelijk waardoor de kans op zo'n digitale inbraak een stuk kleiner wordt. Beveilig de toegang van het toestel en zorg voor veilige instellingen. Daarnaast kun je beschermen door een aantal gedragsregels, bijvoorbeeld bij het downloaden van apps en mobiel bankieren, in acht te nemen. Door je daaraan te houden, wordt de kans dat een cybercrimineel vat op je gegevens krijgt een stuk kleiner. Een back-up van je gegevens is onmisbaar als het toch mis is gegaan. In hoofdstuk 5 leggen we uit hoe je daarvoor zorgt.

Dit boek helpt niet alleen bij het buiten de deur houden van oplichters, hackers en malware. We besteden ook aandacht aan privacy. Advertentiebedrijven gebruiken

de smartphone om je digitale leven in kaart te brengen, bijvoorbeeld welke websites je bezoekt. Adverteerders gebruiken die informatie om je te kunnen bestoken met gepersonaliseerde advertenties. Het volgen gebeurt niet alleen via websites, maar ook via apps. Gelukkig kun je de advertentiebedrijven vaak de pas afsnijden.

Smartphones kennen meer veiligheidsrisico's dan telefoons zonder internetverbinding. Telefoons waarop je geen apps kunt installeren (ook wel 'dumbphones' genoemd) kunnen veel minder. Daardoor zijn ze over het algemeen veiliger, maar ze zijn ook minder aantrekkelijk om te kopen. Sommige tips gelden ook voor dumbphones, zoals het aanmaken van een beveiligingscode en de adviezen rond phishing. Veel tablets gebruiken ook Android of iOS. De tips gelden ook voor die apparaten.

De Android-schermafbeeldingen in dit boek zijn gemaakt met een Samsung-smartphone, het bestverkochte merk Android-smartphones. Op een Android-toestel van een ander merk kan de werkwijze net wat anders zijn.

Foto auteur: Michel Walraven

Dirkjan van Ittersum is webondernemer, IT-journalist en auteur van computerboeken. Hij verkent enthousiast de mogelijkheden van nieuwe technologie en geeft er graag uitleg over.

1

WAT ZIJN DE RISICO'S?

Internet op de smartphone is volledig ingeburgerd. We appen, mailen en surfen massaal op het kleine scherm. Dat is niet zonder risico. In dit hoofdstuk leggen we uit welke gevaren er zijn.

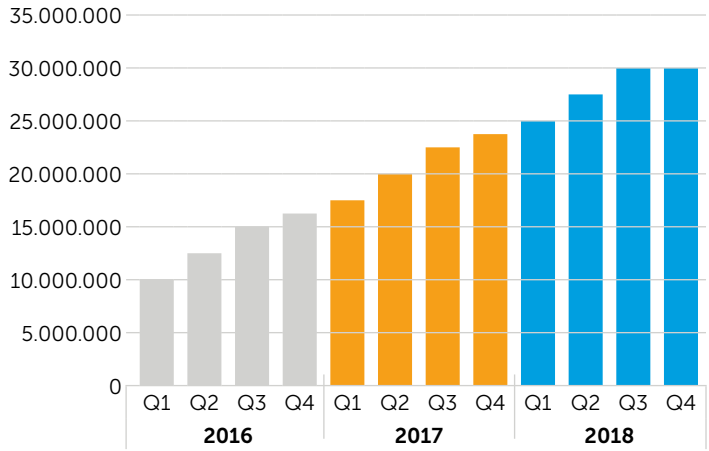
De meeste mensen weten wel dat een computer vatbaar is voor virussen, phishing en hackers, maar dat smartphones aan vergelijkbare gevaren blootstaan, blijft vaak onderbelicht. Ten onrechte, want juist omdat we de mobiele telefoon zo vaak gebruiken en er zo veel persoonlijke gegevens op staan, zijn de risico's niet te onderschatten. Er verschijnen regelmatig berichten in de media over virussen en oplichtingspraktijken op de mobiel.
Het is belangrijk om te beseffen dat internet op de mobiel meer is dan het bezoeken van een website of het versturen van e-mail. Internet komt overal om de hoek kijken. Veel apps gebruiken internet om continu gegevens op te halen. Denk aan Facebook, WhatsApp en Instagram, maar ook aan games, navigatie-, foto- en boekenapps. Daarmee vormen al deze apps – in meer of mindere mate – een risico.

Media berichten regelmatig over mobiele virussen en hackers.

1.1 Steeds meer smartphones

Volgens recente cijfers heeft 87% van de Nederlanders tussen de 16 en 75 jaar een smartphone. Met dergelijke aantallen vormen de apparaten een aantrekkelijk doelwit voor cybercriminelen. Niet verrassend dus dat er in 2018 een flinke stijging was van het aantal virussen en andere malware op de mobiele telefoon. Figuur 1 toont de hoeveelheid door antivirusbedrijf McAfee gesignaleerde malware wereldwijd.

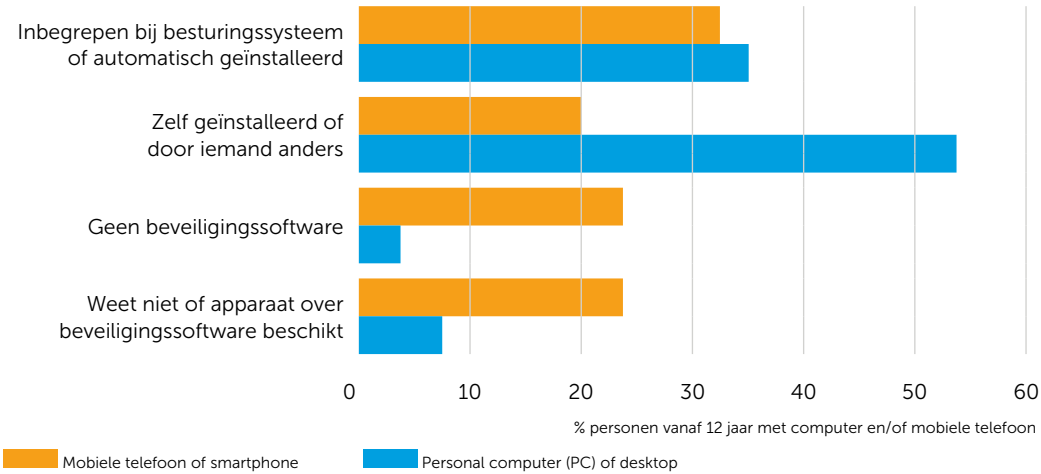
Figuur 1 Door McAfee gesignaleerde mobiele malware



Bron: McAfee Mobile Threat Report Q1, 2019.

Dat veel mensen de gevaren op smartphones onderschatten, blijkt uit cijfers van het Centraal Bureau voor de Statistiek (CBS). Slechts 52% van de gebruikers (ouder dan 12 jaar) heeft beveiligingssoftware op de smartphone. Een kwart weet niet of er sprake is van enige vorm van beveiliging. Op de computer is het beeld heel anders: daar gebruikt 89% een antivirusprogramma.

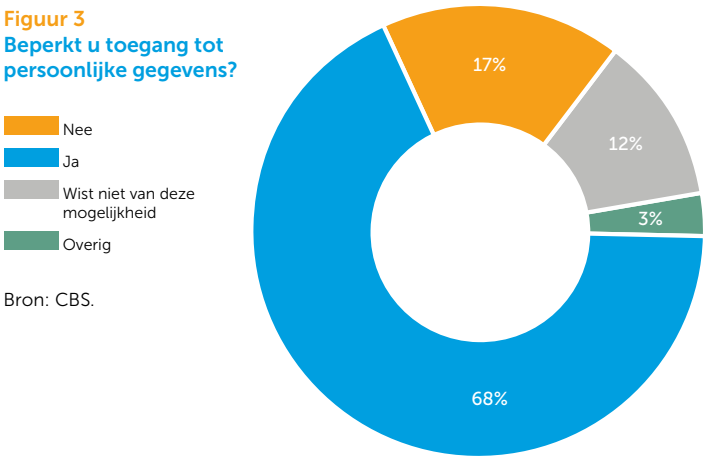
Figuur 2 Gebruik van beveiligingssoftware in 2017



Bron: CBS, ICT-gebruik huishoudens en personen.

Er is ook goed nieuws van het CBS, want veel smartphonegebruikers nemen wel maatregelen om hun privacy te beschermen. 68% zegt bij het gebruiken van een app weleens de toegang tot persoonlijke gegevens, bijvoorbeeld locatie, foto's of contactpersonen, te weigeren. Toch heeft nog altijd 17% dat nooit gedaan en weet 12% niet dat blokkeren mogelijk is. Vooral jongeren blokkeren toegang. Ouderen zijn relatief vaak niet op de hoogte van de mogelijkheden hiertoe.

Figuur 3
Beperkt u toegang tot persoonlijke gegevens?



Bron: CBS.

1.2 Android en iOS domineren

Smartphones beschikken over een besturingssysteem dat alle losse onderdelen tot een geheel maakt en zorgt dat je de functies van je telefoon kunt gebruiken. Op smartphones staan apps en je kunt zelf extra apps installeren om de functionaliteit uit te breiden. Waar we bij smartphones over apps praten, gebruiken we bij computers meestal de term software (of programma's).
Smartphones die Android gebruiken als besturingssysteem worden in Nederland het meest verkocht. Het marktaandeel ligt op ruim 60%. iPhones van Apple, met daarop het besturingssysteem iOS, volgen met 30%. Telefoons met andere besturingssystemen worden nauwelijks verkocht en laten we buiten beschouwing.

Account verplicht

Om optimaal gebruik te maken van smartphones stellen zowel Google als Apple het aanmaken van een account verplicht. Alleen dan is het mogelijk om apps te downloaden.

1.2a Android

Google is de drijvende kracht achter Android. Het besturingssysteem staat op toestellen van meerdere fabrikanten, waaronder Samsung, LG, Huawei, Xiaomi en Sony. In vergelijking met iOS biedt Android de gebruiker en app-ontwikkelaars wat meer vrijheid. Dat klinkt goed, maar het brengt risico's met zich mee. Zo is de controle van apps in de Google Play Store niet waterdicht. Er staat regelmatig malware in de appstore. Ook kan de gebruiker buiten de officiële winkel om apps installeren (al staat die mogelijkheid standaard uit). Dat biedt kansen voor kwaadaardige app-ontwikkelaars.
Bij de keuze voor Android is het belangrijk om te bedenken dat Google informatie verzamelt om het persoonlijke profiel van de gebruiker mee aan te vullen. Google kan bijvoorbeeld bijhouden welke apps je installeert en welke sites je (via Chrome) bezoekt. Dit profiel gebruikt Google om toegespitste advertenties te tonen bij onder meer zoekresultaten en YouTube-video's, maar ook op websites van derde partijen.

1.2b iOS

Op alle iPhones (en iPads) van Apple staat iOS. Het systeem is stevig dichtgetimmerd. Apps buiten de App Store om installeren is niet mogelijk, tenzij je het apparaat hackt (zie kader). De controle van apps in de App Store is streng, waardoor schadelijke apps er niet vaak doorglippen. Omdat Apple vindt dat het virussen voor iOS zelf voldoende kan blokkeren, worden virusscanners niet toegelaten in de appwinkel. Helemaal vrij van virussen zijn iPhones echter niet. In 2014 en 2016 werden er programma's gevonden voor Mac-computers die een verbonden iPhone konden besmetten.

Apple controleert apps niet alleen op kwaadaardige intenties, maar ook op inhoud. Sommige apps worden op inhoudelijke gronden geweigerd. Om iOS te gebruiken heb je wel een Apple-account nodig, maar dit wordt niet gebruikt om een persoonlijk profiel op te bouwen voor het tonen van advertenties. Een account is nodig om apps te kunnen downloaden uit de App Store.

Niet jailbreaken

De meeste virussen voor iOS-apparaten zijn gericht op toestellen die gejailbreakt zijn. Hiermee kraakt een gebruiker zijn eigen apparaat om bijvoorbeeld apps buiten de App Store om te installeren. Zo wordt het systeem direct een stuk minder veilig. We raden jailbreaken daarom af.

1.3 Vormen van cybercriminaliteit

Internetcriminelen hebben een breed arsenaal aan trucs om slachtoffers te maken via smartphones. Ze proberen bijvoorbeeld toegang te krijgen tot een bankrekening om geldbedragen naar zichzelf over te schrijven. Ook kan er sprake zijn van chantage, waarbij het slachtoffer onder dreiging geld afhandig wordt gemaakt. Verkoopsites, zoals Marktplaats en eBay, zijn andere bekende voorbeelden. Dat zijn op zich bonafide sites (en apps), maar er is geregeld sprake van oplichting (zie par. 7.3).

Cyberpesten

Een heel ander probleem is cyberpesten, waarbij het slachtoffer te maken krijgt met ongewenst gedrag van veelal anonieme bekenden, bijvoorbeeld nare (anonieme) berichten via WhatsApp. Cyberpesten komt zowel onder jongeren als volwassenen voor. Cyberpesten kan overgaan in cyberstalking als een slachtoffer continu wordt lastiggevallen.

1.3a Phishing

Phishing is niet alleen op de computer een probleem, maar ook op smartphones. Criminelen hengelen via nepberichten naar privéinformatie als inlogcodes. Over het algemeen gebruiken ze daarvoor phishingwebsites. Dat zijn bijvoorbeeld valse websites die sprekend lijken op de officiële website van een bank.

Lange tijd kwamen phishingberichten vooral per mail binnen, maar criminelen hebben hun werkterrein uitgebreid. Ze sturen de berichten via allerlei mogelijke kanalen, zoals sms, WhatsApp, Twitter, Facebook enzovoort. Zelfs datingapps zijn niet vrij van phishingpogingen.

Het taalgebruik in phishingmails was vroeger slecht, op het lachwekkende af. Daardoor pikte je de pogingen er zo uit. Inmiddels is dat verbeterd. Ook de phishingpogingen via sms en chatapplicaties zijn nu vaak geraffineerd. Het doel van phishing is bijna altijd het achterhalen van persoonlijke gegevens, zodat de crimineel bijvoorbeeld bij je banksaldo kan. Phishing op smartphones neemt toe en is vaak lastiger te doorzien dan op de desktop en laptop, omdat links en webadressen minder goed zichtbaar zijn. Dit komt onder meer door de beperkte schermgrootte en het veelvuldige gebruik van verkorte linkjes. In par. 6.4 leggen we uit hoe je phishing herkent.

1.3b Malware

Malware is kwaadaardige software. Criminelen die malware verspreiden, zijn vaak uit op persoonlijke, inlog- of bankgegevens of proberen slachtoffers ergens voor te laten betalen. Een infectie met malware kan zich op verschillende manieren voltrekken. De schadelijke software kan binnendringen doordat er beveiligingsfouten in het besturingssysteem op de telefoon zitten. Ook kan de gebruiker zelf per ongeluk een verkeerde app installeren. Tot slot blijkt soms op het oog legitieme software toch te beschikken over nare kantjes, bijvoorbeeld spyware of adware. Hierna volgen enkele veelvoorkomende vormen van malware.

- **Ransomware** Dit is gijzelsoftware die persoonlijke bestanden ontoegankelijk maakt. Pas na betaling worden de bestanden vrijgegeven. Dat is althans de belofte, want je ontvangt niet altijd de code om het apparaat te ontgrendelen. Bovendien houd je het systeem in stand door te betalen. Niet doen dus. Om je hiertegen te wapenen is het belangrijk een back-up te maken (zie hoofdstuk 5). Ransomware komt gelukkig lang niet zo veel voor als op de pc, maar er zijn wel enkele varianten die Android-telefoons op de korrel nemen.
- **Sms-malware** Deze malware is in staat om neptelefoontjes en -berichten te versturen naar contacten in het adresboek. De berichten bevatten links naar schadelijke sites of apps. Ook zijn er apps die de gebruiker ongevraagd abonneren op betaalde sms-diensten. Soms kosten ze wel €7,50 per week. Doordat niet iedereen regelmatig zijn bankrekening controleert, kan de schade flink oplopen.
- **Banking malware** Dit is software die bankgegevens onderschept en zo veel schade kan aanrichten. Er zijn verschillende vormen. Het kan gaan om nep-bankapps die op het eerste gezicht van de bank afkomstig lijken te zijn. Er bestaan ook malafide apps die een onzichtbare laag over de echte bankapp tonen en zo gegevens afvangen. Deze vorm van malware werd in het afgelopen jaar veel gesignaleerd door antivirusbedrijven. Soms worden de nep-bankapps geïnstalleerd door onschuldig ogende, maar malafide apps als een zaklamp-app. In 2017 werden dergelijke apps zelfs in de Google Play Store gesignaleerd.
- **Spyware** Deze software kijkt continu mee met wat de gebruiker doet. Zodra bepaalde informatie (bijvoorbeeld creditcardnummer of wachtwoord) wordt ingevoerd, stuurt de software de gegevens door naar de cybercrimineel.
- **Adware** Hoewel deze malware niet zo schadelijk is, is de software wel hinderlijk. Adware zorgt voor pop-ups met advertenties. Het risico bestaat dat er advertenties in beeld komen die schadelijke apps willen installeren.

WhatsApp-fraude

Criminelen proberen mensen geld afhandig te maken door zich via chatapps als WhatsApp voor te doen als een goede bekende. Ze gebruiken hiervoor een eigen account (en verzinnen een smoes over bijvoorbeeld een nieuwe telefoon) of ze breken in en nemen een bestaand profiel over.

1.3c Tikkie-fraude

Via Tikkie kun je iemand terugbetalen die iets heeft voorgeschoten. Handig, maar niet zonder risico. Criminelen gebruiken Tikkie om mensen geld afhandig te maken. De crimineel vindt zijn slachtoffers vaak via Marktplaats, maar ook via eBay en Tweedehands.be. Hij toont interesse in een product en vraagt de verkoper 1 cent over te maken via Tikkie. Zogenaamd om er zeker van te zijn dat hij het bedrag naar de juiste persoon overmaakt. Hij verstuurt een neplink, die leidt naar een nagebouwde betaalsite. Wie daar zijn gegevens invult, loopt grote kans dat zijn bankrekening wordt geplunderd. Het adres moet beginnen met https://tikkie.me.

1.3d Marktplaatsoplichting

Dagelijks komen bij de politie 70 aangiftes binnen van Marktplaatsoplichting. De hiervoor genoemde Tikkie-fraude komt via Markplaats voor, maar er zijn meer risico's. Zo kan het gebeuren dat je een product opstuurt, maar nooit betaald krijgt (zie par. 7.3). Wees ook bedacht voor valse bankapps als een koper een product bij je op komt halen.

1.3e Winacties

Via e-mail en sociale media worden nep-winacties verspreid. Aanbieders beloven honderden euro's aan waardebonnen of het gratis testen van producten. Daarvoor moet je bellen met een duur betaalnummer en een eindeloos lange quiz volbrengen. Naar de waardebonnen of producten kun je fluiten.

Mobiele botnets

Een botnet is een verzameling gehackte computers die door een cybercrimineel wordt ingezet om bijvoorbeeld sites plat te leggen of massaal spam te versturen. Doordat smartphones tegenwoordig behoorlijk krachtig en altijd online zijn, worden ze inmiddels ook gebruikt voor botnets. Malware op de smartphone kan dus als doel hebben het apparaat toe te voegen aan zo'n botnet.

Bewustwording onder jongeren

Recent deed de politie een proef onder scholieren. Ze kregen een linkje toegestuurd met de belofte in te kunnen breken op een Instagramaccount of speelgeld te kunnen stelen bij het spel Fortnite. Bijna tienduizend scholieren klikten op de link. Ze kwamen terecht op een waarschuwingspagina van de politie. Zo'n 40% van de scholieren zei niet te weten dat dergelijke activiteiten strafbaar zijn.

1.4 Hoe raak je besmet met malware?

1.4a Appstores

Een besmetting met malware kan komen doordat je zelf een malafide app hebt gedownload. Controles door Google en Apple kunnen niet altijd voorkomen dat apps van ontwikkelaars met verkeerde bedoelingen in de appstores terechtkomen. Veel van deze apps doen zich voor als legitieme apps. Het gaat niet zelden om games, waarbij ontwikkelaars graag inspelen op hypes. Zo waren er, nog voordat het spel Fortnite in de Google Play Store stond, diverse apps die de naam Fortnite misbruikten. De apps bleken de gebruiker te bespioneren of te vragen om toegang tot allerlei gegevens (zie par. 4.2a). Vaak zijn het simpele apps met achtergronden of fotofilters.