Beveilig je **SMARTPHONE**

Inhoud

1. WAT ZIJN DE RISICO'S? 9

HET KAN IEDEREEN OVERKOMEN 10
- **Besturingssystemen** 10
  - Android 10
  - iOS 11
- **Cybercriminaliteit** 11
  - Phishing 11
  - Malware 13
  - Tweedehandssites 14
  - Winacties 14
  - WhatsApp 14
- **Hoe raak je besmet met malware?** 15
  - Via apps 15
  - Via websites 15
- **Risico's voor de privacy** 16
  - Spiedende bedrijven 16
  - Meeluisterende overheid 17
  - Identiteitsfraude 17

2. TOEGANG BLOKKEREN 19

TOESTEL VERGRENDELEN 20
- **Pincode** 20
- **Sensor** 22
  - Vingerafdruk 22
  - Gezichtsherkenning 22

AUTHENTICATIE VERHINDEREN 25

PINCODE VAN DE SIMKAART WIJZIGEN 26

ACCOUNTS BEVEILIGEN 27
- **Tips voor een goed wachtwoord** 28
- **Een wachtwoordmanager helpt** 28
  - Eerst je wachtwoorden in de browser verwijderen 29
  - Daarna een wachtwoordmanager instellen 30
- **Onze keuze: Bitwarden** 31
- **iCloud-sleutelhanger** 33

3. VEILIGE INSTELLINGEN 35

PRIVÉGEGEVENS AFSCHERMEN 36
- Gegevens versleutelen 36
- Wifiverbinding beveiligen 38
  - Check het type beveiliging 38
  - Voorzichtig met wifihotspots 39
  - Automatische verbinding uitzetten 40
- VPN-netwerken 41
  - Hoe kies je een VPN-aanbieder? 41
- Systeemupdates uitvoeren 42
- Beveiligingsupdates voor Android 45
- Beveiligingsapps 47
  - Malware op Android-toestellen 47
  - Toch getroffen? 48

LOKALISEREN NA VERLIES OF DIEFSTAL 48
- Standaardfuncties activeren 48
- Antidiefstalfunctie controleren 49
- Wat moet je doen na verlies of diefstal? 53

CONTENT VERWIJDEREN 54

4. APPS BEHEREN 57

APPS DOWNLOADEN 58
- Opdringerige apps 59
  - Toegangsrechten controleren 59
- Gerichte advertenties 64
- Ouderlijk toezicht 66
  - Toestel delen 70
- Meldingen beperken of uitschakelen 71
- Apps updaten 72
  - Automatische updates 74
- Ongebruikte apps verwijderen 75
- Dubbele authenticatie 77

5. BACK-UPS MAKEN 81

RESERVEKOPIEËN MAKEN 82

Back-up in Android 82
- Back-up van gegevens 83
- Back-up van foto's en video's 84
- Back-up van bestanden en mappen 85
- Android-toestel opnieuw instellen 86
- Back-up terugzetten 87
- Lokale back-up 88

Back-up in iOS 89
- Back-up via iCloud 90
- iPhone opnieuw instellen 91
- Back-up terugzetten 92
- Lokale back-up 93

Back-up van Samsung 95
- Back-up in de cloud 95
- Back-up terugzetten 96
- Lokale back-up 96

Back-up van contacten 98

Clouddiensten voor back-ups 102

Back-up van WhatsApp 102

6. SURFEN ZONDER RISICO'S 103

NIET AFWACHTEN MAAR HANDELEN 104

Geschikte browser 104
- Firefox 104
- Safari 106
- Chrome 107
- Samsung Internet 107
- Opera 107
- Edge 108
- Overige browsers 109

Advertenties tegenhouden 109
- Cookies verwijderen 109
- Cookies van derden weigeren 118
- Advertenties blokkeren 123

Zoekmotors met een hart voor privacy 127
- Phishing vermijden 133
- Zit je op een versleutelde verbinding? 136

7. ONLINE SHOPPEN 137

RISKANTE TRANSACTIES 138

Online betalen 138

De app van je bank 139

App installeren 139

Toegang beveiligen 139

Zuivere betaalapps 140

Bancontact Pay 140

Apple Pay 140

Google Pay 141

Wero 141

Gewiekste oplichters 141

Betalingen op tweedehandssites 141

Transactie bevestigen met QR-code 142

Misbruik met Itsme 143

Contactloos betalen 143

PRIVÉGEGEVENS AFSCHERMEN

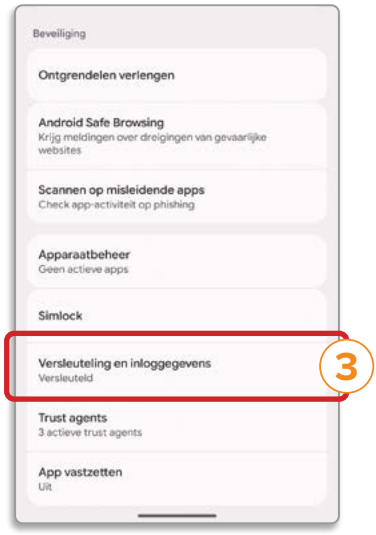
Met onze smartphone dragen we een groot deel van ons leven in onze broekzak. Privégegevens beveiligen is dus geen optie maar een noodzaak. In het vorige hoofdstuk zag je hoe je je apparaat kunt beveiligen. Nu bekijken we hoe je je privégegevens kunt beschermen.

Gegevens versleutelen

Door alle gegevens op het toestel te versleutelen, is de kans klein dat een crimineel met je persoonlijke informatie aan de haal gaat. Op steeds meer toestellen is de inhoud automatisch versleuteld. Controleer dat voor de zekerheid en zet deze optie indien nodig aan.

Android

Voor Android is een toegangscode vereist om de gegevens op het toestel te versleutelen. Als de code is ingesteld, worden de gegevens automatisch versleuteld. Let op: niet alle Android-toestellen volgen dezelfde stappen (hieronder: de stappen op een Google Pixel-apparaat met Android 16).



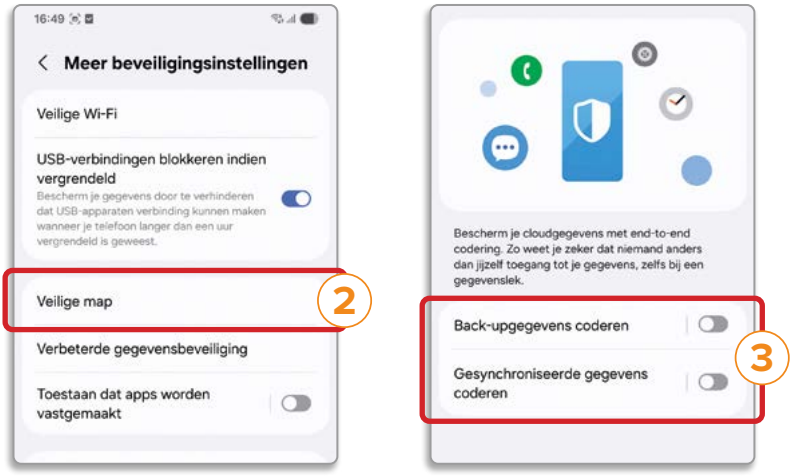
1. Tik op het icoon **Instellingen** en ga naar **Beveiliging en privacy**.
2. Tik helemaal onderaan op **Meer beveiliging en privacy**.
3. Onder **Versleuteling en inloggegevens** zie je of de inhoud versleuteld is.

Samsung

Naast de versleuteling van Android voegen de Galaxy-toestellen van Samsung een extra beveiligingslaag toe met de Knox-architectuur. Die is vooraf geïnstalleerd en staat standaard geactiveerd. Samsung Knox is gekoppeld aan de hardware en kan ook worden gebruikt om bedrijfssmartphones te beheren. Als het standaardbeveiligingsniveau niet voldoende is, kun je gevoelige bestanden of applicaties nog beter beveiligen op de telefoon, maar

ook in de Samsung-cloud. Daar kan je een veilige map aanmaken die alleen toegankelijk is via een toegangscode of biometrische gegevens (vingerafdruk, gezichtsherkenning).

1. De normale beveiliging staat standaard ingeschakeld. Als je het beveiligingsniveau wilt verhogen door een veilige map aan te maken, tik je op het icoon **Instellingen** en ga vervolgens naar **Beveiliging en privacy.**
2. Selecteer **Meer beveiligingsinstellingen** en kies **Veilige map**.
3. Als je ook de gegevensback-up in de Google-cloud wilt versleutelen, klik je op **Verbeterde gegevensbeveiliging** en schakel je **Gegevensversleuteling** in.



iOS

Als op de iPhone een pincode of wachtwoord is ingesteld, wordt de inhoud versleuteld. Dat kun je verifiëren via de instellingen. De toegangscode wordt gebruikt om de gegevens op het apparaat te versleutelen. Hoe sterker de toegangscode, hoe beter de gegevens op de telefoon beveiligd zijn.

1. Tik op het icoon **Instellingen** en kies **Face ID en toegangscode**.
2. Voer de toegangscode in.
3. Controleer of onderaan de melding “Gegevensbeveiliging is ingeschakeld” staat.

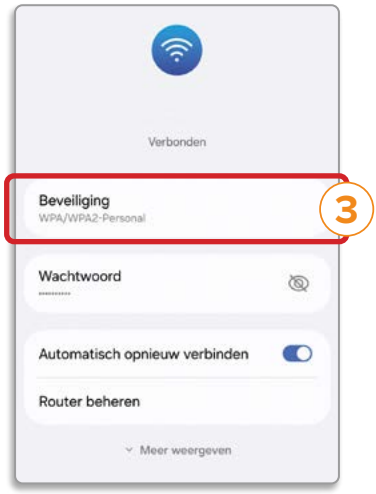
Wifiverbinding beveiligen

Om te voorkomen dat iemand meekijkt terwijl je via wifi verbonden bent met internet, is het belangrijk dat de wifiverbinding versleuteld is. De meeste beveiligde verbindingen maken gebruik van Wi-Fi Protected Access 2 (WPA2), die in 2006 het verouderde WPA en WEP opvolgde. Sinds eind 2019 zijn er ook producten op de markt die gebruikmaken van WPA3. Dat is nog veiliger dan WPA2.

Check het type beveiliging

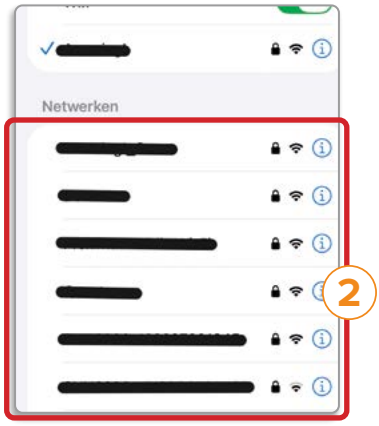
Via de wifi-instellingen kun je controleren of de verbinding beveiligd is. Er is niet altijd informatie over het type beveiliging beschikbaar.

Android



1. Tik op het icoon **Instellingen** en dan op **Verbindingen**.
2. Selecteer **Wifi**. Nu verschijnt de lijst met draadloze netwerken.
3. Tik op het tandwiel naast het netwerk waarmee je verbonden bent. Onder **Beveiliging** vind je informatie over het type beveiliging.

iOS



1. Tik op het icoon **Instellingen** en ga naar **Wifi**.
2. Je krijgt een lijst te zien met de sites waarop je surft. Als er een klein hangslotje te zien is naast het wifinetwerk waarmee je verbonden bent, dan is de verbinding beveiligd.

Voorzichtig met wifihotspots

Op veel plaatsen wordt gratis wifi aangeboden. Denk aan stations, luchthavens, hotels en restaurants. Toch raden we af om vertrouwelijke zaken, zoals internetbankieren en mailen, via een wifihotspot af te handelen. Voor een hacker is het niet moeilijk om een valse hotspot op te zetten en op die manier privéinformatie te stelen van mensen die verbinding met het netwerk maken. Door je bijvoorbeeld naar een nagemaakte banksite te leiden, kan hij je geld afhandig maken. De hacker zal de hotspot een legitiem uitziende naam te geven, bijvoorbeeld “WiFi Brussels Airport”.
Het gevaar komt niet alleen van valse wifihotspots. Een hacker kan vrij eenvoudig meelezen met het onversleutelde verkeer van anderen op een openbare hotspot. Volg deze tips wanneer je verbinding maakt met een openbare hotspot.

1. **Gebruik https.** Als een website gebruikmaakt van https, wordt alle informatie versleuteld verzonden en kan er niemand meekijken. Let dus op of het webadres begint met https. Kijk ook of er een klein hangslotje in de navigatiebalk staat.

2. **Let op waarschuwingen.** Waarschuwt de browser dat er iets mis is met een certificaat of verschijnt een andere waarschuwing dat de website niet veilig is? Bezoek de website dan niet. Mogelijk gaat het om een phishingsite.

3. **Log uit.** Doe dat meteen nadat je een website of app hebt bezocht die is beveiligd met een wachtwoord. Als iemand de verbinding aftapt, heeft hij geen toegang meer tot de website zonder in te loggen.

4. **Zet automatisch verbinden uit.** Stel je smartphone zo in dat hij niet automatisch verbinding maakt met een bekend netwerk (zie blz. 40). Als een hacker zich voordoet als dat netwerk, zal je smartphone niet vanzelf verbinding maken.

5. **Gebruik een VPN.** Door verbinding te maken via een Virtual Private Network (VPN) kan de verbinding niet worden onderschept (zie blz. 41).

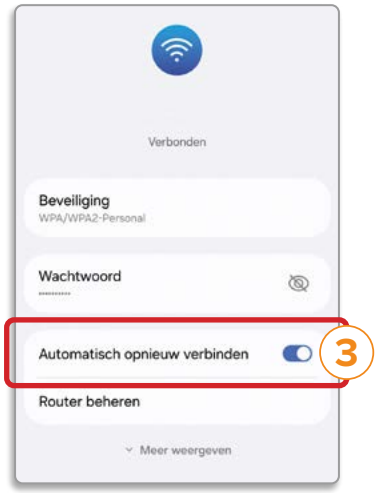
Liever 4G of 5G dan wifi

Voor gevoelige handelingen zoals mobiel bankieren of mailen is een mobiele verbinding (via 4G of 5G) veiliger dan wifi buitenshuis. Het mobiele netwerk is goed beveiligd, waardoor nieuwsgierigen geen schade kunnen aanrichten.

Automatische verbinding uitzetten

Zowel iOS als Android maakt automatisch verbinding met netwerken waarmee eerder verbinding is gemaakt. Helaas is dat niet waterdicht. Als een ander wifinetwerk dezelfde naam gebruikt, probeert het toestel daar toch verbinding mee te maken. Zet automatisch verbinden daarom liever uit.

Android



1. Tik op het icoon **Instellingen**, ga naar **Verbindingen** en dan naar **Wifi**.
2. Tik op het tandwiel naast het wifinetwerk.
3. Zet het schuifje bij **Automatisch opnieuw verbinden** uit.

Op iOS

1. Tik op het icoon **Instellingen** en ga naar **Wifi**.
2. Selecteer het wifinetwerk.
3. Zet het schuifje bij **Automatisch verbinden** uit.

VPN-netwerken

Door een Virtual Private Network (VPN) te gebruiken, kun je veiliger en vrijwel anoniem op het internet surfen. Al het internetverkeer loopt via de computer van de VPN-aanbieder. Die zorgt voor versleuteling en voor een ander IP-adres. Daardoor kunnen je internetactiviteiten niet naar jou voeren. Een crimineel kan zo geen gegevens onderscheppen wanneer je op een openbaar wifinetwerk een onversleutelde mail gebruikt. Bovendien is je privacy beter beschermd tegen censuur door overheidsinstanties en bedrijven die bespioneren. Ook advertentiebedrijven kunnen gebruikers minder goed volgen en kunnen dus geen profiel van ze samenstellen. Internetproviders kunnen ook geen gegevens meer registreren over je activiteiten op internet. Er bestaan verschillende VPN-apps voor smartphones. Bij elk gebruik kies je een land van waaruit je zogenaamd surft. Nadeel aan een VPN is dat je via een omweg surft. Daardoor komen websites, muziek en video wat langzamer binnen. Er zijn verschillende VPN-diensten, maar de meeste zijn betalend.

Geografische beperkingen omzeilen

Tv-omroepen schermen hun online-omgeving soms af voor gebruikers met een buitenlands IP-adres. Met een VPN kun je voor een ander land kiezen, zodat de website denkt dat je bijvoorbeeld toch vanuit België surft. Met een VPN kun je ook censuurmaatregelen omzeilen, bijvoorbeeld in China of Rusland, en zo geblokkeerde websites toch bezoeken. Controleer in zo'n geval wel of het strafbaar is om een VPN te gebruiken.

Hoe kies je een VPN-aanbieder?

Let op de volgende zaken.

– Kies een dienst die **compatibel met OpenVPN of WireGuard** is.

– Onderzoek of er een **mobiele app** is. Zonder app moet je zelf de verbinding instellen en dat kan lastig zijn.

– Kies voor een **Belgische server**. Hoeveel servers heeft de VPN-aanbieder? In welke landen zijn ze gevestigd? De downloadsnelheid hangt af van de afstand tot België. Als je in een buurland woont, kies je beter voor een Belgische server.

– Vermijd diensten die je **privacy niet respecteren**. Als een dienst je “no logging” belooft, betekent dit niet dat hij niets registreert. Gebruik idealiter een VPN-dienst die gegevens in het RAM-geheugen verwerkt in plaats van op een opslagruimte. Hoe minder persoonlijke gegevens (e-mailadres, naam, adres, telefoonnummer) een VPN-dienst vraagt, hoe minder indringend hij is.

– **Betaal anoniem.** Voor betalingen biedt Monero (bitcoin) de meeste anonimiteit. Als je geen bitcoins of kredietkaart hebt, kies dan voor een dienst die PayPal ondersteunt of contant geld via Mullvad VPN accepteert.

Gratis VPN-providers hebben hun beperkingen. Omdat ze over weinig servers beschikken, is de verbinding vaak traag en geldt er meestal een datalimiet. Let goed op de privacyvoorwaarden. Wie weinig video’s bekijkt en niet veel downloadt, heeft aan een gratis dienst voldoende.

Om de beste VPN-dienst te vinden, surf je naar **testaankoop.be/vergelijkvpn** of scan je de QR-code.

Systeemupdates uitvoeren

Om computerapparatuur te beschermen, is het van fundamenteel belang om software up-to-date te houden. Dat geldt ook voor smartphones. Updates zijn bedoeld om fouten te verhelpen die in de software zijn ontdekt. Stel de installatie van updates dus niet uit. Wanneer een update beschikbaar is, verschijnt

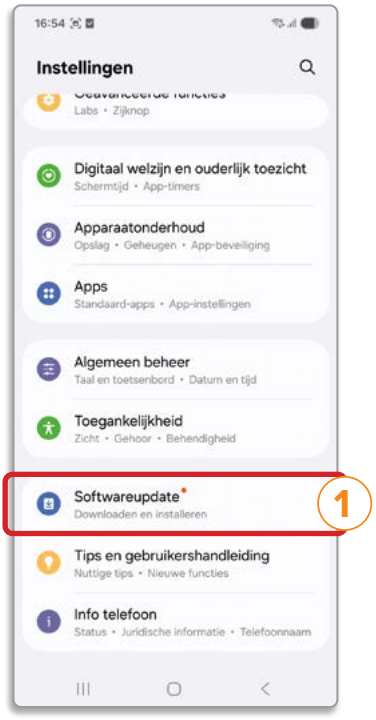
Welke versie is nog goed?

Wanneer je een nieuwe Android-telefoon koopt, check dan of die minimaal versie 15 heeft. Android 16 werd uitgebracht in juni 2025. Apple bracht versie 26 van iOS uit in september 2025. In feite gaat het om de 19de generatie van het besturingssysteem van Apple, maar het cijfer verwijst nu naar het jaar waarin het besturingssysteem voornamelijk zal worden gebruikt.

daar meestal een melding van op je telefoon. Wie schrik heeft dat hij een update heeft gemist, kan ook zelf controleren op systeemupdates en controleren welke versie er momenteel op het toestel staat.

Android

1. Tik op het icoon **Instellingen** en ga naar **Softwareupdate**.
2. Tik op **Downloaden en installeren**.
3. De huidige versie en de al geïnstalleerde beveiligingspatches worden weergegeven.
4. Als er een update beschikbaar is, tik je op **Downloaden en installeren**. Android gaat nu op zoek naar updates. Tik op **Nu installeren** om de update uit te voeren. Je moet de smartphone opnieuw opstarten.



iOS

1. Tik op het icoon **Instellingen** en ga naar **Algemeen**.
2. Selecteer **Software-update**.
3. iOS zoekt nu of er updates zijn. Is dat het geval, tik dan op **Werk nu bij**.

Apps updaten

Ook apps kunnen fouten bevatten. Controleer regelmatig of alle geïnstalleerde apps up-to-date zijn (zie blz. 72). Doe je dat niet, dan is je smartphone kwetsbaar voor aanvallen van hackers.