**tijd:**
>5 min.

**niveau:**
●○○

Het is niet moeilijk om de beveiliging van je smartphone flink te verbeteren. Dan krijgen dieven, hackers en privacy-schenders het een stuk lastiger.

Tekst **Rob Schleiffert /**
**digitaalgids@consumentenbond.nl**

IN 5 MINUTEN

# Beveilig je smartphone

## Verander de pincode van de simkaart

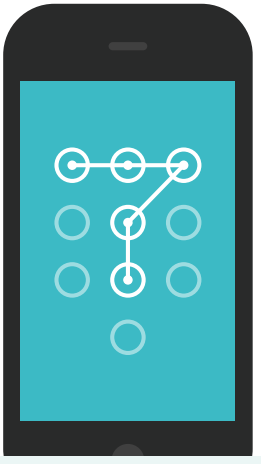
Bij het opstarten van een nieuwe smartphone moet je de pincode van de simkaart intoetsen. De code is vrijwel altijd 0000. Verander deze code dus direct, want een dief kan de simkaart in een ander toestel stoppen en je op kosten jagen. Na drie foute inlogpogingen wordt de simkaart geblokkeerd en is dan alleen nog te deblokkeren met de langere puk-code.

**ANDROID**

1 Ga naar **Instellingen** > **Vergrendelscherm** (of **Schermvergr. en beveilig.**).
2 Tik op **Andere beveiligingsinstellingen** > **Verg. SIM-kaart instellen**.
3 Zorgt dat het schuifje bij 'SIM-kaart blokkeren' op **Aan** staat en tik op **Pin SIM-kaart wijzigen**.
4 Vul de huidige pincode in, voer een nieuwe code in en bevestig die.

**IOS**

1 Ga naar **Instellingen** > **Mobiel netwerk** > **Simpincode**.
2 Zorg dat het schuifje op **Aan** staat en kies **Wijzig pincode**.
3 Vul de huidige pincode in en kies dan een nieuwe.
4 Herhaal de code en tik op **Gereed**.



**De stappenplannen in dit artikel gelden voor smartphones met Android vanaf versie 8 Oreo en voor iOS 12. Bij Android kunnen de instellingen nog per telefoonmerk verschillen.**

# Kies een sterke ontgrendelmethode

Voorkom dat een (on)eerlijke vinder je telefoon kan ontgrendelen en bij je bestanden kan komen: stel een toegangscode in. Afhankelijk van het telefoonmerk heb je de keus uit:

- Patroon – Je ontgrendelt de telefoon door volgens een vast patroon over het scherm te vegen. Pas op: de code is af te kijken en strepen op het scherm geven de code misschien weg. Niet veilig.
- Pincode – Een redelijke beveiliging als je een code van zes of meer cijfers kunt kiezen.
- Wachtwoord – De veiligste methode als je letters, cijfers en leestekens gebruikt.
- Biometrie – Steeds meer toestellen kunnen met een sensor worden ontgrendeld. Dat kan met een vingerafdruk, irisscanner of met gezichtsherkenning. Zie het kader onder.

# Stel de ontgrendelmethode in

### ANDROID

1 Ga naar **Instellingen** > **Vergrendelscherm** > **Type schermvergrendeling**.
2 Als je eerder al een toegangscode had ingesteld, moet je die nu invoeren.
3 Kies **Pincode** of **Wachtwoord** (vegen en Patroon zijn geen veilige methoden).
4 Volg de aanwijzingen op het scherm.
5 Afhankelijk van je telefoon kun je onder 'Biometrie' een biometrische methode toevoegen. Vink de optie aan. Ga een scherm terug en stel die functie in onder 'Biometrie'.


### IOS

1 Ga naar **Instellingen** en kies **Touch ID en toegangscode** of **Face ID en toegangscode**.
2 Tik op **Zet code aan** (als die al niet aanstaat).
3 Standaard wordt een zescijferige code gemaakt, maar je kunt onder **Toegangscodeopties** kiezen voor een ander soort.
4 Je kunt in dit scherm ook een vingerafdruk (**Touch ID en toegangscode**) of gezichtsherkenning (**Face ID en toegangscode**) instellen.
5 Volg de aanwijzingen op het scherm.

## *Inloggen met je vinger, gezicht of iris*

**Steeds meer toestellen kunnen met een vingerafdruk, irisscan of met gezichtsherkenning worden ontgrendeld. Een vingerafdrukscanner is gebruiksvriendelijk, maar net niet 100% veilig: Duitse onderzoekers zijn erin geslaagd een vingerafdruk van een bierglas te halen en daarmee de telefoon te ontgrendelen. Opstarten met een irisscan is nóg iets veiliger. Gezichtsherkenning is niet veilig als de camera aan de voorzijde wordt gebruikt om de vorm van je gezicht te meten. De telefoon kan zich laten foppen als je een portretfoto voor de lens houdt. Lees meer op consumentenbond.nl/gezichtsherkenning.**

# Stel een inloglimiet in

Mocht een dief je toestel in handen krijgen, dan kan hij met behulp van een computer proberen je toegangscode te kraken. Je kunt een limiet stellen aan het aantal pogingen. Vergeet de code niet en zorg voor een goede back-up van je bestanden.

**ANDROID**

1 Ga naar **Instellingen** > **Vergrendelscherm**.
2 Tik op **Instell. veilige vergrendeling**.
3 Vul de toegangscode in en zet 'Aut. reset fabrieksinst.' aan. Na 15 onjuiste pogingen wordt de telefoon gewist.

**IOS**

1 Ga naar **Instellingen** > **Touch ID en toegangscode**.
2 Vul je toegangscode in.
3 Zet – zo mogelijk – het schuifje bij 'Wis gegevens' aan. Na 10 mislukte inlogpogingen wordt de iPhone gewist.


# LastPass instellen

Sterke wachtwoorden kun je het best laten onthouden door een manager. We beschrijven hier LastPass, want die is goed, gratis en eenvoudig in het gebruik.

**ANDROID**

1 Installeer de LastPass-app via de Google Play Store (ontwikkelaar: LogMeIn, Inc).
2 Tik op **Aanmelden** om een account aan te maken en kies een sterk, maar goed te onthouden hoofdwachtwoord.
3 Handig: stel zo mogelijk in dat je de app kunt starten met een vingerafdruk.
4 De app is geopend. Tik op ☰ linksboven om het menu te openen.
5 LastPass vraagt of je wachtwoorden automatisch wilt laten invullen. Tik op **Inschakelen** > **Volgende**.
6 Selecteer in het volgende schermpje LastPass onder 'Service automatisch aanvullen' en tik op **OK**.
7 LastPass vraagt of je wachtwoorden automatisch wilt laten invullen in verouderde toepassingen. Tik op **Inschakelen** > **Volgende**. Op veel Samsung-telefoons wordt nu de functie 'Veilig opstarten' uitgeschakeld. Je kunt die vervolgens gewoon weer inschakelen via **Instellingen** > **Schermverg. en beveilig.** > **Veilig opstarten**.
8 Het Android-menu Toegankelijkheid opent. Kijk onder 'Services' en tik op **LastPass**. Zet het schuifje op **Aan** en tik op **OK**.
9 Druk twee keer op ↩ om terug te gaan naar LastPass.

**IOS**

1 Installeer de LastPass-app via de App Store (ontwikkelaar: LogMeIn, Inc).
2 Tik op **Enable** om LastPass toestemming te geven berichten te sturen en kies **Sta toe**.
3 Selecteer **Sign up** om een account aan te maken.
4 Kies een sterk, maar goed te onthouden moederwachtwoord.
5 Handig: activeer Touch ID of Face ID om de LastPass-kluis snel te openen via een vingerafdruk of gezichtsherkenning.
6 Laat LastPass wachtwoorden in Safari automatisch invullen. Ga in LastPass naar **Instellingen**.
7 Tik op **Automatisch invullen** en kies **Laat zien hoe dit werkt**.
8 Ga naar **Instellingen** van iOS en kies **Wachtwoorden en accounts**.
9 Tik op **Vul automatisch in** en zet het schuifje aan.
10 Plaats een vinkje bij LastPass en verwijder het vinkje bij **iCloud-sleutelhanger**.
11 Tik op **LastPass** en log in.



## LastPass gebruiken

Na het installeren werkt LastPass heel eenvoudig in de browser.

**ANDROID**

1 Op een inlogpagina van een site verschijnt een venstertje van LastPass. Tik op **+**.
2 Vul je gebruikersnaam en wachtwoord voor de site in. Zet een vinkje bij **Automatisch aanmelden** > **Opslaan**.
3 Ga terug naar de site. LastPass vult voortaan automatisch de inloggegevens in.

**IOS**

1 Ga naar de inlogpagina van een site. Er verschijnt een grijs balkje met **Wachtwoorde**n. Tik hierop en log in op **LastPass**.
2 Tik op **+**, vul de inloggegevens in en tik op **Opslaan & invullen**.
3 Je gebruikersnaam en wachtwoord worden ingevuld.
4 Tik op **Inloggen**.

## Firefox en Safari als manager

Wil je geen LastPass gebruiken? Ook browsers kunnen je wachtwoorden onthouden, maar let op: alleen Firefox en Safari doen dat veilig.

**FIREFOX**

Beveilig je wachtwoorden met een sterk hoofdwachtwoord:
1 Start Firefox en tik rechtsboven op ⋮.
2 Tik op **Instellingen** > **Privacy**. Vink 'Hoofdwachtwoord gebruiken' aan.
3 Bedenk een sterk hoofdwachtwoord, herhaal het. Tik op **OK**.

**SAFARI**

Safari heeft de iCloud-sleutelhanger, waarmee je wachtwoorden veilig online kunt opslaan. Zo activeer je de functie:
1 Ga naar **Instellingen** > **Wachtwoorden en accounts** en zet het schuifje bij 'Vul automatisch in' aan.
2 Ga in Safari naar een inlogpagina van een website, vul de accountgegevens in en tik op **Wachtwoorden** > **Bewaar wachtwoord**.
3 Een volgende keer zal Safari voorstellen de inloggegevens automatisch in te vullen.

# HOE HERKEN JE DIGITALE ZAKKENROLLERS?

Met de beste tips en adviezen van de Digitaalgids ben je zelf expert en digitaal veiliger. Kijk meteen op consumentenbond.nl/digitaalgids en kies de aanbieding die bij je past.


HAAL 'M IN HUIS

consumentenbond