Computer en telefoon

Alle seinen op veilig

Controleer geregeld de instellingen van je apparaten om ze veilig te houden. We lopen de belangrijkste knoppen langs voor vier besturingssystemen.

MACOS

We gaan uit van macOS Sequoia 15.0.

1 Werk macOS automatisch bij

Zorg dat je Mac veilig blijft door macOS bijgewerkt te houden. Ga naar ⚙ **Systeeminstellingen** > **Algemeen** > **Software-update**. Hier kun je zien of er een update beschikbaar is. Stel **Automatische updates** in om up-to-date te blijven, en vink alles aan in het scherm erna.

2 Vergrendel je Mac

Stel in dat je Mac altijd om een wachtwoord of TouchID vraagt als je er even niet achter zit. Zo voorkom je dat anderen bij je gegevens kunnen. Doe dit via ⚙ **Systeeminstellingen > Vergrendel scherm**. Stel een tijdsduur in bij 'Schakel schermbeveiliging in'. Kies daarna bij 'Vraag om wachtwoord na activering sluimerstand of uitschakeling scherm' voor **Onmiddelijk**.

3 Stel tweestapsverificatie in

Je kunt ook via de browser toegang krijgen tot je Apple-account en iCloud. Beveilig die route met tweestapsverificatie. Er wordt dan ter controle een zescijferige code gestuurd naar je andere apparaten. Klik op ⚙ **Systeeminstellingen** > [je naam] > **Inloggen en beveiliging**. Klik naast 'Twee-factor-authenticatie' op **Schakel in** en volg de stappen.

4 Schakel FileVault in

Met FileVault worden bestanden op de harde schijf automatisch versleuteld. Kwaadwillenden kunnen dan niet bij je data zonder de juiste inloggegevens, zelfs als ze de harde schijf verwijderen. Controleer of de versleuteling aan staat via ⚙ **Systeeminstellingen** > **Privacy en beveiliging**. Scrol helemaal naar beneden. Staat FileVault uit, klik er dan op en dan op **Schakel in** om FileVault te activeren.

5 Ontkoppel apparaten

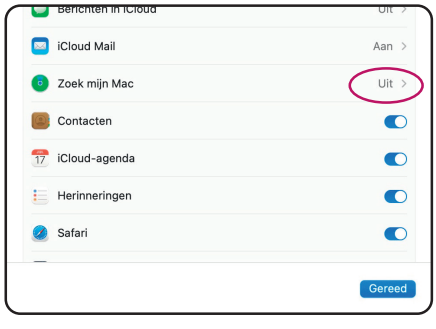
Verbreek de verbinding met apparaten die zijn gekoppeld aan je Apple-account als je ze niet langer gebruikt: klik op ⚙ **Systeeminstellingen** > [je naam]. Onder 'Apparaten' zie je de gekoppelde apparaten. Kies er een en klik op **Verwijder uit account**.

6 Toon bestandsextensies

Door bestandsextensies zichtbaar te maken, kun je makkelijker zien of je een onbetrouwbaar uitvoerbaar (.app-) bestand hebt binnengehaald. In **Finder**: klik op menu **Finder** > **Instellingen** > tabblad **Geavanceerd** en zet een vinkje voor 'Toon alle bestandsnaamextensies'.

7 Schakel Zoek mijn Mac in

MacOS heeft een funcie om je laptop terug te vinden als deze verloren of gestolen is: ⚙ **Systeeminstellingen** > [je naam] > **iCloud** > klik op **Toon alles** > **Zoek mijn Mac** > **Schakel in**.



WINDOWS

We gaan uit van Windows 11. Als het stappenplan afwijkt voor Windows 10, vermelden we dat.

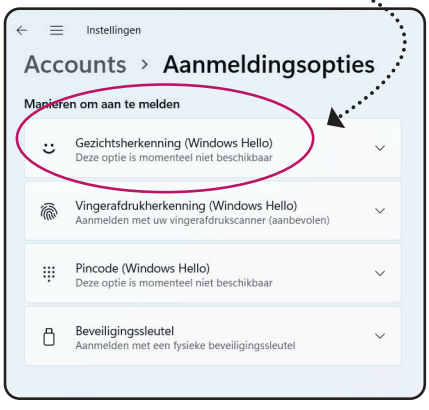
1 Hou de pc up-to-date

Hou Windows veilig met software-updates. Via **Start** > **Instellingen** > **Windows Update** zie je of je computer up-to-date is. Zet het schuifje aan bij 'Krijg de nieuwste updates zodra ze beschikbaar zijn', dan komen nieuwe updates zo snel mogelijk vanzelf binnen en blijft Windows beschermd.

Windows 10: klik op **Start** > **Instellingen** > **Bijwerken en Beveiliging** > **Windows Update**.

2 Veiliger met Windows Hello

Om te voorkomen dat iemand anders met je Microsoft-wachtwoord toegang kan krijgen tot je gegevens, kun je je computer beveiligen met Windows Hello. Dan log je in zonder wachtwoord, maar met een vingerafdruk, gezichtsherkenning of een pincode die wordt gekoppeld aan het apparaat. Stel het in via **Start** > **Instellingen** > **Accounts** > **Aanmeldingsopties**. Kies **Gezichtsherkenning (Windows Hello)** of **Vingerafdrukherkenning (Windows Hello)**, als je computer dat ondersteunt, of anders voor **Pincode (Windows Hello)**. Doorloop de stappen.

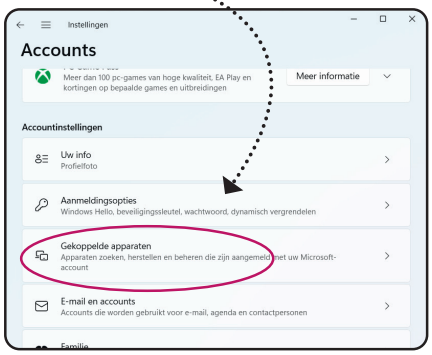


3 Stel tweestapsverificatie in

Je kunt ook via de browser toegang krijgen tot OneDrive en je Microsoft-mail. Beveilig die route met tweestapsverificatie. Dan krijg je een extra controle via je telefoon. Meld je in de browser aan via **login.live.com** > **Geavanceerde beveiligingsopties** > **Extra beveiliging** > **Verificatie in twee stappen** > **Inschakelen**.

4 Ontkoppel apparaten

Misschien zijn er apparaten die je niet meer gebruikt, maar die nog wel automatisch verbinding maken met je computer. Controleer dit via **Start** > **Instellingen** > **Accounts** > **Gekoppelde apparaten**.



Om een apparaat te ontkoppelen: tik op **Apparaat verwijderen**. Log in met je Microsoft-account > **Dit apparaat verwijderen** > **Ik ben klaar om dit apparaat te verwijderen** > **Verwijder**.

Windows 10: klik op **Start** > **Instellingen** > **Apparaten** > **Bluetooth en andere apparaten**.

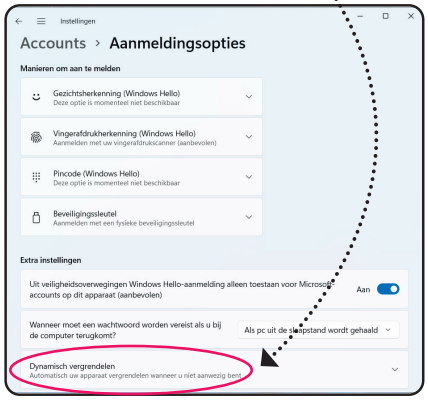
5 Toon bestandsextensies

Standaard verbergt Windows bestandsextensies. Dan kun je mogelijk een riskant uitvoerbaar .exe-bestand over het hoofd zien, omdat die bijvoorbeeld vermomd is als pdf. Wil je de bestandsextensies zien? Open de **Verkenner**, klik bovenin op ••• **Meer informatie** > **Opties** > tabblad **Weergeven**. Scrol naar beneden en vink 'Extensies voor bekende bestandstypen verbergen' uit.

Windows 10: open de **Verkenner** > menu **Beeld** en zet een vinkje bij 'Bestandsextensies'.

6 Automatisch vergrendelen

Voorkom dat iemand anders inlogt op je laptop als je even weg bent. Schakel automatisch vergrendelen in: klik op **Start** > **Instellingen** > **Accounts** > **Aanmeldingsopties** > **Dynamisch vergrendelen.**



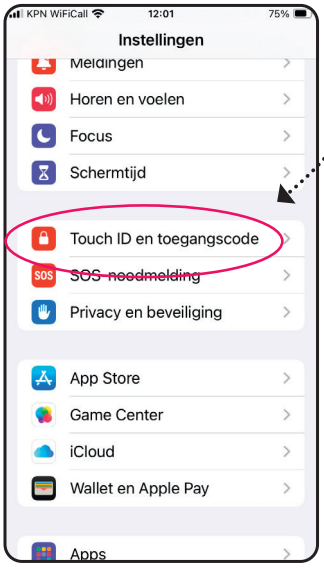
Zet een vinkje bij 'Toestaan dat Windows automatisch uw apparaat vergrendelt wanneer u niet aanwezig bent'.
Je moet hiervoor wel eerst je telefoon via bluetooth koppelen aan je laptop via **Start** > **Instellingen** > **Bluetooth en apparaten** > **Apparaat toevoegen**. Laat bluetooth aanstaan op je telefoon. Als je nu wegloopt van je laptop met je telefoon, wordt de laptop automatisch vergrendeld.

IOS/IPHONE

We gaan uit van het nieuwste besturingssysteem, iOS 18. We hebben het steeds over Touch ID (vingerafdrukherkenning), op nieuwere iPhones zit ook Face ID (gezichtsherkenning).

1 Stel Face ID of Touch ID in

Stel de veiligste inlogoptie in: gezichtsherkenning of een vingerafdruk (op oudere apparaten). Ga naar **Instellingen** > **Touch ID en toegangscode**.



Hier kun je ook bepalen waar je Touch ID nog meer voor wilt gebruiken, zoals voor betalingen en het automatisch invullen van wachtwoorden op websites.

2 Stel Zoek mijn iPhone in

Via **Instellingen** > [je naam] > **Zoek Mijn** kun je instellen dat je de locatie van je iPhone kan achterhalen via icloud.com. Dat komt van pas als het toestel verloren of gestolen is.

3 Beschermen bij diefstal

Zorg voor een extra beveiliging voor het geval je iPhone wordt gestolen door iemand die je toegangscode weet en 'kritieke' wijzigingen wil aanbrengen, zoals het uitschakelen van 'Zoek mijn iPhone'. Ga naar **Instellingen** > **Touch ID en toegangscode** > zet de schuif aan bij **Bescherming voor gesloten apparaat**.

4 Wis gegevens bij foute pin

In aanvulling op bovenstaande tip kun je ook de iPhone automatisch laten wissen als er tien keer een foute toegangscode is ingevoerd: tik op **Instellingen** > **Touch ID en toegangscode** > scrol naar beneden: zet schuifje aan bij 'Wis gegevens'.

Log in met twee-stapsverificatie en maak het hackers een stuk lastiger

5 Stel tweestapsverificatie in

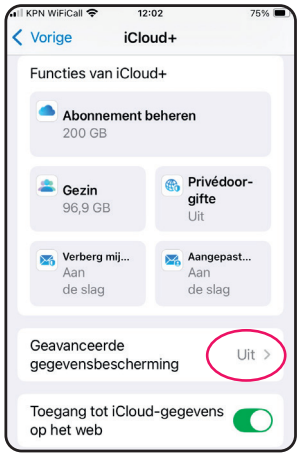
Log in met tweestapsverificatie en maak het voor hackers een stuk lastiger om toegang te krijgen tot je Apple-account en je gegevens. Dit schakel je in via **Instellingen** > [je naam] > **Inloggen en beveiliging** > **Zet twee-factor-authenticatie aan**.

6 Houd iOS up-to-date

Controleer of je telefoon up-to-date is via **Instellingen** > **Algemeen** > **Software-update**. Is er een update beschikbaar, tik dan op **Installeer nu**. Klik op **Automatische updates** en zet de schuifjes aan om je iPhone direct bij te laten werken als er een nieuwe update klaarstaat.

7 Extra databescherming

In iCloud worden je gegevens versleuteld, maar geavanceerde gegevensbescherming voegt nog een extra veiligheidslaag toe: dan kunnen gevoelige gegevenstypen, waaronder notities en Wallet-kaarten, alleen worden ontsleuteld op vertrouwde apparaten. Deze optie vind je bij **Instellingen** > [je naam] > **iCloud** > **Geavanceerde gegevensbescherming** > **Schakel geavanceerde gegevensbescherming in**. Voeg ook een herstelcontact toe, voor het geval je de toegang tot je account verliest.



8 Maak automatisch back-ups

Laat je iPhone automatisch een back-up (reservekopie) maken van je toestel om te voorkomen dat je gegevens kwijtraakt. Dit doe je via **Instellingen** > [je naam] > **iCloud** > **Back-up in iCloud**. Zet 'Maak een back-up van deze iPhone' aan.

ANDROID

We gaan uit van een Samsungtelefoon met Android 14. Op andere telefoons kan de route net iets anders zijn.

1 Kies de veiligste aanmeldoptie

Een Android-telefoon kun je op verschillende manieren ontgrendelen. Kies vingerafdruk of gezichtsherkenning, als de telefoon die optie heeft: ga naar **Instellingen** > **Beveiliging en privacy** > **Vergrendelscherm**. Wil je de veiligste optie, dan kies je (indien mogelijk) voor **Gezicht** of **Vingerafdrukken**.

Beveilig de toegang tot je Google-account met een extra controle

2 Houd Android up-to-date

Houd je telefoon veilig met softwareupdates. Ga naar **Instellingen** > **Softwareupdate**. Tik op **Downloaden en installeren** om te zien of je de laatste Androidversie gebruikt.

3 Stel tweestapsverificatie in

Heb je Android, dan heb je een Googleaccount. Beveilig de toegang tot je account met een extra controle: ga naar **myaccount.google.com** en log in. Ga naar **Beveiliging** > **Inloggen bij Google** > **Verificatie in 2 stappen** > **Aan de slag** en volg de stappen.

4 Alleen apps uit de appstore

Standaard kun je alleen apps uit de Google Play-store installeren. Zo voorkom je dat foute en vage apps op je telefoon belanden. Check voor de zekerheid of die mogelijkheid uit staat: **Instellingen** > **Beveiliging en privacy** > **Meer beveiligingsinstellingen** > **Onbekende apps installeren**.

5 Vind mijn apparaat aanzetten

Om je telefoon op te kunnen sporen als die kwijt of gestolen is, stel je Vind mijn apparaat in: klik op **Instellingen** > **Google** > **Alle services** > **Vind mijn apparaat**. Zet het schuifje aan bij 'Vind mijn apparaat gebruiken'. Samsung heeft zelf een vergelijkbare functie met meer opties, Samsung Find My Mobile.

6 Maak back-ups

Voor het geval je je telefoon kwijtraakt, stel je in dat Android automatisch back-ups maakt van je telefoon: ga naar **Instellingen** > **Google** > **Back-up** > **Back-up beheren**. Onder meer apps, contacten, apparaatinstellingen, foto's en video's worden in de back-up meegenomen.

VERDER LEZEN?

In het boek **Veilig Online** beschrijven we uitgebreid hoe criminelen te werk gaan én hoe je je kunt wapenen tegen online oplichting.

Het boek kost €24,50 (niet-leden €30), inclusief verzending. Als e-book €15,50 (niet-leden €19,50)

consumentenbond.nl/veilig

Consumenten bond

Digitaal bijblijven?

In de Digitaalgids vind je elke 2 maanden alles over digitale trends en online dreigingen. Probeer nu met korting.

Bekijk de aanbieding