TOPTIPS

Online veiligheid en privacy

Zorgeloos en veilig(er) internetten!

SENIORWEB

Veilig internetten en goed letten op je privacy. Het klinkt zo makkelijk, maar waar let je dan op? En wat moet je doen om je privacy online te beschermen? In deze toptips geven we u een aantal algemene handvatten en leggen we per apparaat de belangrijkste zaken en instellingen uit. Zodat u veilig(er) kunt internetten!

Inhoud

SENIORWEB

Algemeen

Waarom moet je op je veiligheid en privacy letten?

Veiligheid staat voorop, ook online. Want al sinds het ontstaan van internet proberen criminelen via het wereldwijde web mensen op te lichten. Het is dus goed om u hier bewust van te zijn en om de nodige maatregelen te nemen om te voorkomen dat u slachtoffer wordt.

Daarnaast laat iedereen die het internet gebruikt sporen achter. Los van elkaar zeggen de stukjes achtergelaten informatie niet zoveel, maar gecombineerd kan er een gedetailleerd beeld van de gebruiker ontstaan. Aan de hand daarvan kunnen bedrijven bijvoorbeeld gericht advertenties plaatsen of uw politieke voorkeur bepalen. Ook hackers kunnen deze persoonlijke informatie gebruiken om kwaad te doen. Het is daarom goed om de privacy-instellingen van uw apparaat, programma's/apps en accounts goed in te stellen.

Kortom: wees u bewust van de manieren die fraudeurs gebruiken om u op te lichten en controleer (en beheer) de sporen die u op internet achterlaat.

Trap niet in de nepperds

Phishing, spam, malware, ransomware en WhatsApp-fraude

Phishing, spam, malware, ransomware en WhatsApp-fraude (ook wel whaling genoemd): het zijn allemaal manieren om mensen via het wereldwijde web op te lichten. Of men nu via nepmails probeert te vissen naar uw persoonlijke informatie, uw computer gijzelt en losgeld eist, of dat u via het downloaden van software nietsvermoedend kwaadaardige software mee-installeert; een ongeluk zit ook op het internet in een klein hoekje. Gelukkig is er genoeg dat u kunt doen om de risico's zoveel mogelijk te beperken:

- Vul nooit zomaar ergens gegevens in.
- Klik niet zomaar op linkjes of bijlagen.
- Maak niet zomaar geld over naar iemand, ook al zegt hij/zij een bekende van u te zijn.

Nepnieuws

Nepnieuws is eigenlijk niets anders dan nieuws dat niet waar is. Maar waarom maakt nepnieuws op internet zo'n grote vlucht? Geld! Door te zorgen dat veel mensen doorklikken op de valse berichten trekt men veel verkeer naar een website. En die sites zijn volgehangen met advertenties. Hoe meer verkeer, hoe hoger de inkomsten. Dat blijkt zo lucratief te zijn dat er een nepnieuwsindustrie is ontstaan. Laat u dus niet om de tuin leiden!

Een ander motief is beïnvloeding. Met nepnieuws kun je de meningen van mensen beïnvloeden. Dat is bijvoorbeeld op grote schaal gebeurd bij de Amerikaanse presidentsverkiezingen van 2016. Rusland verspreidde een berg valse berichten, bedoeld om de verkiezingen te ontregelen.

Nepwebwinkels

Webwinkels zijn er in alle soorten en maten. Klein en groot, betrouwbaar of juist niet. Controleer voordat u een aankoop doet altijd of de shop wel in orde is.

Zijn de aanbiedingen te mooi om waar te zijn? Misschien hebt u wel te maken met een nepwebshop. Soms worden bestaande webwinkels nagebouwd. U denkt bijvoorbeeld dat u bij BCC webwinkelt, terwijl dat helemaal niet zo is. De naam is wel verwerkt in het webadres (bijvoorbeeld BCC-almere.com), maar de website is helemaal niet van BCC, maar van oplichters. Vaak zijn deze webshops maar heel kort online. Zo kort dat ze zelfs niet in Google voorkomen.
Een paar tips, zodat u niet uw winkelwagentje vult (of nog erger: afrekent) in een nepshop:

- Google op de naam en het webadres van de webshop. Wat voor ervaringen leest u, hoelang bestaat de webshop al? Kunt u niks vinden, dan is dat verdacht.
- Ga na of de webwinkel een keurmerk heeft en doe dit op de website van het keurmerk zelf. Verderop leest u daar meer over.

Keurmerk controleren
Het Thuiswinkel Waarborg is een keurmerk voor veilige webwinkels. Er zijn veel grote en middelgrote winkels bij aangesloten. Via de site Thuiswinkel.org doorzoekt u de ledenlijst. Staat een webwinkel ertussen? Dan kunt u er zonder risico winkelen. Hetzelfde geldt voor winkels die zijn aangesloten bij het Webshop Keurmerk. Het is overigens niet zo dat winkels die niet zijn aangesloten meteen onveilig zijn. Het lidmaatschap kost geld en dat hebben kleinere of startende webwinkels misschien niet.

Wees verstandig
Namaakwinkels proberen vaak klanten te trekken met stuntaanbiedingen. Trap er niet in! Zelfs op internet bij betrouwbare webwinkels gelden er minimumprijzen. Als iemand daaronder gaat zitten, is het vaak niet in orde.

Betalen
Probeer waar mogelijk te betalen met PayPal of met de creditcard. Die bieden de mogelijkheid geld terug te laten storten als er iets niet goed is. Bij iDEAL gaat dat niet.

Meer lezen
Wilt u meer weten over de nepperds? Lees dan ook deze artikelen:

- Veiligheidsrisico's op internet: www.seniorweb.nl/artikel/veiligheidsrisico-op-internet
- Alles wat u moet weten over phishing: www.seniorweb.nl/artikel/alles-wat-u-moet-weten-over-phishing
- Laat uw pc niet gijzelen door ransomware: www.seniorweb.nl/tip/tip-laat-uw-pc-niet-gijzelen-door-ransomware
- Trap niet in whaling: www.seniorweb.nl/tip/trap-niet-in-whaling
- Nepnieuws herkennen: www.seniorweb.nl/tip/tip-nepnieuws-herkennen

- Hoe controleer ik een webwinkelkeurmerk?: www.seniorweb.nl/tip/hoe-controleer-ik-een-webwinkelkeurmerk
- Speciaal voor SeniorWeb-leden hebben we de phishingchecker: www.seniorweb.nl/phishing

Veilige internetverbinding

Thuis veilig verbinding maken met wifi

Een draadloos netwerk moet worden beveiligd. Wie dat niet doet, verstuurt een open signaal. Uw buren zouden dan gratis van uw internetverbinding gebruik kunnen maken. En computercriminelen kunnen proberen op uw computer in te breken via het signaal. Een wifi-signaal is meestal door de internetprovider al beveiligd met een wachtwoord. Dit wachtwoord staat op de modem/router vermeld op een sticker. Het is aan te raden het standaardwachtwoord te wijzigen. Verander het in een woord dat bestaat uit cijfers en letters, hoofdletters en kleine letters. Zo maakt u de kans dat iemand uw netwerk binnendringt zo klein mogelijk.

Wat wel en niet doen via wifi-spots?

In veel cafés, winkels, hotels en zelfs in het openbaar vervoer en op de camping kunt u het internet opgaan met behulp van gratis wifi of wifi-hotspots (ook wel wifi-spots). Handig, want u kunt overal uw e-mail bekijken of de vertrektijd van de trein opzoeken. Maar openbare wifi-netwerken zijn in principe onveilig. U kunt prima het nieuws lezen of het weerbericht bekijken. Maar privacy- en fraudegevoelige handelingen, zoals internetbankieren, kunt u beter niet via een openbare wifi-verbinding uitvoeren. Moet u toch die ene betaling doen of even controleren of uw saldo nog hoog genoeg is? Gebruik dan de app in plaats van de website van de bank.

Meer lezen

Wilt u meer weten over internetverbindingen? Lees dan ook deze artikelen:

- Draadloze netwerken: www.seniorweb.nl/artikel/draadloze-netwerken
- Veilig internetten onderweg: www.seniorweb.nl/artikel/veilig-internetten-onderweg

Inlogmethoden

Er zijn verschillende manieren om apparaten en accounts te beveiligen. We zullen ze hieronder kort toelichten.

- Een patroon: op het scherm staan negen stippen in een opstelling van drie bij drie. Met een vinger maakt u een patroon door stippen met elkaar te verbinden. Om bijvoorbeeld uw telefoon te ontgrendelen moet u het patroon weer ‘tekenen’.
- Pincode: een code van minimaal vier cijfers. Hoe meer cijfers u gebruikt, hoe veiliger de pincode.
- Vingerafdruk: via een vingerafdrukscanner wordt een afbeelding van een of meerdere vingers gemaakt. Om uw apparaat of een app te ontgrendelen scant u die vinger(s).

- Gezichtsherkenning: er wordt een foto van uw gezicht gemaakt. Bij het ontgrendelen van uw apparaat wordt uw gezicht gescand en vergeleken met de foto die eerder gemaakt is.
- Wachtwoord: de bekendste en meest gebruikte inlogmanier is het wachtwoord. Een wachtwoord bestaat uit een reeks cijfers, letters en leestekens en moet vaak voldoen aan bepaalde eisen. Bijvoorbeeld 'minstens 8 tekens' of 'minimaal 1 cijfer'. Hieronder leest u een aantal tips om een sterk wachtwoord te maken.

Tips voor het maken van wachtwoorden
Gebruik voor elke dienst een ander wachtwoord.
Gebruik een combinatie van cijfers, letters (groot en klein) en leestekens.
Gebruik een programma als Lastpass als geheugensteuntje om de wachtwoorden niet te vergeten.
Pas de wachtwoorden regelmatig aan.

Truc voor het maken van een sterk wachtwoord

Een sterk wachtwoord bestaat uit een reeks van 6 tot 8 willekeurige letters en cijfers. Vaak bent u ook verplicht leestekens te gebruiken. Hoe lastiger het is om het wachtwoord te onthouden, hoe sterker het is. Gelukkig zijn er trucjes om sterke wachtwoorden te maken die toch redelijk eenvoudig te onthouden zijn. U bedenkt dan een schema dat u altijd toepast.

Bijvoorbeeld: [Geboortedatum][Naam website in kleine letters][Postcode][Leesteken][Huisnummer]

- Een wachtwoord voor een Google-account ziet er dan bijvoorbeeld zo uit: 11031939gmail3500AE!8
- En voor de site van SeniorWeb wordt het dan: 11031939seniorweb3500AE!8

Zo hebt u steeds wisselende sterke wachtwoorden en hoeft u alleen maar te onthouden welk schema u altijd toepast.

Lastpass helpt u uw wachtwoorden te onthouden

Hebt u moeite met het onthouden van alle wachtwoorden, dan kunt u het programma Lastpass gebruiken. Lastpass is een gratis online dienst die binnen uw account alle wachtwoorden bijhoudt van de sites die u gebruikt. U hoeft dan alleen uw hoofdwachtwoord van Lastpass te onthouden.

Meer lezen
Wilt u meer weten over inloggen? Lees dan ook deze artikelen:

- Welke inlogmethoden zijn er?: www.seniorweb.nl/artikel/welke-inlogmethoden-zijn-er
- Een veilig wachtwoord maken en onthouden: www.seniorweb.nl/tip/een-veilig-wachtwoord-maken-en-onthouden
- Lastpass gebruiken: www.seniorweb.nl/artikel/lastpass-gebruiken

Wat zijn cookies?

Veel mensen hebben hun twijfels over cookies. Want zijn ze ergens goed voor? Of maken ze inbreuk op de privacy van internetgebruikers? Een cookie is een klein, op zich onschuldig tekstbestand dat door een website op de harde schijf van de computer, tablet of smartphone wordt geplaatst wanneer u deze website bezoekt. De belangrijkste functionaliteit van cookies is het onderscheiden van de ene gebruiker van de andere. Er zijn verschillende soorten cookies, die in meer of mindere mate invloed hebben op uw privacy. De belangrijkste soorten zijn:

- Functionele cookies zijn nodig om een website goed te kunnen laten functioneren. Bijvoorbeeld voor het onthouden van een inlognaam of de inhoud van een winkelwagentje. Deze cookies worden ook wel first party cookies genoemd; cookies die door de website die u bezoekt zelf worden geplaatst. De functionele cookies hebben geen invloed op uw privacy.
- Analytische cookies houden via statistieken bezoekersgedrag op de site bij. Denk aan hoeveel bezoekers op een bepaalde knop drukken en welke pagina's op de site bezocht worden. Hierdoor verbeteren sitebeheerders de website, omdat ze bijvoorbeeld weten welke pagina's slecht bezocht zijn. Wanneer ze goed worden ingezet, hebben deze cookies geen invloed op uw privacy. De statistische informatie wordt geanonimiseerd opgeslagen.
- Tracking cookies of volgcookies maken het mogelijk om te volgen welke websites mensen bekijken op internet. Adverteerders maken hier gebruik van om gericht hun advertenties aan de juiste personen te tonen. Deze cookies worden ook third party cookies genoemd en hebben invloed op uw privacy. Met de data die wordt verzameld kan uiteindelijk een profiel van u opgebouwd worden, waar adverteerders gebruik van kunnen maken.

Meer lezen
Wilt u meer weten over cookies? Lees dan ook deze artikelen:

- Cookies wat moet u ermee?: www.seniorweb.nl/artikel/cookies-wat-moet-u-ermee
- Cookies verwijderen: www.seniorweb.nl/artikel/cookies-verwijderen
- Cookies verwijderen op tablet en smartphone: www.seniorweb.nl/tip/cookies-verwijderen-op-smartphone-en-tablet

Veiligheid en privacy op een Windows-computer

Veiligheid

Apparaat beveiligen

Wat eigenlijk altijd geldt: zorg ervoor dat uw apparaat is beveiligd. Dit kunt u op verschillende manieren doen, bijvoorbeeld met een wachtwoord, een pincode of zelfs gezichtsherkenning. Daarnaast is het ook aan te raden om, als u bezig bent met persoonlijk zaken en even wegloopt van de computer, het scherm te vergrendelen met de toetsencombinatie Windows+L. Het vergrendelingsscherm komt in beeld en als u de computer weer wilt gebruiken, moet u opnieuw inloggen. En wist u al dat u zelf kunt bepalen wat de

power-knop aan de buitenkant van de pc doet als u erop drukt? Zo zet u de computer snel in slaap- of sluimerstand als u even weg moet van het scherm en niet wilt dat anderen erop kunnen kijken.

Updates

Microsoft voert regelmatig updates door voor het besturingssysteem. Windows 10 haalt, via Windows Update, deze updates zelf binnen. Hier hoeft u dus in principe niets voor te doen. Soms kan de computer aangeven dat hij opnieuw opgestart moet worden om de updates daadwerkelijk te installeren.

Voor apps en software die u op de computer hebt staan, geldt in principe ook dat er eens in de zoveel tijd een nieuwe update wordt uitgevoerd. Daarmee bent u dan weer verzekerd van de laatste veiligheidsupdates. Controleer ook af en toe de software en apps die u op de computer hebt staan. Gebruikt u bepaalde programma's niet meer? Verwijder die dan. Dat scheelt enerzijds ruimte en anderzijds kan het programma inmiddels verouderd zijn, waardoor het kwetsbaar kan zijn geworden.

Firewall en Defender

Met de firewall van Windows kunt u uzelf beschermen tegen kwaadwillende mensen die via internet proberen in te breken op de computer. Standaard staat deze optie aan, maar het kan geen kwaad om te controleren of de firewall ook daadwerkelijk is ingeschakeld. Dat doet u als volgt:

- Klik op de Startknop > **Instellingen**.
- Klik op **Bijwerken en beveiliging** > **Windows-beveiliging**.
- In het overzicht staan verschillende onderdelen met een rode of groene markering erbij. Groen betekent dat alles in orde is, bij rood moet u zelf iets ondernemen. Klik op **Windows-beveiliging** openen.
- Klik links op **Firewall- en netwerkbeveiliging**.
- Ziet u bij de drie onderdelen rechts 'Firewall is ingeschakeld' dan is alles in orde. Is dat niet het geval, wijzig de instellingen dan. Vraag bij twijfel om hulp.

Naast de firewall staat ook Defender, het antivirusprogramma van Microsoft, standaard aan. Ook hier hoeft u dus niet naar om te kijken. Hebt u een betaald pakket aangeschaft en wilt u dat op uw computer installeren, dan zal Defender worden afgesloten. Het hebben van twee antivirusprogramma's kan namelijk een averechts effect hebben.

Privacy

Het onderdeel 'Privacy' in de instellingen van Windows 10 bevat veel opties. Denk aan instellingen voor het tonen van gepersonaliseerde advertenties en het doorsturen van locatiegegevens. Een deel van de privacygevoelige informatie wordt standaard gedeeld met Microsoft, maar dit kunt u aanpassen. Het onderdeel is opgedeeld in enerzijds Windows-machtigingen en anderzijds App-machtigingen.

Windows-machtigingen

Dit onderdeel regelt instellingen die te maken hebben met het besturingssysteem, dus met Windows zelf, en is onderverdeeld in vijf verschillende secties. Per onderdeel kunt u aangeven welke gegevens wel of niet naar Microsoft mogen worden verzonden.

App-machtigingen

Dit onderdeel regelt instellingen die te maken hebben met de verschillende apps en programma's die zijn geïnstalleerd. Bijvoorbeeld of het videobelprogramma Skype toegang heeft tot de camera en microfoon (indien aanwezig). Eventuele aanpassingen die u wilt doen voor programma's en apps kunt u hier doorvoeren. Houd daarbij wel rekening met de werking van deze apps en programma's. Skype werkt bijvoorbeeld niet zonder toegang tot de camera en microfoon. Het uitzetten van bepaalde app-machtigingen kan dus invloed hebben op het functioneren van het programma/de app. Zet u per ongeluk een machtiging uit die het programma nodig heeft, dan zal het programma een melding geven dat die machtiging noodzakelijk is en kunt u die weer inschakelen.

Meer lezen

Wilt u meer weten over het beveiligen van en de privacy-instellingen in Windows 10? Lees dan ook deze artikelen:

- In 10 stappen veilig: www.seniorweb.nl/artikel/in-10-stappen-veilig
- De privacy-instelling in Windows 10: www.seniorweb.nl/de-privacy-instellingen-in-windows-10
- Het privacy-dashboard van Microsoft: www.seniorweb.nl/tip/het-privacy-dashboard-van-microsoft
- Wanneer is een app of programma veilig: www.seniorweb.nl/artikel/wanneer-is-een-app-of-programma-veilig
- Bepalen wat de aan/uit-knop op een Windows 10-pc doet: www.seniorweb.nl/tip/functies-aan-uit-knop-windows-pc

Veiligheid en privacy op Mac-computer

Veiligheid

Apparaat beveiligen

Wat eigenlijk altijd geldt: zorg ervoor dat uw apparaat is beveiligd. Dit kunt u op verschillende manieren doen, bijvoorbeeld met een wachtwoord, een pincode of zelfs gezichtsherkenning. Daarnaast is het ook aan te raden om, als u op de pc bezig bent met persoonlijke zaken en even wegloopt, het scherm te vergrendelen met de toetsencombinatie Control+Command+Q. Het vergrendelingsscherm komt in beeld. Als u de computer weer wilt gebruiken, moet u opnieuw inloggen.

Updates

Apple voert regelmatig updates door voor het besturingssysteem. MacOS haalt deze updates, als u dat hebt ingesteld, zelf binnen. Hier hoeft u dus in principe niets voor te doen. Soms kan de computer aangeven dat hij opnieuw opgestart moet worden om de updates te installeren.

Voor apps en software die u op de computer hebt staan, geldt in principe ook dat er eens in de zoveel tijd een nieuwe update wordt uitgevoerd. Daarmee bent u dan weer verzekerd van de laatste veiligheidsupdates. Controleer ook af en toe de software en apps die u op de computer hebt staan. Gebruikt u bepaalde programma's niet meer? Verwijder die dan. Dat scheelt enerzijds ruimte en anderzijds kan het programma inmiddels verouderd zijn, waardoor het kwetsbaar kan zijn geworden.

Firewall en antivirus

Met de firewall van MacOS kunt u zich beschermen tegen kwaadwillende mensen die via internet proberen in te breken op uw computer. Controleer voor de zekerheid of hij ook daadwerkelijk is ingeschakeld, zodat u beschermd bent tegen hackers.

Het is daarnaast ook voor een Mac aan te raden om antivirussoftware te installeren. U kunt kiezen uit een betaald pakket of een gratis variant. Bekende leveranciers van betaalde virusscanners zijn McAfee en Kaspersky Lab. Een gratis virusscanner is Sophos. Houd hierbij altijd in het achterhoofd dat één antivirusscanner voldoende is. Twee programma's kunnen elkaar tegenwerken en daardoor een averechts effect hebben.

Privacy

In het onderdeel Privacy kunt u, na het invoeren van uw Apple-wachtwoord, de nodige aanpassingen doen in de privacy-instellingen.

Locatievoorziening

Standaard staat de optie locatievoorzieningen aan en kunnen apps die daar toestemming toe hebben dus gebruikmaken van uw locatie en zien waar u bent. U kunt deze optie uitzetten, dan heeft geen enkele app/geen enkel programma toegang tot uw locatie. Nadeel is dat sommige apps daardoor niet goed of niet meer werken. Zo werkt de optie 'Zoek mijn (Mac/iPhone/iPad)' om uw apparaat te lokaliseren niet meer. Wilt u dat bepaalde apps/programma's wel toegang tot uw locatie blijven behouden? Laat de optie aan staan en geef alleen de apps/programma's toegang tot uw locatie waarvan u wilt dat ze uw locatie gebruiken.

App-machtigingen

Naast dat sommige apps/programma's toegang hebben tot uw locatie, zijn er ook enkele andere onderdelen waar apps/programma's graag toegang tot hebben. Denk hierbij onder andere aan contactgegevens, informatie in de agenda, de camera en de microfoon. Om te kijken welke apps/programma's toegang hebben tot deze informatie, klikt u op de onderdelen. U ziet vervolgens een lijst van alle programma's en apps die toegang hebben. Door vinkjes weg of aan te klikken geeft u de apps/programma's toestemming.

Meer lezen

Wilt u meer weten over het beveiligen en de privacy-instellingen van de Mac? Lees dan ook deze artikelen:

- Mac-computers: beveiliging: www.seniorweb.nl/artikel/mac-computers-beveiliging
- Privacy-instellingen op de Mac: www.seniorweb.nl/artikel/privacy-instellingen-op-de-mac
- Privacy-rapport bekijken in Safari: www.seniorweb.nl/artikel/privacyrapport-bekijken-in-safari
- Schermbeveiliging instellen Mac: www.seniorweb.nl/tip/tip-schermbeveiliging-instellen-mac

Veiligheid en privacy op de iPad en iPhone

Veiligheid

Apparaat beveiligen

Om de iPad of iPhone te beveiligen tegen ongewenst gebruik of zelfs diefstal is het van belang dat u het apparaat beveiligt. De makkelijkste manier om een iPad of iPhone te beveiligen is via een pincode of cijfercode. Daarnaast kunnen de meeste iPads en iPhones inmiddels worden beveiligd met een vingerafdruk. Een voordeel daarvan is dat u geen code hoeft te onthouden. Bij nieuwere modellen hebt u nog een extra mogelijkheid: gezichtsherkenning.

Het is daarnaast verstandig om de optie 'Automatisch slot' in te stellen in combinatie met een toegangscode. Met de optie 'Automatisch slot' gaat de iPad of iPhone na het door u aantal ingestelde minuten in de sluimerstand als u 'm niet gebruikt. Om hem weer te kunnen gebruiken, moet de toegangscode worden ingevuld.

Updates

De besturingssystemen van de iPad (iPadOS) en iPhone (iOS) worden regelmatig geüpdatet. Omdat deze updates vaak relevant zijn voor de beveiliging van het apparaat is het raadzaam om nieuwe updates gelijk te installeren.

Ook van de apps die op uw iPad of iPhone staan verschijnen regelmatig updates. Deze updates bevatten vaak optimalisaties voor het gebruik van de app en uw veiligheid. Installeer nieuwe updates dan ook direct op het moment dat ze beschikbaar komen. Verwijder daarnaast apps die u niet meer gebruikt. U zorgt dan voor een opgeschoond apparaat en voorkomt dat u verouderde, en dus minder veilige, apps op de iPad of iPhone hebt staan.

Antivirus

Voor schadelijke software hoeft u op de iPad en iPhone niet bang te zijn. Apple ziet namelijk streng toe op alle programma's die in de App Store worden uitgebracht. Alle apps hierin zijn uitgebreid door Apple gecontroleerd. Verder zijn de Apple-apparaten zo gemaakt dat alle apps los van elkaar werken en geen toegang hebben tot andere delen van het apparaat. Daarom is een antivirusprogramma voor de iPad en iPhone niet nodig.

Privacy

App-machtigingen

Apps willen graag toestemming tot bepaalde onderdelen op de iPad of iPhone, denk aan de locatie, camera of bijvoorbeeld uw agenda. Voor een navigatie-app is het noodzakelijk om toegang te hebben tot uw locatie, maar soms is het minder duidelijk of die locatietoegang of de toegang tot uw camera wel echt nodig is. Via de privacy-instellingen kunt u precies zien welke apps toegang hebben tot welke onderdelen en kunt u de toegang ook wijzigen. Mocht u een app de toegang tot bijvoorbeeld uw locatie ontzeggen, terwijl die wel noodzakelijk is voor die app, dan kunt u de instelling altijd weer wijzigen.

Cookies en advertenties

Zoals u al eerder in deze toptips hebt kunnen lezen, plaatsen websites verschillende cookies om u te volgen en uw gedrag op de website bij te houden. In de app Instellingen kunt u de privacy-instellingen van de app Safari aanpassen. Zo kunt u aangegeven dat u niet gevolgd wilt worden en kunt u websitedata wissen. We raden u af om het schuifje bij 'Blokkeer alle cookies' aan te zetten, omdat het anders onmogelijk wordt om nog in te loggen bij websites of om iets in een winkelmandje te plaatsen en af te rekenen.

Daarnaast maken apps die op uw iPad of iPhone staan gebruik van een zogeheten advertentie-ID. Dit ID is gekoppeld aan het apparaat en verzamelt gegevens van de gebruiker. Op basis van deze informatie worden advertenties aangepast aan uw 'voorkeuren'. Zo komt het dus dat u advertenties krijgt te zien van het dat boek of het vakantiehuisje waar u net naar hebt gezocht. U kunt dit ID uitzetten, maar u krijgt dan nog wel reclame te zien. De advertenties zijn dan echter niet afgestemd op wat u mogelijk interessant vindt. Sommige gebruikers vinden dit juist storender dan gerichte advertenties. Bepaal zelf wat u het liefste hebt en pas uw instelling dan eventueel aan.

Meer lezen
Wilt u meer weten over het beveiligen van en de privacy-instellingen op een iPad of iPhone? Lees dan ook deze artikelen:

- Beveilig uw iPad: www.seniorweb.nl/artikel/beveilig-uw-ipad
- iPhone beveiligen: www.seniorweb.nl/tip/iphone-beveiligen
- Privacy instellen op de iPad en iPhone: www.seniorweb.nl/tip/privacy-instellen-op-ipad-en-iphone
- Betere privacy en meer in iOS14: www.seniorweb.nl/artikel/betere-privacy-en-meer-in-ios-14
- Schermbeveiliging voor de iPad en iPhone: www.seniorweb.nl/tip/schermbeveiliging-voor-ipad-en-iphone

Veiligheid en privacy op een Android-tablet of Android-smartphone

Veiligheid

Apparaat beveiligen

Om uw Android-apparaat te beveiligen tegen ongewenst gebruik of zelfs diefstal is het van belang dat u het apparaat beveiligt. De makkelijkste manier om de smartphone of tablet te beveiligen is via een pincode of cijfercode. Daarnaast kunnen de meeste Android-apparaten inmiddels worden beveiligd met een vingerafdruk. Een voordeel daarvan is dat u geen code hoeft te onthouden. Gebruikers van nieuwere modellen hebben nog een extra optie: gezichtsherkenning.

Het is daarnaast verstandig om de optie 'Slaapstand' in te stellen. Op de meeste toestellen is die standaard actief. Met deze optie wordt het apparaat automatisch vergrendeld als het niet wordt gebruikt gedurende een door u ingestelde tijd.

Wat daarnaast belangrijk is bij Android-apparaten, is dat u altijd alleen apps uit de Play Store downloadt. Het is met Android-apparaten namelijk ook mogelijk om apps van buiten de Play Store te downloaden, maar die zijn niet gecontroleerd en kunnen dus onveilig zijn. Apps in de Play Store worden gecontroleerd en zijn veilig voor gebruik.

Updates

Het besturingssysteem Android wordt regelmatig geüpdatet. Omdat deze updates relevant zijn voor de beveiliging van het apparaat is het raadzaam om nieuwe updates gelijk te installeren.
Ook van de apps die op de tablet of smartphone staan, verschijnen regelmatig updates. Deze updates bevatten vaak optimalisaties voor het gebruik van de app en uw veiligheid. Installeer nieuwe updates dan ook direct op het moment dat ze beschikbaar komen. Verwijder daarnaast apps die u niet meer gebruikt. U zorgt dan voor een opgeschoond apparaat en voorkomt dat u verouderde, en dus minder veilige, apps op de smartphone of tablet hebt staan.

Antivirus

Wilt u het toestel nog eens extra goed nalopen? Gebruik dan een virusscanner. Hiervoor moet u eerst een app downloaden. Er zijn, net als op een pc, gratis en betaalde scanners. Een aantal opties zijn:

- Avast Antivirus
- AVG Antivirus
- Kaspersky Mobile Antivirus
- Malwarebytes Beveiliging

Let op: installeer altijd maar één antivirusapp. Installeert u meerdere apps, dan kunnen ze elkaar tegenwerken.

Privacy

App-machtigingen

Vaak willen apps toestemming tot bepaalde onderdelen van uw Android-apparaat. Denk aan de locatie, camera of bijvoorbeeld uw agenda. In sommige gevallen is dit noodzakelijk. Een navigatie-app moet bijvoorbeeld toegang hebben tot uw locatie om de weg goed te kunnen wijzen. Maar soms is het minder duidelijk of die locatietoegang of toegang tot uw camera wel echt noodzakelijk is. Via de privacy-instellingen kunt u precies zien welke apps toegang hebben tot welke onderdelen en kunt u deze toegang ook wijzigen. Zoals gezegd: soms heeft een app bepaalde toegang echt nodig om goed te kunnen werken. Hebt u een app de toegang ergens toe ontzegd, terwijl die wel echt nodig is, kunt u dat eenvoudig weer wijzigen in de privacy-instellingen.

Cookies en advertenties

Zoals u al eerder in deze toptips hebt kunnen lezen, plaatsen websites verschillende cookies om u te volgen en om uw gedrag op de website bij te houden. Browset u op een Android-apparaat in Chrome, pas de privacy-instelling van deze browser dan aan in de Chrome-app. Wis bijvoorbeeld de cookies of geef aan dat u niet wilt dat pagina's sneller laden door het gebruik van deze tekstbestandjes.

Daarnaast maken apps die op uw tablet of smartphone staan ook gebruik van een zogeheten advertentie-ID. Dit ID is gekoppeld aan het apparaat en verzamelt gegevens van de gebruiker. Op basis van deze informatie worden advertenties aangepast aan uw 'voorkeuren'. Zo komt het dus dat u advertenties krijgt te zien van het boek of vakantiehuisje waar u net naar hebt gezocht. U kunt deze instelling uitzetten, maar krijgt dan nog wel reclame te zien. Die is dan alleen niet meer afgestemd op uw voorkeuren. Sommige gebruikers zien liever reclames die ze interessant vinden, andere willen dit juist niet. Bepaal zelf wat uw voorkeur heeft en pas de instellingen eventueel aan.

Meer lezen
Wilt u meer weten over het beveiligen van en de privacy-instellingen op een Android-apparaat? Lees dan ook deze artikelen:

- Android-smartphone beveiligen: www.seniorweb.nl/artikel/android-smartphone-beveiligen
- Android-tablet beveiligen: www.seniorweb.nl/artikel/android-tablet-beveiligen
- Privacy instellen op een Android-apparaat: www.seniorweb.nl/artikel/privacy-instellen-op-android-apparaat
- Privacy instellen bij Android-apps: www.seniorweb.nl/artikel/privacy-instellen-bij-android-apps

Gezond verstand

Er zijn altijd zaken waar u weinig tot niets aan kunt doen. Bijvoorbeeld hoe (overheids)instellingen uw gegevens verwerken. Maar online veiligheid begint uiteindelijk wel bij uzelf. Welke gegevens deelt u wanneer? Let altijd op de volgende zaken:

- Beveilig (mobiele) apparaten.
- Houd het besturingssysteem en de software/apps up-to-date.
- Gebruik één virusscanner om het apparaat te beveiligen.
- Let altijd op waar u persoonlijke, financiële en inloggegevens achterlaat.
- Klik niet zomaar op een link in een e-mail, zeker als u de afzender van de mail niet kent.
- Open niet zomaar een bestand/bijlage als u niet zeker weet om wat voor bestand of bijlage het gaat.
- Beantwoord geen spam of andere e-mails waarvan u de afzender niet kent.
- Is een aanbieding te mooi om waar te zijn? Dan is dat ook vaak zo.
- Controleer de betrouwbaarheid van de website als u een programma gaat downloaden en klik op de juiste downloadknop.
- Klik tijdens het installeren van een programma eventueel vinkjes uit om te voorkomen dat u ongewenste software installeert.

Meer informatie

Duizelt het u na het lezen van al deze informatie? Lees alles nog eens rustig door op www.seniorweb.nl/online-veiligheid-en-privacy. Komt u er niet uit? Dan helpen we u graag verder! Kijk hieronder voor meer informatie over hoe we dat doen.

PCHulp

Komt u er niet helemaal uit en/of hebt u hulp nodig? Onze vrijwilligers van PCHulp helpen graag. Vraag hulp via internet of per telefoon aan. PCHulp is exclusief voor leden van SeniorWeb. U leest meer informatie over de werkwijze, kosten en het aanvragen op www.seniorweb.nl/pchulp

Word lid van SeniorWeb

Wilt u ook altijd kunnen terugvallen op computerhulp? Word dan nu lid! Op www.seniorweb.nl/quizactie ziet u de huidige lidmaatschapsactie.

Als SeniorWeb-lid profiteert u onder andere van:

- ✓ Hulp via internet of per telefoon
- ✓ 4 x per jaar exclusieve informatie en tips in tijdschrift Enter
- ✓ Les online of bij u in de buurt
- ✓ Wekelijks informatieve nieuwsbrieven
- ✓ Deskundige controle van verdachte mails

Profiteer direct van onze ledenvoordelen en meld u via www.seniorweb.nl/quizactie aan. Het lidmaatschap geldt tot wederopzegging. Hebt u hier een vraag over? Bel ons op 030 – 276 99 65 of mail naar leden@seniorweb.nl We helpen u graag!