

Gebruik van Android smartphone

- Geavanceerd niveau -

Auteur: RobertTheCoder

Datum: 15/07/2024



Geavanceerd

Inhoud

Vereiste voorkennis

Goede kennis van internet, cloud en Android bediening is vereist.
Deze cursus is bedoeld voor gebruikers met gemiddelde Android kennis.

Omschrijving

- Basiskennis van NFC en Bluetooth voor apparaat-koppeling
- Camera opties om betere foto's te maken
- Gebruik van apps met Artificiele Intelligentie
- Privacy en veiligheid verbeteren in apps
- Data op smartphone veilig backup-en
- Toegang tot apps/sites beter beveiligen

Agenda

- 1) Koppeling van smartphone met andere apparaten
- 2) Betere foto's maken met Camera app
- 3) Artificiele Intelligentie gebruiken
met Google Lens en Assistant app
- 4) Bewust omgaan met digitale fraude
- 5) Openbare WiFi veilig gebruiken met ProtonVPN
- 6) Anoniem gebruik van browser, zoekmachine en email

Agenda

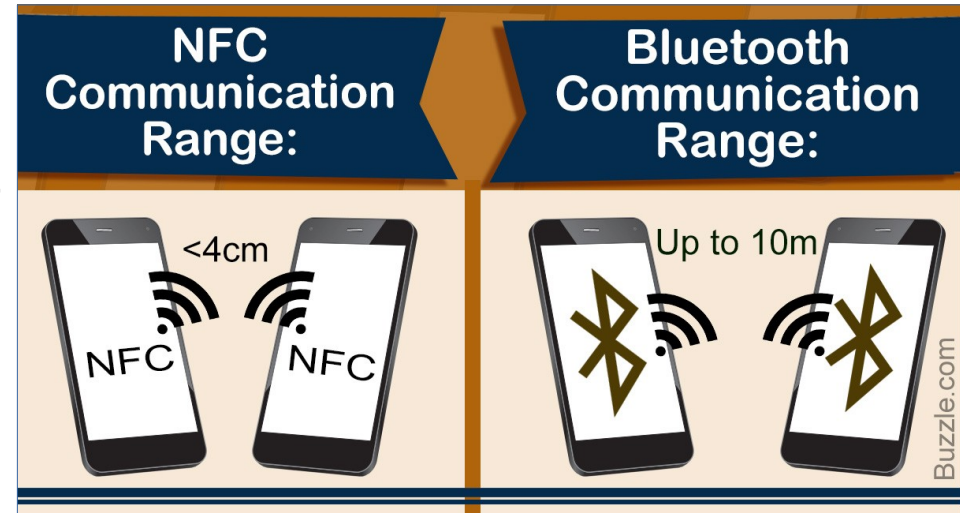
- 7) Toegang tot app en website beveiligen met Password Managers
- 8) Veilige backup maken van bestanden op smartphone
- 9) Toegang tot app en website beveiligen met 2FA
- 10) Toegang tot app en website beveiligen met Passkeys
- 11) Suggesties ?

Deel 1

Koppeling van smartphone met andere apparaten

Welke samenwerking met andere apparaten in smartphone ingebouwd?

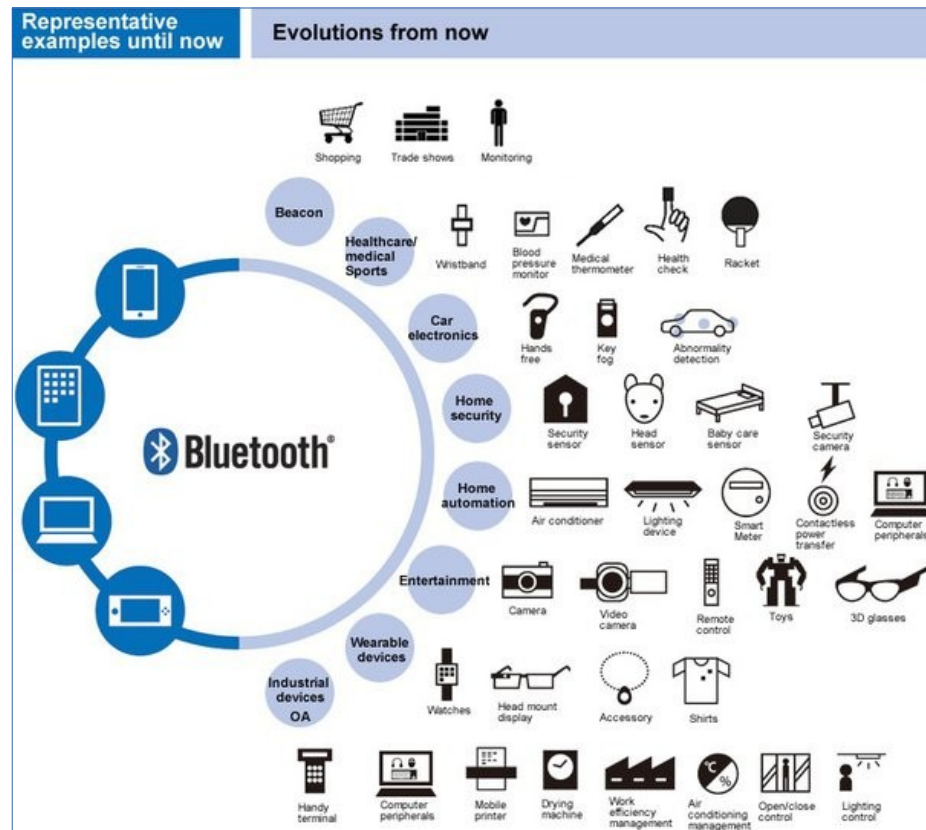
- **Bluetooth:**
technologie voor aanmaak van korte afstand verbinding zonder draad met ander apparaat (meestal tot 10 m);
deze vereist korte setup vooraf (“pairing”);
oa gebruikt bij koppeling van smartphone aan draadloze headset, auto, etc
- **NFC (Near Field Communication):**
technologie voor aanmaak van korte afstand verbinding zonder draad met ander apparaat (meestal tot 10 cm);
deze vereist geen setup vooraf;
oa gebruikt bij contactloos betalen



Voorbeelden van Bluetooth gebruik

Bluetooth wordt voor de koppeling van heel wat apparaten gebruikt; voor de koppeling van je smartphone met een ander toestel met bluetooth is er ondersteuning via apps.

Zo kan bluetooth bijvoorbeeld gebruikt worden om je smartphone te koppelen met het computer-systeem in je auto om handenvrij te kunnen bellen in de auto, of om je favoriete muziek opgeslagen op je phone te kunnen afspelen in auto.



Extra info

Video's met meer uitleg

- * Jabra Elite 85t: How to pair | Jabra Support

<https://www.youtube.com/watch?v=cLRbdQv0c48>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * MY iMOW app - STIHL iMOW® robotmaaier

<https://www.youtube.com/watch?v=pu9zG93cYHU>

- * Hoe koppel je een Android telefoon via Bluetooth aan jouw Opel?

<https://www.youtube.com/watch?v=fA9TerMDNOc>

- * Hoe installeer je Android Auto? - Opel

<https://www.youtube.com/watch?v=9gnadlcoTGE>

- * Android Auto Walkthrough! | + Setup Guide!

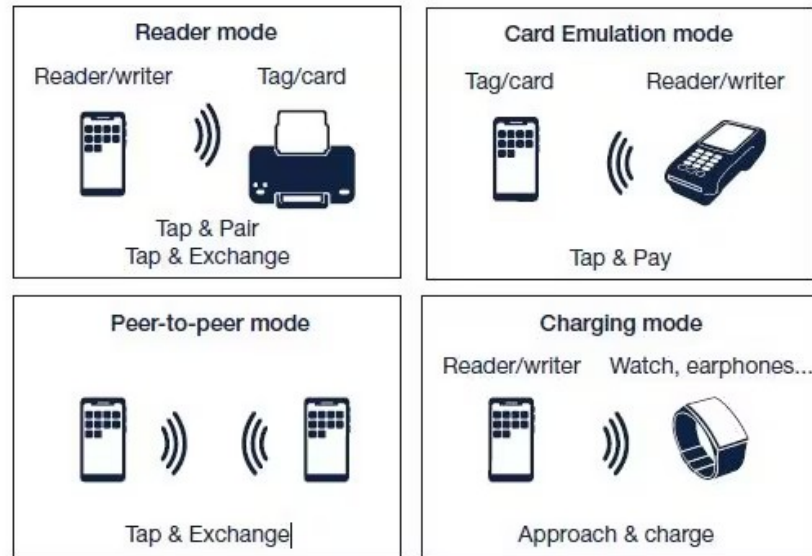
https://www.youtube.com/watch?v=hTSUQNey_jl

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

Voorbeelden van NFC gebruik

Er bestaan 2 soorten van NFC-chips:

- Passief:
 - * **NFC tags** waarop je data kan opzetten met NFC-reader/writer, die dan later door NFC-reader's kan gelezen worden;
 - * **kaarten met NFC-chip**, bijvoorbeeld: bankkaart (om contactloos te betalen), mobib-kaart, voorverkoopkaart van DeLijn
- Actief:
 - * **NFC-reader** in je smartphone of betaalterminal om informatie op een NFC-chip te lezen;
 - * **NFC-reader/writer** in je smartphone of scanner-paal op bus om informatie op een NFC-chip te lezen en te wijzigen



Extra info

Video's met meer uitleg

- * HANDIG: zo gebruik je zelf NFC-chips (ook in je smart home)

https://www.youtube.com/watch?v=9wb_cX6Tcg8

- * Hoe werkt NFC op je speaker of koptelefoon?

<https://www.youtube.com/watch?v=LeUNZZMHLP4>

- * Yes you scan

<https://www.youtube.com/watch?v=BROzRLGTQ1c>

- * ontwaarden 10 ritten kaart: Hoe doe ik: DeLijn

<https://www.youtube.com/watch?v=N0R9zSA4EGE>

Bestanden transferen via Bluetooth

- Bluetooth is beschikbaar op alle android smartphones, en kan gebruikt worden om bestanden te transferen tussen deze toestellen zonder enige wifi- of data-verbinding
- Op Samsung toestellen bestond “Quick Share” en andere android toestellen beschikten over “Nearby Share” om dit te kunnen; sinds begin 2024 werden deze oplossingen gefusioneerd en ook beschikbaar gesteld voor Windows pc’s met bluetooth; functionaliteit heet nu “Quick Share” met een nieuw icon op al deze toestellen
- Om **Quick Share** te gebruiken dien je “Bluetooth” en “Quick Share” via Notification bar te activeren; 
kies de waarde “iedereen (gedurende 10 min)” voor veld “Wie met jou kan delen”; voor geselecteerde bestanden kies je voor “Delen” (Share) en dan “Quick Share” om bestanden via bluetooth te transfereren

Extra info

Video's met meer uitleg

* Quick Share: How to share files | Samsung

<https://www.youtube.com/watch?v=UFcYxW7IE5A>

* How to transfer Data from Android to Android 2024

<https://www.youtube.com/watch?v=y4yS3LETyfQ>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

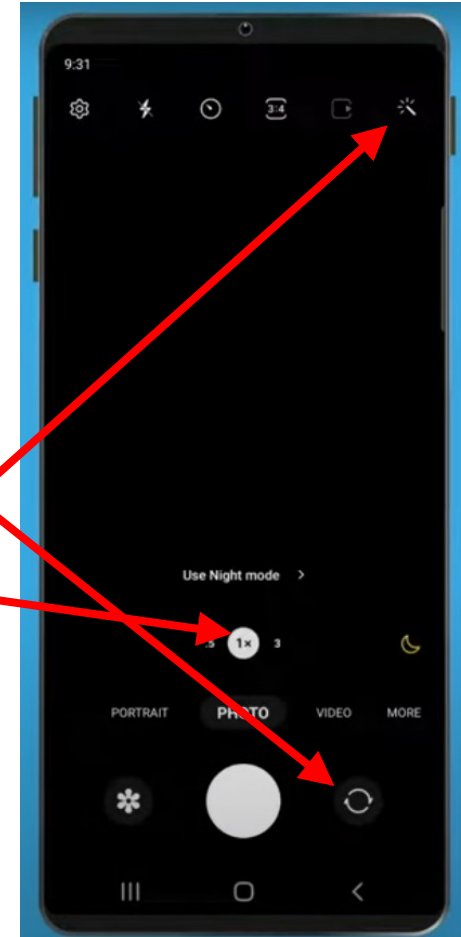
Deel 2

Betere foto's maken met Camera app

Hoe goede foto's met camera maken?

1) Kies het onderwerp voor foto en zet dit op scherm in app

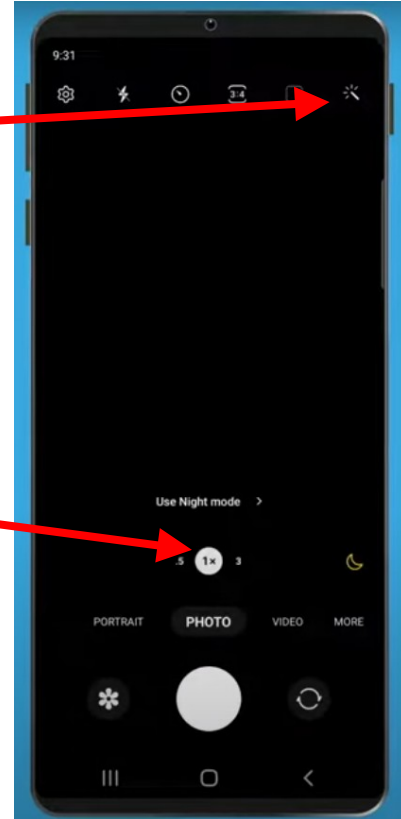
- Keuze van camera vooraan of achteraan:
 - camera vooraan (**selfie**)
 - camera's achteraan (rear; aantal is afh van toestel)keuze tussen camera vooraan/achteraan via pijlen knop
- **Beweeg zelf** naar een optimale afstand (indien mogelijk): rear camera's maken foto's met hogere kwaliteit, maar elke camera heeft een optimale vergrotingsfactor; **zoom** daarom zo **weinig** mogelijk voor optimale kwaliteit
- Zet volgende hulpmiddelen aan (via Instellingen knop):
 - * **Raster** of grid: om recht te houden en voor compositie
 - * Sluitergeluid (Shutter sound): om te horen of foto werd getrokken



Hoe goede foto's met camera maken?

2) Zoom in/uit tot gewenste inhoud op scherm van app

- Kies gewenste **beeldverhouding** (photo size): normaal 3:4, maar ook 1:1, 9:16, enz mogelijk
- In/uit-zoomen:
keuze tussen verschillende camera's achteraan gebeurt automatisch bij in/uit-zoomen (en keuze gezichtshoek);
om te zoomen kan ofwel gewenste **zoom-factor** selecteren, of “Knijp” (Pinch) vingerbeweging op het scherm toepassen;
voor iedere camera heeft een optimale zoom-factor die je best dient te kennen voor optimale kwaliteit;
selectie van **ultra-wide** mode door factor < 1 te kiezen;
selectie van **macro** mode (voor close-ups) is afh van toestel (op mijn toestel dien je op bloem icon  te klikken)



Hoe goede foto's met camera maken?

Bij het zoomen wordt automatisch geschikte rear camera (of lens) gekozen:

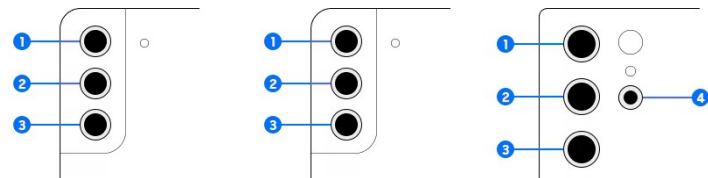
- standaard (main) camera (zoom-factor 1x en hoger)
- ultragroothoek/macro (ultra-wide) camera met autofocus (zoom-factor lager dan 1x voor “wide”, en bloem icon voor macro)
- telephoto camera's (zoom vanaf bepaalde factor, bv 5x);
deze zijn echter niet altijd aanwezig,
waardoor ver inzoomen meestal ten koste van kwaliteit gaat;
indien meerdere aanwezig, dan spreekt men van “optical zoom”

Elk van deze camera's beschikt over:

- lens met een bepaalde opening (aperture):
bepaalt hoeveel licht binnen kan,
bv “f/2” is breder en laat veel meer licht binnen dan “f/4”
- sensor met een bepaalde resolutie (resolution):
bepaalt aantal pixels (puntjes waar licht gemeten wordt),
bv “16 MP” zijn 4000 x 4000 pixels (16 miljoen pixels) op sensor;
kwaliteit van info per pixel hangt af hoeveel licht ontvangen wordt (anders ruis)

Hoe goede foto's met camera maken?

*Camera specificaties
van Samsung voorbeeld-toestellen:*



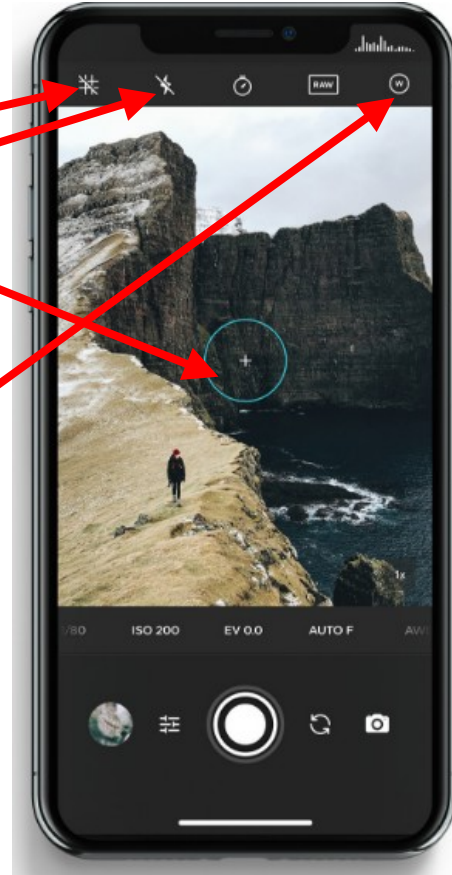
Camera	Galaxy S22	Galaxy S22+	Galaxy S22 Ultra
Front - Wide	10MP F2.2 [Dual Pixel AF], FOV 80°, 1/3.24", 1.22µm	10MP F2.2 [Dual Pixel AF], FOV 80°, 1/3.24", 1.22µm	40MP F2.2 [PDAF], FOV 80°, 1/2.8", 0.7µm
① Rear - Ultra Wide	12MP F2.2 [FF], FOV 120°, 1/2.55", 1.4µm	12MP F2.2 [FF], FOV 120°, 1/2.55", 1.4µm	12MP F2.2 [Dual Pixel AF], FOV 120°, 1/2.55", 1.4µm
② Rear - Wide angle	50MP F1.8 [Dual Pixel AF], OIS, FOV 85°, 1/1.56", 1.0µm with Adaptive Pixel	50MP F1.8 [Dual Pixel AF], OIS, FOV 85°, 1/1.56", 1.0µm with Adaptive Pixel	108MP F1.8 [PDAF], OIS, FOV 85°, 1/1.33", 0.8µm with Adaptive Pixel
③ Rear - Telephoto 1	10MP F2.4 [3x, PDAF], OIS FOV 36°, 1/3.94", 1.0µm	10MP F2.4 [3x, PDAF], OIS FOV 36°, 1/3.94", 1.0µm	10MP F2.4 [3x, Dual Pixel AF], OIS, FOV 36°, 1/3.52", 1.12µm
④ Rear - Telephoto 2	-	-	10MP F4.9 [10x, Dual Pixel AF], OIS, FOV 11°, 1/3.52", 1.12µm
Rear - Space Zoom	3x Optical Zoom Super Resolution Zoom up to 30x	3x Optical Zoom Super Resolution Zoom up to 30x	3x, 10x Dual Optical Zoom Super Resolution Zoom up to 100x



Hoe goede foto's met camera maken?

3) Verbeter kwaliteit van het beeld (focus en belichting)

- Tik op het scherm en sleep scherpstel-ring (**focus**):
geef aan welk deel van beeld het scherpste moet zijn
- Wijzig belichting bij te weinig licht:
 - * Gebruik **flits** ⚡ (flash) enkel indien nodig
 - * **Nachtzicht**-modus 🌙 (night mode):
fusie van foto's met korte (voor beeldstructuur)
en lange belichting (voor meer licht en minder ruis)
- Gebruik **HDR**-modus bij veel tegenlicht of grote contrasten:
open menu met HDR opties via Instellingen knop:
camera maakt snel opnamen met verschillende belichtingen
(exposures), en combineert die tot 1 foto, waardoor kleuren
levendiger en meer details in zowel lichte als donkere gebieden



Hoe goede foto's met camera maken?

4) Voeg gewenste effecten toe

- Portrait Mode (vervaagde achtergrond):
creeert perceptie van diepte door tegelijk meerdere camera's te gebruiken
- Panorama Mode
- Filters (opties zijn sterk afhankelijk van toestel):
 - * meestal gebruikt om temperatuur van beeld bij te stellen, bv b&w, natural, etc
 - * ook andere mogelijk, bv schoonscheidingsfilter (face-unblur mode)

5) Trek foto

- Zelftimer:
Met zelftimer kan je kiezen dat na afdrukken het nog 3 of 10 seconden duurt voor de foto gemaakt wordt (bv interessant bij groepsfoto's)
- Na trekken van foto, tik op miniatuur onder om resultaat-beeld te controleren

Extra info

Video's met meer uitleg

- * Android Camera App Walkthrough // Mobile Photography for Beginners Pt. 1

<https://www.youtube.com/watch?v=V83Na0fUfDw>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * Top 10 Smartphone Photography Beginner Mistakes

<https://www.youtube.com/watch?v=9db09xY30Xc>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * How smartphone cameras ACTUALLY work!

<https://www.youtube.com/watch?v=NzE7qj20Xwo>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

Deel 3

**Artificiele Intelligentie gebruiken
met Google Lens en Assistant app**

Hoe AI in apps gebruiken?

- **Google Lens** app heeft AI (Artificiele Intelligentie) of KI (kunstmatige intelligentie) mogelijkheden om objecten in beelden te herkennen (andere AI apps oa ook geluidsdelen);
deze app is automatisch op android smartphones aanwezig
- De functionaliteit van deze app is tevens geïntegreerd in andere apps die beelden leveren: Camera, Foto's (Photos) en Zoeken (Search) app;



in de instellingen van Camera app dien je wel Google Lens te activeren

- Google Lens zal dan in de door deze apps geleverd beelden, gedeeltes herkennen en transformeren, waarna verdere acties kunnen uitgevoerd worden

Hoe AI in apps gebruiken?



Oefeningen

- * Herken streepjes/QR-code in beeld, en zet om in tekst of hyperlink (reeds gezien in eerder gedeelte)
- * Herken geschreven of gedrukte tekst in beeld, en zet om in tekst of wijzig tekst in andere taal (via Vertaal app) op oorspronkelijke beeld:
gebruik Camera app om menukaart tijdens je reis in Spanje automatisch om te zetten naar Nederlands
- * Herken objecten in beeld en zoek gespecificeerde object in andere beelden of op verkoopsites:
- * gebruik Camera app om plant tijdens wandeling te herkennen en eigenschappen weer te geven
- * gebruik Camera app om kledingstuk dat iemand draagt, terug te vinden op verkoopsites met prijzen
- * gebruik Foto's app om te weten waar foto waarop speciaal gebouw getrokken werd

Extra info

Video's met meer uitleg

* De Handigste App voor op jouw Telefoon? | Zo Gebruik je Google Lens!

<https://www.youtube.com/watch?v=KHI-9HQ4HMQ>

Wat zijn virtuele assistenten?

- **Spraak gestuurde** virtuele assistenten bestaan reeds enige tijd; Siri van Apple, Assistant van Google, Alexa van Amazon, Bixby van Samsung zijn de meest bekende
- Deze virtuele assistenten kunnen via **AI** helpen bij verschillende taken: beantwoorden van rekenkundige vragen, aan/uit-zetten van licht (of aansturen van andere **geconnecteerde apparaten**), foto trekken in 5 sec, vragen over weer (gebruik internet), telefoon bedienen, vragen naar titel van lied na zang, vertellen van grap of maken van speech, enz



Hoe Google Assistant gebruiken?

- **Google Assistant** app staat standaard geïnstalleerd op Android; zijn opvolger (Google Gemini) is ook al beschikbaar via Play Store
- Om Assistant te initialiseren, start Google app, klik op de Profile knop (bovenaan rechts) en kies Instellingen > “Google Assistant”; klik “Algemeen” om de Assistant te activeren of deactiveren; klik “Hey Google en Voice Match” om “Hey Google” te activeren (zodat Google je stem leert herkennen)
- Om Assistant te starten, klik lange tijd op Home knop of zeg “Hey Google”; om Assistant te muten, ga naar “Google Assistant” menu en kies “Assistent-stem en -geluiden” > Telefoon



Oefeningen

- * Via Instellingen > Meldingen > “Apparaat- en app-meldingen” toestaan dat Google app meldingen kan tonen
- * Spreek “Hey Google” en vervolgens “Toon Meldingen” in

Extra info

Video's met meer uitleg

- * De Google App en Google Assistant (Android 13)

<https://www.youtube.com/watch?v=yONBaBWmYi4>

- * Probeer de Google Assistant. Vanaf nu helemaal Nederlands.

<https://www.youtube.com/watch?v=RAoRaz7mMIA>

- * Google Assistant - What you need to know

https://www.youtube.com/watch?v=CusRswT-1_U

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * Android 101: Google Assistant | Android Voice Control

<https://www.youtube.com/watch?v=ZXRSZhQQ-yc>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * De 10 ChatGPT prompts die ik dagelijks gebruik

<https://www.youtube.com/watch?v=QqF2u8zEi9Q>

Deel 4

Bewust omgaan met digitale fraude



Waarom zijn onderstaande tips niet voldoende voor beveiliging?

6 Tips to Secure Your Mobile Devices



Use screen locks and biometrics



Update your OS and apps regularly



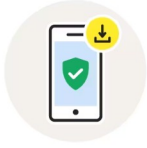
Use a VPN to protect your traffic



Create encrypted backups of personal information



Create strong passwords and enable 2FA



Use mobile security software for efficient security

Kennis opdoen over gevaren bij meer informatisering om er bewuster mee te kunnen omgaan



Je kan dan je **gedrag** aanpassen om deze **gevaren** zoveel mogelijk te **beperken**; dikwijls is je keuze een afweging van voordelen (gebruiksgemak) en nadelen (technische complexiteit en gevaren voor misbruik)

Wat is computer fraude?

- Fraudeurs zijn erg inventief om computer beveiligingen te omzeilen; regelmatig komt dit type van fraude in het nieuws
- Om je tegen malafiden beter te wapenen en om na een fraude beter te kunnen reageren, dien je je best hierover te informeren; in dit deel worden daarom veel voorkomende fraude-gevallen onder de loep genomen in de hierop volgende videos

Extra info

Video's met meer uitleg

- * Is mijn smartphone goed beveiligd?

<https://www.youtube.com/watch?v=jUIAebdkv6I>

- * Hacking en bankkaartfraude bij een bedrijf in Wetteren

<https://www.youtube.com/watch?v=NAOopIR5VGg>

- * Whatsapp-fraude

<https://www.youtube.com/watch?v=2xqa-VgGMuQ>

- * Webinar Fraude herkennen en voorkomen

https://www.youtube.com/watch?v=pQ_Sz2xsJhI

- * Webinar - Fraude, stel ons je vraag | ING België

<https://www.youtube.com/watch?v=zb3Q5ZSc7Rs>

- * Wat is de FSMA?

<https://www.youtube.com/watch?v=0Hte2beGZ14>

Extra info

Video's met meer uitleg

- * Bescherm je debetkaart als je geld afhaalt

<https://www.youtube.com/watch?v=7mLymTi2KxI>

- * Wanneer fraudeurs zich voordoen als ING aan de telefoon

<https://www.youtube.com/watch?v=U5DhStikpil>

- * Kun je mijn geld stelen via WhatsApp?

<https://www.youtube.com/watch?v=StRLdxUwKIY>

- * Kun je geld stelen met mijn rekeningnummer?

<https://www.youtube.com/watch?v=IGVMgfEazcA>

- * Kan men geld stelen via de contactloze functie van mijn kaart?

<https://www.youtube.com/watch?v=GiPX1pxmg6Q>

- * Kan er geld verdwijnen van mijn rekening als ik geen codes gedeeld heb?

<https://www.youtube.com/watch?v=dzgsIY6uc-A>

Deel 5

Openbare WiFi veilig gebruiken met ProtonVPN en Hotspot



Waarom VPN gebruiken?

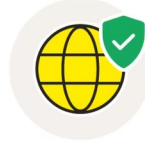
6 Tips to Secure Your Mobile Devices



Use screen locks and biometrics



Update your OS and apps regularly



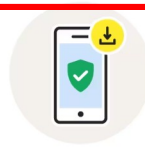
Use a VPN to protect your traffic



Create encrypted backups of personal information



Create strong passwords and enable 2FA

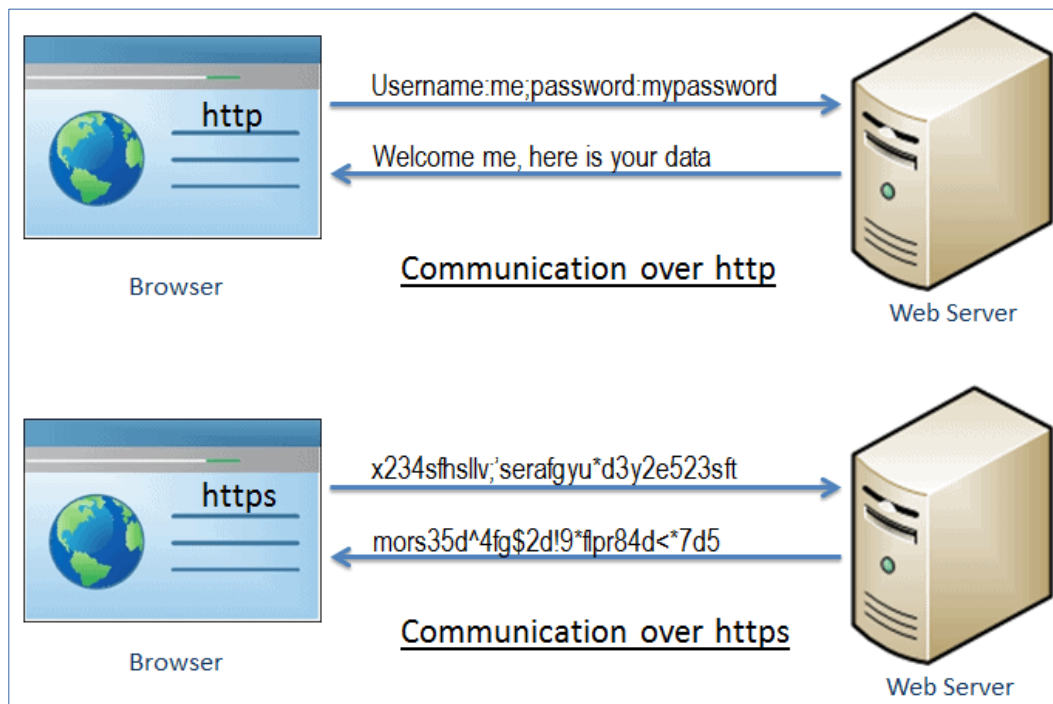
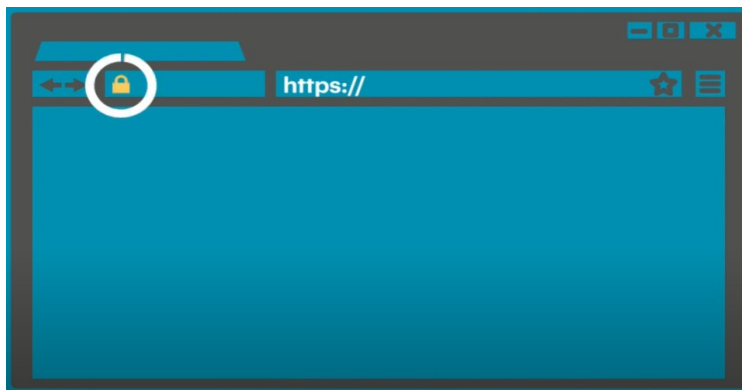


Use mobile security software for efficient security



Wat is een beveiligde verbinding?

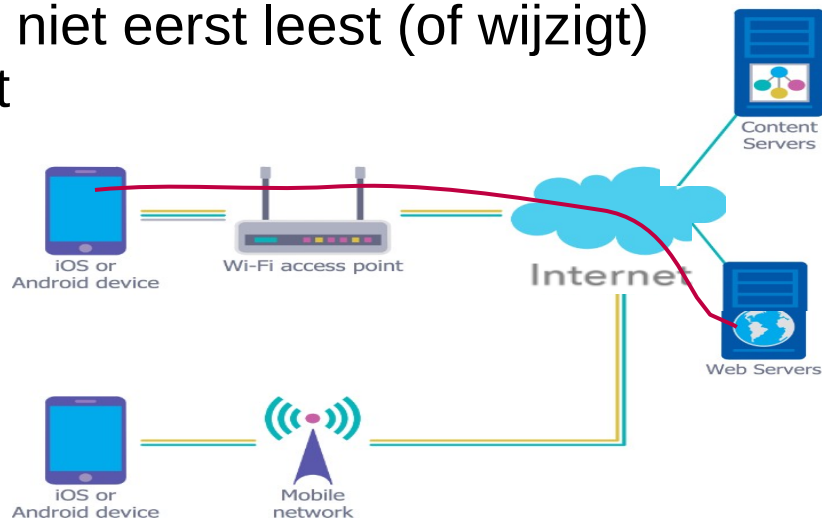
- Bij een beveiligde verbinding tussen mobile en web server, wordt alle communicatie versleuteld (encrypted) via **https**, en wordt nagegaan of het wel degelijk de gewenste web server is





Waarom VPN-netwerk gebruiken?

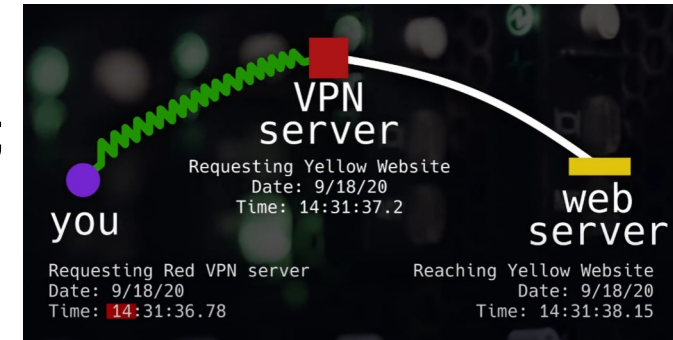
- Niet alle web servers maken gebruik van een beveiligde verbinding (communicatie is leesbaar door onbevoegden) en zelfs bij een beveiligde verbinding is zichtbaar wie wanneer met welke web servers communiceert
- **Openbare Wifi**-netwerken (in stations, hotels, terras, enz) verhogen hierbij nog het **risico**, omdat je niet weet of aangeboden Wifi-toegangspunt echt te vertrouwen is en je communicatie niet eerst leest (of wijzigt) alvorens door te sturen naar internet





Wat is een VPN-netwerk?

- **VPN** (Virtual Private Network):
geen rechtstreekse communicatie met gewenste web server,
maar enkel geencrypteerde communicatie met vooraf gekozen VPN server
die dan jouw request doorstuurt naar gewenste web server
- Voordelen:
 - * tussen jou en VPN server is alles geencrypteerd
en veilig, ook over openbaar of onbekend netwerk;
 - * web server kan jouw ip-adres niet achterhalen
(enkel dat van VPN server door hun gezien)
- Nadelen:
 - * vertrouwen in VPN provider is noodzakelijk,
omdat deze wel je ip adres ziet en je communicatie decodeert;
 - * tragere communicatie omdat alles via VPN server moet passeren





Hoe Proton VPN op mobile gebruiken?

- Er bestaan vele VPN client apps;
een populaire VPN app met een gratis versie is “Proton VPN”
- Installeer “**Proton VPN**” app via Play Store,
en kies bij de setup voor de gratis installatie en gebruik;
voeg een account toe tijdens setup (email adress, password)
- Na het starten van de app klik je op “Verbind” knop en al je
communicatie zal via Proton VPN server gebeuren
- Om het gebruik van VPN te stoppen klik je op “Verbinding verbreken”
knop in de app
- Via volgende website welke informatie je met/zonder VPN vrijgeeft:
<https://surfshark.com/nl/what-is-my-ip>





Hoe mobile hotspot gebruiken?

- Indien je zelf geen mobile data hebt en geen gebruik wil (of kan) maken van een wifi netwerk, dan kan iemand anders tijdelijk een **hotspot** op zijn mobile opzetten zodat je via zijn mobile (en zijn mobile data) op het internet kan
- Via Instellingen > “Netwerk en ...” > “Hotspot en ...” kan je de Wifi-hotspot aanzetten



Extra info

Video's met meer uitleg

- * Veilig internetten op vakantie | Slim & Veilig Online

https://www.youtube.com/watch?v=4RnKfz_a1Wc

- * Gratis wifi tijdens je vakantie: zo surf je veilig

<https://www.youtube.com/watch?v=PIFruISQSNs>

- * Wat is een VPN en hoe werkt het? | NordVPN

https://www.youtube.com/watch?v=_KeU7pmBFnU

- * Veilig internetten op vakantie | Slim & Veilig Online

https://www.youtube.com/watch?v=4RnKfz_a1Wc

- * How to use ProtonVPN Tutorial Proton VPN FREE ... - Review 2024

<https://www.youtube.com/watch?v=otKaa2dANIM>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * Wifi-hotspot maken met je Android-smartphone: zo doe je dat

<https://www.youtube.com/watch?v=VBriRsmPAds>

Deel 6

**Anoniem gebruik van browser,
zoekmachine en email**



Wat wordt met “privacy” bedoeld?

- Wanneer een bedrijf zijn digitale diensten aanbiedt, dan dien je om daar gebruik van te kunnen maken dikwijls de door hun opgestelde voorwaarden te aanvaarden (deze voorwaarden worden slechts door weinigen gelezen); doordat je hun diensten gebruikt, zal dit bedrijf hierdoor allerlei **informatie over jou** beschikken en jij geeft door jouw aanvaarding aan wat dit bedrijf hiermee mag doen: bijhouden/**verzamelen** (en hoelang), **analyseren**/combineren, **doorspelen** aan derden, enz; soms is dit door jou **ongewild** en wordt hier **misbruik** van gemaakt door derden
- Zo is Google bekend om het gebruiken en verzamelen van alle gegevens over jou en deze door te spelen aan derden voor reclame-doeleinden om geld te verdienen; vele bedrijven halen op deze manier hun inkomsten binnen; Bv gratis 15GB Cloud opslag, gratis gebruik van zoekmachine in browser Veel gebruikte uitspraak: "Als je niet moet betalen voor een dienst, dan ben je geen klant maar zelf het product waar geld aan wordt verdiend"



Hoe meer privacy bij browser gebruik?

- Bij het gebruik van de populaire **browsers** (Google Chrome, MS Edge, Mozilla Firefox, Apple Safari) wordt al jouw surfgedrag verzameld: welke websites bezocht je, waar bevind je je en wanneer, welke pc/smartphone gebruik je en nog veel meer
- Je kan deze blootstelling beperken door te kiezen voor meer private browsers;
je kan bijvoorbeeld kiezen voor “**Brave**”, een private browser die jouw gegevens niet bijhoudt;
dit gaat ten koste van wat gebruiksgemak: je zal bijvoorbeeld bij herhaaldelijk bezoek van een website telkens opnieuw moeten inloggen
- Vele personen gebruiken daarom ook meerdere browsers;
bv Google Chrome voor normaal gebruik en Brave indien privacy gewenst





Hoe meer privacy bij zoeken op web?

- **Zoekmachines** zijn populaire websites in browsers en worden gebruikt om interessante web pagina's over een onderwerp terug te vinden; Google Search is verreweg de meest populaire zoekmachine



- Deze zoekmachine zal al je zoekopdrachten en gekozen websites verzamelen, en verzamelde gegevens over jou doorspelen aan derden die voor reclame willen betalen; je zal dan deze gesponsorde reclame specifiek gericht aan jou als eerste terugvinden in de zoekresultaten
- Je kan deze blootstelling beperken door te kiezen voor meer private zoekmachines; je kan bijvoorbeeld kiezen voor **DuckDuckGo**, een private zoekmachine die jouw gegevens niet bijhoudt en doorgeeft





Hoe meer privacy bij email gebruik?

- **Email inbox** is een account waar emails worden ontvangen en opgeslagen; **email alias** is een email adres gecreeerd voor een welbepaald doel; een email inbox kan de uiteindelijke bestemming zijn van vele aliases
- Je kan bijvoorbeeld al je emails opdelen in aparte email inboxes:
 - * persoonlijke inbox: enkel gekend door familie en vrienden
 - * gedeelde inbox: voor alle andere communicatie met bedrijven, enz
 - * pseudoniem inbox: hoort bij een fictieve persoon en wordt gebruikt waar een email-adres moet verplicht maar ongewild ingegeven worden
- Er bestaan **anonieme email-diensten** die je echte email-adres te verbergen via email aliasen: AnonAddy, MailDrop, SimpleLogin, Yahoo, Gmail, enz; deze creëren willekeurige email aliasen die alle emails doorsturen naar je echte inboxes; op deze manier kan je email-spam vermijden en je email inbox anoniem te houden; je kan dan een email alias voorzien per groep, bv een alias voor alle nieuwsbrieven, een voor alle shopping accounts, enz



Hoe meer privacy bij email gebruik?

- **SimpleLogin** is een populaire email alias service met gratis versie; open web pagina <https://simplelogin.io/nl/> of installeer “Simple Login” app



Oefeningen

- * Open SimpleLogin en creëer een account (sign in) gekoppeld aan jouw email inbox
- * Login, creëer subdomein “mytest.aleaas.com” (subdomain) en defineer dit subdomein als “default subdomain for aliases” (settings)
- * Creeer alias “john.doe@mytest.aleaas.com”
- * Verstuur een email naar dit email adres

Pricing	
SimpleLogin is open source , can be self-hosted and is 100% funded by the community. We do not use your data, track you or show you ads. SimpleLogin depends on your support to keep the service running and develop new features.	
Free \$0	Premium \$30/year or \$4 billed monthly
✓ 10 aliases ✓ Unlimited Bandwidth ✓ Unlimited Reply/Send from alias ✓ 1 mailbox ✓ Browser extensions Chrome, Firefox and Safari ✓ iOS, Android App ✓ Secure your account with TOTP and/or Webauthn (FIDO) ✓ Sign in with SimpleLogin	✓ Everything in the Free Plan ✓ Unlimited aliases ✓ Unlimited custom domains Bring your own domain to create aliases like contact@your-domain.com ✓ Catch-all (or wildcard) domain ✓ Initiate a new email from your alias You can create a reverse-alias to send an email to a new contact. ✓ 5 subdomains ✓ 50 directories/usernames ✓ Unlimited mailboxes ✓ PGP Encryption

Extra info

Video's met meer uitleg

- * Zoekmachine vs. browser

<https://www.youtube.com/watch?v=AjNh3545Gsg>

- * Anoniem surfen

<https://www.youtube.com/watch?v=nbrAe6RESuE>

- * Brave - basics van de browser

<https://www.youtube.com/watch?v=b-27BGzb3-U>

- * How To Update Brave Browser On Android

<https://www.youtube.com/watch?v=8RNetKpyyRo>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * How to Use Brave Private Web Browser

<https://www.youtube.com/watch?v=9UxnRTgO6Yk>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

Extra info

Video's met meer uitleg

- * Zoekmachines - Klik & Tik. Het internet op - Oefenen.nl

https://www.youtube.com/watch?v=2R79ZQX_IHw

- * Protecting Personal Privacy

<https://www.youtube.com/watch?v=vTWywg4DVpg>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * Why Is Everyone Switching To DuckDuckGo?

<https://www.youtube.com/watch?v=BMYYlVaJlr8>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * Is DuckDuckGo veilig? Beoordeling van Zoekmachine DuckDuckGo in 2021

<https://www.youtube.com/watch?v=YJWWyh1btbU>

Extra info

Video's met meer uitleg

- * STOP Giving Your Real Email Address (do this instead)

<https://www.youtube.com/watch?v=J7uGUD9kprs>

I Tested 5 Secure Email Providers (THIS is the best Gmail alternative)

<https://www.youtube.com/watch?v=72eG84gGR0s>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * STOP Giving Out Your Email - Do This Instead

<https://www.youtube.com/watch?v=i4PBq-jBCwg>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * SimpleLogin Review - How Have I Survived Without It!?

<https://www.youtube.com/watch?v=JMWfsOVrDkw>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

Extra info

Video's met meer uitleg

* Why Care About Internet Privacy?

<https://www.youtube.com/watch?v=85mu9PLWCul>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

* Data Brokers: The Dark Industry of Selling Your Identity for Profit

<https://www.youtube.com/watch?v=uZ2l-kk5ihk>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

* How To Delete Yourself Off The Internet

<https://www.youtube.com/watch?v=t0Wr8TuFz1o>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

* GDPR: What Is It and How Might It Affect You?

<https://www.youtube.com/watch?v=j6wwBqfSk-o>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

Deel 7

Toegang tot app en website beveiligen met Password Managers



Hoe toegang tot app/site beveiligen?

6 Tips to Secure Your Mobile Devices



Use screen locks and biometrics



Update your OS and apps regularly



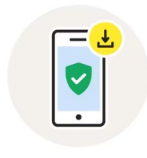
Use a VPN to protect your traffic



Create encrypted backups of personal information



Create strong passwords and enable 2FA



Use mobile security software for efficient security



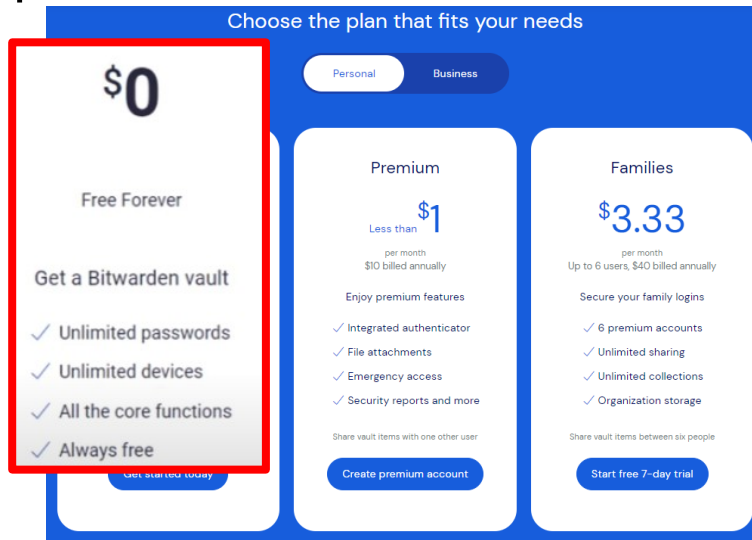
Wat is een password manager?

- Zelfs indien iemand kan inloggen op je phone of pc, heeft deze persoon nog geen toegang tot apps en websites met een eigen aparte login
- Meeste smartphone of pc gebruikers hebben vele online accounts elk met een eigen paswoord, bv voor je email, bank, federale-overheid, doccle, enz; ofwel gebruik je voor elk van deze accounts hetzelfde (of variatie van) paswoord (wat erg onveilig is), ofwel gebruik je een ander paswoord voor elke account (veiliger maar onhandiger)
- Het onthouden van al deze paswoorden is een echte uitdaging; een wachtwoord-beheerder (**password manager**) is een programma dat dit gemakkelijker maakt, door al je account-gegevens inclusief paswoord te bewaren in een soort digitale kluis (**vault**) die op je phone of in cloud staat; je hoeft nu slechts 1 paswoord (van manager) te onthouden om toegang tot je kluis te krijgen en om zo al je paswoorden te kunnen gebruiken



Wat is een password manager?

- Er bestaan vele password managers; Google heeft ook een password manager ingebouwd in Chrome browser; deze heeft echter nogal wat nadelen (enkel in Chrome, beperkt)
- **Bitwarden** is een veilige en populair keuze,  gebruikt E2E encryptie en is beschikbaar op Android en Windows
- We zullen gratis versie van Bitwarden app installeren op je phone, en daarna een account met sterk paswoord aanmaken; de kluis zal altijd in Bitwarden Cloud staan
- Daarna kunnen we site per site al ieder account met paswoord voor een site opslaan in de Bitwarden kluis



Choose the plan that fits your needs

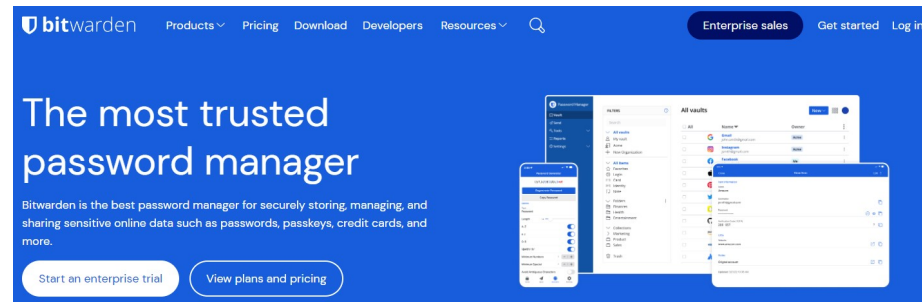
Personal	Business	
\$0 Free Forever Get a Bitwarden vault ✓ Unlimited passwords ✓ Unlimited devices ✓ All the core functions ✓ Always free	Premium Less than \$1 per month \$10 billed annually Enjoy premium features ✓ Integrated authenticator ✓ File attachments ✓ Emergency access ✓ Security reports and more Share vault items with one other user Create premium account	Families \$3.33 per month Up to 6 users, \$40 billed annually Secure your family logins ✓ 6 premium accounts ✓ Unlimited sharing ✓ Unlimited collections ✓ Organization storage Share vault items between six people Start free 7-day trial



Hoe Bitwarden gebruiken?

(1) Aanmaak van een Bitwarden account

- Open de Bitwarden site in je browser:
<https://bitwarden.com/>
- Kies “Get started” en breng vereiste account-gegevens in;
”email address”, “name” en
”master password” zijn belangrijkste gegevens die je niet mag vergeten;
kies steeds een **sterk wachtwoord**
- Klik “Create account” en je account met private, geencrypteerde kluis (vault) wordt dan aangemaakt



bitwarden Products Pricing Download Developers Resources

Enterprise sales Get started Log in

The most trusted password manager

Bitwarden is the best password manager for securely storing, managing, and sharing sensitive online data such as passwords, passkeys, credit cards, and more.

Start an enterprise trial View plans and pricing

bitwarden

The Bitwarden Password Manager

Trusted by millions of individuals, teams, and organizations worldwide for secure password storage and sharing.

- Store logins, secure notes, and more
- Collaborate and share securely
- Access anywhere on any device
- Create your account to get started

Forbes
"Bitwarden boasts the backing of some of the world's best security experts and an attractive, easy-to-use interface"

Email address (required)

You'll use your email address to log in.

Name

What should we call you?

Master password (required)

Important: Master passwords cannot be recovered if you forget it! 12 character minimum

Re-type master password (required)

Master password hint

A master password hint can help you remember your password if you forget it.

☒ Check known data breaches for this password

☐ By checking this box you agree to the following:
[Terms of service](#), [Privacy policy](#)

Create account



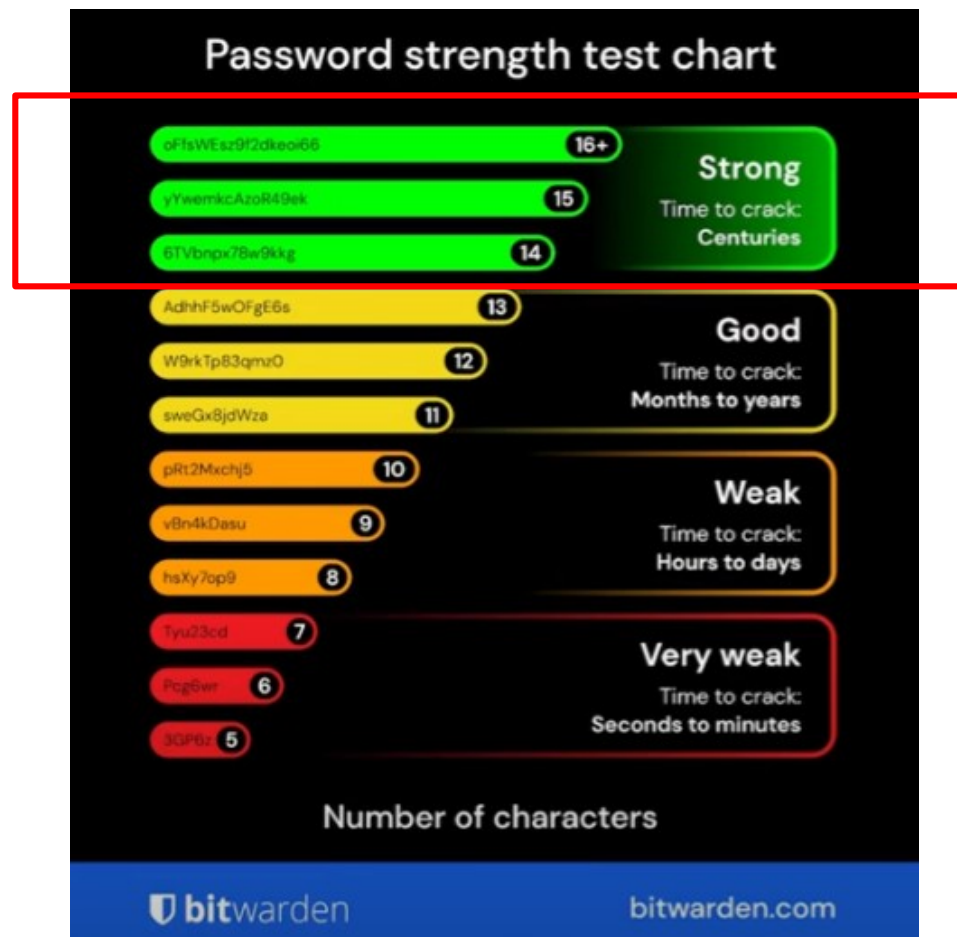
Hoe Bitwarden gebruiken?

Wat is een sterk master password?

minstens 16 tekens

volgens aanbeveling van Bitwarden;

dit kunnen we eenvoudig bekomen door een “passphrase” te gebruiken (een reeks woorden die eenvoudig te onthouden is, maar wel veel karakters bevat), bijvoorbeeld: “Aan het strand van Oostende, op 1 zomerse dag...”





Hoe Bitwarden gebruiken?

(2) Installatie van Bitwarden en login op al je apparaten

- Installeer “Bitwarden – Wachtwoordbeheer” app via Play Store op je android phone, en via download page <https://bitwarden.com/download/> op je Windows pc
- Voor de meeste browsers kan je ook een Bitwarden extension installeren; ik installeerde deze voor de Chrome en Brave browsers op phone en pc; de Bitwarden extension kan je nu vast-pinnen in de browser-toolbar
- Via de app of browser extension kan je nu inloggen in Bitwarden met je email adres en master password



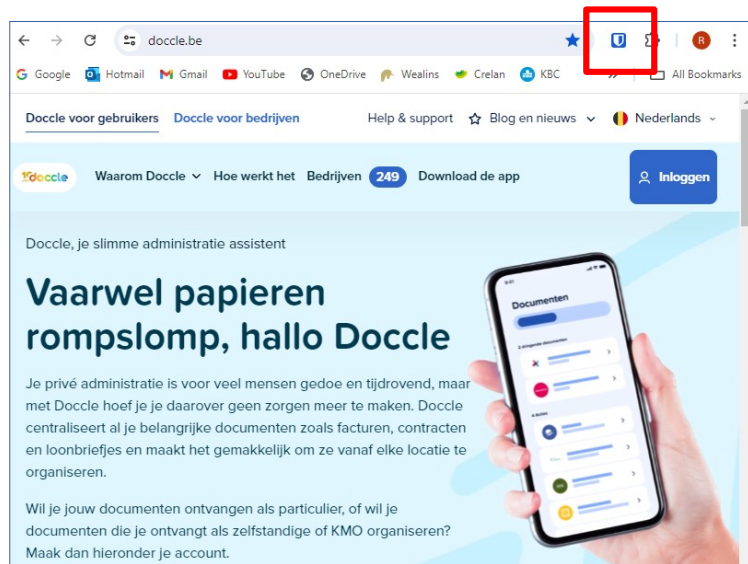
Hoe Bitwarden gebruiken?

- Om conflicten tussen verschillende password managers te voorkomen, dien je best de andere managers te disable-en;
om de Google password manager in Chrome te disable:
 - * klik “3 puntjes” icoon bovenaan rechts, kies “Settings > Autofill and passwords”
 - * wis alle paswoorden in je Google password manager, nadat je deze hebt ge-exporteerd naar een csv file (zullen we later importeren in Bitwarden)
 - * disable “Google Password Manager”, “Payment methods” en “Addresses and more”
- Je Bitwarden kluis wordt end-to-end encrypted opgeslagen in de Cloud gebruik makend van je master password van je account;
de belangrijkste **items** opgeslagen in je individuele **vault** zijn:
 - * **security settings**: gekozen beveiliging voor toegang tot je kluis
 - * **logins**: alle gegevens om te kunnen inloggen in een beveiligde web site; bevat meestal een name, username, password en uri
 - * logins kan je organiseren in **folders** of als **favorite** aanduiden



Hoe Bitwarden gebruiken?

- (3) Importeer bestaande of creeer nieuwe logins voor beveiligde web sites
- Importeer de eventueel in Chrome ge-exporteerde accounts in Bitwarden
 - Om een nieuwe login te creeeren, gebruik je best de browser-extension:
 - * navigeer naar de site waarvoor je een nieuwe login wil hebben, bv *https://doccle.be/* in Chrome op pc
 - * klik op Bitwarden icon en daarna op “+” om nieuwe login voor Doccle te creeeren
 - * het “Add item” venster verschijnt met Type, Name en URI al ingevuld
 - * breng Username, Password, Notes, enz in (sterk paswoord kan gegenereerd worden)
 - * klik “Save” om deze login te bewaren





Hoe Bitwarden gebruiken?

(4) Gebruik van Bitwarden om toegang te krijgen tot beveiligde site

- We willen nu inloggen op de Doccle web site via Bitwarden op android; eerst dienen we hiertoe in te loggen via Bitwarden app
- Open <https://doccle.be/> in Chrome op onze smartphone; klik op “Inloggen” knop om de “Log in” pagina te openen; klik op “Bitwarden” icon (boven toetsenbord na klikken in een veld) en kies Login om scherm-gegevens in te vullen; je kan setting “Options > Auto-fill on page load” (of “Instellingen > Auto-invullen”) in Bitwarden app aanpassen, zodat extensie automatisch login gegevens zal trachten in te vullen bij laden van pagina
- Installeer de Doccle app op je smarphone via Play Store; open de Doccle app en automatisch ga je naar dezelfde “Log in” pagina als hierboven



Hoe Bitwarden gebruiken?

(5) Bitwarden instellen om kluis te ontgrendelen via biometrics

- Een Web Vault wordt meestal ontgrendeld (unlocked) via een master password, maar dit kan ook gebeuren via vingerafdruk of gezichtscan om meer gebruiksgemak te hebben
- Hiervoor moeten enkele Instellingen in Bitwarden aangepast worden: login je kluis via browser of app, klik “Instellingen” (Settings) icon onderaan en kies “Accountbeveiliging” (Account security) > “Ontgrendelen via Biometrie” (Unlock with biometrics)

(6) Maak regelmatig een backup van je Bitwarden kluis

- Login je kluis via browser of app, klik “Instellingen” (Settings) icon onderaan en kies “Kluis” (Vault) > “Kluis exporteren” (Export vault)
- Bewaar deze file op een veilige plaats en verwijder mogelijke copies op je systeem

Extra info

Video's met meer uitleg

- * Wachtwoordmanager: wat is het en welke moet je hebben?

<https://www.youtube.com/watch?v=DGIDM8BH0OQ>

- * Wachtwoordmanager Bitwarden

<https://www.youtube.com/watch?v=g-Z5BUT4muw>

- * Bitwarden - desktopapplicatie

<https://www.youtube.com/watch?v=rGuJ9SgTVqI>

- * Bitwarden 101: User Walkthrough (6 video's)

https://www.youtube.com/watch?v=0VJMM6-nwy0&list=PL-IZTwAxWO4VKISOqPdMBXAtKBAu0gd4_

How to use Bitwarden on Android

<https://www.youtube.com/watch?v=qyFeEZMZpEY>

How to Fix Password Autofill Not Working on Android...

https://www.youtube.com/watch?v=QZlb-4E_z4M

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

Extra info

Video's met meer uitleg

- * How to unlock your Bitwarden vault with biometrics

<https://www.youtube.com/watch?v=IOaxuHwf4Bs>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * The Most Important Bitwarden Setting You Never Heard Of

<https://www.youtube.com/watch?v=ELp3V1j3rhU>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * How to Retrieve Your Bitwarden Recovery Code

<https://www.youtube.com/watch?v=-jimy3nXm1g>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * I Tested 7 Password Managers: the BEST of 2024 is...

<https://www.youtube.com/watch?v=BsVkVa0n0T0>

Bitwarden Review 2024 | Is it Actually Secure?

<https://www.youtube.com/watch?v=kXg02mmMako>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

Deel 8

Veilige backup maken van bestanden op smartphone



Waarom backup's maken?

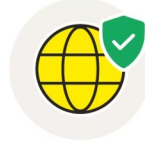
6 Tips to Secure Your Mobile Devices



Use screen locks and biometrics



Update your OS and apps regularly



Use a VPN to protect your traffic



Create encrypted backups of personal information



Create strong passwords and enable 2FA



Use mobile security software for efficient security



Wat is een goede backup?

- **Backup**-en is het maken van reserve-copies van al je belangrijke folders en bestanden en deze copies dan te bewaren op een veilige plaats; bij verlies van de originele bestanden, kan je deze bestanden vanaf je copies dan terugzetten (**restore**) op de originele (of andere) plaats
- Het regelmatig aanmaken van een goede backup is belangrijk om geen belangrijke gegevens te verliezen bij virusinfecties of bij verlies/beschadiging van je mobile; gevolgen van virusinfecties ontdek je mogelijk pas na enige tijd; het is daarom niet voldoende om enkel een copie van de laatste toestand te bewaren, maar een **aantal copies in de tijd** te maken en bewaren (om te kunnen teruggaan naar de copie gemaakt voor de infectie)
- Backups dienen best ook zo **automatisch** mogelijk te gebeuren, omdat ze eenvoudig en frequent dienen uitgevoerd te worden



Wat is een goede backup?

- Bestanden met vertrouwelijke of gevoelige informatie wil je ook **niet toegankelijk maken voor derden**;
bij opslag in de cloud door derden, dienen je folders en bestanden daarom met jouw privé-sleutel eerst geencrypteerd te worden alvorens deze door te sturen over het internet en op te slaan in een data center;
dit wordt End-to-End (E2E) encryption genoemd
- **Google One** opslag is meer bedoeld om bestanden ruimer beschikbaar te maken en voor phone device backup, maar biedt **geen E2E encryption**:
bestanden worden wel geencrypteerd doorgestuurd en geencrypteerd opgeslagen, maar de versleuteling zelf gebeurt door Google;
Google kan dus al de opgeslagen bestanden decrypteren en bekijken, en doet dit ook om allerlei redenen

Wat is de “3-2-1” backup-aanbeveling?



3

copies:
1 production +
2 backups



2

types
of storage
media



1

off-site –
in the Cloud



Hoe een goede backup maken?

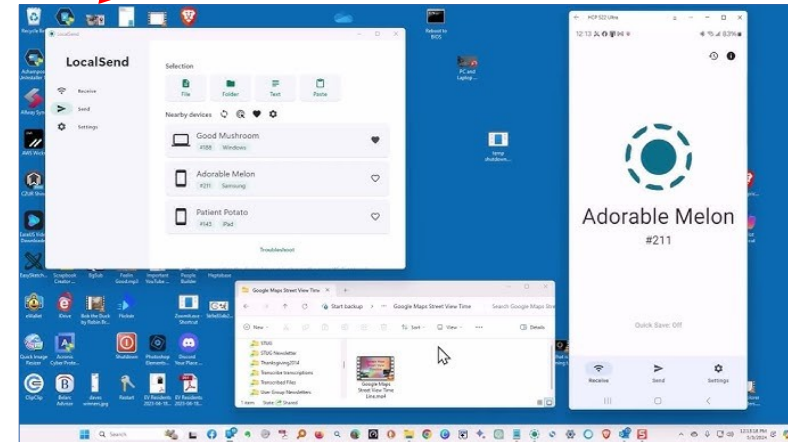
- Een goede backup dient dus 2 zaken te ondersteunen:
 - * aanmaak (en beperken) van verschillende generaties van copies
 - * geen toegang tot copies door derden
- Je kan een eenvoudig backup-systeem voor je smartphone realiseren indien je bijvoorbeeld beschikt over **eigen pc in je lokaal thuis-netwerk**:
 - * voor je eigen pc heb je waarschijnlijk reeds een backup-systeem voorzien om belangrijke bestanden op je pc veilig te stellen tegen verlies; meestal wordt hierbij ge-backup-ed naar een externe harde schijf
 - * het is daarom voldoende om een gemakkelijke manier te vinden om alle belangrijke bestanden van smartphone te copieren naar je eigen pc (via Wifi en niet over internet, waardoor geen encryptie nodig); de gecopieerde bestanden van de smartphone worden dan mee ge-backup-ed door het voorzien backup-systeem op de pc

Hoe bestanden eenvoudig transferen tussen apparaten?

- Met **LocalSend** app kan je gemakkelijk bestanden en folders transferen tussen apparaten via Wifi en zonder kabels; app vervangt andere oplossingen, zoals "Near By" van Android, "Quick Share" van Samsung, "AirDrop" van iPhone of Cloud apps; hiervoor dien je eerst op al deze apparaten (pc, tablet, iphone, android) de app te installeren



- Met **Syncthing** app kan je gemakkelijk bestanden tussen twee computers/tablets/mobiles synchroniseren



Hoe folders en bestanden backup-en op een Windows pc?

- Er bestaan vele gratis backup softwares voor Windows pc's;
“**EaseUS Todo Free**” is populaire en gratis backup-software
- Je kan met deze software en volgende planning beginnen voor backups:
 - * een Image backup wordt slechts eenmalig gemaakt (indien gewenst)
 - * een **Full backup** in het begin van iedere maand;
we houden slechts Full backup's bij van de laatste 3 maanden
 - * een **Incremental backup** (enkel wijzigingen tov vorige) iedere dag;
we houden slechts Incremental backup's bij van na laatste Full backup
- Denk eraan dat je meestal niet enkel foto's en video's op je smartphone dient te backup-en, bv ook contacten, sms-berichten, WhatsApp chats, Keep notities

Hoe folders en bestanden organiseren voor een efficiënte backup?

- Om het te backup-en data volume te beperken en je backup dus sneller te laten verlopen, kan je vooraf enkele maatregelen treffen:
 - * folders en bestanden die nooit meer zullen veranderen, dien je best apart te plaatsen, bv in een “Archief” folder; deze folder copieer je enkel manueel indien hier subfolders bijkomen; op je smartphone zou deze “**Archief**” folder de foto’s en video’s van de voorbije jaren kunnen bevatten
 - * alle folders en bestanden die regelmatig dienen gebackup-ed te worden, plaats je best als subfolders van één te backup-en folder; op je smartphone zou je de “**DCIM**” folder als enige te backup-en folder kunnen aanwijzen; de “Archief” folder dien je dus apart te plaatsen en alle andere bestanden (zoals contacten) dien je als subfolders van de “DCIM” folder te exporteren

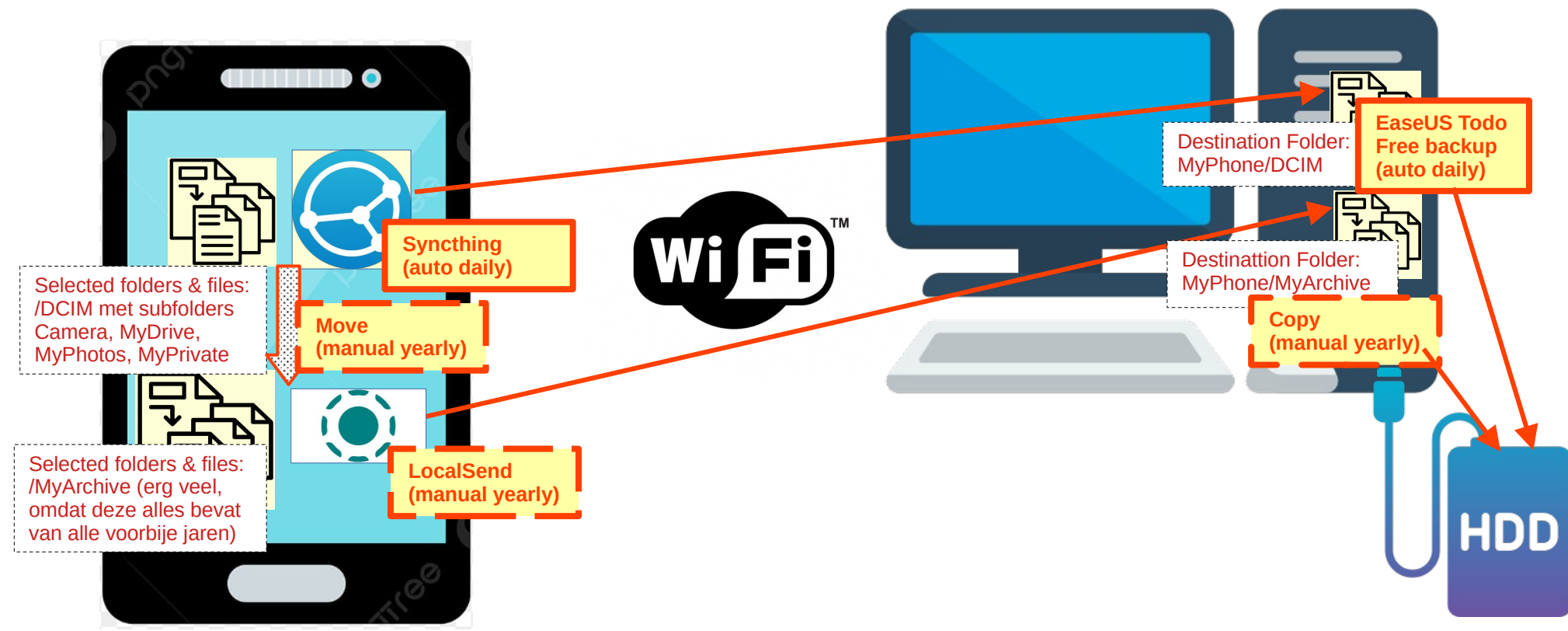
Hoe folders en bestanden organiseren voor een efficiënte backup?

Foto's en video's worden in “/DCIM/Camera” en “/DCIM/MyPhotos” folders opgeslagen; export data van andere apps als bestanden in “/DCIM/MyDrive” of “/DCIM/MyPrivate” folder:

- Gebruik “**Super backup – SMS en Contacts**” app voor export in SmsContactsBackup folder:
 - * Contacts
(open Contacts app, klik “Organiseren” knop onderaan en kies “Exporteren naar bestand”)
 - * Calendar Events
 - * Text messages (sms) en Call Logs (Phone)
- Exporteer WhatsApp chats in “WhatsApp” subfolder:
open WhatsApp app, klik 3 puntjes knop bovenaan
en kies “Instellingen > Chats > Chatgeschiedenis > Chat exporteren”
- Exporteer Keep notes in “KeepNotes” subfolder
open KeepNotes app, selecteer notities, klik 3 puntjes knop bovenaan;
kies ofwel “Sturen > CxFileExplorer” (vele txt), ofwel “Kopieren naar Documenten > Open” (1 pdf)
- Andere bestanden kan je bv exporteren in “Other” subfolder

Hoe veilige backup in praktijk?

Gebruik je eigen pc ook voor maken van veilige backups van smartphone (niet toegankelijk door derden); hiervoor dien je de gewenste data op smartphone te synchroniseren met een folder op je pc via lokale Wifi (waarbij ook geen opslagbesparend maar origineel formaat gebruikt wordt)



Extra info

Video's met meer uitleg

* Don't Use Google For Photo Backup!

https://www.youtube.com/watch?v=n_kTzu8NEyg

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

* Meet LocalSend - A Cross-Platform, Open Source Alternative to ...

<https://www.youtube.com/watch?v=2ITezMkbAqE>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

* Syncthing Made EASY

<https://www.youtube.com/watch?v=PSx-BkMOPF4>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

* Syncthing - Automatic Phone Backup to Your Computer

<https://www.youtube.com/watch?v=pClFiCZDpZk>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

Extra info

Video's met meer uitleg

- * Hoe maak je een back-up van jouw windows computer?

<https://www.youtube.com/watch?v=icj2bCoH2dk>

- * What Backup Type Do I Want: Full, Incremental, or Differential?

<https://www.youtube.com/watch?v=N1FJS-JEL9I>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * What Backup Software Should I Use?

<https://www.youtube.com/watch?v=jbSjS2owxkE>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

Extra info

Video's met meer uitleg

* Installing EaseUS Todo Free

<https://www.youtube.com/watch?v=6bGF2WNcIXo>

Creating an EaseUS Todo Emergency Disk

<https://www.youtube.com/watch?v=3fpzGxeYu-Y>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

* Backing up With EaseUS Todo Free

<https://www.youtube.com/watch?v=GwKSt0U1G6g>

Restoring an Image Using EaseUS Todo

<https://www.youtube.com/watch?v=r0d23dcTBac>

Restoring a File From an EaseUS Todo Image Backup

https://www.youtube.com/watch?v=7jR9L9B_t48

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

Deel 9

Toegang tot app en website beveiligen met 2FA



Hoe toegang tot app/site beveiligen?

6 Tips to Secure Your Mobile Devices



Use screen locks and biometrics



Update your OS and apps regularly



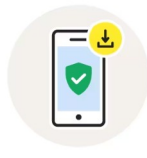
Use a VPN to protect your traffic



Create encrypted backups of personal information



Create strong passwords and enable 2FA



Use mobile security software for efficient security



Wat is 2FA?

- Toegang tot websites met persoonlijke gegevens wordt meestal beschermd met paswoorden;
op een smartphone zijn er echter heel wat apps (Google Drive, Microsoft Outlook, WhatsApp, enz) die automatisch vertrouwen op login van het toestel; indien je toegang tot dit toestel hebt, dan heb dus automatisch ook toegang tot al deze apps (wat natuurlijk onveilig is)
- Voor websites met vertrouwelijke of gevoelige informatie wil je echter meer beveiliging dan enkel via wachtwoorden;
zo gebruiken overheid en banken al reeds geruime tijd een extra beveiliging in de vorm van eID of bankkaart met kaartlezer; je dient dus naast pincode te kennen, ook een kaart in je bezit te hebben
- Met **Tweestapsverificatie** (2FA = Two Factor Authentication) wordt de toegang tot een app of website enkel verleend na 2 verschillende types van checks; de term MFA (Multi Factor Authentication) wordt soms ook gebruikt



Wat is 2FA?

- Een nog veel gebruikte, eenvoudige vorm van 2FA beveiliging voor login:
 - * eerst dien je een correct wachtwoord in te geven
 - * een sms met cijfercode wordt automatisch naar jouw telefoon gestuurd
 - * deze steeds wisselende cijfercode moet je dan inbrengenPas na correcte uitvoering van dit inlog-proces krijg je toegang tot website
- Voor een toegangsbeveiliging met 2FA dien je dus niet alleen een paswoord **kennen**, maar ook een correct toestel in bezit te **hebben**;
bijvoorbeeld smartphone met jouw telefoonnummer in vorig geval
- Om WhatsApp te beveiligen met hun 2FA:
open WhatsApp app, klik puntjes knop, kies “Instellingen > Account > Verificatie in twee stappen”;
extra verificatie gebeurt door inbreng van pincode bij login in app
- Om Microsoft Outlook te beveiligen:
open Outlook app, klik menu knop, dan klik “Instellingen” knop en kies “App-vergrendeling”;
extra verificatie gebeurt door inbreng van vingerafdruck bij unlock in app



Wat is 2FA?

Meest voorkomende vormen van 2FA (geordend van minst naar meest veilige):

- **Email** met een eenmalig bruikbare code
- **SMS en Telefoon oproep** met een eenmalig bruikbare code
- **Push Notification** verstuurt een prompt naar betrouwbare toestellen wanneer een login poging wordt uitgevoerd
- **Biometric** met een vingerafdruk of gezichtsherkenning
- **Software** vorm van 2FA vereist dat gebruiker eerst een 2FA-authenticatie-app installeert op zijn phone of desktop en daarna instelt door een geheime lange tekst of geheime QR-code van iedere te beveiligen website ontvangt en inbrengt ("seed"); om daarna in te loggen dient gebruiker eerst correct username en password in te brengen, en vervolgens via deze **Authenticator app** (op ander toestel) een door software-gegenereerde, seed-en-tijd-gebaseerde eenmalige passcode (ook TOTP of software token genoemd) af te lezen en in te brengen in hun login; deze passcode verandert meestal om de 30 sec
- **Hardware** vorm van 2FA vereist dat je een security key inpluigt in de USB poort; deze genereert nieuwe cijfercode in regelmatige tijdsintervallen en stuurt deze automatisch door



Waar wordt 2FA zoal gebruikt?

- Al heel wat bedrijven hebben websites met 2FA-ondersteuning; op volgende web pagina vind je een lijst: <https://2fa.directory/be/>
- *Om Gmail (en hierdoor alle Google Cloud services) te beveiligen met 2FA:*
 - * *open Chrome browser, klik op je Profiel icoon (bovenaan rechts), kies “Beheer Google account” om “Google account” pagina te openen*
 - * *klik op “Beveiliging” (Security) optie in linker-menu, en scroll naar beneden tot sectie “Inloggen bij Google” (How you sign in to Google)*
 - * *klik “Verificatie in 2 stappen” (2-Step Verification), en kies optie “Telefoonnummer” (Phone number) in “2e stappen” (Second steps)*
- Enkele andere voorbeelden:
WhatsApp (via SMS, Phone call), Gmail (via SMS, Phone call, HW, SW), Microsoft Outlook (via SMS, Phone call, SW), Bitwarden (via SMS, Phone call, Email, HW, SW), PayPal (via SW), Pocket (via SW), enz



Welke 2FA Authenticator app kiezen?

- Er bestaan vele van Authenticator apps waarvan sommigen betalend; een authenticator app kan in principe werken zonder internet-verbinding, maar in de praktijk zijn velen niet privaat en verzamelen data over u
- *Populaire Authenticator apps voor software-gebaseerde security:*
 - * *software, niet privaat: Twilio Authy, Microsoft Authenticator, Google Authenticator*
 - * *software, privaat: FreeOTP, Aegis Authenticator*
 - * *hardware: Yubico Authenticator (niet gratis)*
- We willen hier een gratis, software-gebaseerde 2FA Authenticator app kiezen met een goede reputatie en die voldoende privacy biedt:
Google Authenticator is erg populair;
Bitwarden kan ook als Authenticator app ingezet worden, maar wordt hier weinig voor gebruikt;
Twilio Authy app wordt door experts aanbevolen (sinds 2024 enkel beschikbaar op mobile en niet meer op pc)
- Wij zullen **Authy** gebruiken als 2FA Authenticator app



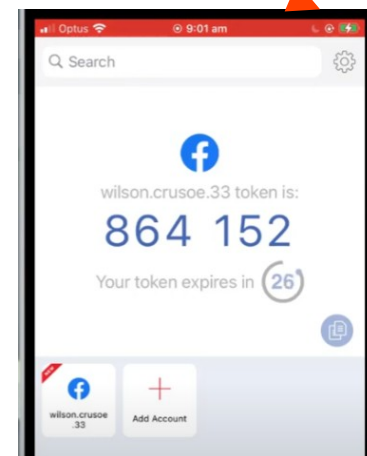
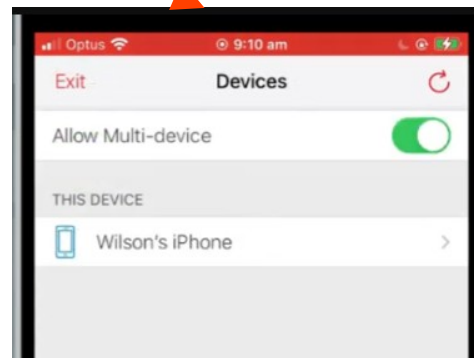
Hoe 2FA in praktijk gebruiken?

(1) Installeer een Authenticator app op je smartphone

- **Authy** app kan je gratis downloaden en installeren via Play Store; meer info van bijbehorende website <https://authy.com/>



- Mobile met Authy app kan je nu gaan gebruiken als authenticator toestel; je voorziet best dadelijk ook backup voor authenticator toestel door een “backup password” te voorzien of “multi device access” beschikbaar te maken





Hoe 2FA in praktijk gebruiken?

(2) Maak een account op PayPal website,
die we daarna als voorbeeld-site voor 2FA beveiliging gaan gebruiken

- Open browser en ga naar PayPal website <https://www.paypal.com/>

The image displays three overlapping screenshots of the PayPal website. The leftmost screenshot shows the PayPal homepage with the headline "Wij helpen je om te shoppen en te betalen." and a "Meld je gratis aan" button. The middle screenshot shows the "Open een rekening bij PayPal" page, where the "Privé-rekening" option is selected. The rightmost screenshot shows the "ITEM INFORMATION" sidebar on the PayPal website, displaying details for a PayPal account, including the name "www.paypal.com", username "john.doe@mytest.aleeas.com", and password "*****".



Hoe 2FA in praktijk gebruiken?

- Open PayPal rekening

 [Inloggen](#)

Open een rekening bij PayPal

E-mailadres
john.doe@mytest.aleeas.com

Volgende

Bevestig je telefoonnummer

Code verzonden naar +32 [REDACTED]

[Code opnieuw verzenden](#)

[] [] [] [] [] []

Telefoonnummer

Code +32 ▼

Telefoonnummer
487 12 34 56

Als je doorgaat, bevestig je dat je gemachtigd bent dit telefoonnummer te gebruiken en ga je akkoord met het ontvangen van sms-berichten. Je provider kan hiervoor kosten in rekening brengen.

Volgende

Wachtwoord maken

Wachtwoord maken
.....

- ✓ Gebruik 8 tot 20 tekens
- ✓ Gebruik 2 van de volgende tekens: letters, cijfers of symbolen ()

Volgende

Persoonlijke gegevens

Deze gegevens moeten overeenkomen met je officiële identiteitsbewijs.

Nationaliteit
België ▼

Voornaam

⚠ Voornaam is vereist.

Achternaam

⚠ Achternaam is vereist.

Geboortedatum

⚠ Voer een geldige datum in

Je adres

Zorg ervoor dat je je factuuradres gebruikt.

Adresregel 1

⚠ Adres is vereist.

Adresregel 2

Postcode

Plaats

☐ Je gaat akkoord met de [Gebruikersovereenkomst](#) en [Privacyverklaring](#) van PayPal. Raadpleeg je [Herroepingsrecht](#) voor meer informatie.

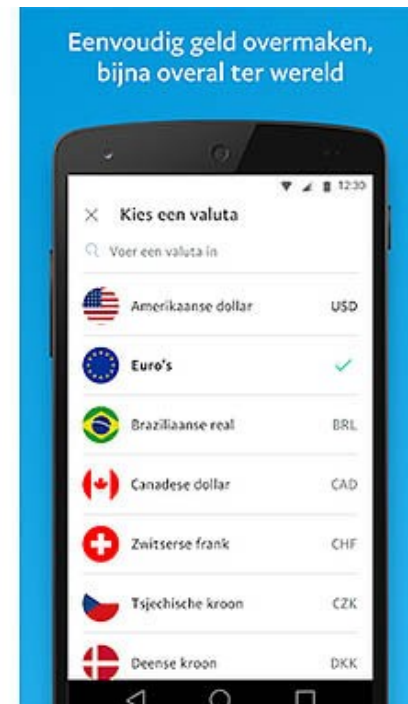
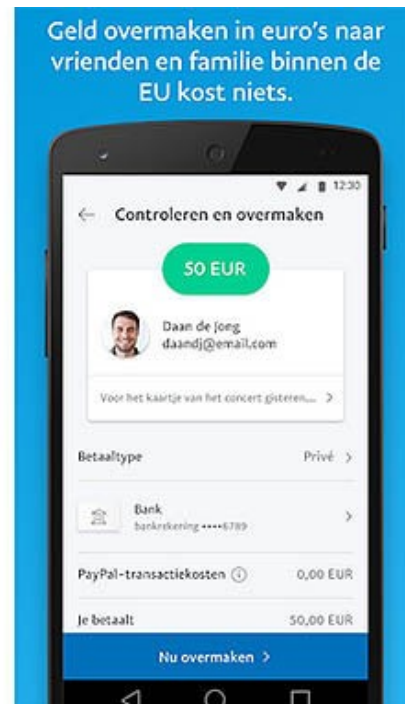
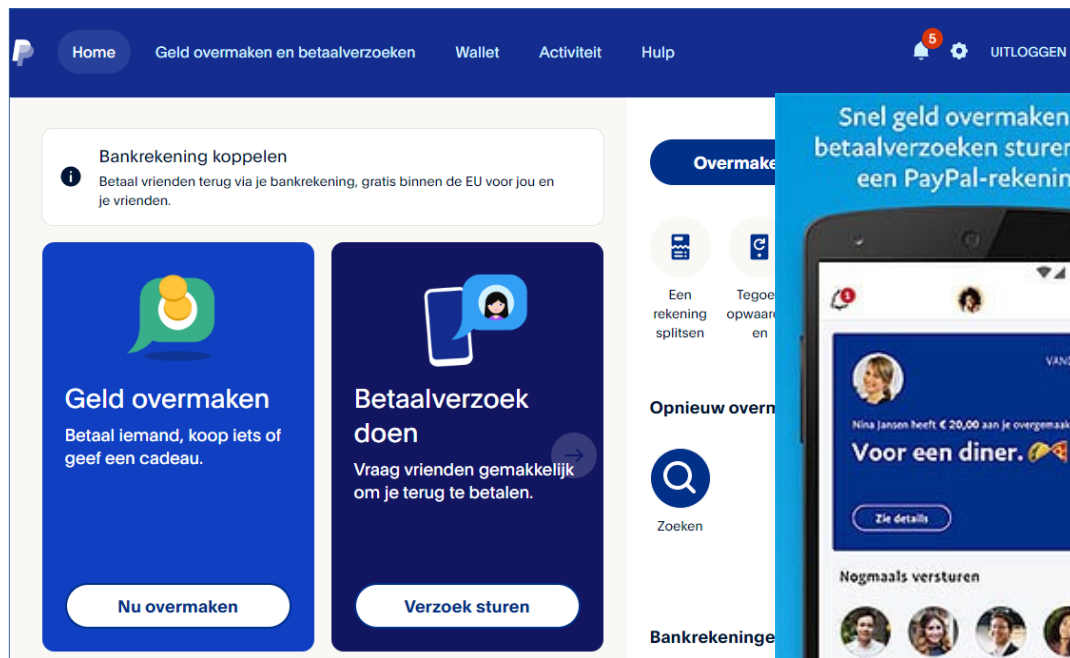
☒ Je gaat akkoord met de ontvangst van marketingcommunicatie. Je kunt dit op elk gewenst moment wijzigen in je instellingen.

Akkoord en rekening openen



Hoe 2FA in praktijk gebruiken?

- Installeer PayPal app via Play Store op je mobile en login





Hoe 2FA in praktijk gebruiken?

(3) Pas instellingen in Paypal aan voor gebruik 2FA

The image shows a screenshot of the PayPal account settings page, specifically the 'Veiligheid' (Security) section. The page is in Dutch. The top navigation bar includes 'Home', 'Geld overmaken en betaalverzoeken', 'Wallet', 'Activiteit', 'Hulp', and 'UITLOGGEN'. The 'Veiligheid' tab is selected and highlighted with a red box. Below the navigation bar, there are several sections: 'Bankrekening koppelen', 'Overmaken', 'Betaalverzoek', 'E-mailadressen', and 'Telefoonnummers'. The 'Tweestapsverificatie' (Two-step verification) option is highlighted with a red box. The description for this option reads: 'Voeg een extra beveiligingsniveau toe aan je rekening door telkens wanneer je inlogt gebruik te maken van een eenmalige beveiligingscode naast je wachtwoord.' The 'Instellen' (Set up) button is visible next to it. Other options shown include 'Wachtwoord' (Password), 'Wachtwoordsleutels' (Password keys), and 'Je logins beheren' (Manage your logins).



Hoe 2FA in praktijk gebruiken?

(3) Pas instellingen in Paypal aan voor gebruik 2FA

Rekening **Veiligheid** Gegevens en privacy Betalingen Berichten Tools voor verkopers

Veiligheid

- Wachtwoord
Maak een wachtwoord of werk je huidige wachtwoord bij
- Wachtwoordsleutels
Log eenvoudig in met je vingerafdruk, gezicht of sleutel
- Tweestapsverificatie**
Voeg een extra beveiligingsniveau toe aan je account. Wanneer je inlogt gebruik je een eenmalige code.
- Je logins beheren

Je rekening beschermen met tweestapsverificatie

Elke keer dat je inlogt, gebruik je naast je wachtwoord een eenmalige code. Kies hoe je je code wilt ontvangen.

[Een verificatie-app nodig?](#)

- Een verificatie-app gebruiken
Beveiligingscodes worden binnen een minuut bijgewerkt.
- Een beveiligingssleutel gebruiken
Veel beter bestand tegen phishing.

Codes ontvangen via een verificatie-app

Elke keer dat je inlogt, gebruik je behalve je wachtwoord een verificatie-app om een eenmalige code te genereren.

Stap 1: Scan de onderstaande QR-code met de verificatie-app of de geheime sleutel handmatig in.

4VCL KNKK 43Y3 6FR

Stap 2: Voer de zescijferige code in die de verificatie-app ziet.

Verificatiecode

Bevestigen

Bevestig dat jij het bent

☒ Een sms ontvangen
Mobiel +32 [redacted]

☐ Laat ons jou bellen

Door verder te gaan bevestig je dat je gemachtigd bent dit telefoonnummer te gebruiken en ga je ermee akkoord sms-berichten te ontvangen om je identiteit te bevestigen voor deze sessie. Je provider kan hier kosten in rekening brengen.

Volgende

Tweestapsverificatie beheren

Nadat je een wachtwoord hebt ingevoerd, word je gevraagd om iedere keer wanneer je inlogt een eenmalige code in te voeren.

Tweestapsverificatie staat **AAN** [Uitschakelen](#)

Je primaire apparaat:

Verificatie-app
Codegenerator van externe partij

Je back-ups:

[+ Een apparaat toevoegen](#)

Klaar

Voer je code in

We hebben een beveiligingscode verzonden naar +32 [redacted]

[Nieuwe code verzenden](#)

[Input field]

Volgende



Hoe 2FA in praktijk gebruiken?

(4) Inloggen met 2FA

The screenshot shows the PayPal Dutch homepage. The top navigation bar is dark blue with the PayPal logo on the left and links for 'Home', 'Geld overmaken en betaalverzoeken', 'Wallet', 'Activiteit', 'Hulp', and a notification bell with '4' alerts. The 'UITLOGGEN' button is highlighted with a red box. Below the navigation bar, there's a section for 'Bankrekening koppelen' and buttons for 'Overmaken' and 'Betaalverzoek'. At the bottom, there's a blue banner with the text 'Wij helpen je om te shoppen en te betalen.' and the PayPal logo.

The screenshot shows the PayPal login form. It has a blue header with the PayPal logo. The form contains two input fields: 'E-mailadres of mobiel nummer' with the value 'john.doe@mytest.aaleas.com' and 'Wachtwoord' with masked characters. There's a 'Weergeven' link next to the password field. Below the fields is a link 'Wachtwoord vergeten?' and a large blue 'Inloggen' button, which is highlighted with a red box.

The screenshot shows the PayPal 2FA verification screen. It has a blue header with the PayPal logo. The text reads 'Voer je code in' and 'Voer de zescijferige beveiligingscode uit je verificatie-app in.' Below this is a row of six empty input boxes for the security code. At the bottom is a large blue 'Doorgaan' button and a link 'Heb je problemen met inloggen?'.



Hoe Authy als Authenticator app voor 2FA gebruiken?

- Indien je 2FA wil gebruiken om je account op een website extra te beveiligen, dan maak je best een backup van je 2FA codes (seeds) die je veilig bewaart (nodig bij diefstal of defect van mobile)
- Hoe?
 - * open Authy app, klik puntjes icon (bovenaan rechts) en kies “Settings”
 - * kies “Accounts” tab en zet “Backup” aan
 - * kies een nieuwe “Backup Key” en bewaar deze op een veilige plaats (bv als extra veld bij je PayPal login in je Bitwarden kluis)

Extra info

Video's met meer uitleg

- * Webinar Accountbeheer en -beveiliging

<https://www.youtube.com/watch?v=NcwQbwjLH9A>

- * Al gehoord van tweestapsverificatie? - safeonweb.be

<https://www.youtube.com/watch?v=ooslWr2K2jY>

- * Digiwatte? Tweestapsverificatie activeren

<https://www.youtube.com/watch?v=iEYomc2VavU>

- * How To Use Two-Step Verification | Privacy Tips | WhatsApp

<https://www.youtube.com/watch?v=rA0VIXPdgl>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * Why You Should Turn On Two Factor Authentication

https://www.youtube.com/watch?v=hGRii5f_uSc

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

Extra info

Video's met meer uitleg

- * Authy - The Best Free Two Factor Authenticator App

<https://www.youtube.com/watch?v=HrbaXiCySV4>

How To Use Authy on Desktop and Mobile

<https://www.youtube.com/watch?v=tmnS821wCyc>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * How to set up Two-Factor Authentication (2FA) for all your accounts

<https://www.youtube.com/watch?v=hlpoc3C1kWM>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * I Lost My Two-Factor Authentication (2FA) Device. How Do I Sign In?

<https://www.youtube.com/watch?v=6bt4ab7QOoc>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * Don't Use 2FA Without These! What Are 2FA Backup Codes?

<https://www.youtube.com/watch?v=UzrLj7DU1jY>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

Extra info

Video's met meer uitleg

* Most PRIVATE 2FA apps

<https://www.youtube.com/watch?v=JHIAIzOPz3I>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

* Rob Braxman is WRONG about 2FA. Here's why.

<https://www.youtube.com/watch?v=2kIVVEzEBHs>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

* Authy killed their desktop apps

<https://www.zoho.com/blog/index.php/accounts/authy-alternative-zoho-oneauth-app.html>

Secure your online accounts with Zoho OneAuth

<https://www.zoho.com/accounts/oneauth/>

Zoho OneAuth for Android

<https://www.youtube.com/watch?v=anCepBrfRVE>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

Extra info

Video's met meer uitleg

* How to set up 2FA in Bitwarden

<https://www.youtube.com/watch?v=MeKyZP4KIQ0>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

* How to use the Bitwarden Integrated Authenticator

<https://www.youtube.com/watch?v=sMShYi7R674>

* Is Bitwarden's 2FA Code a Security Risk?

<https://www.youtube.com/watch?v=646dlqdcBmk>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

Deel 10

**Toegang tot app en website
beveiligen met passkey's**



Hoe toegang tot app/site beveiligen?

6 Tips to Secure Your Mobile Devices



Use screen locks and biometrics



Update your OS and apps regularly



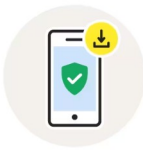
Use a VPN to protect your traffic



Create encrypted backups of personal information



Create strong passwords and enable 2FA



Use mobile security software for efficient security



Wat zijn passkey's?

Hoe kunnen we toegang tot sites beter en makkelijker beschermen dan met wachtwoorden?

- **Passkey's** zijn een vrij nieuwe manier van beveiligen die gebruik van paswoorden volledig vervangt;

momenteel zijn er weinig websites met ondersteuning voor 2FA en Passkey's; grote bedrijven (Google, Microsoft, Apple, Amazon, Meta, Samsung, enz) zijn momenteel echter passkey's sterk aan het promoten, en zullen langzaam paswoorden volledig gaan vervangen

- Per account waarop je moet kunnen inloggen, wordt een bij elkaar horende public key en private key gegenereerd (gebaseerd op Asymmetric Cryptography); dit key-paar zal worden gebruikt bij elke inlog-poging; de public key wordt gedeeld met de website waarop je wil inloggen, en de private key blijft prive (enkel door jou gekend) en voor jou prive opgeslagen; het sleutelpaar is niet enkel uniek voor ieder account, maar wordt ook gekoppeld aan 1 specifieke website en dikwijls ook aan 1 fysiek apparaat (mobile, pc, Yubikey)
- Voordelen:
 - * zelfs bij het hacken van alle (public) keys op de website, dan is er nog geen gevaar omdat de private keys nodig zijn om in te loggen
 - * phishing is ook niet meer mogelijk omdat de sleutels gekoppeld zijn aan een website



Wat zijn passkey's?



Private Key



Public Key



Wat zijn passkey's?

Hoe gebruik je passkey's in de praktijk (voor websites die dit ondersteunen) ?

- Ga naar de gewenste website in Google Chrome, en automatisch zal je de vraag krijgen om passkey opgeslagen op je mobile te gebruiken
- je dient je dan te identificeren om je passkey te krijgen, bv met vingerafdruk; je wordt dan direct ingelogd

Hoe worden passkey's opgeslagen? Er zijn 2 mogelijkheden:

- **Device-bound passkey:** voor elk van je apparaten een aparte passkey te maken voor iedere website, en deze op je lokale toestel bijhouden
- **Synchronized passkey:** één aparte passkey te maken voor elke website, deze E2E encrypted opslaan in de cloud, en deze laten gebruiken door al je apparaten; hiervoor is synchronisatie over al je apparaten vereist (of doorgeven via QR-code)

Opgeslagen passkey's dienen uiteraard steeds ge-backup-ed te worden; Passkey's kan je al gebruiken op iOS 16+, Android 6+ en Windows 10+

Extra info

Video's met meer uitleg

- * Wachtwoorden zijn dood. Lang leve Passkeys!

https://www.youtube.com/watch?v=z3ooX3_qRrY

- * Een wereld zonder wachtwoorden en phishing dankzij passkey

<https://www.youtube.com/watch?v=Uyd5a4JcPbk>

- * What Is WebAuthn?

<https://www.youtube.com/watch?v=zJPNuORkvvk>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * What is a Passkey?

https://www.youtube.com/watch?v=6lBixL_qpro

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

- * Learn passkeys for simpler and safer sign-in

<https://www.youtube.com/watch?v=SF8ueIn2Nlc>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten



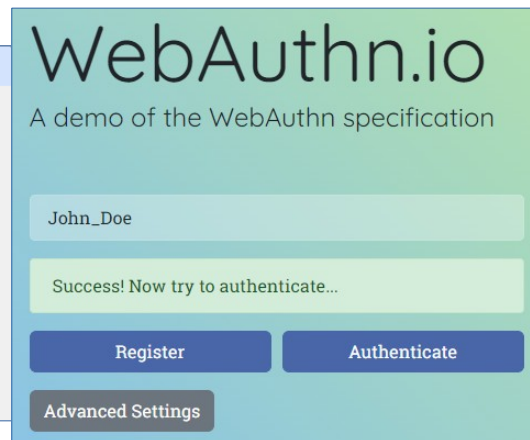
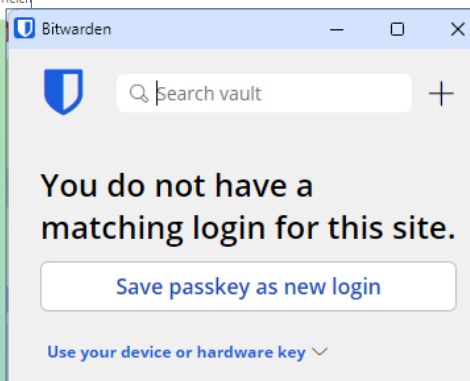
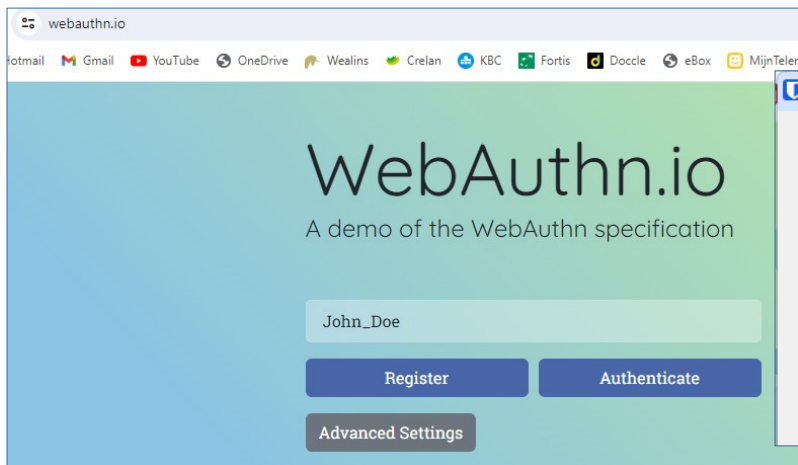
Hoe passkey's opslaan in Cloud met Bitwarden?

- De gratis versie van Bitwarden ondersteunt zowel 2FA als passkey's; de gratis versie ondersteunt enkel passkey's via YubiKey, en enkel 2FA via authenticator app of email (betalende versie ondersteunt ook hardware key, sms, telefoon oproep); Bitwarden slaat paswoorden en passkey's E2E encrypted op in cloud
- Indien je Bitwarden gebruikt om passkey's voor websites op te slaan, dan:
 - * gebruik niet tegelijk paswoorden voor deze websites
 - * kan automatisch slechts 1 login met passkey per site opgeslagen worden; voor een 2de login dien je de bestaande login voor deze site manueel te clonen (voor verschillende accounts op dezelfde website)
- Bitwarden heeft momenteel nog geen mogelijkheid om passkey's opgeslagen in je kluis te exporteren en terug te importeren



Hoe passkey's gebruiken met Bitwarden?

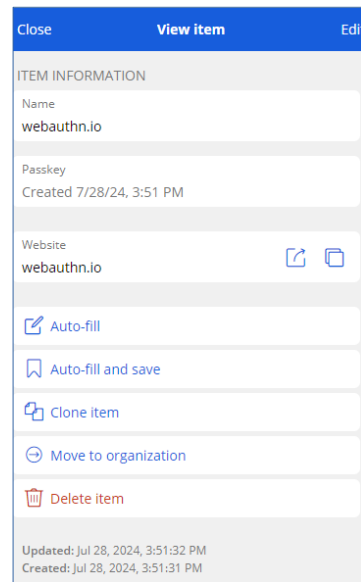
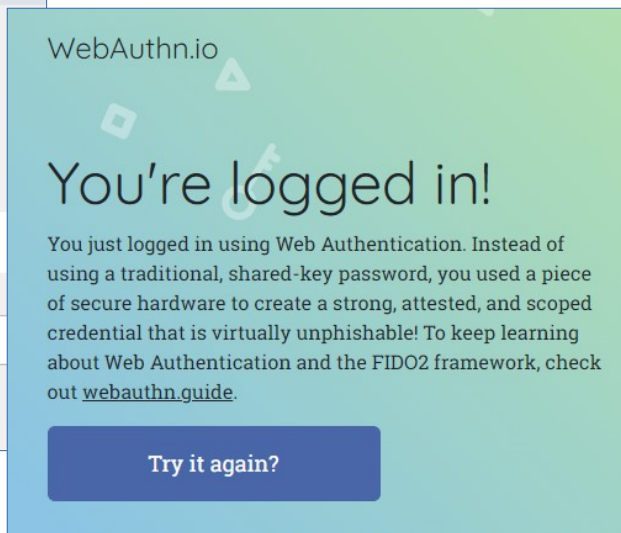
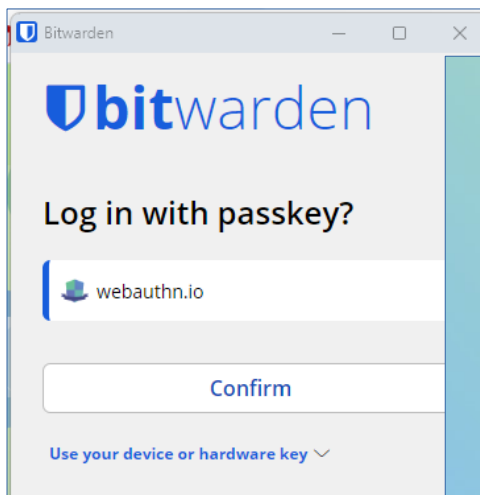
- Open website *https://webauthn.io/* die we zullen gebruiken om te oefenen met passkey's; Bitwarden-extensie dient geïnstalleerd zijn in je browser
- Type "John_Doe" in als gebruikersnaam in inputveld "example_username", en klik op "Register" knop;
Bitwarden dialoogvenster opent en klik op "Save passkey as new login";
passkey voor deze user voor deze site is nu gecreeerd in Bitwarden kluis





Hoe passkey's gebruiken met Bitwarden?

- Klik “Authenticate” knop om in te loggen op deze website; klik “Confirm” knop in Bitwarden venster om gekozen passkey te bevestigen
- Open Bitwarden kluis en bekijk de opgeslagen login met passkey





Hoe inloggen met passkey in Bitwarden?

- Bitwarden login instellen:
 - * open <https://vault.bitwarden.com/> in browser en login je kluis; klik Profiel icoon bovenaan rechts, en “Accountinstellingen > Beveiliging”
 - * voor login met 2FA gebruik (authenticator gebruikt): selecteer tab “Tweestapsaanmelding”
 - * voor login met passkey gebruik (in beta): selecteer tab “Hoofdwachtwoord” en klik “Nieuwe passkey” in sectie “Inloggen met passkey”
- Gebruik voorlopig nog geen passkey voor login in Bitwarden, omdat dit momenteel nog in experimentele fase is

Extra info

Video's met meer uitleg

* Faster Logins with Passkeys | Bitwarden Passkey Tutorial

<https://www.youtube.com/watch?v=o4asbRziCD0>

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

* Sign into Bitwarden with a passkey

https://www.youtube.com/watch?v=m5642STzh_Q

... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten



Welke websites ondersteunen passkey's voor account-beveiliging?

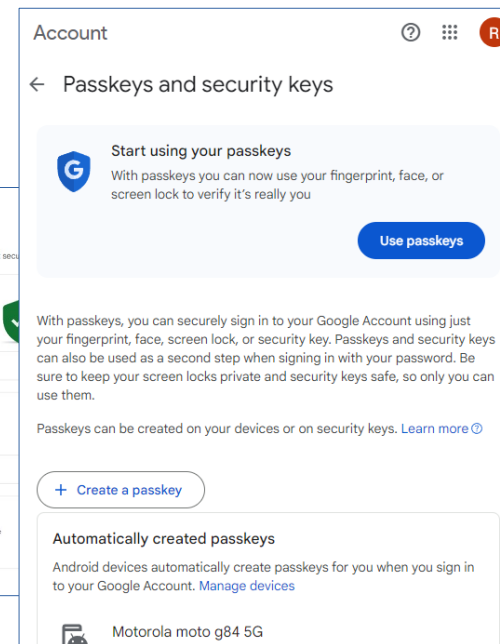
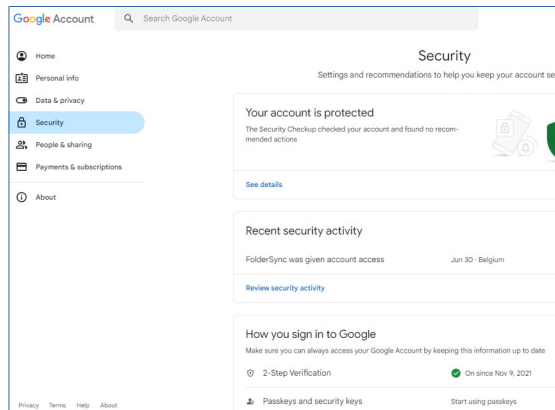
- Lijst van websites die passkey's ondersteunen, kan je vinden op:
 - * Websites that support passkeys:
<https://www.passkeys.io/who-supports-passkeys>
 - * GitHub repo for Bitwarden:
<https://github.com/bitwarden/passkeys-index>
- WhatsApp ondersteunt login via passkey's:
open WhatsApp app en klik op puntjes icoon (bovenaan rechts);
kies "Instellingen > Account > Passkeys" en klik "Passkey maken"



Welke websites ondersteunen passkey's voor account-beveiliging?

Google apps beveiligen met passkey's:

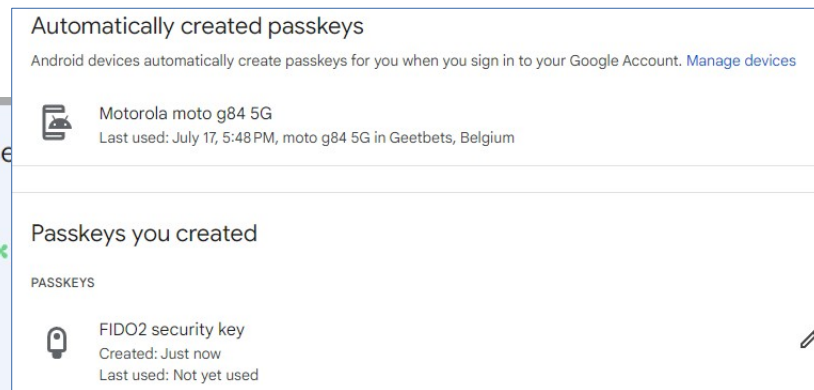
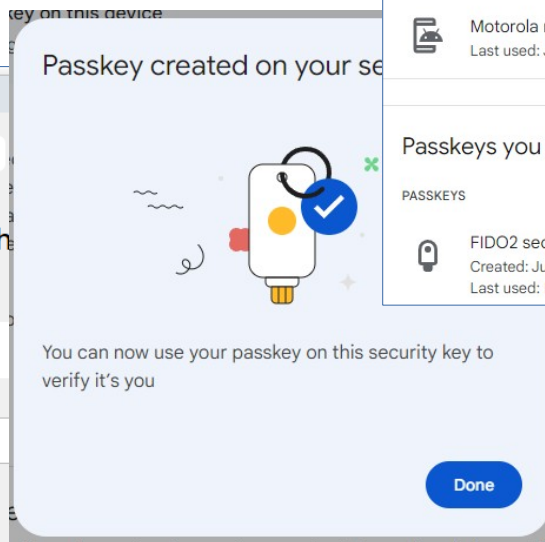
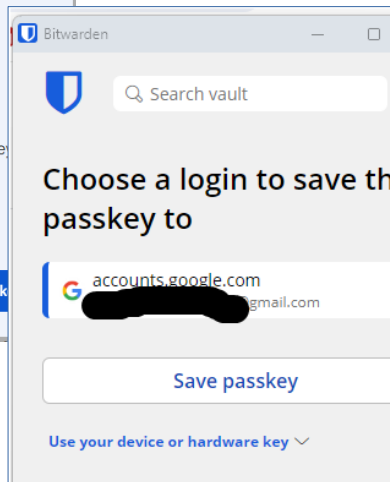
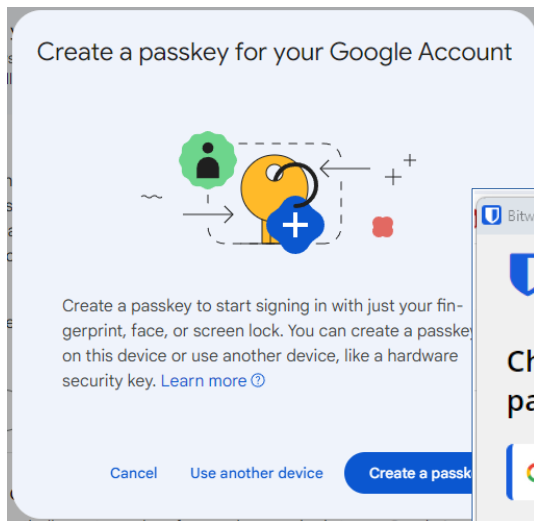
- Open <https://mail.google.com/> en log in; klik op profile icoon (bovenaan rechts) en daarna op "Manage your Google Account"
- Klik op "Security" tab in menu links, en daarna op "Passkeys and security keys"; je kan nu de reeds gecreeerde passkey's zien





Welke websites ondersteunen passkey's voor account-beveiliging?

- Klik op “Create a passkey” knop om een passkey te creëren op je huidige toestel in Bitwarden kluis





Welke websites ondersteunen passkey's voor account-beveiliging?

- Loguit en login terug in Gmail om passkey-beveiliging te testen

The screenshot shows a web browser window with several tabs: Telenet, TEC Home - TEC, PWA, MyBelgium, mypension, LibreView, and Bitwarden. The main content area displays the Google sign-in page. At the top, it says "Signed out - syncing is paused" and shows a red "R" icon next to a blacked-out email address. Below this, a message states: "Your bookmarks, history, passwords, and more are no longer being synced to your account but will remain on this device. Sign in to start syncing again." At the bottom, there are two buttons: "Continue" and "Sign in again".

Overlaid on the right side of the browser is a Bitwarden window titled "Log in with passkey?". It shows the Bitwarden logo and a text input field containing "accounts.google.com" and a blacked-out email address. Below the input field is a "Confirm" button.

At the bottom of the browser window, there is a Google Account menu. It includes a search bar "Search Google Account" and a list of links: Home (highlighted), Personal info, Data & privacy, Security, People & sharing, and Payments & subscriptions. On the right side of the menu, it says "Welcome," and "Manage your info, privacy, and sec". At the bottom right, there is a link for "Privacy &".

Extra info

Video's met meer uitleg

- * How to Create a Passkey on WhatsApp || Whatsapp new update 2023
<https://www.youtube.com/watch?v=E0WzADthzq0>
... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten
- * Google Passkeys Tutorial | Step by Step Guide to Set Up Google Passkeys
<https://www.youtube.com/watch?v=ckvrKdFNF78>
... dit is een engelstalige Youtube video, maar je kan nederlandstalige ondertiteling aanzetten

Nog vragen ?

dit is het laatste deel van een 3-delige presentatie over android phones