

Using Android smartphone

- Advanced level -

Author: RobertTheCoder

Date: 15/07/2024



Geavanceerd

Required prior knowledge

Good knowledge of internet, cloud and Android operation is required. This course is intended for users with average Android knowledge.

Description

- Basic knowledge of NFC and Bluetooth for device pairing
- Camera options to take better pictures
- Use of apps with Artificial Intelligence
- Improve privacy and security in apps
- Securely back up data on smartphone
- Better secure access to apps/sites

Sections

- 1) Connecting your smartphone to other devices
- 2) Take better photos with the Camera app
- 3) Use Artificial Intelligence
with Google Lens and Assistant app
- 4) Deal consciously with digital fraud
- 5) Use public WiFi safely with ProtonVPN
- 6) Anonymous use of browser, search engine and email

Sections

- 7) Secure access to app and website with Password Managers
- 8) Securely back up files on smartphone
- 9) Secure access to app and website with 2FA
- 10) Secure access to app and website with Passkeys
- 11) Suggestions?

Section 1

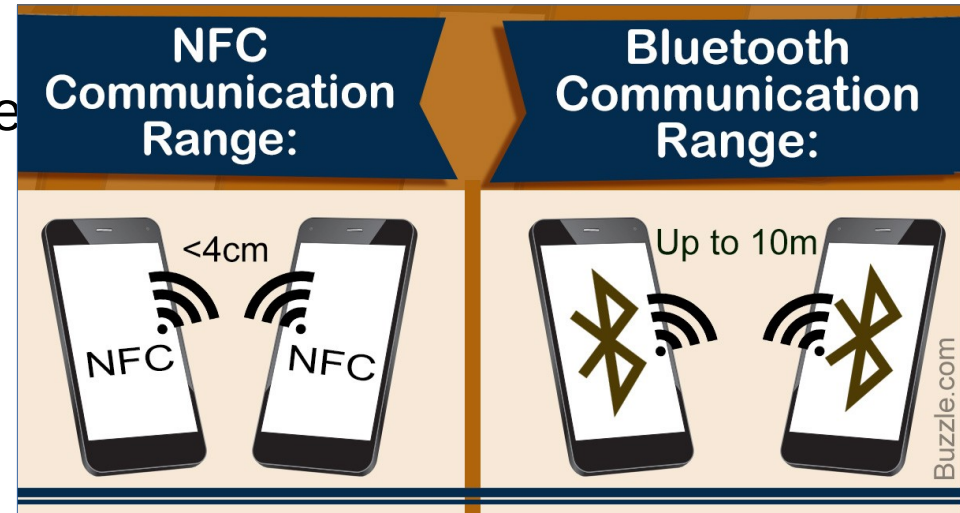
Connecting your smartphone to other devices

What collaboration with other devices built into smartphone?

- **Bluetooth:**

technology for creating short distance wireless connection with other device (usually up to 10 m);
this requires short setup in advance ("pairing");
used for connecting smartphone to wireless headset, car, etc.

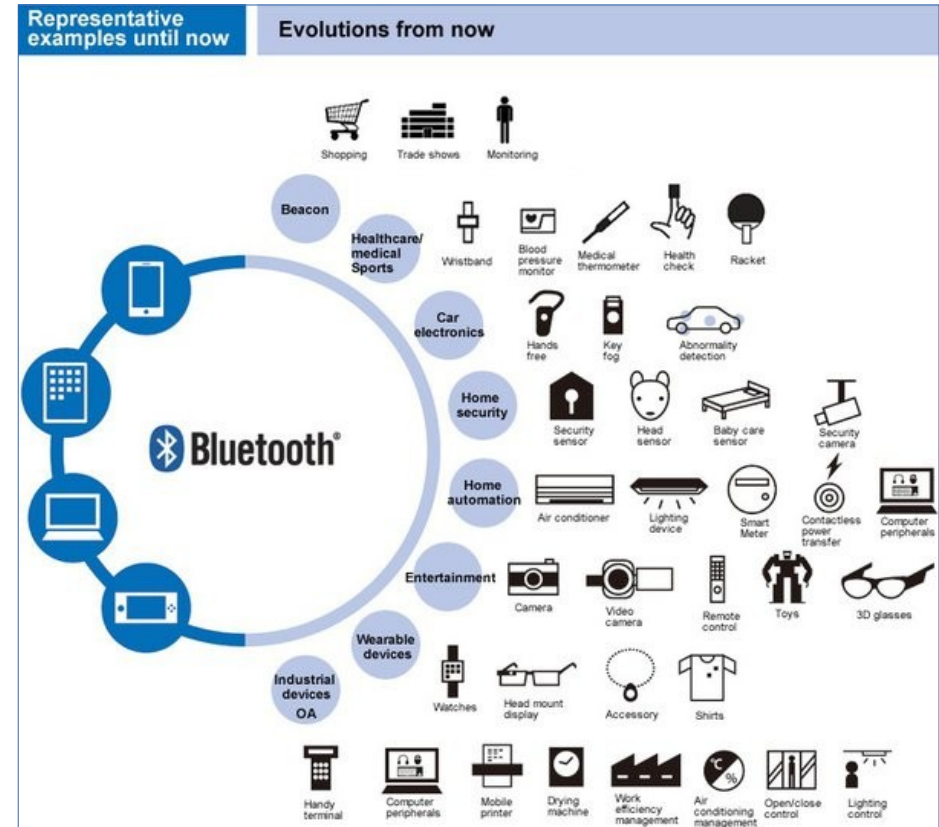
- **NFC** (Near Field Communication):
technology for creating short-distance wire-free connections with other devices (usually up to 10 cm);
this requires no setup in advance;
used for contactless payments



Examples of Bluetooth usage

Bluetooth is used to connect many devices;
for connecting your smartphone to another device with Bluetooth, there is support via apps.

For example, Bluetooth can be used to connect your smartphone to the computer system in your car to be able to call hands-free in the car, or to be able to play your favorite music stored on your phone in the car.



Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

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

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

- * 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>

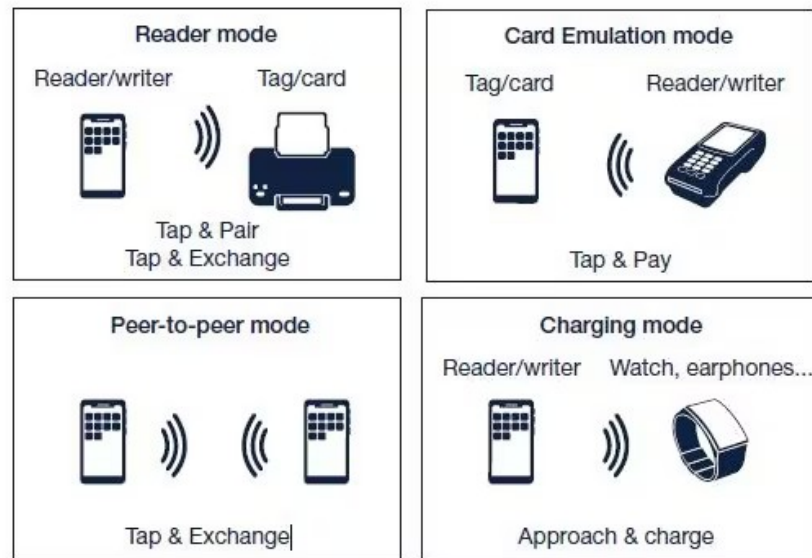
- * Android Auto Walkthrough! | + Setup Guide!

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

Examples of NFC usage

There are 2 types of NFC chips:

- Passive:
 - * **NFC tags** on which you can store data with NFC reader/writer, which can then be read later by NFC readers;
 - * **cards with NFC chip**, for example: bank card (for contactless payment), mobib card, DeLijn advance ticket
- Active:
 - * **NFC reader** in your smartphone or payment terminal to read information on an NFC chip;
 - * **NFC reader/writer** in your smartphone or scanner post on bus to read and change information on an NFC chip



Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

- * 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>

Transfer files via Bluetooth

- Bluetooth is available on all Android smartphones, and can be used to transfer files between these devices without any WiFi or data connection
- On Samsung devices there was “Quick Share” and other Android devices had “Nearby Share” to be able to do this;
since the beginning of 2024 these solutions were merged and also made available for Windows PCs with Bluetooth;
functionality is now called “Quick Share” with a new icon on all these devices
- To use **Quick Share** you need to activate “Bluetooth” and “Quick Share” via Notification bar;
choose the value “everyone (for 10 min)” for the field “Who can share with you”; for selected files choose “Share” (Share) and then “Quick Share” to transfer files via Bluetooth



Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

* Quick Share: How to share files | Samsung

<https://www.youtube.com/watch?v=UFcYxW7lE5A>

* How to transfer Data from Android to Android 2024

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

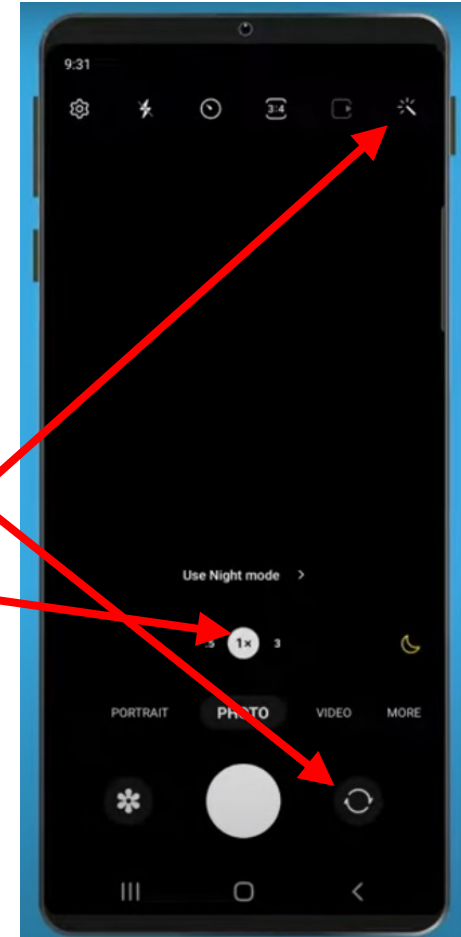
Section 2

**Take better photos
with the Camera app**

How to take good photos with camera?


1) Select subject for photo and place it on screen in app

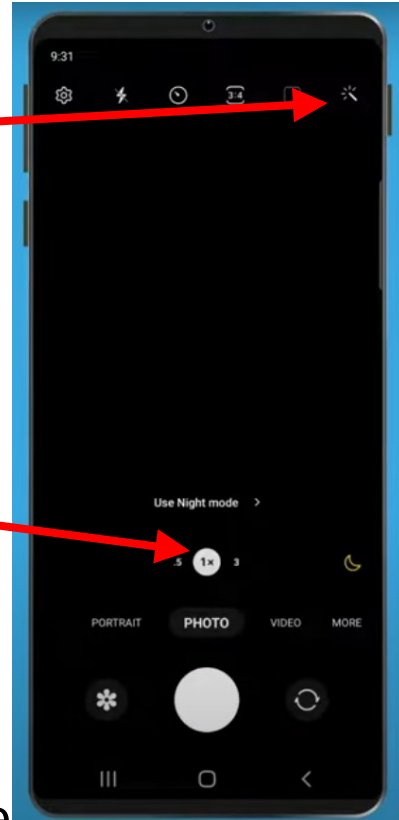
- Choice of front or rear camera:
 - front camera (**selfie**)
 - rear cameras (rear; number depends on device)choice between front/rear camera via arrow button
- **Move** to an optimal distance **yourself** (if possible):
rear cameras take photos with higher quality,
but each camera has an optimal magnification factor:
therefore zoom as little as possible for optimal quality
- Turn on the following tools (via Settings button):
 - * **Grid**: to keep straight and for composition
 - * Shutter sound: to hear if photo was taken



How to take good photos with camera?

2) Zoom in/out to desired content on app screen

- Select desired **aspect ratio** (photo size): normally 3:4, but also 1:1, 9:16, etc. possible
- **Zoom in/out:**
choice between different cameras on the back is done automatically when zooming in/out (and choosing a viewing angle);
to zoom you can either select the desired **zoom factor**, or apply a “Pinch” finger movement on the screen;
each camera has an optimal zoom factor that you should know for optimal quality;
select **ultra-wide** mode by choosing factor < 1 ;
selection of **macro** mode (for close-ups) depends on the device (on my device you have to click on the  flower icon)



How to take good photos with camera?

When zooming, a suitable rear camera (or lens) is automatically selected:

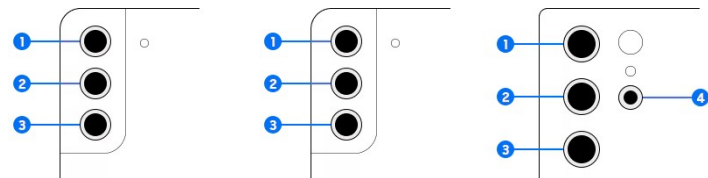
- standard (main) camera (zoom factor 1x and higher)*
- ultra-wide angle/macro (ultra-wide) camera with autofocus (zoom factor lower than 1x for “wide”, and flower icon for macro)*
- telephoto cameras (zoom from a certain factor, e.g. 5x); however, these are not always available, which means that zooming in far usually comes at the expense of quality; if more than one is available, it is called “optical zoom”*

Each of these cameras has:

- lens with a certain opening (aperture): determines how much light can enter, e.g. "f/2" is wider and lets in much more light than "f/4"*
- sensor with a certain resolution: determines the number of pixels (points where light is measured), e.g. "16 MP" are 4000 x 4000 pixels (16 million pixels) on the sensor; quality of information per pixel depends on how much light is received (otherwise noise)*

How to take good photos with camera?

*Camera specifications
for Samsung devices as example:*



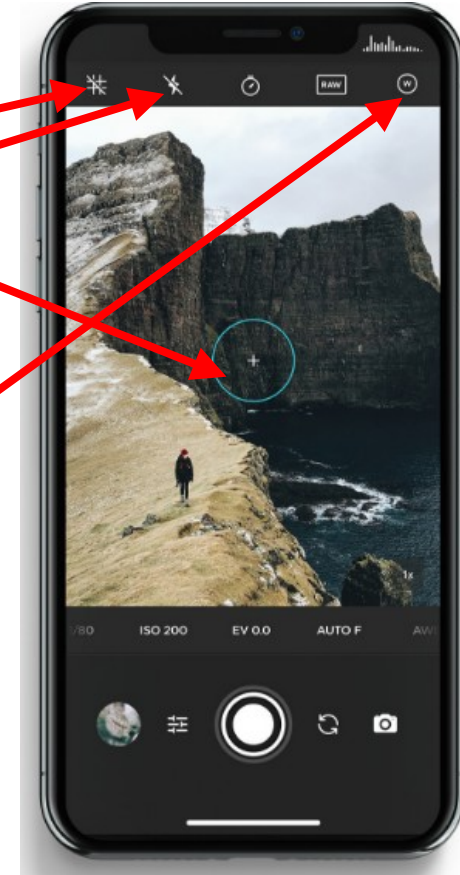
Camera	Galaxy S22	Galaxy S22+	Galaxy S22 Ultra
Front - Wide	10MP F2.2 [Dual Pixel AF], FOV 80°, 1/3.24", 1.22µm	10MP F2.2 [Dual Pixel AF], FOV 80°, 1/3.24", 1.22µm	40MP F2.2 [PDAF], FOV 80°, 1/2.8", 0.7µm
① Rear - Ultra Wide	12MP F2.2 [FF], FOV 120°, 1/2.55", 1.4µm	12MP F2.2 [FF], FOV 120°, 1/2.55", 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



How to take good photos with camera?

3) Improve image quality (focus and exposure)

- Tap the screen and drag the focus ring:
indicate which part of the image should be the sharpest
- Change exposure in low light:
 - * Use **flash** ⚡ only when necessary
 - * **Night vision** mode: 🌙
fusion of photos with short (for image structure)
and long exposure (for more light and less noise)
- Use **HDR** mode in strong backlight or high contrasts:
open menu with HDR options via Settings button:
camera quickly takes shots with different exposures,
and combines them into 1 photo, making colours
more vivid and more detailed in both light and dark areas



How to take good photos with camera?

4) Add desired effects

- Portrait Mode (blurred background):
creates perception of depth by using multiple cameras at the same time
- Panorama Mode
- Filters (options are highly dependent on the device):
 - * usually used to adjust the temperature of the image, e.g. b&w, natural, etc.
 - * also other possible, e.g. clean separation filter (face-unblur mode)

5) Take photo

- Self-timer:
With self-timer you can choose that after printing it takes 3 or 10 seconds before the photo is taken (e.g. interesting for group photos)
- After taking a photo, tap on thumbnail below to check result image

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

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

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

- * Top 10 Smartphone Photography Beginner Mistakes

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

- * How smartphone cameras ACTUALLY work!

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

Section 3

**Use Artificial Intelligence with
Google Lens and Assistant app**

How to use AI in apps?

- **Google Lens** app has AI (Artificial Intelligence) or KI (artificial intelligence) capabilities to recognize objects in images (other AI apps also include sound parts);
this app is automatically present on Android smartphones
- The functionality of this app is also integrated into other apps that provide images: Camera, Photos and Search app;



in the settings of the Camera app you must activate Google Lens

- Google Lens will then recognize and transform parts of the images provided by these apps, after which further actions can be performed

How to use AI in apps?



Exercises

- * Recognize bar codes/QR codes in images, and convert them into text or hyperlinks (already seen in previous section)
- * Recognize written or printed text in images, and convert them into text or change text in another language (via Translate app) on original image: use Camera app to automatically convert menu card to Dutch during your trip in Spain
- * Recognize objects in images and search for specific objects in other images or on sales sites:
 - * use Camera app to recognize plants during walks and display properties
 - * use Camera app to find clothing that someone is wearing on sales sites with prices
 - * use Photos app to know where a photo of a special building was taken

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

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

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

What are virtual assistants?

- **Voice-controlled** virtual assistants have been around for some time; Apple's Siri, Google's Assistant, Amazon's Alexa, Samsung's Bixby are the most well-known.
- These virtual assistants can help with various tasks via **AI**: answering arithmetic questions, turning lights on/off (or controlling other connected devices), taking a photo in 5 seconds, asking about the weather (using the internet), operating a phone, asking for the title of a song after singing, telling a joke or making a speech, etc.



How to use Google Assistant?



- **Google Assistant** app is pre-installed on Android; its successor (Google Gemini) is also available via Play Store
- To initialize Assistant, start Google app, click on the Profile button (top right) and choose Settings > “Google Assistant”; click “General” to activate or deactivate Assistant; click “Hey Google and Voice Match” to activate “Hey Google” (so that Google learns to recognize your voice)
- To start Assistant, long-press the Home button or say “Hey Google”; to mute Assistant, go to “Google Assistant” menu and choose “Assistant voice and sounds” > Phone



Exercises

- * Via Settings > Notifications > “Device & app notifications” allow Google to show app notifications
- * Say “Hey Google” and then “Show notifications”

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

- * 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

- * Android 101: Google Assistant | Android Voice Control

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

- * De 10 ChatGPT prompts die ik dagelijks gebruik

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

Section 4

Deal consciously with digital fraud



Why are the tips below not sufficient for security?

6 Tips to Secure Your Mobile Devices



Use screen locks and biometrics



Update your OS and apps regularly



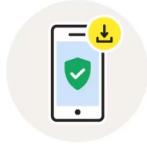
Use a VPN to protect your traffic



Create encrypted backups of personal information



Create strong passwords and enable 2FA



Use mobile security software for efficient security

Gain knowledge about the dangers of increased computerization in order to be able to deal with them more consciously



You can then adjust your **behavior** to **limit** these **dangers** as much as possible; your choice is often a weighing of advantages (ease of use) and disadvantages (technical complexity and dangers of abuse)

What is computer fraud?

- Fraudsters are very inventive in circumventing computer security; this type of fraud regularly appears in the news
- To better arm yourself against fraudsters and to be able to respond better after a fraud, you should inform yourself about this; in this section, therefore, common fraud cases are examined in the following videos

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

* 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

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

- * 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>

Section 5

**Use public WiFi safely
with ProtonVPN**



Why use VPN?

6 Tips to Secure Your Mobile Devices



Use screen locks
and biometrics



Update your OS
and apps regularly



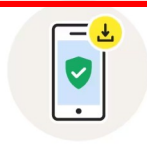
Use a VPN to
protect your traffic



Create encrypted
backups of personal
information



Create strong
passwords and
enable 2FA

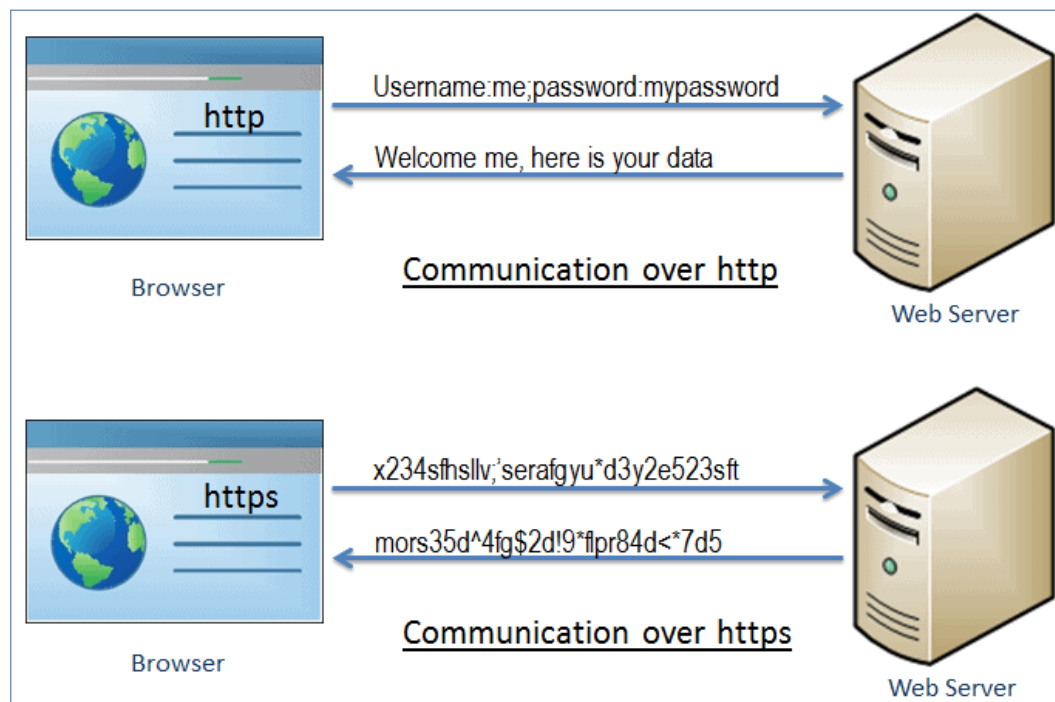
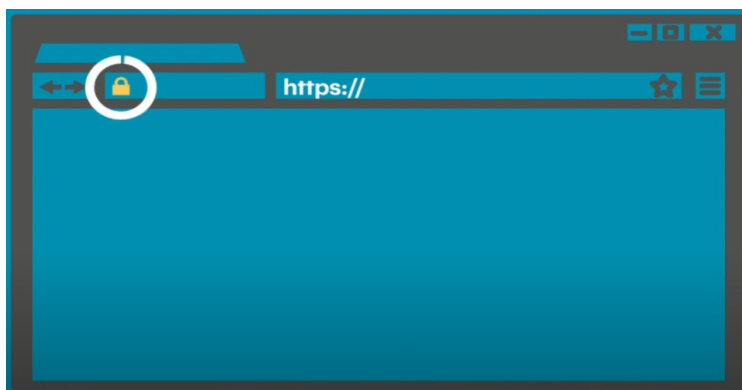


Use mobile security
software for
efficient security



What is a secure connection?

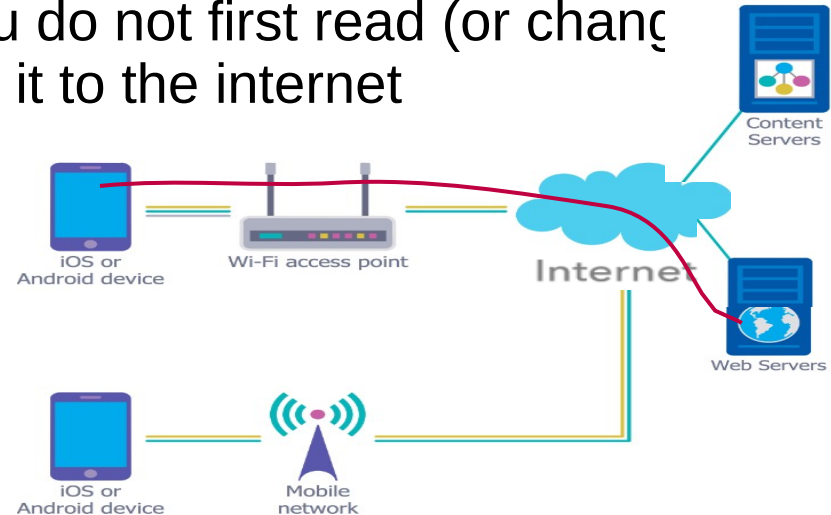
- With a secure connection between mobile and web server, all communication is encrypted via **https**, and it is checked whether it is indeed the desired web server





Why use VPN network?

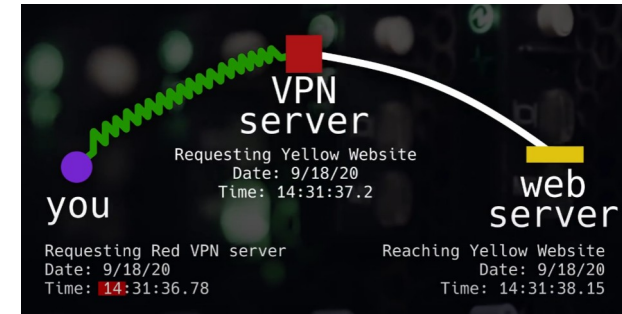
- Not all web servers use a secure connection (communication can be read by unauthorized persons) and even with a secure connection it is visible who communicates with which web servers and when
- **Public WiFi** networks (in stations, hotels, terraces, etc.) increase the **risk** even more, because you do not know whether the WiFi access point offered can really be trusted and you do not first read (or change) your communication before sending it to the internet





What is a VPN network?

- **VPN** (Virtual Private Network):
no direct communication with desired web server,
but only encrypted communication with pre-selected VPN server that then forwards your request to desired web server
- Advantages:
 - * between you and VPN server everything is encrypted and secure, also over public or unknown network;
 - * web server cannot find out your IP address (only that of VPN server seen by them)
- Disadvantages:
 - * trust in VPN provider is necessary, because they do see your IP address and decode your communication;
 - * slower communication because everything has to pass through VPN server





How to use Proton VPN on mobile?

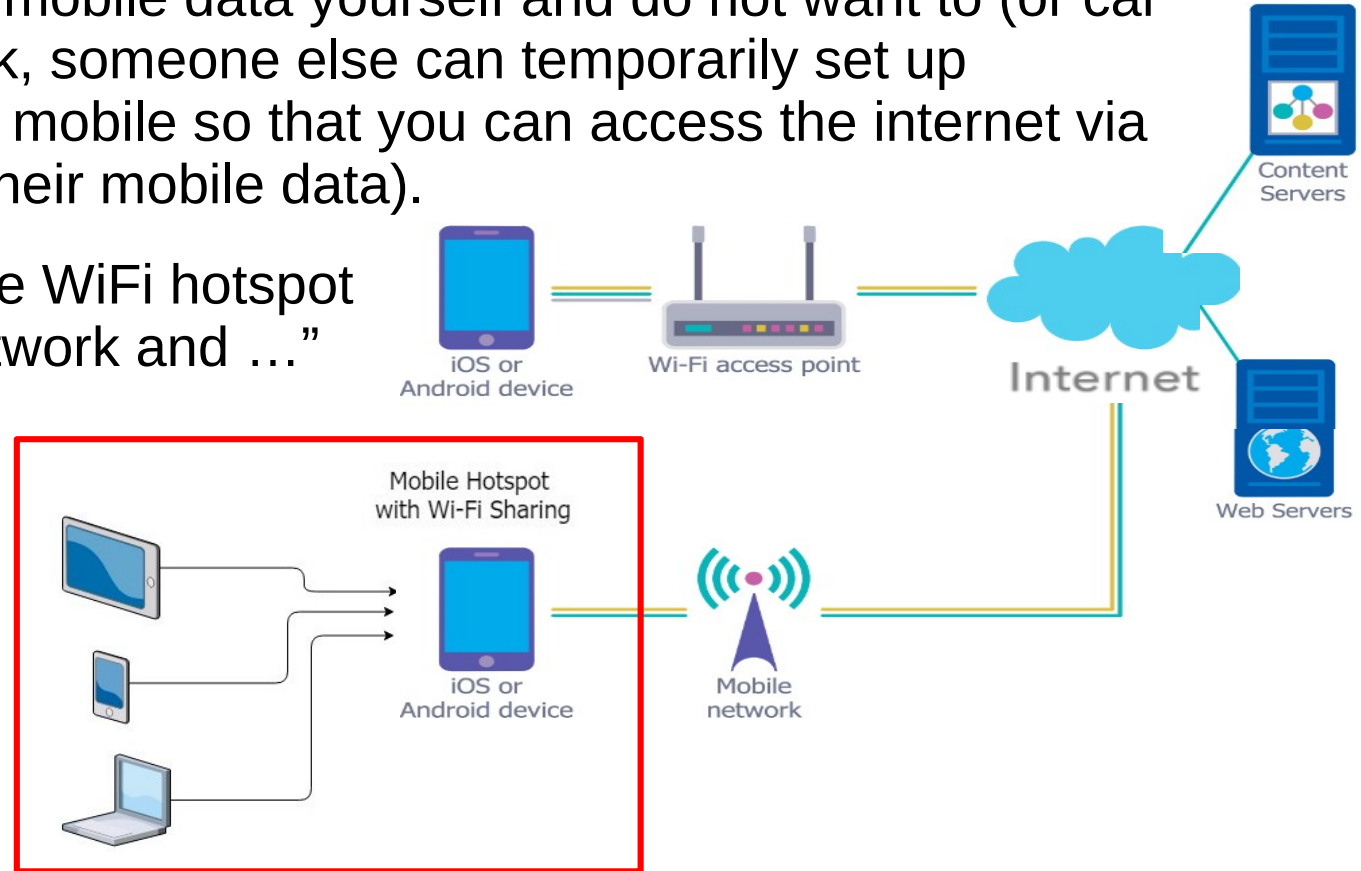
- There are many VPN client apps; a popular VPN app with a free version is “Proton VPN”
- Install “**Proton VPN**” app via Play Store, and choose the free installation and use during setup; add an account during setup (email address, password)
- After starting the app click on “Connect” button and all your communication will be done via Proton VPN server
- To stop using VPN click on “Disconnect” button in the app
- Via the following website which information you release with/without VPN: <https://surfshark.com/nl/what-is-my-ip>





How to use mobile hotspot?

- If you do not have mobile data yourself and do not want to (or cannot) use a WiFi network, someone else can temporarily set up a **hotspot** on their mobile so that you can access the internet via their mobile (and their mobile data).
- You can turn on the WiFi hotspot via Settings > “Network and ...” > “Hotspot and ...”



Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

- * 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>

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

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

Section 6

**Anonymous use of browser,
search engine and email**



What is meant by “privacy”?

- When a company offers its digital services, you often have to accept the terms and conditions drawn up by them in order to use them (these terms and conditions are only read by a few); because you use their services, this company will have all kinds of information about you and by accepting it, you indicate what this company may do with it: keep/**collect** (and for how long), **analyze**/combine, **pass** on to third parties, etc.; sometimes this is unintentional by you and is abused by third parties
- For example, Google is known for using and collecting all data about you and passing it on to third parties for advertising purposes to earn money; many companies generate their income in this way; For example, free 15GB Cloud storage, free use of search engine in browser: A frequently used statement: "If you don't have to pay for a service, then you are not a customer but the product from which money is earned"



How to increase privacy when using your browser?

- When using popular **browsers** (Google Chrome, MS Edge, Mozilla Firefox, Apple Safari), all your surfing behavior is collected: which websites you visited, where you are and when, which PC/smartphone you use and much more
- You can limit this exposure by choosing more private browsers; for example, you can choose “**Brave**”, a private browser that does not keep track of your data; this is at the expense of some ease of use: for example, you will have to log in again every time you visit a website repeatedly
- Many people therefore use multiple browsers; e.g. Google Chrome for normal use and Brave if privacy is desired





How to increase privacy when searching the web?

- **Search engines** are popular websites in browsers and are used to find interesting web pages on a topic;
Google Search is by far the most popular search engine



- This search engine will collect all your searches and chosen websites, and pass on collected data about you to third parties who want to pay for advertising;
you will then find this sponsored advertising specifically aimed at you first in the search results
- You can limit this exposure by choosing more private search engines; for example, you can choose **DuckDuckGo**, a private search engine that does not keep or pass on your data





How to increase privacy when using email?

- **Email inbox** is an account where emails are received and stored; **email alias** is an email address created for a specific purpose; an email inbox can be the final destination of many aliases
- For example, you can divide all your emails into separate email inboxes:
 - * personal inbox: only known by family and friends
 - * shared inbox: for all other communication with companies, etc.
 - * pseudonym inbox: belongs to a fictitious person and is used where an email address must be entered but is not wanted
- There are **anonymous email services** that hide your real email address via email aliases: AnonAddy, MailDrop, SimpleLogin, Yahoo, Gmail, etc.; these create random email aliases that forward all emails to your real inboxes; this way you can avoid email spam and keep your email inbox anonymous; you can then provide an email alias per group, e.g. one alias for all newsletters, one for all shopping accounts, etc.



How to increase privacy when using email?

- **SimpleLogin** is a popular email alias service with free version; open web page <https://simplelogin.io/nl/> or install “Simple Login” app



Exercises

- * Open SimpleLogin and create an account (sign in) linked to your email inbox
- * Login, create subdomain “mytest.aleaas.com” (subdomain) and define this subdomain as “default subdomain for aliases” (settings)
- * Create alias “john.doe@mytest.aleaas.com”
- * Send an email to this email address

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
<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

* 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>

* How to Use Brave Private Web Browser

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

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

* 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>

* Why Is Everyone Switching To DuckDuckGo?

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

* Is DuckDuckGo veilig? Beoordeling van Zoekmachine DuckDuckGo in 2021

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

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

- * 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>

- * STOP Giving Out Your Email - Do This Instead

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

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

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

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

* Why Care About Internet Privacy?

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

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

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

* How To Delete Yourself Off The Internet

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

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

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

Section 7

Secure access to app and website with Password Managers



How to secure access to app/site?

6 Tips to Secure Your Mobile Devices



Use screen locks and biometrics



Update your OS and apps regularly



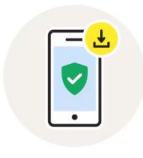
Use a VPN to protect your traffic



Create encrypted backups of personal information



Create strong passwords and enable 2FA



Use mobile security software for efficient security



What is a password manager?

- Even if someone can log in to your phone or PC, this person still does not have access to apps and websites with their own separate login
- Most smartphone or PC users have many online accounts each with their own password,
e.g. for your email, bank, federal government, doccle, etc.;
either you use the same (or variation of) password for each of these accounts (which is very unsafe), or you use a different password for each account (safer but more inconvenient)
- Remembering all these passwords is a real challenge;
a **password manager** is a program that makes this easier, by storing all your account data including password in a kind of digital safe (**vault**) that is on your phone or in the cloud;
you now only have to remember 1 password (of manager) to gain access to your safe and to be able to use all your passwords



What is a password manager?

- There are many password managers; Google also has a password manager built into Chrome browser; however, it has quite a few drawbacks (only in Chrome, limited)
- **Bitwarden** is a safe and popular choice, uses E2E encryption and is available on Android and Windows
- We will install the free version of Bitwarden app on your phone, and then create an account with a strong password; the vault will always be in Bitwarden Cloud
- After that, we can save each account with password for a site in the Bitwarden vault site by site



Choose the plan that fits your needs

Personal Business

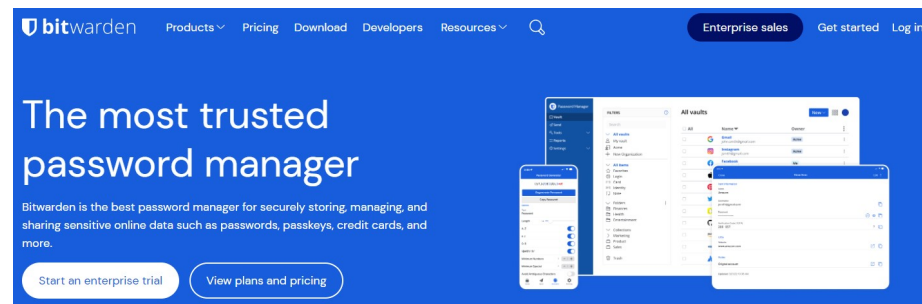
Free Forever	Premium	Families
\$0	Less than \$1 per month \$10 billed annually	\$3.33 per month Up to 6 users, \$40 billed annually
Get a Bitwarden vault	Enjoy premium features	Secure your family logins
✓ Unlimited passwords	✓ Integrated authenticator	✓ 6 premium accounts
✓ Unlimited devices	✓ File attachments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



How to use Bitwarden?

(1) Creating a Bitwarden account

- Open the Bitwarden site in browser:
<https://bitwarden.com/>
- Select “Get started” and enter required account details;
“email address”, “master password” and “name” are the most important details that you should not forget; always choose a **strong password**
- Click “Create account” and your account with private, encrypted vault will be created



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

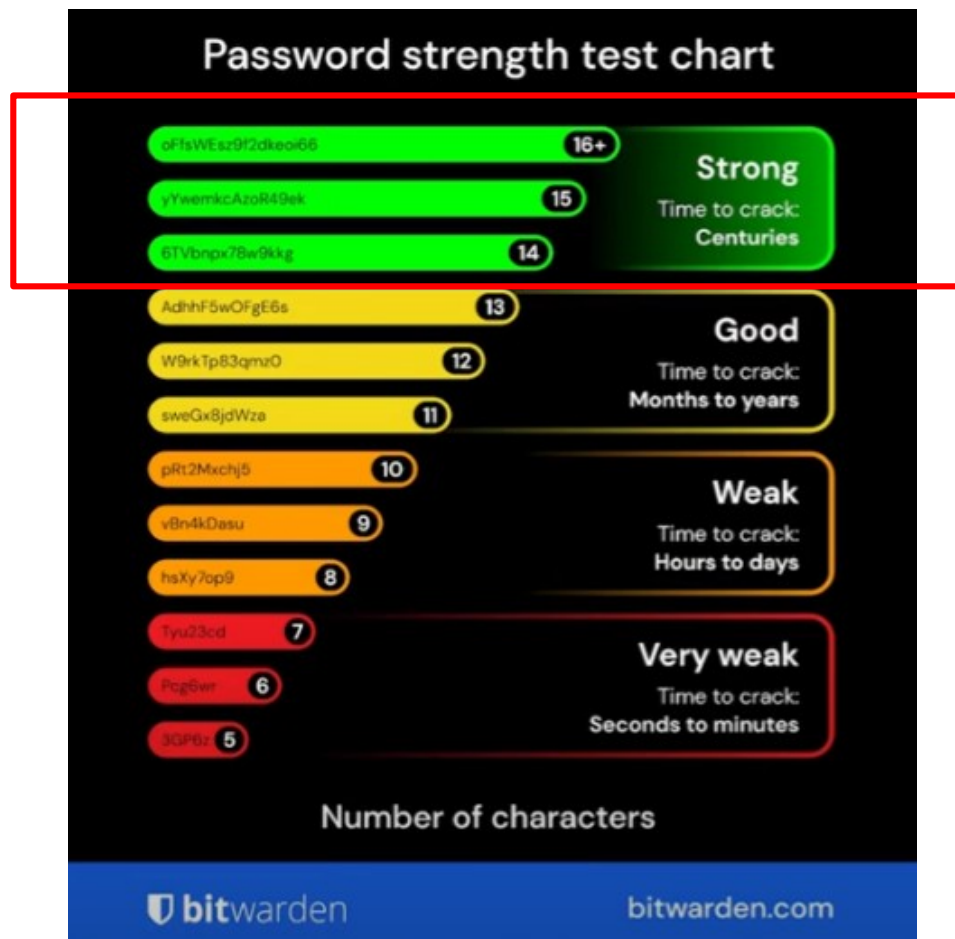


How to use Bitwarden?

What is a strong master password?

at least 16 characters according to Bitwarden's recommendation;

we can easily achieve this by using a "passphrase" (a series of words that is easy to remember, but contains many characters), for example:
"December '63 (Oh What a Night)"





How to use Bitwarden?

(2) Install Bitwarden and log in to all your devices

- Install “Bitwarden – Password Manager” app via Play Store on your android phone, and via download page [*https://bitwarden.com/download/*](https://bitwarden.com/download/) on your Windows pc
- For most browsers you can also install a Bitwarden extension; I installed this for the Chrome and Brave browsers on phone and pc; You can now pin the Bitwarden extension to the browser toolbar
- You can now log in to Bitwarden via the app or browser extension with your email address and master password



How to use Bitwarden?

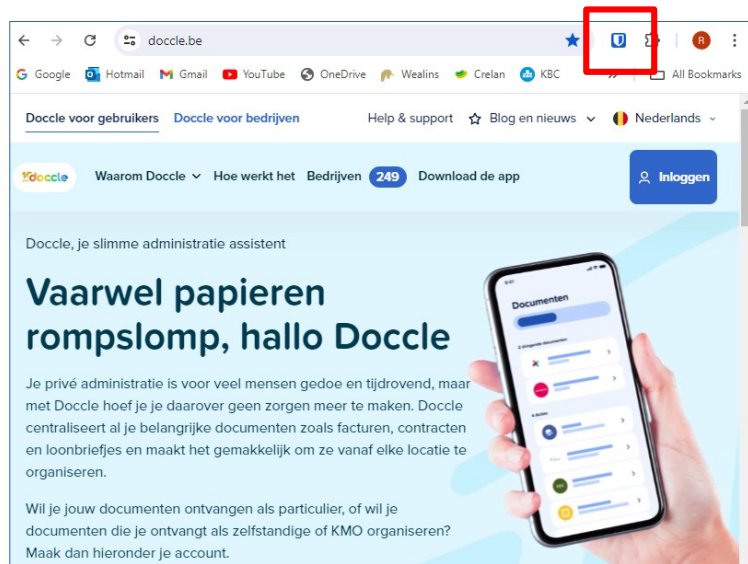
- To avoid conflicts between different password managers, you should disable the other managers;
to disable the Google password manager in Chrome:
 - * click “3 dots” icon at the top right, choose “Settings > Autofill and passwords”
 - * delete all passwords in your Google password manager, after you have exported them to a csv file (we will import them into Bitwarden later)
 - * disable “Google Password Manager”, “Payment methods” and “Addresses and more”
- Your Bitwarden vault is stored end-to-end encrypted in the Cloud using your account master password;
the most important **items** stored in your individual **vault** are:
 - * **security settings**: chosen security for access to your vault
 - * **logins**: all data to be able to log in to a secure website;
usually contains a name, username, password and uri
 - * logins can be organized in **folders** or marked as **favorites**



How to use Bitwarden?

(3) Import existing or create new logins for secure websites

- Import any accounts exported in Chrome into Bitwarden
- To create a new login, it is best to use the browser extension:
 - * navigate to the site for which you want a new login, eg *https://doccle.be/* in Chrome on pc
 - * click on Bitwarden icon and then on “+” to create new login for Doccle
 - * the “Add item” window appears with Type, Name and URI already filled in
 - * enter Username, Password, Notes, etc (strong password can be generated)
 - * click “Save” to save this login





How to use Bitwarden?

(4) Using Bitwarden to access secured site

- We now want to log in to the Doccle website via Bitwarden on Android; first we need to log in via the Bitwarden app
- Open <https://doccle.be/> in Chrome on our smartphone; click on “Login” button to open the “Log in” page; click on “Bitwarden” icon (above keyboard after clicking in a field) and choose Login to fill in screen data; you can adjust setting “Options > Auto-fill on page load” (or “Settings > Auto-fill”) in Bitwarden app, so that extension will automatically try to fill in login data when loading the page
- Install the Doccle app on your smartphone via Play Store; open the Doccle app and automatically you will go to the same “Log in” page as above



How to use Bitwarden?

(5) Set up Bitwarden to unlock vault via biometrics

- A Web Vault is usually unlocked via a master password, but this can also be done via fingerprint or face scan for more ease of use
- For this, some settings in Bitwarden need to be adjusted: log in your vault via browser or app, click “Settings” icon at the bottom and choose “Account security” > “Unlock with biometrics”

(6) Back up your Bitwarden vault regularly

- Login to your vault via browser or app, click “Settings” icon at the bottom and choose “Vault” > “Export vault”
- Save this file in a safe place and delete any possible copies on your system

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

- * 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

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

- * How to unlock your Bitwarden vault with biometrics

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

- * The Most Important Bitwarden Setting You Never Heard Of

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

- * How to Retrieve Your Bitwarden Recovery Code

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

- * 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>

Section 8

**Securely back up
files on smartphone**



Why make backups?

6 Tips to Secure Your Mobile Devices



Use screen locks
and biometrics



Update your OS
and apps regularly



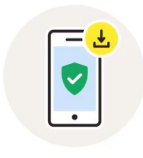
Use a VPN to
protect your traffic



Create encrypted
backups of personal
information



Create strong
passwords and
enable 2FA



Use mobile security
software for
efficient security



What is a good backup?

- **Backups** are the process of making backup copies of all your important folders and files and then storing these copies in a safe place; if you lose the original files, you can **restore** these files from your copies to the original (or another) location
- Regularly creating a good backup is important to avoid losing important data in the event of a virus infection or loss/damage to your mobile; you may only discover the consequences of virus infections after some time; it is therefore not enough to just keep a copy of the last state, but to make and store a **number of copies over time** (to be able to go back to the copy made before the infection)
- Backups should also be done as **automatically** as possible, because they should be performed easily and frequently



What is a good backup?

- You also **don't** want to make files with confidential or sensitive information **accessible to third parties**;
when storing in the cloud by third parties, your folders and files must therefore first be encrypted with your private key before sending them over the internet and storing them in a data center;
this is called End-to-End (E2E) encryption
- **Google One storage** is more intended to make files more widely available and for phone device backup, but does **not** offer **E2E encryption**:
files are sent encrypted and stored encrypted, but the encryption itself is done by Google;
Google can therefore decrypt and view all the stored files,
and does so for all kinds of reasons

What is the “3-2-1” backup recommendation?



3

copies:
1 production +
2 backups



2

types
of storage
media



1

off-site –
in the Cloud



How to make a good backup?

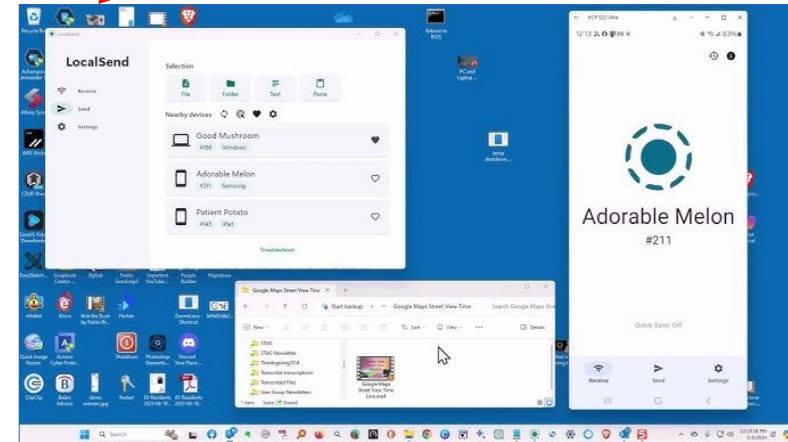
- A good backup should therefore support 2 things:
 - * creation (and limitation) of different generations of copies
 - * no access to copies by third parties
- You can create a simple backup system for your smartphone if, for example, you have **your own PC in your local home network**:
 - * for your own PC you probably already have a backup system provided to protect important files on your PC against loss; usually backups are made to an external hard drive
 - * it is therefore sufficient to find an easy way to copy all important files from the smartphone to your own PC (via Wifi and not over the internet, so no encryption is required); the copied files from the smartphone are then backed up by the backup system provided on the PC

How to transfer files between devices easily?

- With **LocalSend** app you can easily transfer files and folders between devices via Wifi and without cables; app replaces other solutions, such as "Near By" from Android, "Quick Share" from Samsung, "AirDrop" from iPhone or Cloud apps; for this you first need to install the app on all these devices (pc, tablet, iphone, android)



- With **Syncthing** app you can easily synchronize files between two computers/tablets/mobiles



How to backup folders and files on a Windows pc?

- There are many free backup softwares for Windows PCs;
“**EaseUS Todo Free**” is a popular and free backup software
- You can start with this software and the following schedule for backups:
 - * an Image backup is made only once (if desired)
 - * a **Full backup** at the beginning of each month;
we only keep Full backups of the last 3 months
 - * an **Incremental backup** (only changes compared to the previous one) every day;
we only keep Incremental backups of the after last Full backup
- Remember that you usually do not only need to backup photos and videos on your smartphone, e.g. also contacts, text messages, WhatsApp chats, Keep notes

How to organize folders and files for efficient backup?

- To limit the volume of data to be backed up and to make your backup run faster, you can take a few measures in advance:
 - * folders and files that will never change, should be placed separately, e.g. in an "Archive" folder; this folder should only be copied manually if subfolders are added; on your smartphone, this "**Archive**" folder could contain the photos and videos from the past years
 - * all folders and files that need to be backed up regularly, should be placed as subfolders of one folder to be backed up; on your smartphone, you could designate the "**DCIM**" folder as the only folder to be backed up; the "Archive" folder should be placed separately and all other files (such as contacts) should be exported as subfolders of the "DCIM" folder

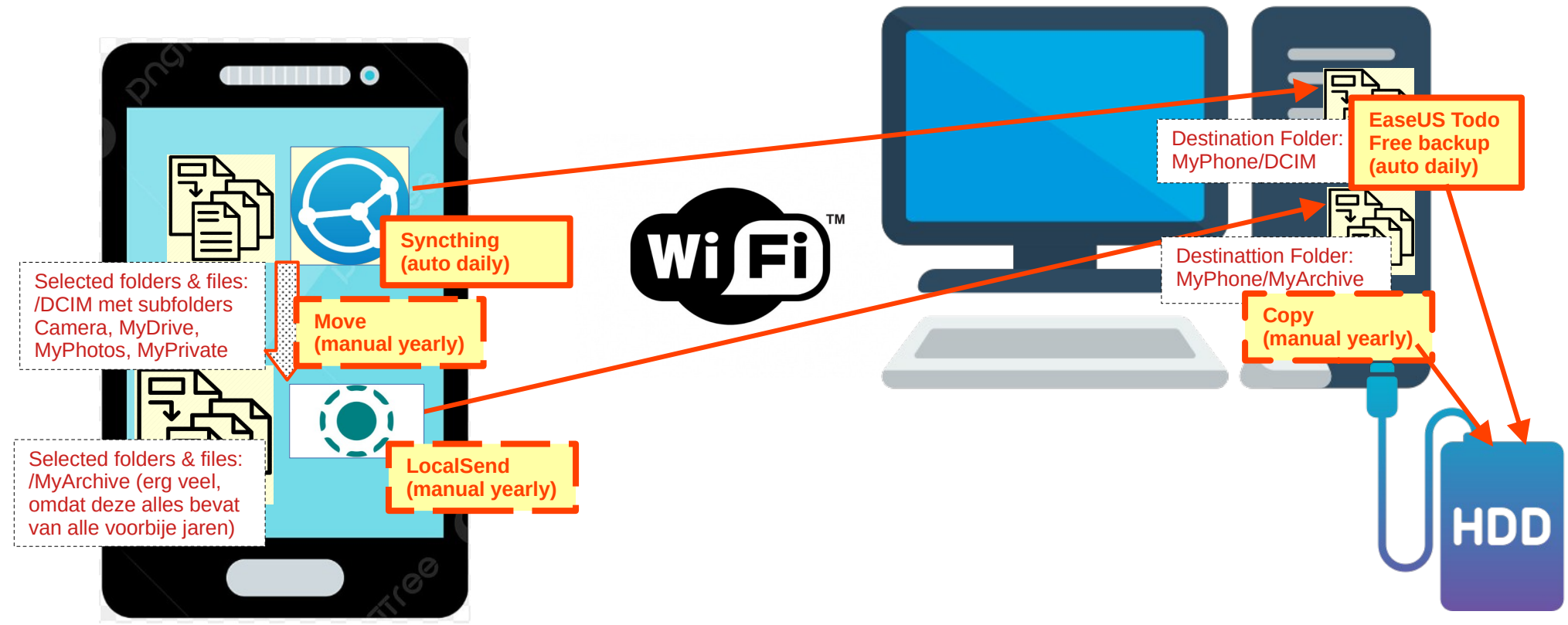
How to organize folders and files for efficient backup?

Photos and videos are stored in “/DCIM/Camera” and “/DCIM/MyPhotos” folders;
export data from other apps as files in “/DCIM/MyDrive” or “/DCIM/MyPrivate” folder:

- Use “**Super backup – SMS and Contacts**” app to export in SmsContactsBackup folder:
 - * Contacts
(open Contacts app, click “Organize” button at the bottom and choose “Export to file”)
 - * Calendar Events
 - * Text messages (sms) and Call Logs (Phone)
- Export WhatsApp chats in “WhatsApp” subfolder:
open WhatsApp app, click 3 dots button at the top
and choose “Settings > Chats > Chat history > Export chat”
- Export Keep notes in “KeepNotes” subfolder
open KeepNotes app, select notes, click 3 dots button at the top;
choose either “Send > CxFileExplorer” (many txt), or “Copy to Documents > Open” (1 pdf)
- You can export other files in “Other” subfolder

How to implement secure backup in practice?

Use your own PC also for making secure backups of smartphone (not accessible by third parties); for this you need to synchronize the desired data on smartphone with a folder on your PC via local WiFi (where no storage-saving but original format is used)



Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

- * Don't Use Google For Photo Backup!

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

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

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

- * Syncthing Made EASY

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

- * Syncthing - Automatic Phone Backup to Your Computer

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

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

* 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>

* What Backup Software Should I Use?

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

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

* 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>

* 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

Section 9

**Secure access to app and website
with 2FA**



How to secure access to app/site?

6 Tips to Secure Your Mobile Devices



Use screen locks and biometrics



Update your OS and apps regularly



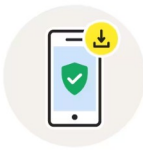
Use a VPN to protect your traffic



Create encrypted backups of personal information



Create strong passwords and enable 2FA



Use mobile security software for efficient security



What is 2FA?

- Access to websites with personal data is usually protected with passwords; however, on a smartphone there are quite a few apps (Google Drive, Microsoft Outlook, WhatsApp, etc.) that automatically rely on the device's login; if you have access to this device, then you automatically have access to all these apps (which is of course unsafe)
- However, for websites with confidential or sensitive information, you want more security than just via passwords; for example, the government and banks have been using extra security in the form of eID or bank card with card reader for some time now; so in addition to knowing the PIN code, you must also have a card in your possession
- With **Two-step verification** (2FA = Two Factor Authentication), access to an app or website is only granted after 2 different types of checks; the term MFA (Multi Factor Authentication) is sometimes also used



What is 2FA?

- A still widely used, simple form of 2FA security for login:
 - * first you must enter a correct password
 - * an SMS with a numerical code is automatically sent to your telephone number
 - * you must then enter this constantly changing numerical code
- Only after correctly executing this login process will you be granted access to website
- For access security with 2FA, you must not only know a password, but also have a correct device in your possession;
for example, a smartphone with your telephone number in the previous case
- To secure WhatsApp with their 2FA:
open WhatsApp app, click the dots button, choose “Settings > Account > Two-step verification”;
additional verification is done by entering a PIN code when logging in to the app
- To secure Microsoft Outlook:
open Outlook app, click the menu button, then click the “Settings” button and choose “App lock”;
additional verification is done by entering a fingerprint when unlocking the app



What is 2FA?

Most common forms of 2FA (ranked from least to most secure):

- **Email** with a one-time use code
- **SMS and Phone call** with a one-time use code
- **Push Notification** sends a prompt to trusted devices when a login attempt is made
- **Biometric** with a fingerprint or facial recognition
- **Software** form of 2FA requires the user to first install a 2FA authentication app on their phone or desktop and then set it up by receiving and entering a secret long text or secret QR code from each website to be secured ("seed"); to then log in, the user must first enter a correct username and password, and then read a software-generated, seed-and-time-based one-time passcode (also called TOTP or software token) via this Authenticator app (on another device) and enter it into their login; this passcode usually changes every 30 sec
- **Hardware** form of 2FA requires you to plug a security key into the USB port; this generates new numerical code at regular time intervals and sends it automatically



Where is 2FA used?

- Many companies already have websites with 2FA support; you can find a list on the following web page: <https://2fa.directory/be/>
- *To secure Gmail (and therefore all Google Cloud services) with 2FA:*
 - * *open Chrome browser, click on your Profile icon (top right), choose “Manage Google account” to open “Google account” page*
 - * *click on “Security” option in left menu, and scroll down to section “How you sign in to Google”*
 - * *click “2-Step Verification”, and choose option “Phone number” in “Second steps”*
- Some other examples:
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), etc



Which 2FA Authenticator app to choose?

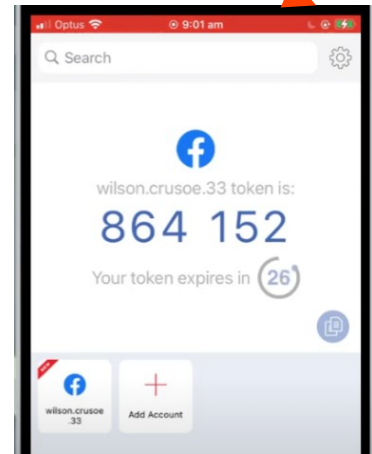
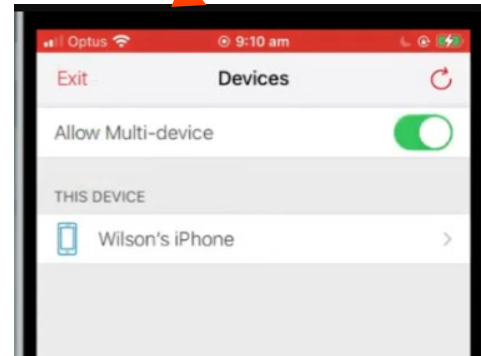
- There are many Authenticator apps, some of which are paid; an authenticator app can in principle work without an internet connection, but in practice many are not private and collect data about you
- *Popular Authenticator apps for software-based security:*
 - * *software, non-proprietary: Twilio Authy, Microsoft Authenticator, Google Authenticator*
 - * *software, proprietary: FreeOTP, Aegis Authenticator*
 - * *hardware: Yubico Authenticator (not free)*
- Here we want to choose a free, software-based 2FA Authenticator app with a good reputation and that offers sufficient privacy:
Google Authenticator is very popular;
Bitwarden can also be used as an Authenticator app, but is rarely used for this purpose;
Twilio Authy app is recommended by experts (only available on mobile since 2024 and no longer on PC)
- We will use **Authy** as 2FA Authenticator app



How to use 2FA in practice?

(1) Install an Authenticator app on your smartphone

- **Authy** app can be downloaded and installed for free via Play Store; more information from the corresponding website <https://authy.com/>
- Mobile with Authy app you can now start using as authenticator device; you should also provide a backup for authenticator device by providing a “backup password” or making “multi device access” available






How to use 2FA in practice?

- (2) Create an account on the PayPal website,
which we will then use as an example site for 2FA security
- Open browser and go to PayPal website *<https://www.paypal.com/>*



How to use 2FA in practice?

- Open PayPal account

 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.

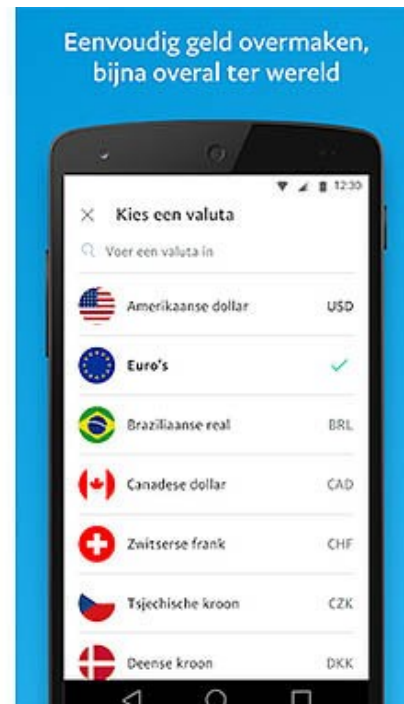
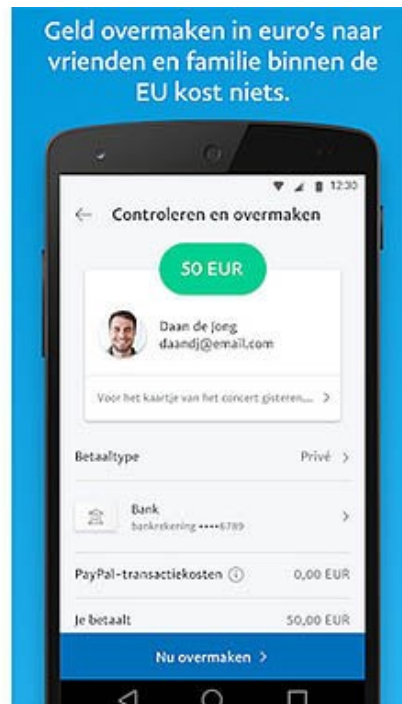
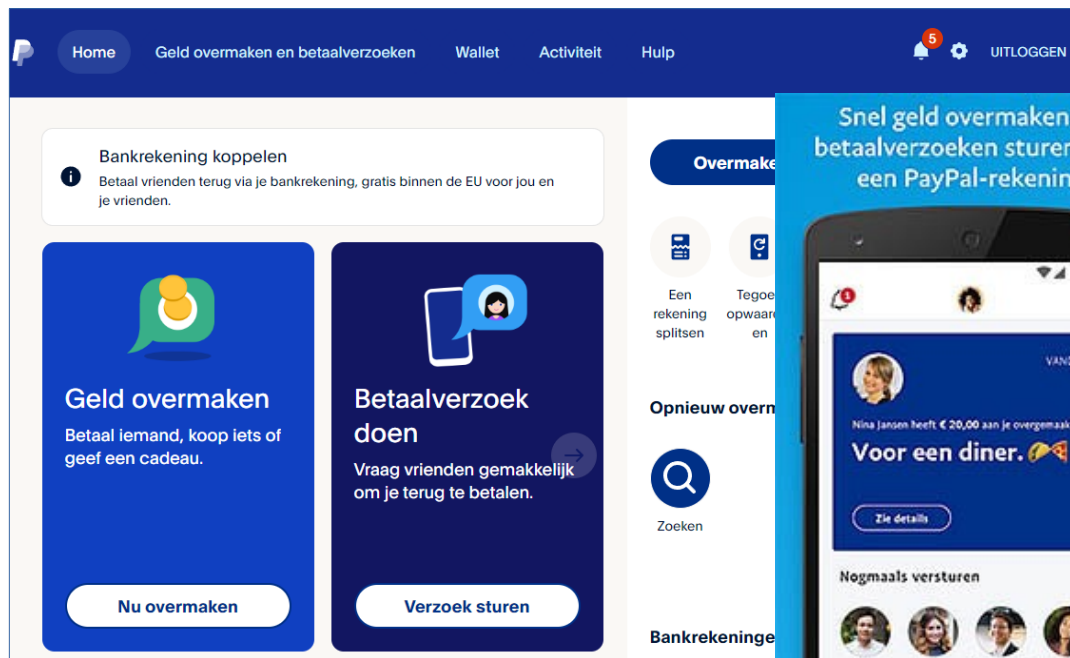
☒ Je gaat akkoord met de ontvangst van marketingcommunicatie. Je kunt dit op elk gewenst moment wijzigen in je instellingen.

Akkoord en rekening openen



How to use 2FA in practice?

- Install PayPal app via Play Store on your mobile and login





How to use 2FA in practice?

(3) Adjust settings in Paypal to use 2FA

The image shows a screenshot of the PayPal account settings page. The top navigation bar includes 'Home', 'Geld overmaken en betaalverzoeken', 'Wallet', 'Activiteit', 'Hulp', and 'UITLOGGEN'. The 'Veiligheid' (Security) tab is selected and highlighted with a red box. Below the navigation bar, the 'Veiligheid' section is visible, showing options for 'Wachtwoord' (Password), 'Wachtwoordsleutels' (Security keys), 'Tweestapsverificatie' (Two-step verification), and 'Je logins beheren' (Manage your logins). The 'Tweestapsverificatie' option is highlighted with a red box. The 'Tweestapsverificatie' section includes a description: 'Voeg een extra beveiligingsniveau toe aan je rekening door telkens wanneer je inlogt gebruik te maken van een eenmalige beveiligingscode naast je wachtwoord.' and a link to 'Instellen' (Set up).



How to use 2FA in practice?

(3) Adjust settings in Paypal to use 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
Gebruik je account op andere apparaten?

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 camera van je verificatie-app of een geavanceerde afbeeldingsapp.

4VCL KNKK 43Y3 6FR

Stap 2: Voer de zescijferige code in die je in 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 om 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

Voer je code in

We hebben een beveiligingscode verzonden naar +32 [redacted]

[Nieuwe code verzenden](#)

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

Je hebt tweestapsverificatie toegevoegd aan je rekening.



How to use 2FA in practice?

(4) Log in with 2FA

The image shows a screenshot of the PayPal Dutch website interface. The top navigation bar includes links for Home, Geld overmaken en betaalverzoeken, Wallet, Activiteit, and Hulp. A red box highlights the 'UITLOGGEN' button in the top right corner. Below the navigation bar, there is a section for 'Bankrekening koppelen' (Link bank account) and buttons for 'Overmaken' (Transfer) and 'Betaalverzoek' (Payment request). The bottom navigation bar includes the PayPal logo, 'CONSUMENTEN' (Consumers), 'BEDRIJVEN' (Businesses), 'ONTWIKKELAARS' (Developers), and 'HULP' (Help). A red box highlights the 'Inloggen' (Log in) button in the bottom right corner. To the right of the main interface, there is a login form with fields for 'E-mailadres of mobiel nummer' (Email address or mobile number) and 'Wachtwoord' (Password). Below the password field is a link for 'Wachtwoord vergeten?' (Forgot password?). The 'Inloggen' button is highlighted with a red box. Below the login form, there is a section for 'Voer je code in' (Enter your code) with six input boxes for a 6-digit verification code. A 'Doorgaan' (Continue) button is highlighted with a red box. At the bottom of this section is a link for 'Heb je problemen met inloggen?' (Having trouble logging in?).

PayPal

Home Geld overmaken en betaalverzoeken Wallet Activiteit Hulp

UITLOGGEN

Bankrekening koppelen
Betaal vrienden terug via je bankrekening, gratis binnen de EU voor jou en je vrienden.

Overmaken Betaalverzoek

Een rekening splitsen Tegoed opwaarderen Rechtstreeks naar bank Contant afhalen Meer

PayPal CONSUMENTEN BEDRIJVEN ONTWIKKELAARS HULP

Inloggen Aanmelden

Wij helpen je om te shoppen en te betalen.

Voer je code in
Voer de zescijferige beveiligingscode uit je verificatie-app in.

Doorgaan

Heb je problemen met inloggen?



How to use Authy as an Authenticator app for 2FA?

- If you want to use 2FA to further secure your account on a website, it is best to make a backup of your 2FA codes (seeds) that you keep safe (necessary in case of theft or defect of mobile)
- How?
 - * open Authy app, click dots icon (top right) and choose “Settings”
 - * choose “Accounts” tab and turn on “Backup”
 - * choose a new “Backup Key” and keep it in a safe place (e.g. as an extra field with your PayPal login in your Bitwarden vault)

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

* 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>

* Why You Should Turn On Two Factor Authentication

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

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

- * 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>

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

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

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

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

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

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

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

* Most PRIVATE 2FA apps

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

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

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

* 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>

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

- * How to set up 2FA in Bitwarden

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

- * 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>

Section 10

**Secure access to app and website
with Passkeys**



How to secure access to app/site?

6 Tips to Secure Your Mobile Devices



Use screen locks and biometrics



Update your OS and apps regularly



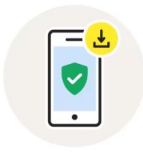
Use a VPN to protect your traffic



Create encrypted backups of personal information



Create strong passwords and enable 2FA



Use mobile security software for efficient security



What are passkeys?

How can we protect access to sites better and more easily than with passwords?

- **Passkeys** are a relatively new way of securing that completely replaces the use of passwords;
currently there are few websites with support for 2FA and Passkeys;
large companies (Google, Microsoft, Apple, Amazon, Meta, Samsung, etc.) are currently strongly promoting passkeys, and will slowly replace passwords completely
- For each account that you need to be able to log in, a matching public key and private key are generated (based on Asymmetric Cryptography);
this key pair will be used for every login attempt;
the public key is shared with the website that you want to log in to, and the private key remains private (known only to you) and stored privately for you;
the key pair is not only unique for each account, but is also linked to 1 specific website and often also to 1 physical device (mobile, pc, Yubikey)
- Advantages:
 - * even when hacking all (public) keys on the website, there is still no danger because the private keys are needed to log in
 - * phishing is also no longer possible because the keys are linked to a website



What are passkeys?



Private Key



Public Key



What are passkeys?

How do you use passkeys in practice (for websites that support this)?

- Go to the desired website in Google Chrome, and you will automatically be asked to use the passkey stored on your mobile
- you will then need to identify yourself to get your passkey, e.g. with a fingerprint; you will then be logged in immediately

How are passkeys stored? There are 2 possibilities:

- **Device-bound passkey:** create a separate passkey for each of your devices for each website, and keep it on your local device
- **Synchronized passkey:** create one separate passkey for each website, store it E2E encrypted in the cloud, and let all your devices use it; this requires synchronization across all your devices (or passing it on via QR code)

Saved passkeys should of course always be backed up;

Passkeys can already be used on iOS 16+, Android 6+ and Windows 10+

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

- * 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>

- * What is a Passkey?

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

- * Learn passkeys for simpler and safer sign-in

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



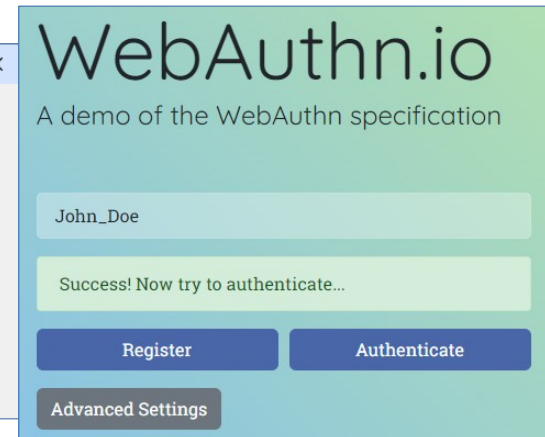
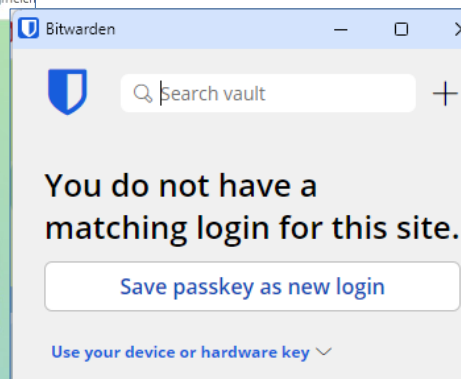
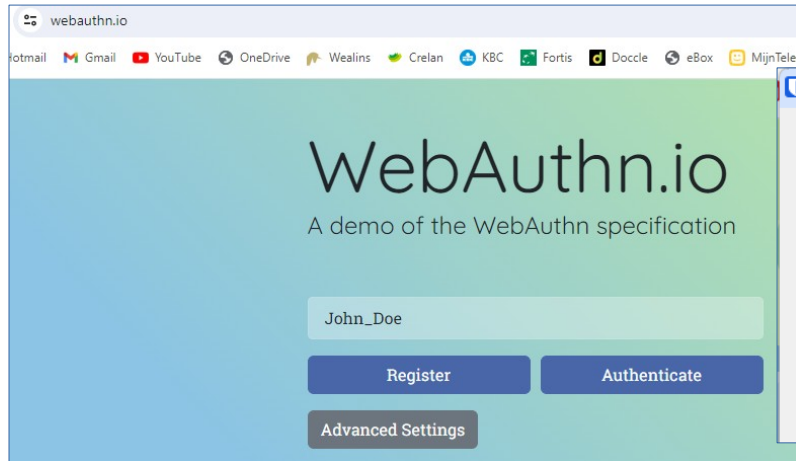
How to store passkeys in Cloud with Bitwarden?

- The free version of Bitwarden supports both 2FA and passkeys; the free version only supports passkeys via YubiKey, and only 2FA via authenticator app or email (paid version also supports hardware key, sms, phone call); Bitwarden stores passwords and passkeys E2E encrypted in the cloud
- If you use Bitwarden to store passkeys for websites, then:
 - * do not use passwords for these websites at the same time
 - * only 1 login with passkey can be automatically stored per site; for a 2nd login you need to manually clone the existing login for this site (for different accounts on the same website)
- Bitwarden currently does not have the option to export and re-import passkeys stored in your vault



How to use passkeys with Bitwarden?

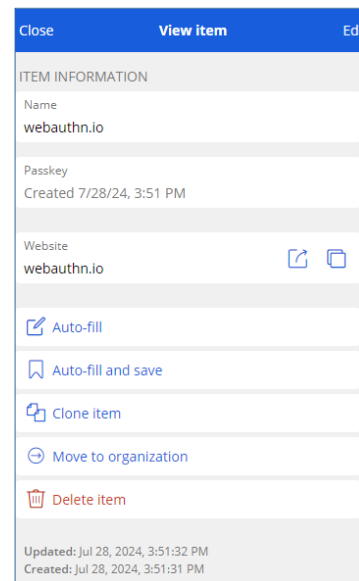
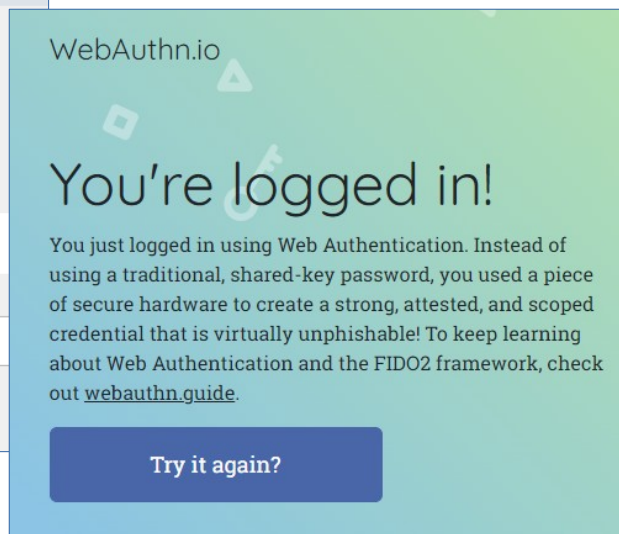
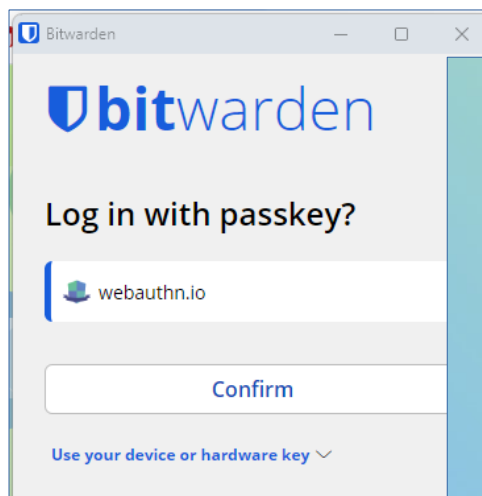
- Open website <https://webauthn.io/> which we will use to practice with passkeys; Bitwarden extension must be installed in your browser
- Type “John_Doe” as username in input field “example_username”, and click “Register” button;
Bitwarden dialog box opens and click “Save passkey as new login”;
passkey for this user for this site is now created in Bitwarden vault





How to use passkeys with Bitwarden?

- Click “Authenticate” button to login to this website;
Click “Confirm” button in Bitwarden window to confirm chosen passkey
- Open Bitwarden vault and view saved login with passkey





How to login with passkey in Bitwarden?

- Set up Bitwarden login:
 - * open <https://vault.bitwarden.com/> in browser and login to your vault; click Profile icon at the top right, and “Account Settings > Security”
 - * for login with 2FA use (authenticator used): select tab “Two-step login”
 - * for login with passkey use (in beta): select tab “Master password” and click “New passkey” in section “Login with passkey”
- Do not use a passkey for Bitwarden login for now, as this is currently still in experimental phase

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

* Faster Logins with Passkeys | Bitwarden Passkey Tutorial

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

* Sign into Bitwarden with a passkey

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



Which websites support passkeys for account security?

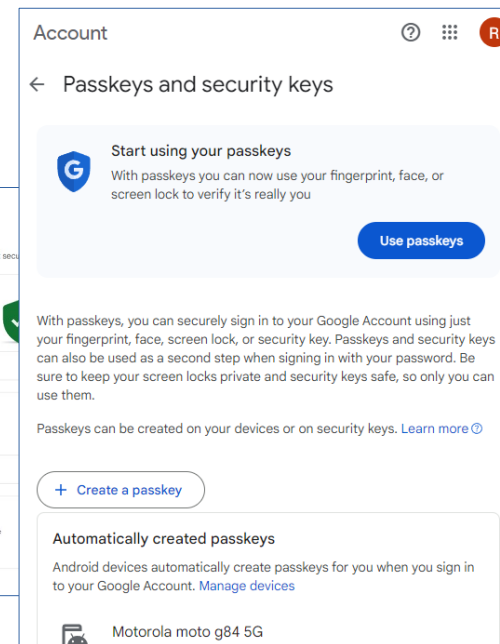
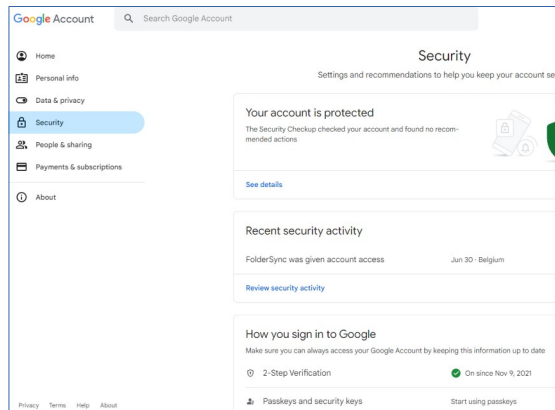
- List of websites that support passkeys can be found at:
 - * Websites that support passkeys:
<https://www.passkeys.io/who-supports-passkeys>
 - * GitHub repo for Bitwarden:
<https://github.com/bitwarden/passkeys-index>
- WhatsApp supports login via passkeys:
open WhatsApp app and click on dots icon (top right);
choose “Settings > Account > Passkeys” and click “Create Passkey”



Which websites support passkeys for account security?

Securing Google apps with passkeys:

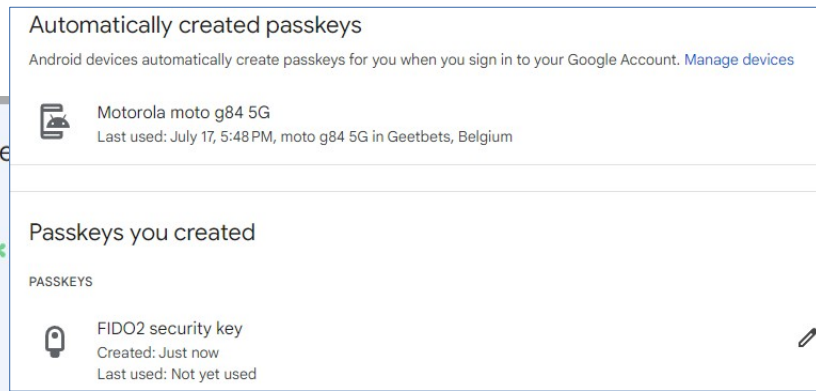
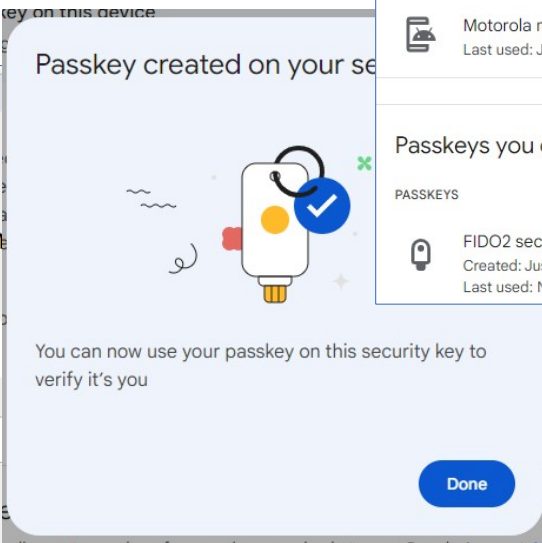
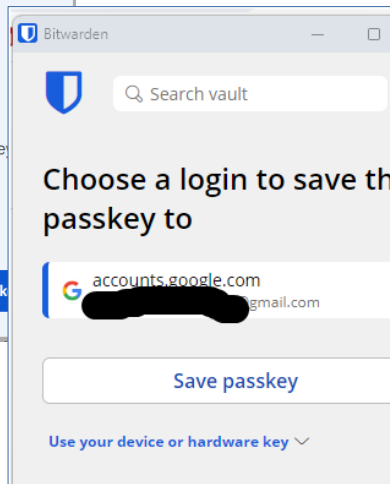
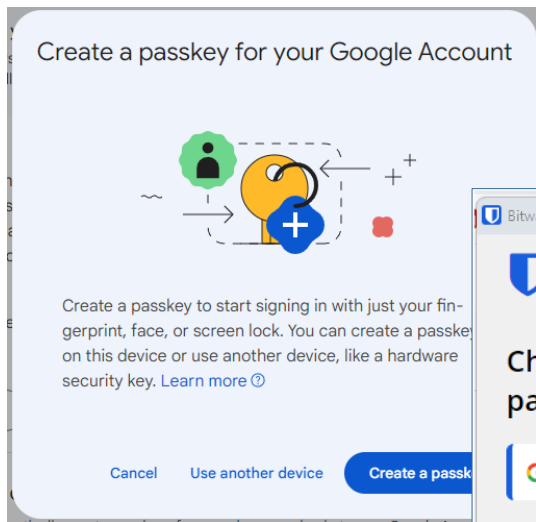
- Open <https://mail.google.com/> and log in; click on profile icon (top right) and then on “Manage your Google Account”
- Click on “Security” tab in menu on the left, and then on “Passkeys and security keys”; you can now see the already created passkeys





Which websites support passkeys for account security?

- Click on “Create a passkey” button to create a passkey on your current device in Bitwarden vault





Which websites support passkeys for account security?

- Log out and log back into Gmail to test Passkey security

The screenshot illustrates the process of logging out and back into Gmail to test passkey security. It shows three overlapping browser windows:

- Google Sign-in Page:** Displays "Signed out - syncing is paused" and a message: "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." Buttons for "Continue" and "Sign in again" are visible.
- Bitwarden Extension:** A modal window titled "Log in with passkey?" for the account "accounts.google.com". It includes a "Confirm" button.
- Google Account Menu:** A sidebar menu with options: Home, Personal info, Data & privacy, Security, People & sharing, and Payments & subscriptions. It also includes a search bar and a "Welcome," message.

Extra info

Videos with more explanation

for Dutch spoken Youtube video's, you can turn on English subtitles

- * How to Create a Passkey on WhatsApp || Whatsapp new update 2023
<https://www.youtube.com/watch?v=E0WzADthzq0>
- * Google Passkeys Tutorial | Step by Step Guide to Set Up Google Passkeys
<https://www.youtube.com/watch?v=ckvrKdFNF78>

Still questions?

this is the last part of a 3 part presentation about android phones