

Uitleg

Wat is online privacy?

Online privacy gaat over **wie toegang heeft tot jouw persoonlijke gegevens** en **hoe die gegevens worden gebruikt**.

Persoonlijke gegevens kunnen bijvoorbeeld zijn:

- Je naam, adres, telefoonnummer
- Je e-mailadres of schoolaccount
- Foto's en video's
- Locatiegegevens (bijvoorbeeld via je smartphone)
- Inloggegevens of bankinformatie

“📌 **Belangrijk:** veel apps en websites verzamelen automatisch gegevens over jou, vaak zonder dat je het doorhebt.

Wat deel je wel en niet online?

Niet alle informatie is geschikt om openbaar te maken. Vraag jezelf altijd af:

“Wie kan dit zien, nu en later?”

Veilig om te delen	Beter niet delen
Voornaam	Volledige adresgegevens
Hobby's of interesses	BSN, paspoortnummers, wachtwoorden
Openbare schoolprojecten	Intieme foto's of privégesprekken
Profielen op schoolplatforms	Locatiegegevens in realtime

Tip: stel altijd in wie je berichten kan zien. Gebruik **privacy-instellingen** op sociale media.

Sterke wachtwoorden en beveiliging

Wat is een sterk wachtwoord?

Een sterk wachtwoord is:

- Minimaal **12 tekens**
- Bestaat uit **hoofdletters, kleine letters, cijfers en symbolen**
- Uniek per website of app
- Moeilijk te raden, maar makkelijk voor jou te onthouden

Voorbeeld:

`!ZonEnMaan_2025!`

Gebruik geen simpele wachtwoorden zoals "**Welkom123**" of "**School2024**".

Tips voor betere beveiliging

- Gebruik **tweestapsverificatie (2FA)** → extra beveiligingscode bij inloggen
- Gebruik een **wachtwoordmanager** om al je wachtwoorden veilig op te slaan
- Log uit op gedeelde apparaten
- Stel een **schermvergrendeling** in op je telefoon en laptop

Gevaren van onvoorzichtig delen

Oversharing

Te veel persoonlijke informatie delen kan leiden tot:

- Identiteitsdiefstal
- Misbruik van foto's
- Ongewenste aandacht
- Problemen bij sollicitaties in de toekomst

Phishing

Phishing is een nepbericht of e-mail die probeert je gegevens te stelen.

Kenmerken van phishingmails:

- Urgente taal ("Je account wordt geblokkeerd!")
- Onbekende afzenders of vreemde links
- Vragen om persoonlijke informatie of inloggegevens

Tip: klik nooit zomaar op links. Controleer altijd de afzender en webadressen.

Privacy-instellingen controleren

Elke sociale media-app heeft instellingen waarmee je bepaalt wie je content ziet. Check vooral:

- Wie kan je foto's bekijken?
- Wie kan je berichten sturen?
- Welke apps hebben toegang tot je gegevens?
- Waar wordt je locatie gedeeld?

Praktijktip:

Neem één keer per maand 5 minuten om je instellingen door te lopen op **Instagram**, **Snapchat**, **TikTok** of andere apps.

Jouw digitale voetafdruk

Alles wat je online zet, laat sporen achter. Dit heet je **digitale voetafdruk**.

Voorbeelden:

- Berichten op sociale media
- Likes en reacties
- Zoekopdrachten
- Online aankopen

☐ **Bedenk:** toekomstige werkgevers, scholen en organisaties kunnen jouw digitale voetafdruk ook vinden.

Revision #1

Created 26 August 2025 19:03:16 by Admin

Updated 26 August 2025 19:12:47 by Admin