

Je account op slot zetten

Naam:

Klas:

Opdracht #1

Is een van jouw accounts ooit gehackt? Vertel hieronder jouw ervaring. Weet je hoe het kwam dat ze toegang hadden tot je account?

Kijk zo meteen op de volgende website. Deze site houdt bij welke data ooit 'op straat' is beland. Hackers plaatsen bijvoorbeeld alle data die ze gestolen hebben soms openbaar. Je kunt op deze site aan de hand van jouw e-mailadres zien of jouw account ooit in zo'n datalek is geweest, en misschien wel welke data er van jou te zien was.

Vul jouw e-mailadres in op deze website:
<https://haveibeenpwned.com/>

Is er ooit iets met een van je accounts gebeurd? Zo ja wat voor gegevens zijn openbaar geworden?

Wist je dit? Denk je dat je iets moet gaan doen?

Het is nooit verkeerd om je wachtwoord te wijzigen in het geval dat je denk dat je account niet meer veilig is. Maar je kunt ook nog meer doen! Zoals de password managers en 2FA aanzetten zoals je net de in presentatie had gehoord.

Opdracht #2

Leg in je eigen woorden uit wat two-factor autorisatie (2FA) is.

Gebruik je al op een website 2FA? Zo ja, welke? En hoe doe je dat?

Nu ga je zelf onderzoeken hoe je 2FA kan gebruiken. Daarvoor moet je naar een website waar jij een inlog account hebt. Dit kan bijvoorbeeld bij je e-mail zijn of een social media account.

Welke site kies jij?

Waar op de website kan je je inloggegevens, en dus 2FA aanzetten?

Hoe werkt dat voor deze website? Via een sms of anders?

Teken of beschrijf het proces hieronder!

Ben jij van plan 2FA aan te zetten? Waarom wel? Of waarom niet?

Gefeliciteerd! Nu zijn jouw accounts altijd goed beveiligd!