

Docentenhandleiding

Module Digitale overheid en veiligheid - les 2

Inleiding

In de module Digitale overheid en veiligheid maken leerlingen in de eerste module kennis met de digitale overheid. Ze ontdekken welke rol de overheid in hun leven speelt, en met welke digitale overheidsinstanties ze tussen hun 14^e en 21^e te maken kunnen krijgen. Jongeren leren over de functie van DigiD en hoe je dit kunt aanvragen als je nog geen eigen DigiD hebt. Ook leren ze om hun DigiD gegevens nooit met anderen te delen, en maken ze kennis met de berichtenbox van de overheid.



In de tweede les leren leerlingen meer over digitale veiligheid. Ze leren over het belang van een veilig wachtwoord en het gebruik van een wachtwoordmanager. Ook komen ze erachter dat het slim is om tweestapsverificatie aan te zetten, bijvoorbeeld om te voorkomen dat bijvoorbeeld je socialmedia-account wordt gehackt en je het slachtoffer wordt van identiteitsfraude. Tenslotte gaan leerlingen bij zichzelf na of zij hun eigen digitale veiligheid goed op orde hebben.

In deze docentenhandleiding vind je alles wat je nodig hebt om de lessen te geven. De digibord-presentatie ondersteunt je bij de lessen en leidt je er doorheen. Bij iedere slide van de digibord-presentatie vind je in deze docentenhandleiding een toelichting met daarin antwoorden op de quizvragen, extra informatie en mogelijke vragen die je aan de leerlingen kunt stellen.

Doelgroep

Bovenbouw havo/vwo-leerlingen

Duur

De module bestaat uit twee lessen van ieder ongeveer 45 minuten.

Vorbereiding

- Neem de docentenhandleiding en de online digibordpresentatie door en bekijk de online oefenopdrachten.
- Onderzoek welke lokale hulpplekken er binnen jullie school en gemeente zijn om jongeren te ondersteunen bij het regelen van hun digitale regelzaken.

Leerdoelen

Doe je digiding! werkt aan de onderstaande algemene leerdoelen:

- Vergroten van kennis van de (overheids)wereld
- Vergroten van digitale geletterdheid: informatievaardigheden en mediawijsheid
- Vergroten van financiële vaardigheden
- Vergroten van woordenschat

Leerdoelen les 1

- De leerling kan benoemen welke rol de (digitale) overheid in zijn leven speelt.
- De leerling kan vijf overheidsinstanties benoemen waar hij tussen zijn 14^e en 21^e mee te maken krijgt.
- De leerling kan uitleggen wat de functie van DigiD is.
- De leerling kan in eigen woorden formuleren wat de gevolgen kunnen zijn als iemand jouw DigiD-gegevens heeft.
- De leerling kan onderzoek doen naar verschillende hulpplekken bij hem in de buurt.

Leerdoelen les 2

- De leerling kan uitleggen waar een sterk wachtwoord aan moet voldoen.
- De leerling kan zelfstandig onderzoek doen naar veelgebruikte wachtwoordmanagers en virusscanners.
- De leerling kan benoemen wat je kunt doen om de kans te verkleinen dat je wordt gehackt.
- De leerling kan uitleggen wat identiteitsfraude is.
- De leerling kan een inschatting maken van zijn eigen digitale veiligheid.

Kennischeck

Iedere les kan worden afgesloten met een kant- en klare online kennischeck, aangeboden via Microsoft Forms. Je kunt de kennisquiz in je eigen account dupliceren om vervolgens zelf met je leerlingen te delen en de resultaten van de klas achteraf te bekijken.

Lesbeschrijving les 2

Klaarzetten

- [Digibord met online digibordpresentatie les 2](#)
- [Online oefenopdrachten les 2](#)
- Computers voor de leerlingen
- Deze docentenhandleiding (geprint)
- [Kennischek les 2 \(Digitale veiligheid\)](#) (gedupliceerd in eigen account via Microsoft Forms)
- Optioneel: [Checklist 'Regel je digitale \(overheids\)zaken op tijd](#) (geprint)

Opbouw

- Terugblik & Introductie (klassikaal)
- Digitale veiligheid (klassikaal)
- Aan de slag! - online oefenopdrachten (individueel of in tweetallen)
- Jouw online veiligheid (klassikaal)
- Afsluiting (klassikaal), met eventueel Kennischek les 2 (individueel)

Duur

+/- 45 minuten

Leerdoelen

- De leerling kan uitleggen waar een sterk wachtwoord aan moet voldoen.
- De leerling kan zelfstandig onderzoek doen naar veelgebruikte wachtwoordmanagers en virusscanners.
- De leerling kan benoemen wat je kunt doen om de kans te verkleinen dat je wordt gehackt.
- De leerling kan uitleggen wat identiteitsfraude is.
- De leerling kan een inschatting maken van zijn eigen digitale veiligheid.

De les in stappen



Open de [digibordpresentatie](#) en introduceer de les. Vertel dat jullie vandaag aan de slag gaan met de tweede les van de module Digitale overheid en veiligheid: digitale veiligheid.



Vertel dat de les uit vijf delen bestaat.



Bespreek kort wat jullie in de vorige les hebben behandeld.
 Wat betekent de (digitale) overheid voor mij?
 Wat is DigiD?
 Hoe vraag ik DigiD aan?
 Welke (digitale) overheidszaken moet ik regelen?
 Waar kan ik terecht voor hulp bij (digitale) overheidszaken?



Vertel wat de leerlingen gaan leren in deze les.

Hoe maak ik een sterk wachtwoord?
 Hoe werkt een wachtwoordmanager?
 Wat is tweestapsverificatie?
 Wat kunnen de gevolgen zijn van online identiteitsfraude?
 Hoe zit het met mijn eigen online veiligheid?



Bespreek met de leerlingen waar zij aan denken bij digitale veiligheid. Maak eventueel een woordweb op het digibord.



Bekijk klassikaal de video van Veilig Internetten over het gebruik van veilige wachtwoorden.



Bespreek nu klassikaal:

Hoeveel verschillende wachtwoorden heb jij?
Wie heeft er een wachtwoordmanager?
Maak jij gebruik van tweestapsverificatie?

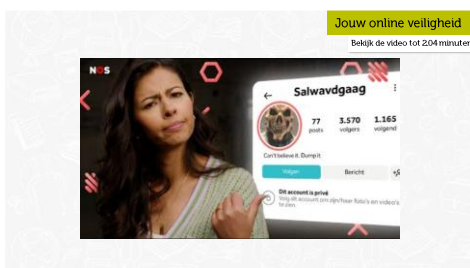


Vertel de leerlingen dat ze in het volgende onderdeel aan de slag gaan met online oefenopdrachten. Vraag de leerlingen om naar havovwo.doejedigiding.nl/digitaal-les2 te gaan. Ze hoeven niet in te loggen. Leerlingen gaan individueel of in tweetallen aan de slag met de online opdrachten. Loop tijdens dit onderdeel door de klas om eventuele vragen te beantwoorden.



Blik samen met de leerlingen terug op de online oefenopdrachten. Bespreek enkele vragen uit de online opdrachten. Bijvoorbeeld:

Hoe sterk zijn jouw wachtwoorden?
Ben jij wel eens gehackt?
Wat is identiteitsfraude?
Heb je een virusscanner?
Voer je alle updates altijd direct uit?



Bekijk klassikaal de video van NOS op 3. Hierin vertelt Salwa wat er gebeurde toen haar Instagram-account werd gehackt. Bekijk de video tot 2.04 minuten.

Jouw online veiligheid

Wat zou jij doen?

Je sociale media-account is gehackt en de hacker vraagt 300 euro om je account terug te krijgen.

doe je digiding!



Bespreek klassikaal het dilemma: Je socialmedia-account is gehackt en de hacker vraagt 300 euro om je account terug te krijgen.

Wat zouden de leerlingen doen?

Jouw online veiligheid

Doe de test

Hoe veilig is jouw digitale leven?



Vertel dat jullie een korte test gaan doen waarin je kunt testen hoe veilig jouw eigen digitale leven is. Vraag de leerlingen om bij iedere vraag hun antwoord (a, b, of c) te noteren.

Vraag 1

Jouw online veiligheid

Gebruik je unieke en sterke wachtwoorden (minimaal 12 tekens, met een combinatie van hoofdletters, kleine letters, cijfers en speciale tekens) voor al je accounts?

A) Altijd
B) Soms
C) Zelden of nooit

doe je digiding!



Gebruik je unieke en sterke wachtwoorden (minimaal 12 tekens, met een combinatie van hoofdletters, kleine letters, cijfers en speciale tekens) voor al je accounts?

Vraag 2

Jouw online veiligheid

Gebruik je tweestapsverificatie op je belangrijkste accounts?

A) Ja, op al mijn accounts waar dat kan
B) Alleen op sommige accounts
C) Nee

doe je digiding!



Gebruik je tweestapsverificatie op je belangrijkste accounts?

Vraag 3

Jouw online veiligheid

Hoe vaak update je software (zoals apps, besturingssystemen en antivirusprogramma's) op je apparaten?

A) Altijd direct als er een update beschikbaar is
B) Soms, als ik eraan denk
C) Bijna nooit

doe je digiding!



Hoe vaak update je software (zoals apps, besturingssystemen en antivirusprogramma's) op je apparaten?

Vraag 4

Jouw online veiligheid

Hoe vaak deel je een kopie van je identiteitsbewijs online of via e-mail?

A) Nooit, tenzij het echt noodzakelijk is. Ik gebruik dan een afgeschermd kopie met alleen relevante gegevens
B) Af en toe, zonder veel voorzorgsmaatregelen
C) Regelmatig, zonder erbij na te denken

doe je digiding!



Hoe vaak deel je een kopie van je identiteitsbewijs online of via e-mail?

Vraag 5 Jouw online veiligheid

Hoe ga je om met linkjes of bijlagen in e-mails?

- A) Ik controleer altijd eerst nauwkeurig de afzender voordat ik iets open
- B) Ik klik soms als het urgent lijkt
- C) Ik controleer niet en open meestal direct

doe je digiding!



Hoe ga je om met linkjes of bijlagen in e-mails?

Jouw score Jouw online veiligheid

Meeste A's: Veilig!
Je neemt je online veiligheid serieus. Blijf dit volhouden en houd je kennis up to-date

Meeste B's: Redelijk, maar met ruimte voor verbetering
Je doet een aantal dingen goed, maar er zijn verbeterpunten. Focus op het versterken van wachtwoorden, 2FA en regelmatige updates

Meeste C's: Risico's aanwezig
Je online veiligheid is kwetsbaar. Het is belangrijk om direct stappen te ondernemen. Zoals het gebruik van sterkere wachtwoorden, tweestapsverificatie en veilige omgang met persoonlijke gegevens.

doe je digiding!

Vraag de leerlingen naar hun score. Wie heeft de meeste C's? En wie de meeste B's? en wie de meeste A's?

Afsluiting

Test je kennis over digitale veiligheid

Kennisscheck

doe je digiding!



Iedere les kan worden afgesloten met een kant- en klare online kennisscheck, aangeboden via Microsoft Forms. Je kunt de kennisquiz dupliceren om vervolgens zelf met je leerlingen te delen en de resultaten van de klas achteraf te bekijken.

[Ga naar kennisscheck les 2 \(Digitale veiligheid\)](#)

Wat heb je geleerd? Afsluiting

- Hoe maak ik een sterk wachtwoord?
- Wat is tweestapsverificatie?
- Hoe zit het met mijn eigen online veiligheid?
- Hoe werkt een wachtwoordmanager?
- Wat kunnen de gevolgen zijn van online identiteitsfraude?

doe je digiding!

Bespreek kort wat jullie in deze les hebben geleerd:

Hoe maak ik een sterk wachtwoord?
Hoe werkt een wachtwoordmanager?
Wat is tweestapsverificatie?
Wat kunnen de gevolgen zijn van online identiteitsfraude?
Hoe zit het met mijn eigen online veiligheid?

Afsluiting

Fix je online veiligheid sneller dan deze pannenkoek!

WOENSDAG ONGEHACKT DAG



Bekijk klassikaal de video van Veilig Internetten. Op de website van veiliginternetten.nl vind je tips, trucs en praktische stapsgewijze uitleg om veilig online te gaan. Het platform behandelt o.a. onderwerpen zoals online privacy, veilig gebruik van wifi en sociale media. Ook vind je tools waarmee je kunt controleren of een website betrouwbaar is.



Sluit de les af.

Tip

Ken je de **kletskaarten** van Digidingen-desk al? Hiermee ga je aan de hand van vragen, stellingen en dilemma's met elkaar in gesprek over de digitale overheid. Gebruik de kletskaarten in de (mentor)les of geef ze mee aan ouders tijdens een ouderbijeenkomst.

Vraag de kletskaarten gratis aan via digidingen-desk.nl/kletskaarten

