# DigiVeiliger

Uitleg – Bordspel DigiVeiliger

## Introductie van het spel

Het DigiVeiliger-spel wordt ingezet tijdens de introductieles ‘DigiVeiliger – Kennismaking met online veiligheid’. In dit interactieve online bordspel maken deelnemers op een toegankelijke manier kennis met de vier thema’s die in de daaropvolgende workshops centraal staan: online bankieren, online communiceren, online winkelen en veilig en beschermd online.

Aan de hand van vragen, stellingen, korte filmpjes en kansvragen worden herkenbare situaties en dilemma’s rondom online veiligheid verkend. Het spel heeft als doel om voorkennis te activeren en eerste gesprekken over digitale veiligheid op gang te brengen. Door het spel klassikaal te spelen ontstaat direct betrokkenheid. Deelnemers denken actief mee, overleggen in teamverband en worden uitgedaagd om hun kennis en intuïtie te gebruiken. Het spel is daarmee een laagdrempelige manier om in te gaan op de verschillende onderwerpen.

## Opzet en doel

Het DigiVeiliger-spel wordt gespeeld via het digibord. Als docent vervul je de rol van spelleider, begeleid je het spelverloop en voer je de handelingen uit (zoals pionnen verplaatsen en vragen/antwoorden aanklikken). Verdeel de groep in maximaal vier teams. Elk team krijgt een vaste kleur: groen, geel, blauw of oranje. Het doel van het spel is om als eerste team de finish te bereiken.

Teams zetten hun pion één stap vooruit door vragen correct te beantwoorden. Een pion kan tijdens het spel nooit achteruit worden gezet.

## Benodigdheden en voorbereiding

- Digibord
- Internetverbinding
- Geluid

Voorafgaand aan de workshop is het belangrijk dat je het spel bekijkt om vertrouwd te raken met de werking. Bekijk ook de vragen om te zien wat je kunt verwachten. Verdeel vervolgens de groep deelnemers in maximaal vier teams. Wijs per team een kleur toe en laat teamleden bij elkaar zitten zodat zij gemakkelijk kunnen overleggen.

## Spelverloop

Op de overzichtspagina van het spel staan de pionnen van de verschillende teams. Aan de linkerkant van het scherm bevindt zich een vraagteken. Door hierop te klikken verschijnt een overzicht met genummerde opdrachten.

De teams zijn om de beurt aan de beurt. Het team dat speelt, kiest een nummer uit het overzicht. Wijs op de verschillende categorieën die er zijn: online bankieren, online communiceren, online winkelen, veilig en beschermd online en de kansvraag. Klik vervolgens op het gekozen nummer zodat er een vraag, stelling of filmpje in beeld verschijnt. Na het tonen van de opdracht krijgt het team kort de tijd om te overleggen, waarna zij hun antwoord geven. Klik vervolgens op het gekozen antwoord. Bij een correct antwoord wordt dit groen weergegeven. Je klikt dan op de pijl rechtsonder in beeld om terug te keren naar het overzicht en verplaats de pion van het betreffende team één stap vooruit door op de pion te klikken.

Wanneer een antwoord fout is, wordt dit rood weergegeven. De pion blijft dan op dezelfde plaats staan. In sommige gevallen verschijnt extra uitleg in beeld of mogen één of meerdere teams een stap vooruit zetten. Dit staat expliciet bij de opdracht vermeld. Het spel eindigt zodra een team de finish bereikt.

Nadat je de pion al dan niet een stap vooruit hebt gezet, is het volgende team aan de beurt. Zij mogen een getal kiezen. Getallen die al eerder gekozen zijn, worden automatisch grijs.

## Kansvragen

Bij bepaalde nummers verschijnt een kansvraag waarbij gebruik wordt gemaakt van een rad. Laat de deelnemers eerst overleggen over de vraag en laat ze een toelichting geven. Daarna start je het rad door op de groen/witte play-knop te klikken. Het team dat aan de beurt is zegt op een zelfgekozen moment “stop”. Je stopt het rad door op de rood/witte pauze-knop te klikken. Het getal waarop het rad eindigt bepaalt of het team 1 of 2 stappen vooruit mag zetten of dat het volgende team/speler 1 stap vooruit mag zetten.

## Filmpjes

Kom je op een getal waarbij een filmpje wordt getoond? Laat dan eerst het filmpje zien en bespreek dit eventueel kort na. Na afloop van het filmpje mag elk team zijn pion één stap vooruit zetten.

## Inhoudelijke begeleiding

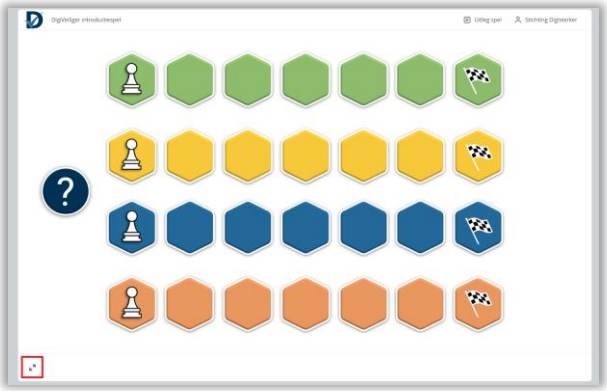
De vragen en stellingen in het spel zijn gekoppeld aan de vier thema’s van de komende workshops. Het is belangrijk dat je bij elk antwoord kort toelicht waarom dit het juiste antwoord is. Verderop in deze handleiding staat per vraag een toelichting.

Houd toelichtingen beknopt zodat het speltempo behouden blijft. Bij stellingen kan kort worden besproken waarom een uitspraak juist of onjuist is.

## Praktische aandachtspunten

Houd de uitleg van het spel kort en vraag of dit duidelijk is. Wanneer de teams overleggen, is het belangrijk de tijd goed in de gaten te houden. Laat discussies niet te lang voortduren en geef bij twijfel een korte toelichting voordat het spel wordt vervolgd.

Om het spel goed zichtbaar te maken op het digibord, is het handig om het scherm te vergroten. Zie het rood-omlijnde icoon in de afbeelding hiernaast.



Is het spel gestart en weet je de spelregels niet meer? Klik dan op ‘Uitleg spel’, zie het rood-omlijnde kader in de afbeelding hiernaast.

## Variaties

Afhankelijk van de groepsgrootte en de beschikbare tijd kan het spel worden aangepast. Bij kleinere groepen kan ervoor worden gekozen om met de hele groep te spelen, maar dan in kleinere teams of met minder teams. Zo kunnen bijvoorbeeld ook drie teams van twee deelnemers worden gemaakt. Als er weinig tijd is, kan worden afgesproken dat het eerste team dat vier stappen zet wint, in plaats van dat de finish moet worden bereikt. Een andere mogelijkheid is om na bijvoorbeeld 15 minuten te kijken welk team het verst op het speelbord staat.

**Vraag**

**1**

Iedereen kan je een betaalverzoek (of Tikkie) sturen. Dus ook bekenden, zoals een familielid of een vriend.
Krijg je een betaalverzoek van een onbekend nummer? Let dan wel goed op. Zeker als je het betaalverzoek niet verwacht of als er druk wordt uitgeoefend om snel te betalen.

**2**

Dit is een voorbeeld van bankhelpdeskfraude. Een bank zal nooit vragen om geld over te maken naar een 'veilige rekening', je pincode, inlogcodes of software installeren om 'mee te kijken'.
Twijfel je? Hang dan op en bel zelf het officiële nummer van je bank om te vragen of ze je net gebeld hebben.
De bank belt niet vaak, maar het kan voorkomen. Dit is vaak om je te waarschuwen. Bijvoorbeeld als er veel geld naar een verdachte rekening wordt overgemaakt.

**3**

Vriend-in-noodfraude (vaak WhatsApp-fraude of hulpvraagfraude) is een vorm van oplichting waarbij een oplichter zich voordoet als een bekende. De dader zegt in de problemen te zitten en vraagt dringend om geld. Ze gebruiken vaak een nieuw nummer en beweren dat hun oude telefoon is gestolen of stuk is.
Vertrouw je het niet? Bel dan altijd het oude nummer van de bekende. Betaal nooit zomaar het betaalverzoek.

**4**

Je hebt zelf de creditcard aangevraagd. Het is dan logisch dat je hier bericht over krijgt van de bank waar je dit hebt aangevraagd. Bovendien klopt de aanhef in de mail (je eigen naam staat weergegeven). Andere punten waar je op kunt letten: afzender (klopt het e-mailadres?), wordt er druk uitgeoefend, klopt de link?
Als je zelf geen creditcard hebt aangevraagd, dan is het wel een verdachte mail.

**5**

Een bank vraagt nooit om je pincode, inloggegevens of verificatiecodes.

**6**

Een 'kluisrekening' of 'veilige rekening' bestaat niet. Een bank vraagt nooit om geld over te boeken om het veilig te stellen. Banken kunnen wel jouw rekening blokkeren bij verdachte overboekingen. Hierover nemen ze dan contact met je op. Een bank zal nooit vragen zelf actie te ondernemen.

**7**

Je hebt zelf de instellingen van je betaalpas aangepast. In dat geval is het logisch dat de bank je een bevestiging stuurt. Dit kan een sms of e-mail zijn. Daarnaast is het een informatief bericht om je op de hoogte te brengen dat de instellingen zijn aangepast. Je wordt niet onder druk gezet om een handeling uit te voeren.

**Vraag**

**8**

Phishing-mails kunnen er heel professioneel uitzien en toch nep zijn. Een logo is eenvoudig te kopiëren en toe te voegen aan de mail. Oplichters proberen de vormgeving van de mails zo echt mogelijk te laten lijken.
Kijk naar: wie is de afzender, verwacht je het bericht, wordt er druk uitgeoefend, verwijst de link naar de officiële website?

**9**

Het is fijn om ook anderen op de hoogte te houden van verdachte berichten die je ontvangt. Door anderen te waarschuwen, help je voorkomen dat hij of zij slachtoffer wordt van oplichting.
Dit soort berichten kun je ook melden bij de Fraudehelpdesk.

**10**

Dit is een voorbeeld van vriend-in-nood-fraude (vaak WhatsApp-fraude of hulpvraagfraude). De oplichter doet zich voor als een bekende, gebruikt een nieuw telefoonnummer, vraagt om geld en stuurt een betaalverzoek/Tikkie.
Vertrouw je het niet? Bel dan altijd het oude nummer van de bekende. Betaal nooit zomaar het betaalverzoek.

**11**

Als een vriend wat heeft voorgeschoten, dan is het gebruikelijk dat hij later een betaalverzoek stuurt. Je krijgt het bericht van een bekend nummer en je verwacht dat je nog moet terugbetalen. Daarnaast kun je controleren of het bedrag klopt. Dus niet alle betaalverzoeken zijn verdacht.

**12**

Krijg je een mail? Controleer deze dan voordat je iets doet. Klik dus nooit zomaar op een link en vul ook niet je gegevens in.
Heb je dit wel gedaan en gaat het om geldzaken? Neem dan contact op met je bank. Wijzig ook je wachtwoord.

**13**

Vroeger was dit wel het geval, maar oplichters worden hier steeds beter in. Er staan vaak geen taalfouten meer in en de mail lijkt qua opmaak erg op een mail van de organisatie/bank. Let dus op andere zaken: de afzender, verwacht je het bericht?, wordt er druk uitgeoefend?, verwijst de link naar de officiële website?

**14**

Dit is een voorbeeld van een phishing-mail. Door aan te geven dat er maar een kleine voorraad is en je snel moet reageren, probeert de oplichter je onder druk te zetten om snel te handelen zonder na te denken. Oplichters voegen vaak een link toe van een nepwebsite waar je je gegevens moet invullen en moet betalen. Deze website kan er heel echt uitzien. Bovendien stuurt de overheid geen commerciële aanbiedingen.

**15**

Oplichters kunnen dit doen. Zo doen ze zich voor als een bekende. Je beschermt jezelf hiertegen door altijd terug te bellen naar het bekende nummer van diegene. Stel ook een controlevraag die alleen jullie weten.

**Vraag**

**16**

Dit is een filmpje van de website veiliginternetten.nl. Bekijk eerst samen het filmpje over oplichtingsmails. Vraag of er naar aanleiding van het filmpje nog vragen zijn.
Aangezien elk team wat heeft geleerd over oplichtingsmails, mag iedereen één stap vooruit zetten met zijn pion.

**17**

Nadat je een bestelling hebt geplaatst bij een webwinkel, is het logisch dat je een bevestigingsmail ontvangt. Als het bestelnummer hetzelfde is als in je account bij de webwinkel en het bedrag overeenkomt, dan is het een betrouwbare mail.
Webwinkels sturen bijna altijd een orderbevestiging, een factuur (als pdf) en een track & trace-link om je pakket te volgen.

**18**

Dit is een filmpje van RTL Z. Bekijk eerst samen het filmpje over online winkelen. Vraag of er naar aanleiding van het filmpje nog vragen zijn.
Aangezien elk team wat heeft geleerd over online winkelen, mag iedereen één stap vooruit zetten met zijn pion.

**19**

Nepwebwinkels hebben vaak grote kortingen. De prijzen zijn te mooi om waar te zijn. Soms zien de websites er ook professioneel uit, staan er professionele foto's bij de producten en nep-recensies.

**20**

Dit is een oplichtingstruc. Vaak vraagt de koper of jij 1 cent wilt overmaken. Dit is niet logisch. Op Marktplaats betaalt de koper de verkoper, niet andersom.
De link die de oplichter heeft gestuurd brengt je naar een nep-website. Alle gegevens die je hier invult, komen bij de oplichter terecht. Denk aan je bankrekeningnummer en inloggegevens.
In uitzonderlijke gevallen kan er gevraagd worden om 1 cent te pinnen. Bijvoorbeeld als je een telefoonabonnement afsluit en de koerier aan de deur staat met jouw nieuwe telefoon en abonnement. Maar dit wordt van tevoren goed gecommuniceerd door de provider.

**21**

Aangezien je niks besteld hebt, is dit bericht al vreemd. Daarnaast vragen pakketdiensten zelden via een algemene mail om direct te betalen via een link. Krijg je zo'n mail? Controleer dan altijd: wie is de afzender, verwacht je het bericht, wordt er druk uitgeoefend, verwijst de link naar de officiële website? Controleer ook op de officiële website van de pakketdienst de track & trace-code.

**22**

Aanbiedingen die te mooi zijn om waar te zijn, zijn al een eerste waarschuwingssignaal. Door beoordelingen te controleren, via bijvoorbeeld Trustpilot, kun je kijken of de webwinkel betrouwbaar is.

**Vraag**

**23**

Dit is een bekende oplichtingstruc. Als verkoper stuur je via Marktplaats een betaalverzoek. Zodra de koper deze betaald heeft, kun je het verzendlabel activeren. Je krijgt het verzendlabel in je mailbox. Dit regel je dus allemaal in de Marktplaats-omgeving. Een koper die jou een link stuurt voor een verzendlabel is ongebruikelijk.

**24**

Dat is verstandig om te doen. Let wel op de beoordelingen. Beoordelingen op de site van de webwinkel zelf kunnen nep zijn. Als er op internet alleen maar 5-sterren beoordelingen zijn, moet je ook kritisch zijn. Zeker als de beoordelingen in een kort tijdsbestek zijn geschreven. Controleer ook altijd de webwinkel zelf: welke contactgegevens zijn bekend? Hoe kun je betalen?

**25**

Iedereen kan slachtoffer worden. Oplichters proberen je onder tijdsdruk te zetten, je bang te maken, hebzucht aan te wakkeren enzovoorts. Het maakt niet uit hoe oud je bent, iedereen kan hierin trappen.
Krijg je een bericht? Neem dan altijd even de tijd. Voer niet zomaar een actie uit. En controleer het op officiële websites.

**26**

Het is belangrijk om sterke, veilige wachtwoorden te gebruiken. Als je wachtwoord te makkelijk is, dan kunnen oplichters het sneller raden. Probeer ook niet hetzelfde wachtwoord voor meerdere accounts te gebruiken. Als een oplichter je wachtwoord voor één account weet, kan hij dan bij veel meer accounts inloggen.

**27**

https betekent alleen dat er een veilige verbinding is tussen jouw apparaat en de website. Het zegt niets over of de website ook veilig is. Ook een hangslotje in de adresbalk geeft niet automatisch aan dat de website betrouwbaar is. Je moet altijd het webadres zelf controleren: ing.nl vs ing-controle.nl (1e wel veilig, 2e niet). Meer informatie over veilige links komt aan bod in de workshop Veilig en beschermd online.

**28**

Dit is verstandig om te doen. Als één website gehackt wordt, kan jouw wachtwoord niet op andere sites gebruikt worden. De schade blijft dan beperkt tot dat ene account.

**29**

Als je telefoon geen updates meer krijgt, betekent dit dat je geen beveiligingsupdates krijgt en ben je niet goed beschermd tegen malware. Dit is kwaadaardige software die wordt gebruikt om gegevens te stelen.
Overweeg dus om je toestel te vervangen als je al langere tijd geen updates meer krijgt.

**Vraag**

**30**

Dit is een filmpje over inloggen in twee stappen (tweestapsverificatie). Bekijk eerst samen het filmpje over inloggen in twee stappen. Vraag of er naar aanleiding van het filmpje nog vragen zijn.
Aangezien elk team wat heeft geleerd over tweestapsverificatie, mag iedereen één stap vooruit zetten met zijn pion.

**31**

De eerste link op Google is lang niet altijd een betrouwbare link. De eerste link kan ook een advertentie zijn. Bedrijven betalen om hun link zo hoog mogelijk in de zoekresultaten weer te geven. Verder wil de medewerker dat je software installeert om mee te kijken. Dit kan verdacht zijn. Zoek de contactgegevens op de officiële website van de organisatie. Dat is de meest veilige manier om contact op te nemen met het bedrijf.

**32**

Antivirussoftware helpt, maar beschermt je niet tegen alle virussen of vormen van oplichting. Het blokkeert bijvoorbeeld verdachte software en scant bestanden en downloads. Maar je bent niet beschermt tegen phishing-mails en onbekende virussen.

**33**

Eigen antwoord. Help deelnemers eventueel op weg met een aantal voorbeelden: zelf bankzaken online regelen, iets besteld via een webwinkel, bijlagen toevoegen aan een e-mail, de route zoeken via Google Maps, online een afspraak gemaakt met de huisarts, een wachtwoord veranderd naar een sterker wachtwoord, een app verwijderd.

**34**

Eigen antwoord. Voordelen van een landkaart: je bent niet afhankelijk van internet of een batterij van je telefoon. Voordelen Google Maps: je kunt direct zien of je de juiste kant op gaat, je kunt informatie krijgen over files, als je verkeerd rijdt krijg je direct een alternatieve route.

**35**

Eigen antwoord. Misschien staan er oude klassenfoto's op internet, bijvoorbeeld op de social-media pagina van je oude basis- of middelbare school, of oude foto's van het dorp waar je bent opgegroeid. Misschien ben je wel eens iets tegengekomen over tv-programma's van vroeger die nu niet meer op tv zijn of een speciaal sportfragment.

**36**

Eigen antwoord. Als je een dag geen internet hebt, zijn er genoeg andere hobby's, denk aan lezen of een wandeling maken. Een dag zonder internet kan dus best fijn zijn.
Het kan ook zijn dat je een dag zonder internet niet ziet zitten. Je hebt het bijvoorbeeld nodig om contact te houden met mensen die verder weg wonen.

**Vraag**

**37**

Eigen antwoord. Misschien wil je wel leren hoe je veilige wachtwoorden bedenkt, of waar je op moet letten om verdachte mails te onderscheppen. Misschien snap je een aantal instellingen van je telefoon niet en wil je dus je telefoon beter leren begrijpen. Of misschien wil je graag een serie kijken via Videoland of Netflix, maar weet je niet hoe.

**38**

Eigen antwoord. Je telefoon heb je meestal wel bij de hand. Je kunt snel een bericht sturen, iets opzoeken of een foto maken.
Een laptop heeft een groter scherm. Dan kun je het allemaal wat beter lezen/zien. Bovendien is het toetsenbord handig om te typen. En het is fijn dat je een laptop ook op andere plekken neer kunt zetten.
Een computer heeft een nog groter scherm. Een (draadloze) muis vinden sommigen ook fijner om te gebruiken.
Een tablet heeft een handig formaat om mee te nemen. Touchscreen kan ook handig zijn.
Misschien zeggen deelnemers wel dat het ook afhangt van wat ze willen doen. Filmpjes kijken ze wellicht liever op een tablet dan op een telefoon. Of zaken waarbij je veel moet lezen, dan is een groter scherm ook praktischer.