## 3 Veiligheid en privacy
## Subdoel 1: Hoe zorg je voor online veiligheid?

### Les 1: Scammers herkennen

**Leerdoel:** Studenten leren wat scams zijn en hoe ze deze kunnen herkennen.
**Doelgroep:** Studenten in gesloten instellingen met de nadruk op mbo-cluster drie en vier.

---

### Lesduur

**Totale tijd: 15 minuten**

- **Introductie: 5 minuten**
- **Herkennen van scams: 5 minuten**
- **Bespreking en tips: 5 minuten**

---

### Benodigdheden

- **Het juiste aantal geprinte hand-outs, afhankelijk van het formaat van de groep en of de studenten individueel of in groepjes te werk gaan.**
- **Genoeg potloden of pennen om de bijlagen in te vullen.**
- **Optioneel: een whiteboard waarop de docent mee kan schrijven tijdens het bedenken van manieren om iemand online op te lichten.**

---

### Les opbouw

**Introductie (5 minuten):** Bespreek het begrip 'scam' met de groep en vraag of iemand weleens te maken heeft gehad met een scam. Geef een definitie van scams: een poging om mensen op te lichten door middel van valse beloftes of dreigingen.

Vraag de groep welke manieren van scams ze kunnen bedenken en wat het doel van de scam zou kunnen zijn. Schrijf eventueel mee. Zorg er voor dat in ieder geval deze manieren en doelen worden benoemd:

DIGIPAD

- **Inloggegevens achterhalen**: met jouw gegevens kunnen ze zich als jou voordoen en via jou andere mensen oplichten. Ook kunnen ze je gegevens verkopen aan andere partijen. Ze kunnen informatie over jou verzamelen en dit gebruiken om een andere scam betrouwbaarder te laten lijken, bijvoorbeeld door zich voor te doen als een bank of een vriend in nood.
- **Directe betaling**: door het verkopen van niet bestaande producten of het vragen om een transactie. Bijvoorbeeld: dreigingen - "*als je niet binnen zoveel uur geld stort, lek ik je gegevens*", valse beloftes - "*je hebt geld gewonnen!*" of "*als ik het geld binnen heb, stuur ik de PlayStation 4 op*".
- **Het verkrijgen van bankgegevens:** door zich voor te doen als jouw bank en je te vragen in te loggen kunnen ze jouw geld op hun eigen rekening storten. Door jou een kleine betaling te laten doen kunnen ze toegang krijgen tot je account, bijvoorbeeld door zich voor te doen als een betaalverzoek van tikkie of van een bezorgservice ("*uw ups pakket is klaar voor verzending, we wachten nog op uw betaling van de verzendkosten..*").
- **Het laten downloaden van een virus:** als je een virus hebt gedownload kunnen ze alles zien dat er op je beeldscherm gebeurt en soms ook gebruik maken van je microfoon en webcam. Voorkom het downloaden van onbekende sites om de kans op een virus aanzienlijk te verlagen. Je kunt herkennen dat je een virus hebt doordat je apparaat plots veel langzamer wordt, verdachte pop-ups toont of je browser (Google, Safari..) er anders uitziet.

Het uiteindelijke doel is eigenlijk altijd **geld aftroggelen**. Scammers worden steeds lastiger te herkennen en zetten soms meerdere stappen om betrouwbaar te lijken.

**Activiteit (5 minuten):** Maak groepjes, laat groepjes maken of laat iedereen individueel werken. Deel de hand-out uit. Deze bevat een checklist die kan helpen bij het herkennen van scam, en het invulformulier voor de opdracht. Op Mediawise staat de bijlage met de zeven voorbeelden. De opdracht is om bij ieder voorbeeld een inschatting te maken of het **echt of een scam** is. Laat de studenten (in groepjes) bepalen of de berichten scam of echt zijn. Laat de studenten in steekwoorden opschrijven hoe ze tot die conclusie zijn gekomen. Gebruik hiervoor de checklist in de bijlage. Dit wordt in het laatste deel van de les besproken. *De juiste antwoorden zijn:*

- *1, scam (onpersoonlijke aanhef, urgentie en druk, verzoek om persoonlijke of financiële gegevens, geen komma na vriendelijke groet, vreemde afzender) -*
- *2, scam (begint met "hoi", onprofessionele afsluiting, vraagt om financiele gegevens, te mooi om waar te zijn) -*
- *3, scam (dreiging, onprofessioneel, vraagt om een transactie, urgentie en druk) -*
- *4, echt -*

- *5, scam (onpersoonlijke aanhef, vreemd mailadres, vraagt om buiten de beveiligde en officiële webomgeving persoonlijke gegevens in te vullen, verdachte linkjes) -*
- *6, echt -*
- *7, scam (fouten in de tekst zoals hoofdlettergebruik en onjuiste leestekens, spelfouten)*

**Bespreking (5 minuten):** Ga klassikaal de verschillende voorbeelden langs en vraag of studenten hun hand willen opsteken als ze denken dat er sprake is van oplichting. Benoem het juiste antwoord en waar ze dat aan kunnen zien. Geef de tip om bij twijfel op te zoeken hoe een officieel bericht eruit ziet (google bijvoorbeeld: "hoe ziet een echte veiligheidswaarschuwing van Facebook er uit"), contact op te nemen met de klantenservice (niet via de verdachte melding, maar via een site waarvan je weet dat het de echte is), of veiligheidsmaatregelen te nemen zoals het veranderen van je wachtwoord via de vertrouwde site. Als je er niet uitkomt kun je altijd de hulp inschakelen van **gratis ict hulp vanuit een bibliotheek in de buurt** of kun je contact opnemen met de politie. Veel van deze scams zijn strafbaar, de politie kan passende maatregelen nemen.

## Tips voor de docent

- **Controleer de bijbehorende bijlage op Mediawise. Bijlage 3.1.1-1 en 3.1.1-2**
- **Er zijn meer voorbeelden in de opdracht dan waarschijnlijk haalbaar is in de tijd. Kijk hoe ver de studenten komen en zorg voor voldoende tijd om de antwoorden te bespreken. Bespreek in ieder geval de eerste drie voorbeelden.**

---

## Bijlagen

- Zie de bijlage met zeven voorbeelden op Mediawise. **Bijlage 3.1.1-1**
- Zie de bijlage "**Bijlage 3.1.1-2**" (Scam or Safe checklist)

DIGIPAD