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

Les 2: Pincodes en Wachtwoorden

Leerdoel: Na deze les kunnen leerlingen het belang uitleggen van veilige pincodes en wachtwoorden en weten ze hoe ze sterke, veilige wachtwoorden kunnen maken en onthouden.
Doelgroep: Studenten in gesloten instellingen met de nadruk op mbo-cluster drie en vier.

Lesduur

Totale tijd: 15 minuten

- **Introductie**: 3 minuten
- **Wachtwoordtest**: 6 minuten
- **Bespreking en tips**: 6 minuten

Benodigdheden

- Computer met toegang tot Mediawise per leerling of per tweetal.

Voorbereiding

1. Zorg ervoor dat de leerlingen via Mediawise website kunnen bezoeken waar ze kunnen testen hoe lang het duurt om een wachtwoord te kraken. Controleer of de website veilig en toegankelijk is (zie de bijbehorende site binnen Mediawise, of navigeer naar het eind van het lesplan voor de link).
2. Voorzie enkele voorbeelden van wachtwoorden (zie **Activiteit** voor suggesties).

Lesopbouw

Introductie (3 minuten)

DIGIPAD

1. **Begin de les** door aan de leerlingen te vragen of ze een idee hebben waarom het belangrijk is om een sterk wachtwoord te gebruiken.
2. **Leg uit** dat eenvoudige wachtwoorden zoals "1234" of "wachtwoord" makkelijk te raden zijn door hackers, en dat ze dan toegang kunnen krijgen tot persoonlijke informatie.
3. **Voorbeeld geven**: Noem simpele wachtwoorden en leg uit dat deze snel door computers gekraakt kunnen worden.
4. **Doel uitleggen**: Vertel de leerlingen dat ze vandaag gaan leren hoe ze sterke, veilige wachtwoorden en pincodes kunnen maken die moeilijk te raden of te kraken zijn.
5. **Site openen:** Laat iedereen de site openen. Benadruk dat het niet veilig is om echte of bestaande wachtwoorden in te voeren op de site.

Activiteit: Wachtwoordtest (6 minuten)

1. **Toegang tot de website**: Vraag de leerlingen om enkele voorbeelden van wachtwoorden op de website in te voeren om te zien hoe lang het zou duren om deze te kraken.
2. **Voorbeelden**:
    - **Simpel wachtwoord**: "1234" of "wachtwoord" – deze worden vaak binnen enkele seconden gekraakt.
    - **Gemiddeld wachtwoord**: "Wachtwoord2023" – iets moeilijker te raden maar nog steeds niet veilig genoeg.
    - **Sterk wachtwoord**: "9&gT#2a*Zp!" – door de combinatie van cijfers, hoofdletters, speciale tekens en lengte is dit veel moeilijker te kraken.
3. **Laat leerlingen observeren**: Vraag hen te letten op wat het effect is van het toevoegen van cijfers, hoofdletters, speciale tekens, en de lengte van het wachtwoord.
4. **Notities maken**: Moedig de leerlingen aan om op te schrijven wat hen opvalt tijdens deze test.

Bespreking en Tips (6 minuten)

1. **Bespreken van bevindingen**: Vraag de leerlingen wat ze hebben opgemerkt. Waarom werden sommige wachtwoorden sneller gekraakt dan andere?
2. **Uitleg over sterke wachtwoorden**:
    - Leg uit dat wachtwoorden veiliger worden als ze bestaan uit een combinatie van:
        - Hoofdletters en kleine letters
        - Cijfers
        - Speciale tekens (zoals !, @, #, of %)
        - Minimaal 8 karakters (hoe langer, hoe beter)
3. **Geheugensteuntje: wachtwoordzin**:

- Stel een wachtwoordzin voor als makkelijk te onthouden en sterk: zoals “DeZonSchijnt2!” of “IkHouVanPizza$!”
- Bespreek dat het gebruik van een zin het makkelijker maakt om een veilig wachtwoord te onthouden, vooral als het iets persoonlijks is.

4. **Opgeslagen wachtwoorden beheren**:
   - Bespreek dat het slim kan zijn om wachtwoorden niet overal hetzelfde te maken.
   - Noem ook dat er veilige plekken zijn om wachtwoorden op te slaan, zoals wachtwoordmanagers (leg simpel uit wat dit is).
5. **Vergeten wachtwoorden opvragen:**
   - Bespreek dat bij het vergeten van een wachtwoord er vaak een nieuw wachtwoord kan worden aangemaakt via een mail naar het gekoppelde e-mailadres. Leg uit dat het belangrijk is dat je altijd toegang hebt tot dit mailadres, er zijn stappen die je kunt zetten zoals het opgeven van een telefoonnummer of tweede mailadres.
6. **In het geval van een veiligheidsmelding:**
   - Vertel kort welke stappen je kunt ondernemen als je een veiligheidsmelding ontvangt: "pas op! Uw account is gehackt!”. Check eerst of het geen scam is (Domein A, kerndoel 3, subdoel 1, les 1), verander vervolgens het wachtwoord. Controleer of je hetzelfde wachtwoord op andere plekken hebt gebruikt, als dat zo is, verander dan ook deze wachtwoorden.

Tips voor de docent

- Moedig leerlingen aan om geen echte wachtwoorden die ze nu gebruiken te testen, maar juist fictieve wachtwoorden die voldoen aan de kenmerken van veilige wachtwoorden.
- Voor jongere kinderen kun je ook eenvoudige wachtwoordzinnen voorstellen, zoals “MijnHond8#!” – iets wat persoonlijk is, maar veilig door de combinatie van hoofdletters, kleine letters, cijfers, en een speciaal teken.

Optioneel: Vraag aan het einde van de les een paar leerlingen om een sterk wachtwoord op te schrijven (fictief, niet hun echte wachtwoord) en bespreek deze klassikaal.

Bijlagen:

- **Tips voor Sterke Wachtwoorden:**

- Gebruik een combinatie van hoofdletters, kleine letters, cijfers en speciale tekens.

DIGIPAD

- Kies een wachtwoord dat minimaal 8 tekens heeft.
- Vermijd voorspelbare woorden zoals "wachtwoord" of "1234".
- Maak een zin als wachtwoord: dit is makkelijker te onthouden en kan net zo veilig zijn.
- Gebruik voor elk account een uniek wachtwoord.

- **Benodigde Website:** Wachtwoordkraak-test van Veiliginternetten.nl

DIGIPAD