
ICT & Web

MBO Verkorte opleiding Informatiebeveiliging

Kennismakingsopdracht



Kijk voor actuele startmomenten op
www.capabel.nl/opleidingen

Kennismakingsopdracht

Informatiebeveiliger

Introductie

Een Informatiebeveiliger heeft brede kennis en vaardigheden om digitale veiligheid te waarborgen. Je onderzoekt dreigingen, voert risicoanalyses uit en implementeert beveiligingsmaatregelen zoals firewalls, encryptie en toegangscontrole. Je leert werken met security basics, cloud security, risk management en ethisch hacken. Ook verdiep je je in wetgeving zoals AVG en cybersecuritynormen. Je leert realistische beveiligingsdoelen stellen, een risicoprofiel opstellen en omgaan met tijdsdruk bij incidenten.

Het vakgebied van informatiebeveiliging is veel in beweging vanwege nieuwe ontwikkelingen in de hele wereld. Er is daarom ook veel foutieve informatie te vinden op het internet. Tijdens je opleiding besteed je veel aandacht aan analyseren, rapporteren en het opstellen van verbetervoorstellen om digitale omgevingen veiliger te maken.

Wat ga ik doen?

- Lees eerst opdracht 1: 'Mail van de directeur'.
- Vul je antwoorden in op het invulblad.
- Maak opdracht 2 en vul je antwoorden in op het invulblad.
- Controleer je antwoorden met het antwoordblad en lees de afsluiting.

Opdracht 1: Mail van de directeur

Lees de onderstaande casus. Beantwoord daarna de vragen op het invulblad.

Je werkt als Informatiebeveiliger bij een zorginstelling met 23 medewerkers. Een collega van de administratie krijgt een e-mail van "de directeur" met een betaalverzoek. De directeur vraagt in de mail om € 5.000 over te maken naar een onbekend rekeningnummer, vanwege een dringende factuur. Over twee dagen heeft een patiënt een operatie, waarvoor dure materialen nodig zijn. De operatie is volgens de directeur erg complex. Als de factuur niet wordt betaald, kan de operatie niet doorgaan. De directeur sluit de mail af met naam en handtekening.

De collega twijfelt en belt jou voor advies. Wat zou jij in deze situatie doen? Wat zou jij je collega adviseren en waarom? Beantwoord de vragen op het invulblad.

Opdracht 2: Beveiliging van informatie

De zorginstelling uit opdracht 1 heeft veel gegevens van patiënten. Deze worden op een veilige locatie bewaard. Toch denkt jij dat de informatiebeveiliging beter kan.

Bekijk de 7 zeven tips voor informatiebeveiliging in de bijlage. Jij wil deze tips inzetten in de zorginstelling van opdracht 1. Controleer eerst of de informatie betrouwbaar is. Welke tips moet je aanpassen? Beantwoord de vragen op het invulblad.

Invulblad opdracht 1

Beantwoord de volgende vragen:

Vraag	Antwoord
Wat zou jij in deze situatie doen?	
Wat zou jij je collega adviseren en waarom?	
Wat zou er fout kunnen gaan als je niet goed oplet?	
Waarom is het belangrijk dat mensen in de organisatie jou als Informatiebeveiligers altijd kunnen bereiken?	

Invulblad opdracht 2

Beantwoord de volgende vragen:

Vraag	Antwoord
Vindt je de tips betrouwbaar? Waarom wel of niet?	
Wat zijn 3 aanpasvoorstellen voor de tips?	
Welke tips wil je zelf toevoegen?	
Welke tips geef je aan de collega's van de zorginstelling?	

Afsluiting

Ben je klaar met de opdrachten? Denk dan na over de volgende vragen:

- Wat spreekt je vooral aan in de opleiding?
- Welke vragen heb je nog over de opleiding?
- Wat wil je nog vragen aan de voorlichters?

Ben je geïnteresseerd in de opdracht van een andere opleiding?

Ga dan naar www.capabel.nl/beroepsopdrachten-voorlichtingen



We kunnen je wel vertellen hoe de lessen van Capabel eruitzien, maar als je werkelijk wilt ervaren hoe het is om bij ons te studeren, nodigen we je uit voor een vrijblijvende meelooples. Je volgt dan een echte les in een klas met studenten, die jou graag vertellen waarom ze voor Capabel hebben gekozen. Lijkt je dat wat? Geef je dan op voor een meelooples door je naam op de lijst te zetten, of door ons te bellen (088-2701270) of te mailen (info@capabel.nl).

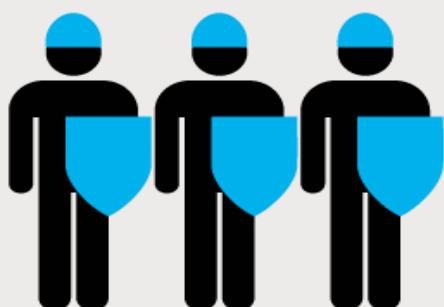


Bijlage

INFORMATIEBEVEILIGING

7 praktische tips

Met deze zeven praktische tips kunt u als zorginstelling of praktijk uw informatiebeveiliging verbeteren. Sommige tips lijken voor de hand liggend. De praktijk wijst echter uit dat de informatiebeveiliging juist op deze praktische punten nog wel eens beter kan. Dit blijkt uit een inventarisatie over informatiebeveiliging bij 40 apotheken en 36 huisartsenpraktijken. We hebben onze bevindingen in deze tips 'versleuteld'.



1. STIMULEER BEVEILIGINGS-BEWUSTZIJN BIJ MEDEWERKERS

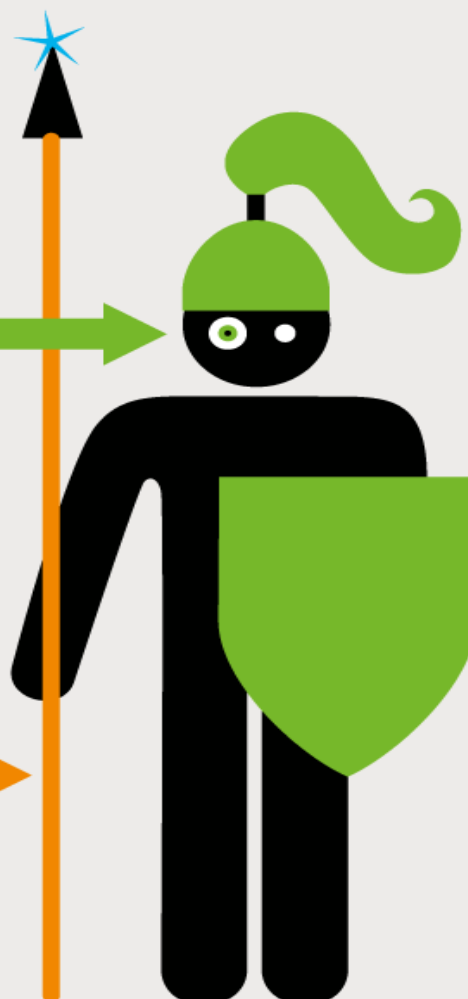
- Geef het goede voorbeeld aan collega's door zelf beveiligingsbewust te werken.
- Zorg voor duidelijke en werkbare instructies voor het veilig werken met digitale informatie.
- Creëer een werksfeer waarbij medewerkers elkaar stimuleren veilig om te gaan met patiëntgevoelige informatie en elkaar indien nodig kunnen aanspreken.

2. CONTROLEER REGELMATIG OP VERDACHT INZAGE IN PATIËTENGEGEVENS

- Controleer regelmatig (bij voorkeur dagelijks, maar minimaal wekelijks) de logbestanden op verdachte inzage in patiëntgegevens.
- Informeer uw omgeving dat u de logbestanden controleert.
- Raadpleeg uw ICT-leverancier indien niet duidelijk is hoe u de logbestanden kunt bekijken.

3. BESCHERM PC'S TEGEN COMPUTERVIRUSSEN

- Zorg dat iedere pc is voorzien van een actuele virusscanner.
- Zorg dat de virusscanner up-to-date is.
- Wees voorzichtig met het openen van bijlagen in e-mails.
- Installeer geen programma's van onbekende herkomst.





Antwoordblad opdracht 1

Meerdere antwoorden zijn goed. Hier staat een voorbeeld van een antwoord:

Vraag	Antwoord
Wat zou jij in deze situatie doen?	Ik zou zelf contact opnemen met de directeur over deze mail. Ook zou ik bij andere collega's navragen of zij een mail hebben gehad die ze verdacht vinden.
Wat zou jij je collega adviseren en waarom?	Ik zou adviseren om het mailadres en het rekeningnummer goed na te lopen. Ook zou ik vragen of de directeur vaker op deze manier een betaalverzoek doorstuurt. Zo
Wat zou er fout kunnen gaan als je niet goed oplet?	Als je niet goed oplet kun je geld overmaken naar een onbekende of patiëntgegevens uitlekken.
Waarom is het belangrijk dat mensen in de organisatie jou als Informatiebeveiligers altijd kunnen bereiken?	Als mensen je niet makkelijk kunnen bereiken, nemen ze misschien zelf een besluit om toch te reageren op een verdacht bericht en bijvoorbeeld geld over te maken.

1.1.1.1 Antwoordblad opdracht 2

Meerdere antwoorden zijn goed. Hier staat een voorbeeld van een antwoord:

Vraag	Antwoord
Vindt je de tips betrouwbaar? Waarom wel of niet?	De tips zien er betrouwbaar uit en zorgen voor extra beveiliging. Ook staat in de tips dat je zelf waakzaam moet zijn op wat er met de patiëntgegevens gebeurt. Het zou verdacht zijn als je volgens de tips geen regelmatige controle hoeft te doen.
Wat zijn 3 aanpasvoorstellen voor de tips?	1: De tips zijn geschreven voor een informatiebeveiligers, maar het is onduidelijk wat andere werknemers moeten doen. 2: Er wordt niet genoemd wat het effect van elke tip is. Je weet niet waarom je de tips moet uitvoeren. 3: Geef aan waarom patiëntgegevens goed beveiligd moeten worden.
Welke tips wil je zelf toevoegen?	1: Bewaar wachtwoorden op een veilige plek. 2: Collega's moeten altijd bereiken bij vragen. 3: Maak geen gebruik van verdachte netwerken.
Welke tips geef je aan de collega's van de zorginstelling?	Onder andere: De collega's moeten zelf controleren of de patiëntgegevens goed zijn beveiligd. Verdachte situaties moeten ze melden bij de informatiebeveiligers. Patiëntgegevens zijn erg gevoelige informatie, dus ga er over het algemeen erg zorgvuldig mee om. Zet niet alle gegevens van een patiënt zomaar in een mail of berichtje naar iemand anders.