

Windesheim

# Spion op je pad

Uitbreiding vragenset met antwoorden - Spelleider



Versie: 2024-04-18

Auteur: M. de Blaeij (Min EZ), IBD, Anita Polderdijk (am.polderdijk-rijntjes@windesheim.nl)

Licentie: 

## Spelvragen en antwoorden 'Spion op je Pad'

---

De spelleider kan ervoor kiezen om de vragen in een vaste volgorde aan te bieden. In dat geval kan gewerkt worden met een Powerpoint bestand waarin de vragen opvolgorde op groot scherm getoond kunnen worden. Er kan ook worden gekozen om gebruik te maken van de vraagkaartjes, bijgeleverd in een apart bestand om af te drukken. Door de kaarten te schudden is de volgorde niet van te voren bepaald.

### Vraag 1

Je wilt gebruik maken van internet in de trein. Hoe doe je dat?

- a) Je zit zo vaak in de trein. Je mobiel selecteert standaard de Wifi van NS.
- b) Je maakt gebruik van je mobiele netwerk op je telefoon (hotspot).
- c) Je maakt geen gebruik van de NS wifi, je gebruikt de openbare Wifi beveiligd met een wachtwoord in de Starbucks als je aankomt op het station.

### Antwoord 1

- a) Omdat je direct internetverbinding hebt: **snelheid +1**. Helaas heb je verbinding gemaakt met een vals netwerk en ingelogd op je bankrekening, waardoor een hacker nu je inloggegevens bezit: **spion stap vooruit**.
- b) Dit is een voldoende veilige verbinding tussen je mobiel en het internet, waardoor anderen verkeer niet kunnen lezen. Inbreken op dit netwerk is een stuk moeilijker dan op een Wifi netwerk: **informatiebeveiliging +1 en kwaliteit +1**.
- c) De Wifi van NS is zeer traag; een ander netwerk is sneller: **kwaliteit +1**, maar helaas is ook een openbaar netwerk met wachtwoord niet veilig. Authenticatie is namelijk niet hetzelfde als encryptie. Alle gegevens worden onbeschermd over het netwerk verstuurd: **Actieve speler 1 stap vooruit**.

### Vraag 2

Je vindt een USB stick bij de ingang van het hoofdgebouw. Wat doe je?

- a) Je kijkt wat er op staat via je werk-PC om de eigenaar te achterhalen.
- b) Je geeft de USB stick direct af bij de ICT Servicedesk.
- c) Je gooit de USB stick weg.

### Antwoord 2

- a) Terwijl je op je beeldscherm kijkt naar de inhoud worden al je eigen bestanden versleuteld door een Cryptolocker/ransomware: **spion stap vooruit**. Het is wel een snelle manier: **snelheid +1**
- b) Dit is de meest veilige en efficiënte oplossing. Omdat je de informatie op de USB stick niet te zien krijgt is er geen datalek en je weet nooit of een vreemde USB stick bijvoorbeeld besmet is met een virus: **informatiebeveiliging +1, kwaliteit +1 en snelheid +1**
- c) De USB stick wordt in het afval gevonden door de spion: **actieve speler stap vooruit**. De eigenaar zoekt zich rot naar zijn USB stick met vertrouwelijke bestanden: **kwaliteit -1**.

**Vraag 3**

Je ontvangt een e-mail met in het onderwerp het woord: "VERTROUWELIJK" Wat doe je?

- a) E-mail lezen en direct verwijderen.
- b) E-mail lezen, daarna opslaan als beveiligde PDF op je Onedrive en tot slot verwijderen uit je inbox.
- a) E-mail printen, opslaan in een papieren dossier en verwijderen uit je mailbox.

**Antwoord 3**

- a) Omdat je de e-mail direct verwijdert kan niemand het meer zien; **snellheid +1**, maar jijzelf een half jaar later ook niet meer: **kwaliteit -1**.
- b) Omdat je de mail uit je mailbox verwijdert en onder de juiste condities opslaat gaat de: **informatiebeveiliging +1**. Helaas vergt dit nogal wat handelingen: **snellheid -1**.
- c) Omdat je de mail hebt verwijderd uit je mailbox en dus niemand het meer kan zien: **informatiebeveiliging +1** Het proces van uitprinten en aanmaken papieren dossier kost tijd: **snellheid -1**. Als je een half jaar later de mail weer wilt inzien kost dat veel gedoe om het dossier en de betreffende mail te vinden: **kwaliteit -1**.

**Vraag 4**

Je collega belt je in de trein. Zij heeft een dringende vraag over een gevoelig dossier. Wat doe je?

- a) Het gesprek voeren.
- b) Het gesprek afhandelen via Whatsapp.
- c) Terugbellen als je thuis bent.

**Antwoord 4**

- a) Je collega is blij dat je hem zo snel hebt kunnen antwoorden: **snellheid +1**. Helaas luisterde er iemand mee in de treincoupe: **spion stap vooruit**.
- b) Je collega is niet blij met jouw reactie via Whatsapp, dat overlegt minder makkelijk: **kwaliteit -1**.
- c) Je collega is woest want nu moet hij vanavond overwerken: **snellheid -1**, gelukkig heeft niemand het gesprek kunnen afluisteren, je zat immers thuis: **informatiebeveiliging +1**.

**Vraag 5**

Je moet vanavond thuis een concept memo schrijven met gevoelige gegevens. Hoe doe je dat?

- a) Je logt thuis in op Microsoft Office365 omgeving van de instelling.
- b) Je maakt het concept op je eigen computer en mailt het via je privémail naar je werkmail.
- c) Je werkt het op kantoor uit, niet thuis.

**Antwoord 5**

- a) Dit is de snelste manier: **snellheid +1** en de meest veilige manier van thuiswerken is via de O365 omgeving van de instelling. **actieve speler 1 stap achteruit**.
- b) Dit is niet de snelste manier: **snellheid -1**. Je privé mail wordt gehackt vanuit het buitenland, al je mailtjes inclusief deze met de memo worden gepubliceerd op WikiLeaks: **actieve speler 1 stap vooruit**.
- c) Je kan niet zo laat overwerken op kantoor want het pand gaat dicht, dus je kan er morgen pas weer mee verder **snellheid -1**. Op kantoor werk je altijd in een veilige omgeving: **informatiebeveiliging +1**.

**Vraag 6**

Je verliest je USB stick met vertrouwelijke documenten op het station. Wat doe je als eerste?

- a) Je doet aangifte bij politie.
- b) Je zoekt eerst nog een keer alles af en spreekt met jezelf af nooit meer met usb sticks te werken.
- c) Je belt je manager.

**Antwoord 6**

- a) Het doen van aangifte bij de politie duurt best lang, je werk loopt hierdoor vertraging op: **snelheid -1**. Ondertussen vindt de spion jouw USB stick op het station: **actieve speler stap vooruit**.
- b) Het zoeken duurt uren: **snelheid -1**. Je vindt je USB stick wel weer terug: **informatiebeveiliging +1**.
- c) Je manager is boos en laat jou nooit meer aan dit soort documenten werken: **kwaliteit -1**. Ondertussen vindt de spion jouw USB stick: **spion stap vooruit**.

**Vraag 7**

Je collega vraagt met je samen te werken aan een notitie met gevoelige gegevens. Hoe gaan jullie dit doen?

- a) Via e-mail stemmen jullie af.
- b) Het document delen jullie via dropbox.
- c) Het document delen jullie via een gedeelde beveiligde werkmap in Teams.

**Antwoord 7**

- a) Via de mail documenten uitwisselen, dat snapt iedereen. We hoeven dat niet aan elkaar uit te leggen: **snelheid +1**. Helaas wordt na een paar keer heen en weer mailen de verkeerde persoon van buiten de organisatie in de cc. gezet. Hij vindt de concept notitie wel erg interessant en verkoopt het aan RTL nieuws: **spion stap vooruit**.
- b) We zijn heel hippe collega's en vinden het fijn om via dropbox veilig met elkaar samen te werken: **snelheid +1**. Helaas voldoet dropbox niet aan de eisen voor informatiebeveiliging, dat wist jij niet. Het wordt gehackt en jullie notitie ligt op straat: **actieve speler stap vooruit**.
- c) Documenten opslaan en delen via ShareNet/SharePoint waarbij aandacht is voor autorisaties, is een veilige oplossing: **informatiebeveiliging +1**. Helaas is het opslaan van documenten en het toevoegen van beveiliging nogal bewerkelijk: **snelheid -1**.

**Vraag 8**

Op de printer vind je een vertrouwelijk document. Wat doe je?

- a) Het printje gooi je direct in papiervernietiging container.
- b) Het printje bewaar je om je collega te confronteren.
- c) Je levert het printje in bij de manager.

**Antwoord 8**

- a) Documenten in de papiercontainer worden altijd zodanig vernietigd dat ze niet meer te lezen zijn: **informatiebeveiliging +1**. Helaas, je collega had haast en moest het document nu weer opnieuw printen: **snelheid -1**.
- b) Het printje blijft uren lang op je bureau liggen, iedereen kan het zien: **informatiebeveiliging -1**. Het document wordt ook door die externe bezoeker die net langs loopt gezien en meegenomen: **spion stap vooruit**.
- c) Je manager is erg blij met jouw melding: **kwaliteit +1**. Je collega voelt zich verraden en snuffelt in jouw documenten naar vertrouwelijke stukken: **actieve speler 1 stap vooruit**.

**Vraag 9**

Je hebt een mail ontvangen van de Wehkamp over een openstaande rekening, toegevoegd in de bijlage.

- a) Je checkt eerst de afzender op Fraudehelpdesk.nl.
- b) Je opent de bijlage, want je wil snel betalen. De herinneringskosten lopen snel op!
- c) Je forward de mail naar je collega van de ICT Servicedesk.

**Antwoord 9**

- a) Goed! Op Fraudehelpdesk.nl kun je controleren welke phishingmails in omloop zijn: **actieve speler 1 stap achteruit**.
- b) Helaas. Je hebt de bijlage van een phishing mail geopend: **actieve speler 1 stap vooruit**.
- c) Je collega van de ICT Servicedesk meldt dit bij de afdeling infrastructuur en plaatst een waarschuwingsbericht op het intranet over de ransomware die in omloop is via deze phishing mail: **informatiebeveiliging +1 en snelheid +1**.

**Vraag 10**

Je ontvangt een e-mail van je bank om je inloggegevens te bevestigen via de link in die mail. Wat doe je?

- a) Mail direct verwijderen, ook uit je verwijderde items map.
- b) Je afvragen wat dit is en doorsturen naar collega.
- c) De mail doorsturen naar de ICT Servicedesk om aan te merken als spam.

**Antwoord 10**

- a) Snel druk je op "delete" en verwijder je de mail uit je *deleted items*, snel weer door met je werk: **snelheid +1**. Helaas kan de ICT Servicedesk de afzender niet blokkeren voor je collega's: **spion stap vooruit**.
- b) Je collega begint direct het TV spotje "*hang op, klik weg, bel uw bank*" te roepen: **kwaliteit +1**. Helaas is het e-mailadres van je collega nu ook bekend bij de afzender: **actieve speler 1 stap vooruit**.
- c) De ICT Servicedesk bedankt je voor deze actie en sluit de afzender uit om berichten naar je collega's te sturen: **informatiebeveiliging +1**.

**Vraag 11**

Je collega heeft zijn scherm niet op “lockscreen” staan. Wat doe je?

- a) Alsnog op lockscreen zetten.
- b) Een e-mail vanaf zijn/haar PC rondsturen met uitnodiging voor gebak.
- c) Je geeft het aan bij je manager. Het is al de 100<sup>e</sup> keer.

**Antwoord 11**

- a) Dat is collegiaal en een snelle oplossing: **snelheid +1** maar of je collega hier de volgende keer zelf aan denkt is de vraag: **informatiebeveiliging -1**.
- b) Je collega kan er wel om lachen en neemt de dag erna gebak mee: **kwaliteit +1** Dit zal hij/zij niet snel vergeten: **informatiebeveiliging +1**.
- c) Je manager is blij met de melding van dit veiligheidsincident en spreekt je collega hierop aan: **kwaliteit +1**. Je collega voelt zich door jou verraden en is zo boos dat hij een vertrouwelijk mailtje stuurt naar de Telegraaf de volgende keer dat jij je scherm niet gelockt hebt. De spion leest de Telegraaf: **spion stap vooruit**.

**Vraag 12**

Hoe zet je eigenlijk je computer op lockscreen?

- a) Windows + L
- b) Ctrl+Alt+Del + Enter
- c) Monitor uitklikken

**Antwoorden 12**

- a) Ja juist: **actieve speler stap achteruit**.
- b) Ja juist: **actieve speler stap achteruit**.
- c) Nee fout, antwoord a of b is juist: **alle spelers 1 stap richting spion**.

**Vraag 13**

Bij het aantreden van de nieuwe directeur vraagt de manager Bedrijfsvoering jou om een feitenrelaas te geven over een kritisch dossier. Wat neem je allemaal mee?

- a) Je beschrijft alles, ook de veiligheids-incidenten.
- b) Je beperkt je tot de inhoud van het dossier.
- c) Je stemt af met de manager Bedrijfsvoering wat wel en wat niet.

**Antwoord 13**

- a) Het is belangrijk dat ook de bestuurders op de hoogte zijn van mogelijke risico's van het lekken van informatie. Heel goed: **actieve speler 1 stap achteruit**.
- b) Het feitenrelaas blijft kort en krachtig: **snelheid +1**. Helaas komt de directeur er bij een deelraadvergadering achter dat de deelraad meer weet over het dossier dan hij van te voren had gedacht: **kwaliteit -1**.
- c) Het feitenrelaas geeft een goede weergave van alle handelingen op het dossier inclusief mogelijke risico's: **informatiebeveiliging +1**.

**Vraag 14**

Je moet in Topdesk (incidentmanagement systeem) wat opzoeken en ziet ineens de naam van die leuke collega in het scherm. Wat doe je?

- a) Even kijken wat ze vraagt en of je haar misschien kan helpen.
- b) Je gaat verder met je eigen werk en raadpleegt alleen gegevens die je nodig hebt.
- c) Je loopt naar de collega die de zaak in behandeling heeft en zegt terloops dat je ziet dat hij met jouw leuke collega bezig is in de hoop dat hij wat loslaat.

**Antwoorden 14**

- a) Die leuke collega is blij met de snelle dienstverlening: **kwaliteit en snelheid +1**. Je hebt echter wel je professionele integriteit geschonden: **spion stap vooruit**.
- b) Je bent integer en schendt niet de privacy van je buurvrouw: **kwaliteit +1** en **informatiebeveiliging +1**.
- c) Je collega vindt dit een ongemakkelijke situatie en twijfelt aan je integriteit **kwaliteit -1**. Daarnaast is hierdoor je eigen werk blijven liggen. **snelheid -1**.

**Vraag 15**

Als nieuwe medewerker moet je een wachtwoord aanmaken voor je werkomgeving. Wat kies je?

- a) Je zet vier of meer woorden die jij makkelijk kan onthouden achter elkaar en voegt leestekens en/of cijfers en hoofdletters toe.
- b) Je gebruikt een wachtwoordgenerator om een wachtwoord voor je te bedenken.
- c) Je gebruikt het wachtwoord dat je altijd gebruikt

**Antwoorden 15**

- a) Dit is de veiligste manier voor het verzinnen van een wachtwoord en je kan het makkelijk onthouden: **actieve speler 1 stap achteruit**.
- b) Het is goed om een complex wachtwoord te gebruiken maar is moeilijk om te onthouden. Je vindt dat niet erg je hebt immer de wachtwoord reset functie geactiveerd. **informatiebeveiliging +1 en snelheid -1**.
- c) Mocht je wachtwoord inlog gekraakt worden, dan loop je direct een risico op al je gegevens en accounts waar je ditzelfde wachtwoord gebruikt: **informatiebeveiliging -1 en kwaliteit -1**.

**Vraag 16**

Je loopt over de afdeling en je ziet in een kamer wat onbekende mensen door de papieren zoeken van jouw collega. Wat doe je?

- a) Je spreekt ze aan en vraagt of je ze kunt helpen.
- b) Je belt je manager.
- c) Persoonlijke veiligheid boven alles. Je belt de beveiliging.



### **Antwoorden 16**

- a) De mannen zijn van een televisieprogramma en voelen zich betrappt. Snel rennen ze het gebouw uit: **snelheid +1 en informatiebeveiliging -1.**
- b) Je manager zit momenteel aan de andere kant van het land en weet ook niet zo goed wat je er mee moet. Je overlegt met je collega's terwijl de mannen door blijven zoeken: **snelheid -1.** Uiteindelijk besluiten jullie als groep op de mannen af te stappen. Helaas, ze zijn al weg: **actieve speler 1 stap vooruit.**
- c) De beveiliging neemt de zaak serieus en komt zo snel mogelijk: **kwaliteit +1.** Het blijkt dat de mannen van een televisieprogramma zijn. De beveiliging zet ze buiten de deur zonder dat ze konden filmen of documenten mee konden nemen: **informatiebeveiliging +1.**

### **Vraag 17**

Je hebt per ongeluk een week geleden van meerdere studenten de contact- en studievoortganggegevens op internet geplaatst. Wat doe je als je er achter komt?

- a) Je haalt alles onmiddellijk weer offline.
- b) Je licht je privacyfunctionaris en de ICT Servicedesk in.
- c) Je doet helemaal niks want je bent bang voor de reactie van je manager en collega's.

### **Antwoorden 17**

- a) Ja, dat is een goede eerste stap **kwaliteit +1**, maar de informatie is een week lang publiek beschikbaar geweest: **actieve speler 1 stap vooruit.**
- b) Dat is de juiste keus. De privacyfunctionaris gaat aan de slag met crisis coördinatie en licht de Autoriteit Persoonsgegevens (AP) in: **actieve speler één stap achteruit**, de ICT Servicedesk overlegt met intern wat nodig is om erger te voorkomen: **informatiebeveiliging +1**
- c) Je fout komt over twee weken alsnog uit door een bericht erover op het journaal: **Spion stap vooruit.** De gegevens hebben daardoor nog veel langer online gestaan: **snelheid -1.** De instelling krijgt ook nog eens een boete van de AP! **Alle spelers 1 stap vooruit.**

### **Vraag 18**

Je gaat tijdelijk aan de slag bij een andere instelling. Hoe neem je jouw vertrouwelijke dossiers mee?

- a) Digitaal op een USB stick.
- b) Je benadert jouw dossier via de Microsoft Office 365 omgeving van je instelling.
- c) Je zorgt vooraf voor een VPN verbinding de Microsoft Office 365 omgeving van je instelling.

### **Antwoorden 18**

- a) Je documenten op USB stick zetten is snel en relatief veilig: **snelheid +1.** Maar wat gebeurt er als je je USB stick kwijt raakt en die in handen komt van de Spion? **actieve speler stap vooruit.**
- b) Een veilige manier om "buiten de deur" te werken is via O365: **informatiebeveiliging +1.**
- c) Dit is nog veiliger omdat je verbinding daarmee extra beveiligd is voor algemeen vertrouwelijke documenten niet vereist. Dit is een te zware beveiligingsmaatregel: **kwaliteit -1 en snelheid -1.**

**Vraag 19**

Je wordt door een onbekende organisatie gebeld. Het gaat over een uitnodiging voor jouw directeur, wat doe je?

- a) Je geeft het nummer van je directeur. Laat ze hem/haar maar direct bellen.
- b) Je vraagt de uitnodiging te mailen naar het mailadres van de directeur.
- c) Je neemt de uitnodiging in ontvangst en vraagt hun telefoonnummer zodat je directeur terug kan bellen.

**Antwoorden 19**

- a) Nooit zomaar het telefoonnummer van collega's aan vreemden geven: **spion stap vooruit**.
- b) Nooit zomaar e-mail adressen van collega's aan vreemden geven: **actieve speler stap vooruit**.
- c) Hoewel dit niet de snelste optie is en meer tijd van jou en van je directeur vraagt is dit wel de meest veilige optie: : **snelheid -1 en informatiebeveiliging +1**.

**Vraag 20**

Iemand vertelt je vertrouwelijke informatie waar je niet om hebt gevraagd. Wat doe je?

- a) Je zegt dat je dit niet wil weten.
- b) Je hoort het aan en informeert je manager.
- c) Je hoort het aan en doet er als integer medewerker niets mee.

**Antwoord 20**

- a) Informatie die je niet weet kun je ook niet lekken: **informatiebeveiliging +1**
- b) Je bent nu op de hoogte van vertrouwelijke informatie en kiest ervoor om deze met nog iemand te delen: **spion stap vooruit**.
- c) Prima. Je hoort het aan en doet er verder niets mee. Je vertelt het aan niemand en geeft dat ook als tip mee aan je collega: **kwaliteit +1 en actieve speler stap achteruit**.

**Vraag 21**

Een mail met daarin een lijst met SMF studenten met details over hun functiebeperking stuur je per ongeluk naar het verkeerde adres. Wat doe je?

- a) Je belt direct de ICT Servicedesk voor hulp en meldt het als beveiligingsincident.
- b) Je trekt het mailtje direct in via Outlook.
- c) Je belt de geadresseerde.

**Antwoorden 21**

- a) De ICT Servicedesk geeft aan dat je het mailtje kunt intrekken. Je weet niet hoe dit moet: **snelheid -1**. De ICT Servicedesk schakelt de functionaris gegevensbescherming in die laat het datalek vast bij de Autoriteit Persoonsgegevens aanmelden: **actieve speler 1 stap achteruit**
- b) Helaas! Hoewel je de mail snel probeert in te trekken: **snelheid +1**, is het mailtje reeds gelezen door de ontvanger: **actieve speler 1 stap vooruit**.
- c) Je legt de ontvanger uit wat er aan de hand is en probeert hem te overtuigen dat hij het mailtje direct moet verwijderen. Dat lukt! Maar hoe weet je zeker dat dit ook is gebeurd? **informatiebeveiliging -1**. En je bent weer 15 minuten kwijt: **snelheid -1**.

**Vraag 22**

Je krijgt een grappig mailtje van je collega met pikante foto's. Wat doe je?

- a) Je lacht en verwijderd het mailtje.
- b) Je stuurt het door naar een andere collega die hier wel om kan lachen.
- c) Je spreekt je collega aan op het feit dat dit op het werk ongepast is.

**Antwoord 22**

- a) Het verwijderen van de mail is een snelle en goede actie: **snelheid +1**. Doordat je het grappig vindt, gaat je collega dit vaker doen: **actieve speler 1 stap richting spion**.
- b) Er ontstaat een cultuur van grappige mailtjes doorsturen binnen jullie afdeling. Ook die phishingmail vol met grappige spelfouten wordt rondgestuurd, hahaha: **hele groep stap richting spion**.
- c) Dit is wat een integer medewerker zou moeten doen: **actieve speler 1 stap achteruit**. Helaas is de sfeer wel een klein beetje verpest tussen jou en je collega, waardoor de samenwerking stroever verloopt: **snelheid-1**.

**Vraag 23**

Je bent in bezit van digitale informatie die de instelling veel geld kost als het wordt gelekt, hoe zorg je ervoor dat deze informatie bij een thuiswerkende collega komt?

- a) Via e-mail.
- b) Je neemt het zelf op een USB stick mee.
- c) Uitgeprint via aangetekende post.

**Antwoord 23**

- a) Dit is wel snel: **snelheid +1**. Maar niet veilig: Mails kunnen onderschept worden en eenvoudig worden doorgestuurd naar andere adressen: **spion stap vooruit**.
- b) Dit is wel snel: **snelheid +1** en relatief veilig. Maar wat nu als onderweg je tas wordt gestolen. Let je wel goed genoeg op je spullen? **informatiebeveiliging -1**.
- c) Dit is niet zo snel: **snelheid -1**, maar wel de veiligste manier. De documenten worden verzegeld in een auto vervoerd en worden niet lopend over straat vervoerd: **informatiebeveiliging +1**.

**Vraag 24 (vervallen)**

~~Jouw vertrouwelijk document moet even gescand worden. Door wie?~~

- ~~a) Alleen door jezelf.~~
- ~~b) Door een secretaresse.~~
- ~~c) Door een speciaal daarvoor aangewezen medewerker van DiVA.~~

#### Antwoorden 24

- a) Dit is een snelle manier: **snelheid +1**, maar weet je wel goed hoe het scanapparaat werkt? **kwaliteit -1**. En mail je het stuk naar jezelf? Mails zijn niet zo veilig, ook al is het een bericht naar jezelf: **informatiebeveiliging -1**.
- b) De secretaresse scant het stuk op het kopieerapparaat, zij heeft dit vaker gedaan dus weet prima hoe dit werkt: **kwaliteit +1**. Maar het stuk wordt wel via mail naar haar gestuurd en zij stuurt het via de mail weer door naar jou. De mail blijft echter in haar mailbox staan en die heeft ze gedeeld met andere secretaresses. Mail is niet zo veilig. Die kan immers onderschept of eenvoudig doorgestuurd worden: **spion stap vooruit**.
- c) De medewerkers van DiVA hebben een procedure voor de behandeling van vertrouwelijke stukken en een speciale scanstraat die aan de veiligheidseisen voldoet: **informatiebeveiliging +1 en kwaliteit +1**. Je moet echter wel een half dagje geduld hebben voordat jouw document verwerkt is: **snelheid -1**.

#### Vraag 25

Met de zoekfunctie op Intranet vind je een document over een nog niet aangekondigde reorganisatie binnen de instelling. Je ziet het onderwerp van het document en denkt: "Hey, dat is een vertrouwelijk stuk!" Maar in de autorisaties staat het document op 'intern openbaar'. Wat doe je?

- a) Even kijken wat het is, het is immers 'intern openbaar'.
- b) Contact opnemen met de auteur.
- c) Contact opnemen met de eigenaar van de SharePoint site waar je het document vond.

#### Antwoorden 25

- a) Als integer medewerker doe je dit uiteraard niet. Je hoeft het stuk niet te zien. Dat het op 'intern openbaar' staat is vast een foutje van de auteur: **actieve speler 1 stap vooruit**.
- b) Dat het op 'intern openbaar' staat is vast een foutje van de auteur. Het is integer en collegiaal om je collega daar op te wijzen zodat hij het kan aanpassen: **actieve speler 1 stap achteruit en snelheid +1**.
- c) Dat het op 'intern openbaar' staat is vast een foutje van de site owner. De site owner kan de autorisatie op de site aanpassen: **informatiebeveiliging +1 en snelheid +1**.

#### Vraag 26

Je wilt de NAW gegevens van een bestand van een andere afdeling gebruiken om mensen te benaderen voor een onderzoek, mag dat?

- a) Ja, na toestemming van de betrokkenen.
- b) Ja, als de leidinggevende van die afdeling het goed vindt.
- c) Nee, want die gegevens zijn voor een ander doel verkregen.

#### Antwoorden 26

- a) Goed zo, een belangrijke grondslag voor verwerking van persoonsgegevens is de ondubbelzinnige toestemming van betrokkenen: **kwaliteit +1 en actieve speler 1 stap achteruit**. Het vragen om toestemming kost je uiteraard wel meer tijd: **snelheid -1**.
- b) Fout, een leidinggevende gaat daar niet over, deze mag alleen toestemming geven als hij daar een grondslag voor heeft: **actieve speler 1 stap richting spion**.
- c) Goed, je mag gegevens in principe niet gebruiken voor een ander doel dan waarvoor ze ingewonnen zijn: **informatiebeveiliging +1**. Je kunt echter zonder gegevens niet je onderzoek uitvoeren: **kwaliteit -1**.

**Vraag 27**

Een collega vraagt je om informatie over een student, wat doe je?

- a) Ik ga er vanuit dat mijn collega integer is en geef de informatie die hij vraagt.
- b) Ik vraag waarvoor hij het nodig heeft en bepaal dan of ik die informatie mag geven.
- c) Ik geef geen informatie onder verwijzing naar de AVG.

**Antwoord 27**

- a) Helaas je collega is niet integer en hij blijkt de informatie te willen hebben voor privé gebruik: **informatiebeveiliging -1 en kwaliteit -1**
- b) Het is goed dat je eerst checkt of je de informatie in dit geval wel mag geven. Dat blijkt het geval; **actieve speler 1 stap achteruit en kwaliteit +1.**
- c) Dit is wel heel veilig: **informatiebeveiliging +1.** Je bent echter iets te strikt geweest en wordt door je leidinggevende op het matje geroepen. Je moet nu alsnog de gevraagde informatie leveren: **snelheid -1.**

**Vraag 28**

Je ontvangt van diverse aanmelders de intake formulieren via mail. Wat doe je?

- a) Je zet de mail, incl. bijlagen, in je mappenstructuur van outlook.
- b) Je slaat de bijlage op, op een speciaal daarvoor bedoelde teamsite (SharePoint) site en mail verwijder je.
- c) Je slaat de mail op, op je OneDrive dan kan je er zowel on- als offline bij.

**Antwoord 28**

- a) Hartstikke handig je hebt alle intake mails in één mapje. Als je iets nodig hebt dan vindt je het heel snel: **snelheid +1.** Er kunnen echter meer mensen bij je mail dan je denkt: **informatiebeveiliging -1.**
- b) Het is even wat meer werk, maar op die teamsite heb je een handige mappenindeling: **snelheid: -1 kwaliteit +1.** Vergeet echter niet het document te verwijderen als je het studie advies hebt uitgebracht.
- c) Wel handig dat je je in de trein alvast kan voorbereiden of je gesprek met deze aanmelder maar je laat je laptop in de trein liggen en nu moet je een datalek gaan melden: **informatiebeveiliging -1.**

**Vraag 29**

Van een vriend ontvang je een privé mailtje op je werk. Hij vraagt of je vanmiddag tijd hebt om te lunchen. Wat doe je?

- a) Je reageert via e-mail dat je het druk hebt, legt uit waar je mee bezig bent en waarom het echt vanmiddag af moet.
- b) Je reageert telefonisch en legt uit met welke klus je bezig bent en waarom je echt geen tijd hebt.
- c) Je reageert dat het je leuk lijkt om wat af te spreken. Morgen weer een dag voor het werk.

**Antwoord 29**

- a) Oeps, de mail van je vriend wordt gehackt en door jouw uitleg weten ze dat jij met het oplossen van een datalek bezig was: **actieve speler 1 stap vooruit.**
- b) Oeps, het raam stond open en laat daar nou net de spion langs lopen: **spion stap vooruit.** Je vriend weet direct waar hij aan toe is. **Snelheid +1**
- c) Je werk loopt vertraging op door deze actie: **snelheid -1.**

**Vraag 30**

Je ontvangt in je mailbox per ongeluk een mail bestemd voor de vertrouwenspersoon. Wat doe je?

- a) Je stuurt hem direct door naar de vertrouwenspersoon.
- b) Je leest hem, hij was immers aan jou gericht, en stuurt hem daarna door naar de vertrouwenspersoon.
- c) Je delete hem uit je mailbox en neemt contact op met de afzender om te vertellen dat hij de verkeerde geadresseerd had.

**Antwoord 30**

- a) Het is goed dat je hem niet leest maar direct doorstuurt. **snelheid +1** Vergeet hem echter niet uit je mailbox te verwijderen. Omdat je de afzender echter niet hebt ingelicht over zijn fout ontvang je later weer een bericht van hem dat niet voor jou bedoeld is: **informatiebeveiliging - 1.**
- b) Als integer medewerker doe je dit uiteraard niet. Je hoeft de mail niet te lezen hij is immers niet voor jou bedoeld. Het was een foutje van de afzender **actieve speler 1 stap vooruit.**
- c) Dat jij het bericht in je mailbox ontving was een foutje van de afzender. Het is integer om de afzender hierop te attenderen: **actieve speler 1 stap achteruit en snelheid +1.**

**Vraag 31**

De zoon van je broer heeft les van jou. Op een verjaardag vraagt je broer aan jou hoe zijn zoon het doet op school. Wat doe je?

- a) Je vertelt hem (in algemene termen) dat je denkt dat hij niet zo op zijn plek zit omdat zijn resultaten wat tegen vallen.
- b) Je zegt hem dat je daar niets over los mag laten en dat hij dat beter zelf aan zijn zoon kan vragen.
- c) Je logt met je mobiel in op het studievolsysteem om te laten zien hoe hij ervoor staat.

**Antwoord 31**

- a) Hoewel je hoopt dat vader en zoon hierover in gesprek zullen gaan is het niet integer om hierover uit de school te klappen. **kwaliteit -1**
- b) Dit is integer handelen. Je neef is meerdere jarig en mag zelf weten welke informatie hij met zijn ouders wil delen. **Informatiebeveiliging: +1**
- c) Je broer ziet dat zijn thuiswonende zoon nog geen vak gehaald heeft en wordt daardoor ook gesterkt in het idee dat ie beter maar werk kan gaan zoeken. Hij besluit hem per direct kostgeld te gaan vragen. De zoon dient een klacht in omdat er een datalek zou zijn bij de instelling **Actieve speler een stap vooruit , informatiebeveiliging -1, kwaliteit -1**

**Uitbreiding**

**Vraag 32**

Een onderzoeksbureau dat in opdracht van de gemeente onderzoek doet naar de studenthuisvesting in jouw stad vraagt jou om een x aantal willekeurige e-mail adressen van studenten aan te leveren om deze te kunnen bevragen. Wat doe je?

- a) Het onderzoek is ook in het belang van de studenten dus ik geef deze adressen.
- b) Je vraagt de studenten om toestemming om hun gegevens door te mogen geven.
- c) Je geeft de informatie niet maar biedt aan om een link naar een vragenlijst intern onder studenten te verspreiden.

**Antwoord 32**

- a) Hoewel misschien ook het belang van de studenten gediend is, is er geen grondslag om deze informatie aan derden te verschaffen. Studenten klagen dat de instelling niet zorgvuldig met hun gegevens omgaat en zijn bang nu vaker door het onderzoeksbureau lastig gevallen te worden. **Informatiebeveiliging -1, kwaliteit -1**
- b) Dan heb je inderdaad een grondslag om de e-mail adressen te verstrekken maar dit levert voor jou veel werk op en gaat. **Snelheid -1, kwaliteit +1**
- c) Je twijfelt niet aan het belang van het onderzoek en op deze manier hoef je geen persoonsgegevens te verstrekken. **Informatiebeveiliging +1**

**Vraag 33**

Een student komt aan de balie en vraagt om een adres van een klasgenoot die al geruime tijd ziek is. Hij wil haar graag een kaartje sturen. Wat doe je?

- a) Je geeft het adres.
- b) Je geeft het adres niet.
- c) Je geeft het adres wel maar pas nadat je hebt gecheckt dat de student ziek is en dit inderdaad een klasgenoot van haar is.

**Antwoord 33**

- a) Helaas de zieke student wil niets met deze persoon te maken hebben en hij komt nu ook nog eens ongevraagd aan de deur. **Actieve speler een stap vooruit, Informatiebeveiliging -1**
- b) Prima. Je zou eventueel kunnen aanbieden het kaartje voor hem te versturen. **Informatiebeveiliging +1, kwaliteit +1**
- c) Helaas werd deze studente al vaker lastig gevallen door deze klasgenoot en nu weet hij ook nog waar ze woont. **Informatiebeveiliging -1. En dit kost extra tijd. Snelheid -1**

**Vraag 34**

Een collega organiseert een seminar op de instelling dat ook interessant is voor jouw relaties en hij vraagt om adres gegevens om ze uit te nodigen. Wat doe je?

- a) Je geeft ze alleen als de relatie toestemming heeft gegeven voor dit soort communicatie.
- b) Je geeft ze niet maar biedt aan een uitnodiging hiervoor in de volgende nieuwsbrief op te nemen.
- c) Je geeft ze want toegang tot het seminar is gratis.

**Antwoorden 34**

- a) Goed, als je toestemming hebt dan mag je de gegevens verstrekken maar verstrek alleen die informatie die echt nodig is. **Kwaliteit +1**
- b) Je collega vindt dit een beetje flauw jouw relaties zijn toch relaties van de hele instelling en met een directe mail is de respons vaak veel groter dan een oproep in een nieuwsbrief.  
**Actieve speler een stap naar achter. Informatiebeveiliging +1**
- c) Veel relaties ervaren dit als spam en melden zich af voor alle communicatie van de instelling omdat ze te veel berichten krijgen. **Kwaliteit -1**. Het instellingsmailadres komt ook nog eens op een spamlijst te staan en de IT afdeling heeft de grootste moeite om daar weer vanaf te komen. **Informatiebeveiliging -1**

**Vraag 35**

Je hebt een Stuurgroep vergadering via Teams georganiseerd en één van de deelnemers meldt zich op het laatste moment af en vraagt of de vergadering opgenomen kan worden. Wat doe je?

- a) Je zegt dat je dat zal doen als de andere deelnemers daarmee akkoord gaan.
- b) Je neemt niet op maar zegt ervoor te zorgen dat er verslag gemaakt wordt.
- c) Je verzet de vergadering.

**Antwoord 35**

- a) Dit is voor jou wel de snelste manier om je collega te helpen. **Snelheid +1**. Beeldopnames zijn persoonsgegevens en toestemming vragen in deze situatie voldoet niet aan de AVG (is niet vrijwillig). Bij het delen van de beelden gaat er ook nog iets mis in de autorisatie.  
**Informatiebeveiliging -1**.
- b) Met het verslag is voor iedereen duidelijk wat er is besproken. **Kwaliteit +1**. Het verslag wordt gedeeld op jullie bestaande samenwerkingsomgeving (Teamssite).  
**Informatiebeveiliging +1**
- c) Hierdoor wordt wel het besluitvormingsproces ook weer vertraagd. **Kwaliteit -1**



**Vraag 36**

Bij de feestelijke opening van het nieuwe gebouw worden foto's gemaakt. Hoe zorg je ervoor dat je deze op de website mag publiceren?

- a) Je vraagt iedereen om toestemming voor publicatie.
- b) Je kondigt van te voren en tijdens het evenement aan dat er een fotograaf rondloopt die foto's maakt voor de website. Als men niet in beeld wil dan kan men dat kenbaar maken.
- c) Je plaatst alleen overzicht foto's op de website.

**Antwoord 36**

- a) Dan weet je inderdaad zeker dat je mag publiceren, **informatiebeveiliging +1** maar dit kost wel veel tijd. **Snelheid -1.**
- b) Je kan deelnemers die niet in beeld willen bijvoorbeeld voorzien van een rood keycord of button. **Snelheid +1.** Helaas ben je vergeten een proces in te richten waarbij deelnemers achteraf nog bezwaar kunnen maken. **Kwaliteit -1.**
- c) Voor foto's waar personen niet herkenbaar opstaan is de AVG niet van toepassing. **Actieve speler een stap achteruit**, maar omdat je deelnemers niet geïnformeerd hebt over de aanwezigheid van de fotograaf en wat er met de foto's gebeurt krijg je daar vragen over. **Kwaliteit -1.**

**Vraag 37**

Je hoort twee collega's op de gang over een student praten die het wat moeilijk heeft. Wat doe je?

- a) Je mengt je in het gesprek want je maakt je ook zorgen over de student.
- b) Je houdt je afzijdig want je hebt er vertrouwen in dat ze de juiste interventie zullen plegen.
- c) Je wijst ze erop dat ze dit gesprek beter niet op de gang kunnen voeren.

**Antwoord 37**

- a) Samen zijn jullie betere in staat tot een oplossing te komen. **Kwaliteit +1.** Maar het gesprek wordt afgeluisterd en nu wordt er over de student geroddeld. **Informatiebeveiliging -1,**
- b) Niet alleen jij maar ook de Spion luistert mee. **Spion een stap naar voren.**
- c) Goed zo, wees niet bang om elkaar aan te spreken! Je weet immers nooit wie er mee luistert. **Informatiebeveiliging +1**

**Vraag 38**

De accreditatiecommissie heeft inzage gevraagd in de beoordelingen van een x aantal studenten en de opleidingskwalificaties van alle docenten van de opleiding. Hoe ga je dit regelen?

- a) Je laat voor hen een tijdelijke autorisatie aanmaken zodat ze zelf in de systemen deze informatie kunnen inzien.
- b) Je stuurt ze de gevraagde informatie via SurfFilesender.
- c) Je verzamelt de informatie op een Teamssite (samenwerkingsomgeving) en geef hen daar inzage rechten.

**Antwoord 38**

- a) Het is niet makkelijk om de autorisatie precies in te regelen op wat de accreditatie commissie nodig heeft. **Informatiebeveiliging -1**. Daarbij weet het commissielid niet hoe de systemen werken en zoekt ie zich wezenloos. **Kwaliteit -1**
- b) Je verzond het wel netjes versleuteld maar de het commissielid heeft zijn laptop in de trein laten liggen en zijn laptop was niet versleuteld. **Informatiebeveiliging -1**
- c) Het kost misschien iets meer tijd **Snelheid -1** maar dit is wel de veiligste optie. Zeker als je ook nog Information Rights Management (IRM) op de documentbibliotheek op de Teamssite aanzet. **Informatiebeveiliging +1**