7 HACKEN, PESTEN & SLACHTOFFERSCHAP

-> weinig bekend over de algemeenheid en/of specificiteit van slachtofferschap

-> veel studies richten zich op het slachtofferschap van 1 bepaald soort criminaliteit, terwijl er aanwijzigingen zijn dat sommige sociale en persoonlijke factoren slachtofferschap in het algemeen kunnen voorspellen

-> in cybercrime is er vraag naar algemene of typologische theorieën over slachtofferschap, terwijl deze al bestaan voor het plegen van cybercriminaliteit, zoals hacken

-> studies bevestigen dat de zelfcontrole-theorie kan helpen bij het voorspellen van cybervictimisatie

-> de zelfcontrole kan echter het slachtofferschap van computerfocused criminaliteit, misdaden die gepleegd kunnen worden via een computer en het internet, minder goed voorspellen

-> geeft aan dat er een verschil is tussen het slachtofferschap van computer-assisted en computerfocused criminaliteit

-> hacken = computer-focused

-> online intimidatie = computer-assisted

-> in dit hoofdstuk vergelijken we hacken en online intimidatie om te kijken of slachtofferschap van deze 2 misdrijven verschilt en kijken we naar divers slachtofferschap, waarbij iemand slachtoffer wordt van beide soorten cybercriminaliteit.

7.1 ZELFCONTROLE- EN ROUTINEACTIVITEITENTHEORIE

- **Zelfcontroletheorie:**

  -> criminologische theorie over gebrek aan individuele zelfcontrole als voornaamste factor

  -> geeft aan dat individuen die niet de juiste ouderlijke aandacht hebben gehad voor hun 10e jaar minder zelfcontrole ontwikkelen dan individuen van ongeveer dezelfde leeftijd die beter ouderschap ervaren

- **Routineactiviteitentheorie:**

  -> hierbij gaat het om de gelegenheidstheorie (gelegenheid maakt de dief), die zich richt op situaties van criminaliteit.

  -> volgens deze theorie hangt criminaliteit niet zozeer af van sociale omstandigheden zoals armoede, ongelijkheid of werkloosheid

a. Internetgerelateerde criminaliteit:

- **Routineactiviteitentheorie:**

-> de routineactiviteitentheorie en de zelfcontrole zijn het meest toegepast in onderzoek naar cybercrime

-> routineactiviteitentheorie is gebaseerd op de samenkomst van tijd en plaats maar in recenter onderzoek is vastgesteld dat het ook toepasbaar is op cybercriminaliteit

-> geldt niet voor alle soorten cybercriminaliteit

-> bij die soorten waar het wel geldt, geldt dat hoe meer een slachtoffer online activiteiten heeft, meer is blootgesteld aan mogelijke cybercriminaliteit

-> controle is ook voorspelbaar voor slachtofferschap

-> comutergebruikers kunnen verschillende soorten software gebriuken die hun online-activiteiten beschermen.

> -> dit soort software is gericht op specifieke soorten van online slachtofferschap en beschermen een gebruiker dus niet voor cybercrime in het algemeen.

-> mensen die beschikken over goede vaardigheden met computers wellicht beter in staat zijn zichzelf te beschermen tegen de risico's van online slachtofferschap

-> de routineactiviteitentheorie veronderstelt een bepaalde nabijheid van daders, als je zelf deelneemt aan afwijkend gedrag op het internet. Je meer kans hebt op blootstelling aan daders en er een grotere kans aanwezig is voor vergelding.

-> online daderschap is dus aan te wijzen als oorzaak voor slachtofferschap bij onder andere intimidatie en phishing

- **Zelfcontroletheorie:**

-> 'general theory of crime' genoemd

-> stelt dat mensen met weinig zelfcontrole meer risico's nemen, minder de consequenties van hun daden inzien en impuulsief handelen

-> lage zelfcontrole kan leiden tot slachtofferschap van cybercrime

-> toch is wetenschappelijk onderzoek het er niet over eens

-> intimidatie lijkt vaker voor te komen bij studenten met lage zelfcontrole

-> mensen met lage zelfcontrole meer delinquente vrienden en dus sneller slachtoffer

b. Gegevens:

-> de gegevens uit dit hoofdstuk komen uit het LISS panel (Longitudinal Internet Studies for Social Sciences)

-> representatief voor individuen die maandelijks meedoen aan een survey.

-> ze zijn 16 jaar of ouder en hebben een online vragenlijst ingevuld over o.a. slachtofferschap, routine-activiteiten en zelfcontrole

c. Metingen:

-> **Slachtofferschap:**

Respondenten is gevraagd of ze slachtoffer zijn geworden van digitale bedreiging of hacking en hoe vaak

-> **online routine-activiteiten:**

Respondenten is gevraagd hoeveel uur per week zij doorbrachten op e-mail, internet zoekopdrachten, online kopen, chatten en bezoeken van for a. het hebben van een profiel op Hyves en het gebruik van een webcam waren dummy variabelen. Tevens is gekeken naar de bescherming van de computer. De nabijheid van daders is gemeten door te vragen of de respondenten zelf iemand geïntimideerd hebben

-> **Lage zelfcontrole:**

Zelfcontrole wordt gemeten aan de hand van de zogenaamde 'Dickman Impuulsitivity Inventory om te kijken hoe iemand zijn impulsen kan reguleren

-> **Controle variabelen:**

Er zijn verschillende soorten controle variabelen gebriukt voor de analyse naar geslacht en leeftijd, zoals opleidingsniveau, huishoudelijke karakteristieken en de graad van stedenbouw (dorp/stad)

7.1.1 resultaten

- **Zelfcontroletheorie:**

  -> Mensen met lagere zelfcontrole hebben hoger risico om slachtoffer te worden

  -> deelname aan communicatieve internetactiviteiten (forums, webcam, sociale media) had geen invloed op slachtofferschap van hacken

  -> weinig kennis van computer beveiligingssoftware hadden een lagere kans om slachtoffer te worden van hacking

  -> overtreders hadden een verhoogd risico op slachtofferschap van hacken dan niet-overtreders

  -> lage zelfcontrole hoger risico om slachtoffer te worden van online intimidatie

  -> deelname aan communicatieve internetactiviteiten (forums, webcam, sociale media) had hogere invloed op slachtofferschap van online intimidatie

  -> online afwijkend gedrag heeft een hogere kans op online intimidatie

  -> jongeren en alleenwonende hogere kans op online intimidatie dan ouderen

  Conclusie: slachtoffer worden van hacken én online intimidatie is meer waarschijnlijk bij mensen met lage zelfcontrole, zoals verwacht volgens voorspellingen van de zelfcontrole theorie

- **Routineactiviteitentheorie**

  -> veel tijd op het internet doorbrengen met communicatie-activiteiten verhoogd het risico van dubbel slachtofferschap

  -> deelname aan sociale netwerksites verlaagt het risico op dubbel slachtofferschap.

  -> jongeren lopen een hoger risico op dubbel slachtofferschap

7.2 RAT EN CYBERSPACE

De routineactiviteitentheorie is één van de belangrijste theorieën van de 'omgevingscriminologie'

De theorie stelt dat een misdaad optreedt wanneer de volgende drie elementen samenkomen in een bepaalde ruimte en tijd:

1. **Een toegankelijk doel**
2. **Het ontbreken van bekwame voogden (capable guardianship) die kunnen ingrijpen**
3. **De aanwezigheid van een gemotiveerde dader**

- **Een toegankelijk doel:**

  -> toegankelijk doel kan een persoon, object of plaats bevatten, de volgende acroniemen zijn gebruikt om beschikbare doelen te beschrijven

  - **VIVA:** Value, Inertia, Visibility, Acces (waarde, traagheid, zichtbaarheid, toegang)
  - **CRAVED:** Concealable, Removable, Available, Valuable, Enjoyable, Disposable (camoufleerbaar, verwijderbaar, beschikbaar, waardevol, plezierig, wegwerpbaar)

  -> de routineactiviteitentheorie als een criminele preventie methodologie richt zich op essentiële elementen die een misdaad vormen

  -> biedt een kader om criminaliteit te voorkomen door ten minste één van deze elementen te wijzigen (de dader, het doel of de aanwezigheid van bekwame voogden)

- **Afwezigheid van bekwame voogd die kan ingrijpen:**

  -> bekwame voogd heeft een menselijk element

  -> meestal een persoon die, door huun aanwezigheid zou afbreuk doen aan potentiële overtreders om een misdaad te plegen

  -> **enkele voorbeelden van een bekwame voogd:**

  - Politie patrouilles
  - Bewakers
  - Deurpersoneel
  - Waakzaam personeel en medewerkers
  - Vrienden
  - Buren

-> sommige bewakers zijn formeel en opzettelijk, zoals beveiligingswachten, sommigen zijn informeel en onbedoeld, zoals buren

-> het is ook mogelijk dat een voogd aanwezig is, maar ondoeltreffend. Bijvoorbeeld: een CCTV-camera is geen bekwame voogd als het onjuist of op de verkeerde plaats is opgesteld of niet wordt gecontroleerd

-> personeel kan aanwezig zijn in een winkel, maar heeft niet voldoende opleiding of bewuustzijn om een effectief afschrikmiddel te zijn

- **Een gemotiveerde dader:**

  -> de routineactiviteitstheorie kijkt naar misdaad vanuit het oogpunt van een dader

  -> een misdaad zal alleen zijn gepleegd als een waarschijnlijke overtreder denkt dat een doelwit geschikt is en dat een bevoegde voogd afwezig is

  -> het is de oorzaak van een overtreding van een situatie die bepaalt of een misdaad plaatsvindt.

  -> misdaad kan verklaard worden door drie factoren:

  - Motivatie
  - Mogelijkheid
  - Afwezigheid van bekwame voogd/bewaker

    -> dit is zowel toepasselijk op individuele incidenten als lange termijn trends, en ook toepasselijk op cybercrime

  -> routineactiviteitentheorie is echter nauwelijks getoetst op digitale criminaliteit

  -> voor het plaatsvinden van criminaliteit moet er een samenkomst in tijd en ruimte zijn van een gemotiveerde dader, een geschikt doelwit en gering toezicht

  -> in algemene zin wordt de VIVA-indeling veelal gehanteerd om te bepalen in hoeverre een doelwit geschikt is om als slachtoffer te worden geselecteerd

  -> de toegankelijkheid wordt bepaald door dagelijkse activiteiten die het doelwit blootstellen

  -> naarmate mensen zich via dagelijkse activiteiten meer blootstellen aan daders, zijn zij toegankelijker en lopen zij een groter risico

  -> zichtbaarheid zou ook een rol kunnen spelen, omdat mensen die zich via een internetprofiel of webcam tonen aan anderen, om die reden grotere risico's op bedreiging kunnen lopen