2 CYBERCRIMECATEGORIEËN

2.1 CYBER TRESPASS

Het overtreden van onzichtbare belangrijke grenzen van eigendommen online. Zonder toestemming toegang krijgen tot een computersysteem, netwerk of databron. Daders zijn vaak hackers en kunnen kwaadaardige malware op de pc's zetten. Tussen de 10-15% doet aan wachtwoord raden. Hackers opereren in een subcultuur die een diepe verbinding en kennis hebben van technologie.

- **Enkele voorspellers van hackgedrag:**

  -> vroege blootstelling aan technologie

  -> belangstelling voor technologie

  -> capaciteit voor zelfmanagement, maar sommige zijn juist antisociaal

  -> hoge scores op persoonlijkheidsevaluaties en analytische besluitvorming

- **Hackvrienden zijn belangrijk voor het neutraliseren van hun gedrag:**

  -> Ze veroorzaken geen schade

  -> slachtoffers hebben zichzelf slecht beveiligd

- **Onderzoek naar slachtofferschap:**

  -> daders vallen geen specifieke mensen aan maar juist grotere groepen

  -> vrouwen zijn waarschijnlijk eerder slachtoffer

  -> daders van cybercrime zijn ook slachtoffer, vooral in de porno of piraterij

  -> hacken in groepen kan er ook voor zorgen dat je eerder slachtoffer bent.

Fysieke en sociale bewakers helpen wsl wel, zoals beschermende software. Technologische vaardigheden kunnen er ook voor zorgen dat je beter beschermd bent.

2.2 CYBERDECEPTIE / DIEFSTAL

Gerelateerd aan trespassing, omdat trespassing wordt gebruikt om de pc in te komen om vervolgens data te stelen. Financiële schade is onbekend.

- **2 delicten die gemakkelijker zijn gemaakt door technologie:**

  -> fraudeurs gebruiken fraudeschema's voor het online milieu. Slachtoffers verliezen enkele honderden euro's per incident

  -> digitale piraterij of het kopiëren van digitale media zorgt voor miljardenverliezen.

- **Scamming:**

  -> versturen van berichten die inspelen op de emoties. Weinig informatie over slachtoffers.

  -> vrouwen reageren eerder op love-emails en mannen op FBI-scams

  -> laag peil van zelfcontrole is niet echt van toepassing op scams.

- **Piraterij:**

  -> groeit het snelst en gaat het meeste aandacht naar uit.

  -> door gunstige wetten zijn personen steeds minder verantwoordelijk voor piraterij.

  -> sociaal leren, positieve beloning & bronnen voor imitatie blijken de kans te verhogen.

  -> lage zelfcontrole speelt wel een rol bij piraterij.

2.3 CYBER PORNO & OBSCEEN GEDRAG

-> Seksuele expressie door computer communicatie en verspreiding van seksueel materiaal online.

-> Sekswerkers die hun diensten aanbieden online.

-> kinderporno, pedofielen zoeken andere pedofielen online en delen hun ervaring

-> steeds meer onderzoek, vooral naar bestiality, bugchasing, recording live streaming seksshows en verscheidene aspecten van de BDSM-cultuur.

-> veel online sekshandel

-> grote aandacht voor de aanbieders van seks door middel van advertenties

-> verder is er ook aandacht voor sekstoerisme

2.4 CYBERGEWELD

- Politieke en sociale bewegingen kunnen hun ideologieën online promoten
- Aanvallen op de overheid en politieke organisaties (cyberattacks)
- Stalking, dreigementen, pesten is toegenomen
- Vrouwen eerder slachtoffer en ervaren de gevolgen erger
- Slechte opvoeding leidt tot pesten en gepest worden
- Strain en negatieve emoties leiden tot cyberpesten, maar ook tegengestelde resuultaten gevonden
- Lage zelfcontrole kan een rol spelen

De theorie van routineactiviteiten kan toegepast worden op cyberpesten: het risico op slachtofferschap is groter wanneer je meer tijd in chatrooms, sociale netwerksites en aan email besteed.

Ook betrokkenheid bij pesten en dreigen verhoogt de kans op slachtofferschap. Programma's en ouders kunnen cyberpesten niet tegengaan. Scholen moeten er meer aandacht aan besteden.