# #DigitSafe

## Versterking van digitale veilige ruimten en veerkracht

# Handboek Digitale Veerkracht

Co-funded by the Erasmus+ Programme of the European Union

# Inhoud


1 CYBERPESTEN

1.1 Wat is Cyberpesten?

1.2 Het belang van cyberpesten en de gevolgen ervan: bewustmaking en het herkennen ervan.

1.3 Richtlijnen: hoe om te gaan met slachtoffers van cyberpesten? (Procedures, empathie, het belang van luisteren, emotionele steun, psychologische steun).

1.4 Preventieve maatregelen

1.5 Hoe cyberpesten te melden (wettelijk kader, instellingen, NGO's, enz.

2. HAATZAAIEN

2.1 Wat is haatzaaien?

2.2 Hoe haatzaaien te voorkomen

2.3 Hoe haatzaaien te melden

3 CYBERBEVEILIGING EN PRIVACY

3.1 Waarom is de bescherming van persoonsgegevens belangrijk?

3.2 Soorten bedreigingen en misdrijven met betrekking tot persoonsgegevens en privacy

3.3 Hoe cyberbeveiligingsdreigingen op sociale media/instellingen te melden

3.4 Hoe risico's voor de beveiliging van gegevens te vermijden

4. CONCLUSIE


# Introductie

Het project #DigitSafe, Boosting Digital Safe Spaces and Resilience, heeft tot doel jongeren in staat te stellen weerbare en veilige digitale burgers te worden, zodat zij een aantal van de uitdagingen en negatieve effecten van het digitale tijdperk kunnen aanpakken. Dit sluit aan bij doel 6, "Informatie en constructieve dialoog", van de EU-strategie voor jongeren 2019-2027.

Het #DigitSafe-project streeft naar een bredere en diepere kennis onder jongeren over de twee belangrijkste onderwerpen: cyberveiligheid en haatzaaien, en veiligheid en privacy. Het project wil met name de meest kwetsbare groepen jongeren bereiken door veiligere digitale gemeenschappelijke ruimten en praktijken te creëren en hun capaciteiten op het gebied van digitale weerbaarheid te vergroten.

Dit project wil ook de volgende drie specifieke hoofddoelstellingen bereiken:

1. Het bevorderen van digitaal burgerschap onder jongeren in de deelnemende landen door hen, in overeenstemming met de EU-strategie voor jongeren 2019-2027, te voorzien van praktische en gebundelde informatie over Veiligheid & Privacy, en Hate Speech & Cyberbullying.

2. Jongeren, met name kansarme jongeren die vaak een gebrek aan informatie- en datageletterdheid hebben, de nodige competenties meegeven om hun digitale weerbaarheid te vergroten.
3. Een innovatieve methodologie ontwikkelen die de verzamelde relevante informatie van dit handboek vertaalt in een bewustmakingscampagne over meerdere kanalen, waarbij gebruik wordt gemaakt van de meest gebruikelijke audiovisuele communicatiepraktijken, taal, instrumenten en trends onder jongeren. Dit wordt een multimedia- en multikanaalsstrategie die gebruik maakt van het enorme aantal mogelijkheden voor het creëren van inhoud die voor elke gebruiker in het huidige sociale medialandschap toegankelijk zijn, met als doel de jongeren beter in staat te stellen rationele keuzes te maken en hun digitale rechten te kennen.

Dit handboek over digitale weerbaarheid zal uitgebreide en uniforme begeleiding bieden, met praktische informatie en tips (waaronder juridische, psychologische, opleidings- en open-leermiddelen), en belangrijke aanbevelingen doen om jongeren te helpen hun rechten beter te leren kennen, digitale risico's en bedreigingen in de context van deze onderwerpen.

Het zal het bewustzijn vergroten van de mogelijkheden en middelen die beschikbaar zijn om vaardigheden op te bouwen voor het omgaan met problemen die voortvloeien uit het huidige digitale leven van jongeren. Het zal jongeren in staat stellen betrokken digitale burgers te worden en een veiliger digitale wereld te bevorderen. Het zal een enorme hoeveelheid informatie verzamelen en deze op een meer bruikbare en omvattende manier samenbrengen.

#DigitSafe
Boosting digital safe spaces and resilience

Co-funded by the
Erasmus+ Programme
of the European Union

# 1. Cyberpesten

## 1.1. Wat is cyberpesten?

Op Europees niveau zijn er meerdere definities van cyberpesten gevonden, waarin verschillende aspecten zijn opgenomen, afhankelijk van de specifieke kenmerken van de landen waarin het onderzoek is uitgevoerd (België, Bulgarije, Nederland en Spanje). De in 2016 door de beleidsafdeling Burgerrechten en constitutionele zaken van het Europees Parlement ontwikkelde studie "Cyberpesten onder jongeren" heeft echter een vrij nauwkeurige en homogene definitie opgeleverd die transnationaal in de Europese Unie kan worden gebruikt:

- Cyberpesten beschrijft die situaties waarin pesten plaatsvindt op het internet, meestal via mobiele telefoons en sociale media. Cyberpesten komt dus overeen met een even agressieve als opzettelijke handeling, uitgevoerd met behulp van informatie- en communicatietechnologieën (ICT)."

Net als bij offline pesten zijn bij cyberpesten meestal de volgende drie hoofdrolspelers betrokken:

- De **dader:** *de persoon die de agressie uitvoert.*
- Het **slachtoffer:** *de persoon die de agressie ondergaat.*
- De **omstanders:** *degenen die zien wat er tussen de pester en het slachtoffer gebeurt, maar die niet rechtstreeks bij het pesten betrokken zijn.*

Het gedrag moet opzettelijk en herhaaldelijk plaatsvinden en er moet sprake zijn van een onevenwichtige machtsverhouding tussen de agressor en het slachtoffer.

Er zijn belangrijke kenmerken van cyberpesten die de identificatie en het begrip ervan vergemakkelijken:

- Cyberpesten is kwaadaardig en nooit toevallig. De cyberpester heeft het duidelijke en bewuste doel het slachtoffer schade toe te brengen, hem/haar pijn te doen, te vernederen, hem/haar lichamelijk of geestelijk te laten lijden.
- Het gebeurt vanuit een machtspositie. De cyberpester is altijd in het voordeel en hij/zij heeft een overwicht. Afhankelijk van de omgeving waarin cyberpesten plaatsvindt, kan het betekenen dat cyberpesten met een groep gebeurt tegen één slachtoffer dat alleen is.

- Agressors kunnen misbruik maken van een niet-agressief of kwetsbaar slachtoffer, dat zich niet kan verdedigen.
- Het is repetitief, gericht op het intimideren, boos maken of in verlegenheid brengen van de slachtoffers. Een geïsoleerde agressieve actie is nog geen cyberpesten. Het wordt cyberpesten wanneer de agressie steeds wordt herhaald tegen dezelfde persoon (of dezelfde personen).

Door de digitalisering zijn de kanalen waarlangs via internet kan worden gepest, verveelvoudigd. Enkele van de meest voorkomende manieren waarop slachtoffers van cyberpesten worden aangevallen zijn echter de volgende:

**Sociale netwerken**

**Mobiele telefoons**

**Berichtenplatforms**

**Spelplatforms**

Om duidelijk te maken welke illegale handelingen onder cyberpesten vallen, volgen hier enkele voorbeelden:

- *Het verspreiden van leugens of het plaatsen van beschamende foto's/video's van iemand op sociale media.*
- *Het versturen van beledigende berichten of bedreigingen via berichtenplatforms.*
- *Kwaadaardige berichten versturen onder de identiteit van iemand anders.*

## 1.2 Het belang van cyberpesten en de gevolgen ervan: bewustmaking en de identificatie ervan

**Cyberpesten herkennen**

Een van de belangrijkste manieren om cyberpesten aan te pakken is cyberpesten te herkennen en te letten op de waarschuwingssignalen. Internationaal of op Europees niveau bestaat er geen algemeen aanvaarde definitie van cyberpesten.

De Europese Commissie definieert cyberpesten echter als "herhaalde verbale of psychologische intimidatie door een individu of een groep tegen anderen via onlinediensten en mobiele telefoons".(2) Volgens de Raad van Europa onderscheidt cyberpesten zich van andere vormen van pesten door het risico van publieke

(2)'Cyberbullying among Young People', Directorate General for Internal Policies (European Parliament), 2016, p.8.

blootstelling, de complexe rol van waarnemers en de omvang van het publiek dat met digitale technologieën en communicatie gepaard gaat.(3)
Om een tolerantere en veiligere online wereld te creëren, moet cyberpesten op grotere schaal worden aangepakt, zowel op individueel als op organisatorisch niveau.

De gevolgen van cyberpesten mogen niet lichtvaardig worden opgevat of als grapjes worden beschouwd, omdat daarmee niet alleen de emoties en het lijden van het slachtoffer worden ontkend, maar dit soort geweld in de digitale omgeving ook wordt genormaliseerd. De gevolgen van cyberpesten kunnen langdurig zijn en de slachtoffers op vele manieren treffen.

We kunnen de belangrijkste gevolgen van cyberpesten noemen:

- **Geestelijke en emotionele gevolgen.** Slachtoffers kunnen zich verdrietig, beschaamd, dom, depressief, boos en angstig voelen. Slachtoffers verliezen meestal hun belangstelling voor de dingen waar ze vroeger van hielden. Ze ontwikkelen een lager zelfbeeld, of ze voelen zich geïsoleerd, niet in staat om met hun leeftijdsgenoten te communiceren. Soms worden slachtoffers van cyberpesten "slachtoffer-agressors", die het gedrag herhalen en anderen pesten.(4)

(3) https://www.coe.int/en/web/campaign-free-to-speak-safe-to-learn/preventing-bullying-and-violence [accessed 27/05/2022)
(4) Joint Research Centre (2013). Social Networks and Cyberbullying among Teenagers

- **Lichamelijke gevolgen** De stress en angst die een slachtoffer ondervindt, kunnen leiden tot lichamelijke problemen zoals zich moe voelen door slaapstoornissen of het ervaren van echte gezondheidsklachten zoals buikpijn of hoofdpijn.
- **Juridische gevolgen** Het gevoel dat zij door anderen belachelijk worden gemaakt of gepest, weerhoudt de slachtoffers van cyberpesten er vaak van aangifte te doen of te proberen het probleem aan te pakken. Samen met de trage evolutie in de wettelijke classificatie van het misdrijf betekent dit dat het vaak onbestraft blijft en dat het de herhaling van aanvallen aanmoedigt.

Bewustmaking van cyberpesten om het te voorkomen is essentieel. De eerste stap om cyberpesten te herkennen is een duidelijke definitie van wat het inhoudt. In Europa zijn beleidsbesluiten genomen en zijn talrijke programma's vastgesteld en uitgevoerd om cyberpesten te voorkomen.

Het Cyberbullying Research Centre heeft een reeks gestructureerde tips ontwikkeld over hoe we te werk moeten gaan om cyberpesten te voorkomen en onszelf als gebruikers te beveiligen. Preventie is altijd de beste optie om dit probleem te bestrijden.

## Gericht tot jongeren:

- Blijf op de hoogte van de privacy-instellingen. Sociale mediasites en programma's wijzigen en updaten hun privacy-instellingen vaak. Zorg ervoor dat je bekend bent met de nieuwe profielopties en houd zoveel mogelijk informatie beperkt tot degenen die je echt vertrouwt.
- Beperk de toegang tot je contactgegevens - Geef je e-mail of telefoonnummer niet aan mensen die je niet kent. Houd je e-mail en telefoonnummer ook weg van sociale mediasites.
- Leer internetetiquette om mogelijke problemen met andere internetgebruikers te voorkomen. Leer de sociale conventies met betrekking tot interactie in cyberspace.
- Stuur geen ongepaste foto's of video's - Vergeet niet dat de vriend, vriendin of partner van vandaag de minnaar van morgen kan zijn. Je wilt niet dat iemand ongepaste foto's of video's van je online plaatst en deelt met de rest van de wereld. Breng jezelf niet in de positie dat je je hierover zorgen moet maken.

- Google jezelf. Je moet altijd weten wat er over je gezegd wordt. Het is vaak verrassend dat informatie waarvan je dacht dat die privé was, opduikt in openbare databases, nieuwe artikelen of op sociale mediapagina's die door zoekmachines zijn geïndexeerd.
- Accepteer geen vriendschapsverzoeken van vreemden. Als je de persoon die je een vriendschaps- of volgersverzoek stuurt niet kent, negeer het dan. De meeste social media sites en apps geven je ook de optie om de gebruiker te blokkeren als je dat wilt.
- Gebruik site-based controls. Schakel zoekopties op bepaalde sociale mediasites uit om te voorkomen dat iemand in het grote publiek naar je zoekt of je berichten stuurt.
- Houd je informatie beschermd - Als je een openbare computer of draadloze verbinding gebruikt, zorg er dan voor dat je je afmeldt bij elke site waar je bent wanneer je wegloopt van die computer. Zelfs voor een minuut.
- Wees sceptisch bij online interacties. Zelfs bij mensen die je vertrouwt, is het riskant om te veel informatie prijs te geven omdat je nooit zeker weet of de persoon met wie je denkt te communiceren er echt is, of dat hij of zij alleen is.

- Bescherm mensen. Vergeet niet dat sommige mensen veel tijd hebben en het enige wat ze willen doen is anderen het leven zuur maken. Laat dat niet toe. Zet niet te veel persoonlijke of privé-informatie online die kan worden gebruikt om je lastig te vallen of te vernederen en verzet je tegen elke vorm van interactie met hen.

## Richt zich tot leerkrachten en ouders:

Het is belangrijk dat organisaties, scholen, werkplekken en individuen zich inzetten om cyberpesten aan te pakken vanwege de impact die cyberpesten op slachtoffers kan hebben. Het onderzoek van het Cyberbullying Research Centre uit 2021 "Cyberbullying: Identification, Prevention and Response" gaf een uitgebreide uitleg over hoe leerkrachten en ouders cyberpesten zouden kunnen aanpakken op het gebied van signalering en preventie.

Voorlichting aan de gemeenschap over een verantwoord gebruik van apparaten gericht op digitaal burgerschap is misschien wel de belangrijkste preventieve stap met betrekking tot onderwijsinstellingen en hun docenten/professoren.

Met andere woorden: het is belangrijk om niet alleen te vertrouwen op formeel onderwijs, maar om niet-formele en informele activiteiten op scholen te gebruiken om cyberpesten vanuit een creatief oogpunt te bestrijden en te voorkomen.

Anderzijds moeten ouders "met woorden en daden aan hun kinderen laten zien dat zij beiden hetzelfde eindresultaat wensen: "dat het cyberpesten stopt en dat het leven niet nog moeilijker wordt."

Hoe moeten ouders reageren als ze ontdekken dat hun eigen kind een cyberpester is? Ten eerste moeten ze hem/haar uitleggen hoe dat gedrag in de echte wereld schade en pijn uitlokt en toebrengt. Daarna moeten de ouders hem/haar de kans geven om verder te gaan en dat gedrag te beëindigen. Kinderen moeten weten dat elke actie, ook online, ernstige gevolgen heeft. Van de kant van de ouders is het essentieel om meer aandacht te besteden aan het gedrag en de acties van hun kinderen online.

## 1.3 Richtlijnen: hoe om te gaan met slachtoffers van cyberpesten?

**(Procedures, empathie, het belang van luisteren, emotionele steun, psychologische steun)**

### Als je zelf slachtoffer bent:

Als je last hebt van cyberpesten, raden we je aan deze reeks stappen te volgen:

- Zoek hulp. Allereerst moet je praten en het bespreken met familieleden of professionals!
- Meld de inhoud. Als het cyberpesten via een sociaal netwerk heeft plaatsgevonden, meld de inhoud dan bij dat platform. Dit is niet altijd effectief, maar het is belangrijk dat het sociale netwerk weet wie de beschuldigde is zodat ze actie kunnen ondernemen, soms na meerdere meldingen.
- Bescherm jezelf. Verander je wachtwoord, vergroot de privacy van je berichten, verwijder persoonlijke informatie zoals je e-mailadres, telefoonnummer of links naar andere accounts. **Verwijder als tijdelijke maatregel je account of verander je nickname.**
- Neem contact op met de Internet Service Provider (ISP). Probeer contact op te nemen met de Internet Service Provider van de persoon die je lastigvalt als deze is geïdentificeerd. De ISP kan dan contact opnemen met de persoon of misschien zijn internetaccount direct afsluiten.

- Dien een klacht in door naar een politiebureau te gaan. Neem bewijsmateriaal mee van de aanval (bijvoorbeeld screenshots). De politie zal nota nemen van uw klacht en alle informatie met betrekking tot uw klacht en deze in een rapport opnemen.
- Meld het cyberpesten publiekelijk. Deel screenshots van de pester (zorg ervoor dat je de gebruikersnaam en profielfoto van de pester verbergt, zodat je niet wordt beschuldigd van laster).

## Als leraar:

Leerkrachten moeten letten op verschillende signalen waaruit kan blijken dat een kind wordt gecyberpest. Sommige van deze signalen kunnen een snelle toename of afname van het apparaatgebruik zijn of een emotionele reactie op wat er op hun apparaat gebeurt. Als een kind zijn scherm of apparaat verbergt wanneer anderen in de buurt zijn en een gesprek vermijdt, moet daar rekening mee worden gehouden.

Daarnaast moeten leerkrachten kinderen ook helpen hoe ze cyberpesten kunnen herkennen, erop kunnen reageren en voorkomen. Enkele richtlijnen zijn:

- Communicatie is heel belangrijk, dus als je ooit denkt dat een kind wordt gecyberpest, spreek het dan privé aan en vraag ernaar. Je kunt er ook met een ouder over praten. Leerkrachten kunnen een bemiddelaar zijn tussen het kind, de ouders en de school.
- Bevorder een veilige klasomgeving. Help kinderen emotionele intelligentie te ontwikkelen, zodat ze zelfbewustzijn en zelfregulatievaardigheden leren en leren hoe ze empathie voor anderen kunnen opbrengen.

- Moedig leerlingen aan te letten op signalen die hen kunnen helpen herkennen wanneer er iets gebeurt op digitale media waardoor ze zich ongemakkelijk, bezorgd, verdrietig of angstig voelen.
- Leer ze na te denken voordat ze iets posten.
- Leg leerlingen de drie manieren uit waarop ze kunnen en moeten reageren als ze getuige zijn van cyberpesten: als je het doelwit van het pesten steunt, ben je een bondgenoot, als je probeert het cyberpesten te stoppen ben je een upstander en als je slachtoffer bent van cyberpesten moet je het melden aan een volwassene.

## Als ouder:

De kans is groot dat kinderen niet herkennen dat ze worden gecyberpest, omdat ze zich misschien schamen. Het komt vaak voor dat jongeren in stilte lijden. Ze kunnen bang zijn dat ouders zullen reageren door hun online toegang te beperken, ze kunnen zich beschaamd voelen dat ze het pesten niet zelf kunnen aanpakken.

Om deze redenen moeten ouders, als ze tekenen bij hun kinderen zien, onmiddellijk actie ondernemen. Probeer allereerst met uw kind te praten en naar hem of haar te luisteren.

Ga rustig met hen in gesprek over wat er aan de hand is. Neem de tijd om precies te begrijpen wat er is gebeurd en in welke context het gebeurde.

Als je het eenmaal weet, bied dan troost en onvoorwaardelijke steun, want slachtoffers van cyberpesten ervaren vaak gevoelens van isolatie. Laat je kind zien dat deze situatie kan worden aangepakt op een manier die niet gepaard gaat met online vergelding. Zorg dat uw kind zich veilig voelt, dat moet de eerste prioriteit zijn, evenals uw kind laten weten dat het niet zijn schuld is.

Probeer daarna zoveel mogelijk bewijsmateriaal te verzamelen. Print of maak screenshots of opnames van gesprekken, berichten, foto's, video's en andere zaken die kunnen dienen als duidelijk bewijs dat uw kind wordt gecyberpest.

De volgende stap is contact opnemen met de aanbieder van de inhoud, aangezien cyberpesten altijd in strijd is met de servicevoorwaarden van alle legitieme dienstverleners. Zij moeten actie ondernemen in deze zaak, zodat uw kind er niet meer onder lijdt.

Als de cyberpester een klasgenoot is of naar dezelfde school gaat als uw kind, moet je de school zo snel mogelijk op de hoogte brengen, omdat zij misschien regels hebben voor het reageren op cyberpesten.

Ouders kunnen ook contact opnemen met de politie als de voorgaande stappen niet helpen om de situatie te verbeteren.

Als het nodig is, probeer dan counseling te zoeken voor uw kind. Kinderen kunnen er baat bij hebben om met een geestelijk verzorger te praten. Zij kunnen er de voorkeur aan geven om met een derde partij te praten die als objectiever kan worden beschouwd.

## 1.4 Preventieve maatregelen

Er is geen waterdichte manier om te voorkomen dat een kind wordt gecyberpest. Er zijn echter verschillende manieren om de kans dat ze het doelwit worden te verkleinen.

Allereerst is het belangrijk om overal wachtwoorden voor te gebruiken en deze wachtwoorden met niemand te delen.

Kinderen moeten weten dat het belangrijk is persoonlijke zaken privé te houden. Ze moeten nooit hun adres, telefoonnummer of e-mailadres online delen. Ze moeten voorzichtig zijn met het delen van te veel informatie over waar ze naar school gaan, vooral als ze online vrienden of volgers hebben die ze niet echt goed kennen.

Ze moeten ook weten dat ze moeten uitloggen als ze openbare apparaten gebruiken, zoals openbare computers of laptops op school of in de bibliotheek. Dit betekent ook uitloggen bij e-mail, social media accounts, hun schoolaccount, of elke andere account die ze openen.

Ten slotte, maar misschien wel het belangrijkst, moeten kinderen weten dat als zij ooit het slachtoffer worden van cyberpesten, zij dit moeten melden aan hun ouders of leerkrachten.

## 1.5 Hoe cyberpesten te melden (Wettelijk kader, instellingen, NGO's, enz.)

Een van de belangrijkste aspecten van het melden van cyberpesten is dat de meeste Europese landen geen specifieke wetgeving inzake cyberpesten hebben.

Ondanks het belang, het grote aantal gevallen en de bezorgdheid onder jongeren heeft de wetgeving op dit gebied nog geen vooruitgang geboekt. Hierdoor is het werk van instellingen en organisaties essentieel geworden om gevallen te helpen opsporen, aan de kaak te stellen en steun te verlenen aan de slachtoffers.

# 2. Haatzaaien

## 2.1 Wat is haatzaaien?

Er bestaat geen algemeen aanvaarde definitie van haatzaaien. In dit deel zullen we een aantal definities schetsen die zowel in de EU-wetgeving als door vooraanstaande organisaties die haatzaaien bestrijden, worden gehanteerd.

- (Illegale) Haatzaaien wordt in het EU-recht gedefinieerd als *"het publiekelijk aanzetten tot geweld of haat op grond van bepaalde kenmerken, waaronder ras, huidskleur, godsdienst, afstamming, nationale of etnische afkomst"*. Hoewel het kaderbesluit betrekking heeft op racisme en vreemdelingenhaat, hebben de meeste lidstaten hun nationale wetgeving uitgebreid tot andere gronden zoals seksuele geaardheid, genderidentiteit en handicap (5).

## 2.2 Hoe haatzaaien te voorkomen

Eén manier om haatzaaien te bestrijden is het blokkeren en rapporteren van accounts met haatzaaiende uitlatingen die je online tegenkomt (zie het volgende deel over tips voor het rapporteren van haatzaaiende uitlatingen). De Verenigde Naties bevelen aan om de volgende praktijken toe te passen om haatuitingen te voorkomen (6):

((5) Code of Conduct- Illegal Online Hate Speech Questions and Answers, (European Commission 2016) https://ec.europa.eu/info/sites/default/files/code_of_conduct_hate_speech_en.pdf
(6) United Nations- how to deal with hate speech? https://www.un.org/en/hate-speech/take-action/engage

- **Pauze.** Onthoud uzelf van hatelijke opmerkingen en/of het delen van dergelijke inhoud.
- **Fact check.** Zorg ervoor dat je valse en bevooroordeelde informatie herkent voordat je verkeerde informatie verspreidt.
- **Uitdagen.** Verspreid je eigen tegenspraak en betwist haatzaaiende uitspraken waar mogelijk
- **Steun.** Neem publiekelijk stelling en betuig solidariteit met de slachtoffers van haatzaaiende uitlatingen.
- **Rapporteer.** Controleer de richtlijnen van de sociale media die je gebruikt en rapporteer gevallen van haatzaaien die deze richtlijnen schenden. In ernstigere gevallen kun je een klacht indienen bij de politie (bijv. als er sprake is van aanzetten tot geweld).
- **Educatie.** Deel educatieve middelen en publieke campagnes of begin gesprekken met uw vrienden en familie.
- **Engageer.** Overweeg je aan te sluiten bij een NGO of een initiatief dat zich inzet voor de aanpak van haatzaaien in jouw gemeenschap.

*www.un.org/en/hate-speech/take-action/engage*

## 2.3 Hoe haatzaaien te melden

Gebruikers kunnen gevallen van haatzaaien rechtstreeks melden via het socialemediakanaal waarin zij die tegenkomen. Op de website van de Raad van Europa staat informatie over hoe men melding kan maken van sociale mediakanalen. In sommige gevallen hoeft je geen account te hebben om aangifte te doen. Op Facebook bijvoorbeeld kunt je dit online formulier invullen zonder een Facebook-account te hebben of daarop ingelogd te zijn.

Sommige Europese landen hebben in het kader van de jongerencampagne "Geen haatzaaien" van de Europese Raad nationale meldingsprocedures en -mechanismen voor haatzaaien, haatmisdrijven en cyberpesten ingevoerd.

Andere suggesties voor het melden van haatuitingen zijn Meld de hate speech bij de politie.

- Doe aangifte bij een gezaghebbende instantie, bijvoorbeeld een burgerlijke of administratieve rechtbank.
- Doe aangifte bij een NGO, bijvoorbeeld MiND, het nationale meldpunt in Nederland voor haatzaaiende en discriminerende inhoud.
- Praat met iemand die je vertrouwt, bijvoorbeeld een ouder, vriend of leraar.

# 3. Cyberveiliging en Privacy

## 3.1. Waarom is de bescherming van persoonsgegevens belangrijk?

De term bescherming van persoonsgegevens wordt gedefinieerd in artikel 4, lid 1, van de algemene verordening gegevensbescherming: persoonsgegevens zijn alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Namen en e-mailadressen zijn uiteraard persoonsgegevens. Locatiegegevens, etniciteit, geslacht, biometrische gegevens, religieuze overtuigingen, webcookies en politieke opvattingen kunnen ook persoonsgegevens zijn. In de volgende paragrafen gaan we verder in op de soorten gegevens die bescherming behoeven.

Gegevensbescherming is belangrijk, want het voorkomt misbruik van de informatie van een individu of een organisatie, het beoogt verschillende privacy- en veiligheidsrisico's te voorkomen, zoals frauduleuze activiteiten, hacken, phishing en identiteitsdiefstal.

## 3.2. Soorten bedreigingen en misdrijven met betrekking tot persoonsgegevens en privacy

**1** **Identiteitsdiefstal**

Identiteitsdiefstal is het misdrijf waarbij persoonlijke of financiële informatie van een andere persoon wordt verkregen om diens identiteit te gebruiken om fraude te plegen, zoals het doen van ongeoorloofde transacties of aankopen. Identiteitsdiefstal wordt op verschillende manieren gepleegd en de slachtoffers blijven meestal achter met schade aan hun krediet, financiën en reputatie. De identiteitsdief kan uw informatie gebruiken om krediet aan te vragen, belastingen in te dienen of medische diensten te verkrijgen.

**2** **Online seksuele intimidatie**

Online seksuele intimidatie wordt gedefinieerd als ongewenst seksueel gedrag op elk digitaal platform en wordt erkend als een vorm van seksueel geweld. Online seksuele intimidatie omvat een breed scala aan gedragingen waarbij gebruik wordt gemaakt van digitale inhoud (afbeeldingen, video's, berichten, pagina's) op verschillende platforms (privé of openbaar).

## 3 Phishing

Bij phishing-aanvallen wordt frauduleuze communicatie verstuurd die afkomstig lijkt te zijn van een gerenommeerde bron. Het gebeurt meestal via e-mail. Het doel is om gevoelige gegevens zoals creditcard- en inloggegevens te stelen of om malware te installeren op de machine van het slachtoffer. Phishing is een veel voorkomende vorm van cyberaanval die iedereen zou moeten leren kennen om zich te beschermen.

## 4 Internetfraude en oplichting

Bij internetfraude worden onlinediensten en software met toegang tot het internet gebruikt om slachtoffers op te lichten of van hen te profiteren. De term "internetfraude" omvat doorgaans cybercriminele activiteiten die plaatsvinden via internet of e-mail, waaronder misdrijven als identiteitsdiefstal, phishing en andere hackactiviteiten die bedoeld zijn om mensen geld afhandig te maken.

## 5 Fraude met wenskaarten

Veel internetfraudeaanvallen richten zich op populaire gebeurtenissen om de mensen die ze vieren op te lichten. Dit omvat verjaardagen, Kerstmis en Pasen, die gewoonlijk worden gevierd door het delen van wenskaarten met vrienden en familieleden via e-mail. Hackers maken hier meestal misbruik van door kwaadaardige software te installeren in een e-mailwenskaart, die wordt gedownload en geïnstalleerd op het apparaat van de ontvanger wanneer deze de wenskaart opent.

## 6 Kredietkaartfraude

Kredietkaartfraude vindt doorgaans plaats wanneer hackers op frauduleuze wijze de krediet- of debetkaartgegevens van mensen bemachtigen in een poging geld te stelen of aankopen te doen. Om deze gegevens te verkrijgen, maken internetfraudeurs vaak gebruik van te mooi om waar te zijn aanbiedingen voor creditcards of bankleningen om slachtoffers te lokken. Een slachtoffer kan bijvoorbeeld een bericht van zijn bank ontvangen waarin hem wordt verteld dat hij in aanmerking komt voor een speciale lening, of dat hem een enorm geldbedrag als lening ter beschikking is gesteld.

## 7 Online Dating Oplichting

Een ander typisch voorbeeld van internetfraude is de overmaat aan online dating applicaties en websites. Hackers richten zich op deze apps om slachtoffers te verleiden tot het sturen van geld en het delen van persoonlijke gegevens met nieuwe liefdesinteresses. Oplichters maken meestal nepprofielen aan om met gebruikers te communiceren, een relatie op te bouwen, langzaam hun vertrouwen op te bouwen, een nepverhaal te creëren en de gebruiker om financiële hulp te vragen.

## 8 Loterijfraude

Een andere veel voorkomende vorm van internetfraude is e-mailoplichting waarbij slachtoffers wordt verteld dat ze de loterij hebben gewonnen. Deze oplichters informeren de ontvangers dat ze hun prijs pas kunnen opeisen nadat ze een kleine vergoeding hebben betaald.

9

**De Nigeriaanse Prins**

Bij deze zwendel wordt uitgegaan van een rijke Nigeriaanse familie of persoon die hun rijkdom wil delen in ruil voor hulp bij het verkrijgen van toegang tot hun erfenis. Het gebruikt phishing-tactieken om e-mails te sturen die een emotioneel verhaal schetsen, en lokt slachtoffers vervolgens naar een belofte van een aanzienlijke financiële beloning. De zwendel begint meestal met het vragen van een kleine vergoeding om te helpen met juridische processen en papierwerk, met de belofte van een grote som geld verderop in de keten.

10

**Spam**

Spam is elke vorm van ongewenste, ongevraagde digitale communicatie die in bulk wordt verstuurd. Vaak wordt spam verzonden via e-mail, maar het kan ook worden verspreid via tekstberichten, telefoongesprekken of sociale media.

## 3.3. Hoe cyberbeveiligingsdreigingen op sociale media/instellingen te melden

Alle sociale netwerken hebben mechanismen ingesteld voor het melden van verschillende soorten bedreigingen voor de cyberveiligheid, waaronder online haatzaaien, identiteitsdiefstal, seksuele intimidatie, cyberpesten, enz.

Hieronder vind je informatie over enkele van de populairste sociale netwerken:

### Facebook

- Facebook beveiligingsproblemen hebben meerdere categorieën. Er kan sprake zijn van beledigende inhoud of een haatpagina die je wilt melden, of misschien doet iemand zich voor als jou op Facebook, enz. De beste manier om beledigende inhoud of spam op Facebook te melden is via de link Rapporteren bij de inhoud zelf.

*https://www.facebook.com/help*

### Twitter

- In het Helpcentrum van Twitter kunt je informatie en ondersteuning vinden in geval van gecompromitteerde en gehackte accounts, over privacy, spam en nepaccounts, gevoelige en beledigende inhoud, beledigend gedrag en de melding daarvan.

*https://help.twitter.com/en*

## Instagram

- Berichten melden:

Als je een post, bericht of account ziet waarvan je denkt dat het in strijd is met de Community Guidelines van Instagram, kun je dit melden. Je kunt individuele stukken inhoud melden door op de drie puntjes boven een bericht te tikken, een bericht vast te houden of door een account te bezoeken en direct vanaf het profiel te rapporteren. Ga voor meer informatie naar het Helpcentrum van Instagram.

- Accounts rapporteren:

Accounts die in strijd zijn met de communityrichtlijnen van Instagram kunnen in-app of via een webformulier worden gemeld. Voor meer informatie kunt je het Helpcentrum raadplegen.

*https://help.instagram.com/*

## TikTok

- Voor vragen, zorgen of problemen met je profiel kun je informatie en ondersteuning vinden door onderstaande code te scannen. In de sectie Veiligheid kun je naar Een probleem melden en een LIVE video, een LIVE commentaar, een video, een commentaar, een direct bericht, een geluid, een hashtag, en je kunt ook iemand rapporteren. De stappen zijn heel eenvoudig te volgen, je hoeft alleen maar de optie Melden te vinden en de instructies te volgen.

*https://support.tiktok.com/en/*

## 3.3. Hoe risico's voor de beveiliging van gegevens te vermijden

Een van de belangrijkste dingen om onze gegevens te beschermen is een sterk wachtwoord. Dat komt goed van pas, want cybercriminelen bedenken tegenwoordig steeds nieuwe en innovatieve manieren om accounts te hacken en persoonlijke gegevens te bemachtigen.

Om uw gegevens beschermd te houden, is het bovendien raadzaam alleen websites te gebruiken die je vertrouwt. Veel mensen weten niet hoe ze moeten controleren of een website veilig is of niet.

1 Controleer allereerst of de URL de juiste spelling heeft, beveiligd is met "https" en een soort indicator heeft dat hij geverifieerd is, zoals een slotje.

2 Ten tweede, websites die er onveilig uitzien zijn dat meestal ook. Als de eigenaar van de website niet investeert in het uiterlijk en de gebruikerservaring, investeert hij waarschijnlijk ook niet in de veiligheid van de site.

3 Ten derde moet je kunnen nagaan of er contactinformatie beschikbaar is en een toegankelijk privacybeleid. Deze staan meestal helemaal onderaan de homepage. Een andere nuttige tip is het lezen van enkele getuigenissen en beoordelingen van de site van andere mensen, zodat je ervaringen kunt opdoen die andere mensen hadden met het gebruik van deze websites.

Er zijn ook andere praktijken die de digitale veiligheid in gevaar kunnen brengen, zoals het gebruik van openbare WIFI. Het is waar dat deze dienst die sommige hotels en luchthavens aanbieden gratis is, maar er hangt wel een prijskaartje aan.

Deze gratis WIFI-hotspots stellen hackers in staat zich te positioneren tussen de persoon die er gebruik van maakt en het verbindingspunt, dus in plaats van rechtstreeks met de hotspot te praten, sturen mensen hun informatie naar de hacker, die er vervolgens op vertrouwt.

**Hoe kunnen particulieren hun persoonsgegevens beschermen?**

**1** Beveilig uw rekeningen

**2** Bescherm uw surfen op het web

**3** Gebruik antivirussoftware op uw computer

**4** Werk uw software en apparaten bij

**5** Installeer geen software die je niet volledig kent en vertrouwt

**6** Schakel Bluetooth uit als je het niet gebruikt

**7** Wees overdreven voorzichtig met het delen van persoonlijke informatie

**8** Kijk uit voor imitators

**9** Deel niet te veel informatie op sociale netwerkplatforms

**10** Pas de privacy-instellingen van uw sociale netwerken aan

**11** Vergeet niet uit te loggen

**12** Open geen e-mails van mensen die je niet kent

**13** Sla geen wachtwoorden op in uw browser

**14** Gebruik geen socialemedia-inloggegevens om te registreren voor of aan te melden bij sites van derden

**15** Kies een veilige, betrouwbare e-mailprovider

## 4. Conclusie

In dit handboek worden Cyberpesten en Hate Speech toegelicht en in hun context geplaatst. Hun definities kunnen per land verschillen, maar beide worden beschouwd als agressie tegen andere mensen. In het geval van cyberpesten zijn er gewoonlijk drie factoren (de dader, het slachtoffer en de omstanders). In het geval van haatzaaien is het moeilijker om een gemeenschappelijk scenario vast te stellen, maar het gaat evenzeer om een persoon die discrimineert en de ontvanger die wordt gediscrimineerd.

Dit handboek bevat verschillende manieren om cyberpesten en haatzaaien te herkennen, aan te pakken en te melden, uiteraard afhankelijk van wie het slachtoffer is (uzelf, een collega, uw kinderen, enz.) maar ook van het wettelijk kader van het land.

In Spanje kun je bijvoorbeeld aangifte doen bij de politie, terwijl er in Nederland een nationale discriminatiehulplijn is. Daarnaast wordt getoond waarom begrippen als gegevensbescherming of CIAD-triade belangrijk zijn, evenals soorten privacybedreigingen zoals identiteitsdiefstal, online seksuele intimidatie, phishing of fraude.

Tot slot biedt dit document niet alleen definities of sleutelbegrippen met betrekking tot cyberpesten en haatzaaien, maar dient het ook als leidraad om dit soort misbruik te voorkomen, erop te reageren en het te melden.

#DigitSafe
Boosting digital safe spaces and resilience

Co-funded by the
Erasmus+ Programme
of the European Union

## Vragen & Informatie:

info@digit-safe.com

www.digit-safe.com