#DigitSafe

Versterking van digitale veilige ruimten en veerkracht

Handboek Digitale Veerkracht

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

#DigitSafe

#DigitSafe-Boosting digital safe spaces and resilience" beoogt 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.

Partners in het project

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

Introductie

Het project #DigitSafe-Boosting digital safe spaces and resilience in navolging van de EU Jongerenstrategie 2019-2017 in lijn met EU Jongerendoelstelling 6 "Informatie & Constructieve Dialoog" heeft als 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.
Het #DigitSafe-project streeft naar een bredere en diepere kennis bij jongeren over de twee hoofdthema's cyberveiligheid en haatspraak en veiligheid en privacy, in het bijzonder bij de meest kwetsbare groepen jongeren, naar het opbouwen van veiligere digitale gemeenschappelijke ruimten en praktijken en naar het vergroten van hun capaciteiten in termen van digitale weerbaarheid.
Dit project wil ook de volgende drie specifieke hoofddoelstellingen bereiken: -Het bevorderen van digitaal burgerschap onder jongeren in het deelnemende land door hen, in overeenstemming met de EU Jongerenstrategie 2019-2027, te voorzien van praktische en gebundelde informatie over Veiligheid & Privacy, Haatspraak & Cyberpesten. -jongeren, vooral kansarme jongeren die vaak niet over de nodige informatie- en datavaardigheden beschikken, de nodige competenties bijbrengen om hun digitale weerbaarheid te vergroten. -Een innovatieve methodologie ontwikkelen die de verzamelde relevante informatie in één handboek vertaalt in een multichannel bewustmakingscampagne, waarbij gebruik wordt gemaakt van de meest gebruikelijke audiovisuele communicatiepraktijken en -taal, instrumenten en trends onder jongeren.
Een multimediale en multikanalenstrategie die gebruik maakt van de enorme hoeveelheid mogelijkheden die het huidige sociale medialandschap biedt om inhoud te creëren en voor elke gebruiker toegankelijk te maken, met als doel jongeren beter in staat te stellen rationele keuzes te maken en hun digitale rechten te kennen.
Dit digitale weerbaarheidshandboek over cyberpesten, haatdragende taal, veiligheid en privacy zal op een alomvattende en uniforme manier begeleiding, praktische informatie (juridische bronnen, psychologische bronnen, tips, open leermiddelen en andere opleidingsbronnen) en belangrijke aanbevelingen bieden over verschillende onderwerpen voor jongeren om een meer diepgaande kennis te verwerven van hun rechten, digitale risico's en bedreigingen in de context van deze onderwerpen. Het zal jongeren bewuster maken 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 veiligere digitale wereld te bevorderen. Het zal een grote hoeveelheid informatie bundelen en op een meer bruikbare en alomvattende manier samenbrengen.
Dit handboek zal worden onderverdeeld in twee modules: Cyberpesten en haatdragende taal en veiligheid en privacy, die niet alleen informatie zullen verstrekken over het rechtskader, bewustmaking en preventie, maar ook actierichtlijnen, tips en aanbevelingen zullen bieden.

1. Cyberbullying

1. Cyberpesten

1.1 Wat is cyberpesten?

Op Europees niveau zijn er meerdere definities van cyberpesten gevonden, waarin een of ander aspect is verwerkt, afhankelijk van de specifieke kenmerken van elk van de landen waarin de studie is uitgevoerd (België, Bulgarije, Nederland en Spanje). De studie die in 2016 werd ontwikkeld door de beleidsafdeling Rechten van de burger en constitutionele zaken van het Europees Parlement "Cyberpesten bij 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, die wordt uitgevoerd door het gebruik van informatie- en communicatietechnologieën (ICT).”

Net als bij offline pesten zijn bij cyberpesten gewoonlijk de volgende 3 hoofdrolspelers betrokken, moet het gedrag opzettelijk en herhaaldelijk plaatsvinden en moet er sprake zijn van een onevenwicht in de machtsverhouding tussen de agressor en het slachtoffer:

- De dader.
De persoon die de agressie uitvoert.

- Het slachtoffer.
De persoon die de agressie ondergaat.

- Omstanders.
Degenen die zien wat er gebeurt tussen de pester en het slachtoffer, maar die niet direct betrokken zijn bij het pesten.

Wat de betrokken personen betreft, is het belangrijk erop te wijzen dat er een belangrijk verschil is tussen pesten en cyberpesten, namelijk dat de dader (de pester) anoniem kan blijven in het geval van cyberpesten, hij/zij kan zich verbergen onder een valse identiteit (of de identiteit van iemand anders) en het kunnen zelfs meerdere personen zijn die zich achter deze identiteit verschuilen. Cyberpesten laat niettemin een elektronisch spoor na - dat kan dienen als bewijs en als middel om dergelijk gedrag te stoppen. Ondanks deze verschillen komen face-to-face pesten en cyberpesten helaas vaak naast elkaar voor.

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

- Cyberpesten is kwaadwillig en nooit per ongeluk. De cyberpester heeft het duidelijke en bewuste doel het slachtoffer te schaden, pijn te doen, te vernederen, lichamelijk of geestelijk te laten lijden.

.

Het wordt uitgevoerd vanuit een machtspositie. De cyberpester is altijd in het voordeel en bekleedt een superioriteitspositie. Afhankelijk van de omgeving waarin cyberpesten plaatsvindt, kan het gaan om cyberpesten met een groep tegen één slachtoffer dat alleen is. Ook kunnen agressors misbruik maken van een niet-agressief of kwetsbaar slachtoffer, dat niet in staat is zichzelf te verdedigen.

- Het is herhaaldelijk gericht op het intimideren, kwaad maken of in verlegenheid brengen van de slachtoffers. Een op zichzelf staande agressieve actie is nog geen Cyberpesten. Het wordt Cyberpesten wanneer de agressie zich keer op keer herhaalt tegen dezelfde persoon (of dezelfde personen).

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

- Sociale netwerken.
- Messaging-platforms.
- platforms voor kansspelen
- mobiele telefoons

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

- Het verspreiden van leugens of het plaatsen van gênante foto's/video's van iemand op sociale media.

- Het versturen van beledigende berichten of bedreigingen via berichtenplatforms.

- Het versturen van kwaadaardige berichten onder de identiteit van iemand anders.

1.2 Leren over het belang van cyberpesten en de gevolgen ervan. Bewustmaking, hoe het te herkennen:

Cyberpesten herkennen

Een van de belangrijkste manieren om cyberpesten aan te pakken is door het te herkennen en op de waarschuwingssignalen te letten. Internationaal of op Europees niveau bestaat er geen algemeen aanvaarde definitie van cyberpesten. De Europese Commissie definieert cyberpesten echter als "het herhaaldelijk verbaal of psychisch lastigvallen van anderen door een individu of een groep via onlinediensten en mobiele telefoons". Volgens de Raad van Europa onderscheidt cyberpesten zich van andere vormen van pesten door het risico van openbaarheid, de complexe rol van de waarnemers en de omvang van het publiek dat digitale technologieën en communicatie met zich meebrengen.

WiredSafety, (de grootste groep ter wereld die zich bezighoudt met onlineveiligheid, -educatie en -hulp) is het niet eens met het voorstel dat cyberpesten "herhaaldelijk" moet voorkomen om als cyberpesten te worden aangemerkt. Sommige ernstige gevallen van cyberpesten hoeven niet herhaald te worden om als cyberpesten te worden aangemerkt. Bijvoorbeeld:

- Sextortion, sext-pesten en ernstige aanvallen op de reputatie (bv. aanvallen in verband met seksuele voorkeur, seksuele activiteit en andere soorten aanvallen op de reputatie die laster vormen)
- Bedreigingen met de dood of met ernstig lichamelijk letsel aan het doelwit of iemand in zijn naaste omgeving, bedoeld om het doelwit te verontrusten.

Om een tolerantere en veiligere online wereld te creëren, moet cyberpesten op bredere schaal worden aangepakt, zowel op individueel als op organisatorisch niveau.
Volgens een verslag van het Europees Parlement uit 2016 is de directe betrokkenheid van kinderen bij de ontwikkeling van oplossingen en beleid met betrekking tot cyberpesten erkend als een van de meest doeltreffende methoden om het probleem aan te pakken. Bovendien werd in een verslag van 2017 aan de Raad van Europa geconcludeerd dat, om cyberpesten aan te pakken, de stem van jongeren op Europees en nationaal niveau moet worden vertegenwoordigd en gehoord. Het is dan ook duidelijk dat de stem van jongeren voorop moet staan in deze discussies.
De gevolgen van cyberpesten mogen niet licht worden opgevat of als louter grapjes worden beschouwd, aangezien hierdoor niet alleen de emoties en het leed 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 velerlei manieren treffen. In sommige extreme gevallen kan cyberpesten zelfs leiden tot zelfmoord. Het #DigitSafe Consortium is tot deze conclusies gekomen na intensief onderzoek op Europees niveau in vier landen en de getuigenissen van slachtoffers van cyberpesten die in het kader van het project zijn verzameld. Social Networks and Cyberbullying among Teenagers, dat door het GCO is ontwikkeld, heeft bijgedragen tot een beter begrip van de omvang van de gevolgen van cyberpesten voor de slachtoffers die er het slachtoffer van zijn:
Als belangrijkste gevolgen van cyberpesten kunnen worden genoemd:
Slachtoffers kunnen zich verdrietig, beschaamd, in verlegenheid gebracht, dom, depressief, boos en angstig voelen. Slachtoffers verliezen meestal hun belangstelling voor de dingen waar ze vroeger van hielden, ze ontwikkelen een lager gevoel van eigenwaarde of ze

voelen zich geïsoleerd, niet in staat om met hun leeftijdgenoten te communiceren. Soms kunnen slachtoffers van cyberpesten "slachtoffer-agressors" worden, die het gedrag imiteren en anderen pesten

Met andere woorden, er is een reële kans dat cyberpesten diepe psychologische schade toebrengt aan de slachtoffers. Slachtoffers van cyberpesten zijn
*meer kans op depressie en angst
*meer kans op slechte schoolprestaties en gedragsproblemen op school
*Studenten die geweld en pesterijen meemaken, hebben meer kans om moeite te hebben met het ontwikkelen van democratische basiscompetenties zoals empathie, respect voor anderen, openheid voor andere culturen en geloofsovertuigingen, verdraagzaamheid en zelfvertrouwen

- Lichamelijke gevolgen

Door de stress en de angst die een slachtoffer ervaart, kan dit leiden tot lichamelijke problemen zoals zich moe voelen door slaapstoornissen of echte gezondheidsklachten krijgen zoals buikpijn of hoofdpijn.

- Juridische gevolgen

Het gevoel dat ze door anderen belachelijk worden gemaakt of worden gepest, weerhoudt de slachtoffers van cyberpesten er vaak van aangifte te doen of te proberen het probleem aan te pakken. Dit, in combinatie met de trage evolutie in de juridische classificatie van het misdrijf, betekent dat het vaak ongestraft blijft, en het moedigt de herhaling van aanvallen aan.
Bewustmaking van cyberpesten om het te voorkomen is van essentieel belang. De eerste stap om cyberpesten te onderkennen is een duidelijke definitie van wat het inhoudt. Om cyberpesten te voorkomen, zijn in Europa beleidsbeslissingen genomen en talrijke programma's opgesteld en uitgevoerd. Gezien de impact van dit fenomeen moeten de Europese instellingen echter onderzoek blijven doen, wetgeving opstellen en collectieve en individuele acties aanmoedigen om het aan te pakken

Gericht tot jongeren

Het Cyberbullying Research Center heeft een reeks gestructureerde tips ontwikkeld over hoe te werk te gaan om Cyberpesten te voorkomen en onszelf als gebruikers te beveiligen. Preventie is altijd de beste optie om dit probleem te bestrijden. Bovendien hebben we deze tips juist geselecteerd omdat de meeste ervan parameters hebben die veel meer gericht zijn op kinderen dan op jongvolwassenen:

- Blijf op de hoogte van privacy-instellingen.
Sociale Media sites en programma's wijzigen en updaten hun privacy instellingen regelmatig. 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 uw contactinformatie.
Geef uw e-mailadres of telefoonnummer niet aan mensen die u niet kent. Houd uw e-mailadres en telefoonnummer ook buiten social media-sites. Je weet nooit wie er toegang toe heeft en je kunt niet iedereen vertrouwen die een "vriend" of "volger" is.

- Leer internetetiquette

Om mogelijke problemen met andere internetgebruikers te voorkomen, moet u sociale conventies leren met betrekking tot interactie in cyberspace. Schrijf bijvoorbeeld niet in hoofdletters. Dit kan door sommigen als schreeuwen worden opgevat. Gebruik online ook geen sarcasme, want dat kan gemakkelijk verkeerd worden geïnterpreteerd.

- Stuur geen ongepaste foto's of video's.

Onthoud dat de vriend of vriendin van vandaag de geminachte minnaar van morgen kan zijn. Je wilt niet dat iemand met ongepaste foto's of video's van jou deze online plaatst en deelt met de rest van de wereld. Breng jezelf niet in de positie dat je je hier zorgen over moet maken.

- Google jezelf.

Je moet altijd weten wat er over je gezegd wordt. Het is vaak verrassend om informatie waarvan je dacht dat die privé was, te vinden in openbare databases, nieuwe artikelen of op social media-pagina's die door zoekmachines zijn geïndexeerd.

- Accepteer geen vriendverzoeken van vreemden

Als je de persoon die je een vriend of volgerverzoek 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-gebaseerde controles

Schakel de zoekopties op bepaalde sociale mediasites uit om te voorkomen dat het grote publiek naar je kan zoeken of je kan berichten. Zo heb je meer controle over met wie je online contact hebt, aangezien jij de enige bent die het initiatief kan nemen.

- Houd uw informatie beschermd

Als u een openbare of draadloze computer gebruikt, zorg er dan voor dat u zich afmeldt van elke site waarop u zich bevindt wanneer u wegloopt van die computer - al is het maar voor een minuut. Doe dit ook op uw andere mobiele apparaten als er een kans bestaat dat iemand langskomt en uw account gebruikt om grappig of ondeugend te zijn. Geef wachtwoorden aan niemand en wijzig uw wachtwoord regelmatig. Zorg er ook voor dat uw telefoon en tablet een wachtwoord hebben en vergrendeld zijn.

- Wees sceptisch bij online interacties

Zelfs onder 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 ook echt is - of dat ze alleen zijn.

- Waak voor mij en mensen

Onthoud dat sommige mensen veel tijd over hebben en het enige wat ze willen doen is anderen het leven zuur maken. Laat ze dat niet doen. Zet niet te veel persoonlijke of privé-informatie online die kan worden gebruikt om je lastig te vallen of te vernederen en weersta interactie met hen op welke manier dan ook. Zoals de conventionele wijsheid aangeeft. Voed de internet trollen niet!

Geadresseerd aan leerkrachten en ouders

Het is belangrijk dat organisaties, scholen, werkplekken en individuele personen zich inzetten om cyberpesten aan te pakken, vanwege de impact die cyberpesten kan hebben op de slachtoffers. Het door het Cyberbullying Research Center in 2021 ontwikkelde onderzoek "Cyberbullying: Identification, prevention and Response in 2021" geeft een uitgebreide uiteenzetting van hoe leerkrachten en ouders cyberpesten kunnen aanpakken op het vlak van identificatie en preventie:

De gemeenschap voorlichten over een verantwoord gebruik van de apparaten, gericht op digitaal burgerschap, is misschien wel de belangrijkste preventieve stap voor onderwijsinstellingen en hun leerkrachten/professoren. Leerlingen die zich bezighouden met het lastigvallen of bedreigen van anderen discipline bijbrengen en hen laten weten dat wat zij doen meer is dan verkeerd, het is een misdaad.

Het is van essentieel belang om in verschillende onderdelen van de leerplannen van onderwijsinstellingen passende online-inhoud op te nemen om cyberpesten en andere digitale bedreigingen te bespreken. Bovendien kunnen de boodschappen worden versterkt in andere lessen, vooral in die waarbij gebruik wordt gemaakt van technologie en digitale hulpmiddelen. Het creëren en versterken van een respectvolle en integere omgeving in de onderwijsinstellingen is van cruciaal belang waar schendingen en pesterijen formeel of informeel worden bestreden.

Bovendien wordt het tegenwoordig steeds belangrijker om nieuwe en creatieve strategieën te ontwikkelen om cyberpesten tegen te gaan, vooral om kleine vormen van pesterijen het hoofd te bieden en te voorkomen. Onderzoekers Hinduja en Patchin (2021) van het Cyberbullying Research Centre geven verschillende voorbeelden:

"Leerlingen kunnen worden gevraagd om anti-cyberpesten posters te maken die in de hele school worden opgehangen, of een public service announcement (PSA) video die een anti-pesten en/of een pro-vriendelijkheid boodschap overbrengt.
Oudere leerlingen kunnen worden gevraagd een korte presentatie te houden voor jongere leerlingen over het belang van ethisch verantwoord gebruik van technologie.

Ook hier gaat het erom het gedrag te veroordelen (zonder het kind te veroordelen) en tegelijkertijd de rest van de schoolgemeenschap de boodschap mee te geven dat pesten, in welke vorm dan ook, verkeerd is en niet getolereerd zal worden.

Met andere woorden, het is belangrijk dat niet alleen formeel onderwijs wordt gegeven, maar dat in het formele onderwijs op school ook non-formele en informele activiteiten worden opgenomen om cyberpesten vanuit een creatief oogpunt te bestrijden en te voorkomen.

Aan de andere kant "moeten ouders hun kinderen met woord en daad laten zien dat ze allebei hetzelfde eindresultaat willen: dat het cyberpesten stopt en dat het leven niet nog moeilijker wordt".
Het Cyberbullying Research Centre benadrukt hoe belangrijk het is om als ouder niet afwijzend te staan tegenover het perspectief van hun kinderen, maar om hun stem en mening te valideren. Het is van vitaal belang dat doelwitten van cyberpesten en omstanders weten dat de volwassenen, aangezien zij kennis hebben van de cyberpesten-situatie, "rationeel en logisch zullen ingrijpen en de situatie niet erger zullen maken".

Hoe moeten ouders reageren als zij ontdekken dat hun eigen kind een cyberpester is? In de eerste plaats moeten zij hem/haar uitleggen hoe dat gedrag in de echte wereld uitlokt en schade en pijn toebrengt. Daarna moeten ouders hem/haar de kans geven om verder te gaan en dat gedrag te beëindigen. Onderzoekers Hinduja en Patchin (2021) stellen ouders voor om "empathie te kweken door hen opzettelijk in situaties te brengen die hen ongemakkelijk maken en die hun hart kunnen verzachten". Kinderen moeten weten dat elke actie, zelfs als die online is, ernstige gevolgen heeft. Van de kant van de ouders is het essentieel om meer aandacht te besteden aan het gedrag en de handelingen 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):

De bundeling van procedures en tips over hoe te werk te gaan, is vooral gevormd door de meer dan afgeronde voorstellen van het Cyberbullying Research Center en Amnesty Jeunes.

Als je zelf slachtoffer bent
Als je zelf slachtoffer bent, willen we je graag een aantal stappen adviseren die je kunt volgen als je last hebt van cyberpesten:
- Zoek hulp
Eerst en vooral moet je praten, overleggen met familie of professionals!
- Meld de inhoud

Als het cyberpesten via een sociaal netwerk is gebeurd, 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 zij actie kunnen ondernemen, soms na meerdere meldingen.
- Bescherm jezelf
Wijzig uw wachtwoord, vergroot de privacy van uw berichten, verwijder persoonlijke informatie zoals uw e-mailadres, telefoonnummer of links naar andere accounts.
Verwijder als tijdelijke maatregel uw account of verander uw bijnaam
Probeer je een tijdje af te sluiten van sociale netwerken, blokkeer de persoon die de bron is van het cyberpesten.

- Antwoord en herinner de persoon die u lastigvalt aan het wettelijke kader door erop te wijzen dat online pesten een misdrijf is dat bij wet strafbaar is.
- Als het in de werkomgeving gebeurt, praat dan met je werkgever

Laat uw werkgever weten of de persoon die u lastigvalt een collega is, of dat het pesten plaatsvindt op een werkgerelateerd forum of blog. Als de pesterijen je verhinderen je werk te doen, moet je werkgever dat weten.

- Verbreek de banden.

Sluit geen vriendschap met de gemeneriken en probeer ze niet naar je toe te lokken. Als u het gevoel hebt dat u moet reageren op de persoon die u mishandelt, doe dat dan met respect. Probeer niet te rationaliseren of vrienden te worden met iemand die wreed is tegen anderen.

Degenen die cyberpesten willen dat je reageert. Het probleem is dat als je boos reageert, degene die pest zich kan voeden met die reactie en doorgaat (en zelfs de ernst van het cyberpesten kan laten escaleren). Bovendien kunnen er consequenties aan je reactie verbonden zijn.

- Neem contact op met de internetprovider (ISP)

Probeer contact op te nemen met de internetprovider van de persoon die je intimideert, als deze is geïdentificeerd. De ISP kan dan contact met de persoon opnemen of misschien zijn internetaccount direct afsluiten.

- Dien een klacht in door naar een politiebureau te gaan

Neem bewijzen van de aanval mee (bijvoorbeeld screenshots). De politie zal nota nemen van uw klacht en alle informatie in verband met uw klacht in een verslag opnemen. U krijgt een kopie van het verslag en een bewijs van klacht. Het proces-verbaal wordt vervolgens naar het parket gestuurd, d.w.z. naar de magistraten die bevoegd zijn voor de onderzoeken. Vraag naar het nummer van het proces-verbaal om de zaak te kunnen volgen en om te weten welk parket (van welke gemeente) bevoegd is.

- Meld het cyberpesten door publiekelijk

Screenshots van de pester te delen (zorg ervoor dat je de gebruikersnaam en profielfoto van de pester verbergt, zodat je niet van smaad wordt beschuldigd).

Als collega (op het werk of op school)

Op dit gebied heeft Save the Children zeer accuraat enkele richtlijnen gegeven over hoe te handelen in geval van pesten:

- Je kunt in deze situatie angst of afwijzing voelen, maar onderneem actie.
- Als je ziet dat je het niet in je eentje kunt stoppen en dat het niet het beste is om te doen, vraag dan een volwassene of een verantwoordelijke om hulp. Dit is geen verklikken, het is een steun zijn voor wie in nood verkeert.
- Steun de collega die gepest wordt. Niemand verdient het om slecht behandeld te worden.
- Stel voor om in je onderwijsinstelling of bedrijf een training te geven of materiaal te ontwikkelen om mensen bewust te maken van het belang van preventie van cyberpesten en het zoeken van hulp.

Als leerkracht

moeten leerkrachten letten op verschillende signalen die erop kunnen wijzen 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 als anderen in de buurt zijn en een discussie uit de weg gaat, moet daar rekening mee worden gehouden.

Daarnaast moeten leerkrachten kinderen ook helpen cyberpesten te herkennen, erop te reageren en het te vermijden. Enkele richtlijnen zouden zijn:

- Communicatie is erg belangrijk, dus als je ooit denkt dat een kind wordt gecyberpest, spreek hem of haar 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.
- Zorg voor een veilige klasomgeving. Help kinderen emotionele intelligentie te ontwikkelen, zodat ze zelfbewustzijn en zelfregulatievaardigheden kunnen aanleren en leren hoe ze empathie voor anderen kunnen hebben.
- Moedig leerlingen aan om 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 hen na te denken voor ze iets posten.

- Leg leerlingen uit op welke drie manieren 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 opstander en als je slachtoffer bent van cyberpesten, moet je dit melden aan een volwassene.

Als een ouder

Het is zeer waarschijnlijk 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 omdat ze het pesten niet zelf kunnen oplossen, ze kunnen bang zijn dat ouders de dingen zullen aanpakken op een manier die het pesten doet escaleren, of dat ze het probleem niet zullen begrijpen. Om deze redenen moeten ouders, als zij signalen bij hun kinderen zien, onmiddellijk actie ondernemen. Probeer in de eerste plaats met uw kind te praten en naar hem te luisteren. De beste manier om dit te doen is hem op een rustige manier te laten praten over wat er aan de hand is. Neem de tijd om te begrijpen wat er precies is gebeurd en in welke context. Het is heel belangrijk voor je kind dat je de situatie niet bagatelliseert. Omdat sociale media een verlengstuk zijn geworden van het dagelijkse leven van kinderen, kan een nare opmerking of sms'je verwoestend voor hen zijn. Als u uw kind prijst voor het feit dat hij het juiste heeft gedaan door er met u over te praten, is dat een goede manier om het vertrouwen tussen u en uw kind te vergroten.

Als je het eenmaal weet, bied dan troost en onvoorwaardelijke steun, omdat slachtoffers van cyberpesten vaak een gevoel van isolement ervaren. Laat je kind zien dat er met deze situatie kan worden omgegaan op een manier die geen online vergelding inhoudt. Zorg dat uw kind zich veilig voelt, dat moet de hoogste prioriteit zijn, evenals uw kind laten weten dat het niet zijn schuld is. Probeer daarna zo veel 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. Houd alle incidenten bij om te helpen bij het onderzoeksproces. Maak ook aantekeningen over relevante details zoals de locatie, de frequentie, de ernst van de schade, de betrokkenheid van derden of getuigen, en het achtergrondverhaal. De volgende stap is contact opnemen met de aanbieder van de inhoud, aangezien cyberpesten altijd in strijd is met de servicevoorwaarden van alle legitieme serviceproviders. Zij moeten actie ondernemen in deze zaak, zodat uw kind er niet opnieuw last van heeft.

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

Ouders kunnen ook contact opnemen met de politie voor het geval de genoemde situatie niet helpt om beter te worden.

Als het nodig is, kunt u proberen om uw kind in therapie te laten gaan. Kinderen kunnen er baat bij hebben om met een professional uit de geestelijke gezondheidszorg te spreken. Zij kunnen de voorkeur geven aan een gesprek met een derde partij die als objectiever kan worden beschouwd. het slachtoffer worden van cyberpesten, zij dit moeten melden bij hun ouders of leerkrachten.

1.4 Preventiemaatregelen

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

Allereerst is het belangrijk om overal wachtwoorden voor te gebruiken en deze wachtwoorden met niemand te delen. Een goede manier om de onlineveiligheid van kinderen te verbeteren is gebruik te maken van de privacytools en -instellingen van sociale media. We moeten ervoor zorgen dat kinderen op de hoogte zijn van de privacy-instellingen en -hulpmiddelen die door de organisatie worden aangeboden en we moeten elke sociale media doorlopen en de privacy-instellingen op de meest veilige instellen. Dit betekent dat accounts privé moeten worden gemaakt, dat mensen hen niet mogen taggen enzovoort.

Kinderen moeten weten dat het belangrijk is om persoonlijke zaken privé te houden. Ze mogen nooit hun adres, mobiele 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 geldt ook voor het uitloggen bij e-mail, social media-accounts, hun schoolaccount of een andere account die ze openen.

Ten slotte, maar misschien wel het belangrijkst: kinderen moeten weten dat als zij ooit het

1.5 Hoe kan cyberpesten worden gemeld (rechtskader, 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, is er op dit gebied nog geen vooruitgang geboekt met de wetgeving. Daardoor is het werk van instellingen en organisaties van essentieel belang geworden om gevallen te helpen opsporen, aan de kaak te stellen en de slachtoffers te steunen:

Belgium

Wettelijk kader

Cyberpesten wordt in België beschouwd als een "strafbaar feit", en is dus strafbaar. Toch bestaat er, net als in veel andere landen, geen specifiek strafrecht met betrekking tot cyberpesten.

Dit betekent echter niet dat het strafbare feit onbestraft blijft, maar wel via andere Belgische wetten:

- Art. 442 bis & art. 442 ter van het Belgisch Strafwetboek = Intimidatie.

"Wie in het openbaar schadelijke leugens vertelt die de eer of de goede naam van een ander kunnen schaden, pleegt een inbreuk op artikel 442 van het Belgisch Strafwetboek".

- Art. 422 bis van het Belgisch Strafwetboek = Stalking

-

- Art. 145.3bis van de wet van 13/06/2005 met betrekking tot elektronische communicatie, smaad en laster

-

- Art. 448 van het Belgisch Strafwetboek= Openbare belediging

-

-

- Art. 383 van het Belgisch Strafwetboek= Openbare zedenschennis

-

-

Cyberpesten is een relatief recent en onontgonnen fenomeen in de arbeidswereld, ondanks het alomtegenwoordige gebruik van ICT in de hedendaagse werkomgeving en ondanks de recent goedgekeurde ILO-conventie inzake geweld en pesterijen van 2019 (nr. 190) en de begeleidende aanbeveling nr. 206, die geweld en pesterijen die ook plaatsvinden "via werkgerelateerde communicatie, met inbegrip van communicatie die mogelijk wordt gemaakt door informatie- en communicatietechnologieën", in hun toepassingsgebied opnemen. In België zijn deze bepalingen opgenomen in de wetgeving inzake veiligheid en gezondheid op het werk (OSH).

Instellingen & NGO's

Als cyberpesten zich in België voordoet in een onderwijsinstelling, kunnen deze instellingen op grond van interne voorschriften en interne regels sancties opleggen.

Daarnaast zijn er een aantal organisaties en platformen die steun en oriëntatie bieden aan slachtoffers die hulp zoeken vóór het gerechtelijke proces dat in de meeste gevallen complex, moeilijk en traumatisch is voor de jongere.

- Cyber Hulp

Een gezamenlijk initiatief van de Belgische federale politie, de universiteit van Bergen en de Federatie Wallonië-Brussel. Het is een app tegen cyberpesten, om het te melden via je eigen smartphone. De app bevat een knop waarmee ze een screenshot kunnen maken van hun chatgeschiedenis met een cyberpester en een tweede knop waarmee ze deze inhoud vervolgens kunnen doorsturen naar de mensen die in hun onderwijsinstelling belast zijn met de afhandeling van dergelijke situaties. In 2021 zal het CyberHelp-team de app aan 12.000 leerlingen presenteren door ongeveer 100 bezoeken te brengen aan scholen in Wallonië en Brussel.

Amnesty Jeugd België

Tele-Helpdesk Brussel

Télé-Accueil is een telefoon- en chatdienst. Wie "iemand om mee te praten" zoekt, vindt via 107 nummer een luisterend oor, gratis, 24 uur per dag, 7 dagen per week, in anonimiteit en vertrouwelijkheid. Het is een uitstekende optie voor slachtoffers die uit verlegenheid of omdat ze niet weten hoe ze moeten omgaan met cyberpesten, cybercriminaliteit of haatdragende taal, hulp krijgen en een luisterend oor en advies krijgen.

Spanje:

Wanneer cyberpesten plaatsvindt, zijn er verschillende dingen waar je op moet letten. In de eerste plaats mag u niet antwoorden op cyberpesten of berichten doorsturen en moet u de persoon die u pest blokkeren. Het is belangrijk om bewijzen van cyberpesten te bewaren. Noteer data, tijdstippen en beschrijvingen van het cyberpesten.
Het is mogelijk om pesten te melden, zowel via het platform waar het plaatsvindt als op legale wijze, bijvoorbeeld bij de politie.
Lees bij het melden via het platform eerst de voorwaarden en bepalingen of de gedeelten over rechten en verantwoordelijkheden. Hierin wordt beschreven welke inhoud wel of niet gepast is. Meld cyberpesten vervolgens bij de sociale-mediasite, zodat zij actie kunnen ondernemen tegen gebruikers die de servicevoorwaarden schenden. Anderzijds, wanneer cyberpesten dreigen met geweld, kinderporno of het versturen van seksueel expliciete berichten of foto's of stalking en haatmisdrijven inhoudt, wordt het beschouwd als een misdrijf. In deze gevallen moet aangifte worden gedaan bij de politie

Er zijn stichtingen die steun en hulp bieden aan kinderen of jongeren en hun families die niet weten hoe ze met deze kwestie moeten omgaan of hoe ze aangifte moeten doen.

Bijvoorbeeld:

- Cybersmile (https://www.cybersmile.org/who-we-are). Het is een non-profitorganisatie die zich inzet voor digitaal welzijn en het aanpakken van alle vormen van pesten en misbruik online.
- AEPAE (https://aepae.es/plan-nacional). Het is een vereniging voor de preventie van pesten in Spanje. Het doel van deze vereniging is het ontwikkelen van preventief gedrag bij kinderen en adolescenten gericht op het oplossen van conflicten in de schoolomgeving.
- INFOACOSO(https://infoacoso.es/telefonos-de-ayuda-contra-el-acoso-y-el-bullying). Deze vereniging biedt op haar website een gids aan over hoe te handelen als je wordt gecyberpest en waar je kunt bellen om dit te melden, afhankelijk van de gemeenschap van Spanje waar je woont.

.

Nederland:

In Nederland kunnen de volgende instellingen en instanties u helpen als u slachtoffer bent van cyberpesten:

MiND- het meldpunt voor internetdiscriminatie dat meldingen van discriminatie op internet registreert en beoordeelt.

Benader een antidiscriminatievoorziening bij jou in de buurt. Alle gemeenten in Nederland hebben een antidiscriminatievoorziening waar je terecht kunt met een vraag of klacht over discriminatie.

Bel de landelijke discriminatiehulplijn (0900 235 5345)

Neem contact op met de politie als u bent lastiggevallen, geïntimideerd, bedreigd of erger

Sommige van de hierboven genoemde diensten zijn specifiek voor mensen die met discriminatie te maken hebben gehad. Discriminatie wordt meestal gedefinieerd als de ongelijke behandeling van een andere persoon op grond van zijn etnische afstamming, geslacht, geslacht of genetische kenmerken. Discriminatie is verboden op grond van de EU-wetgeving:

Artikel 21: ‘Elke discriminatie, met name op grond van geslacht, ras, kleur, etnische of sociale afkomst, genetische kenmerken, taal, godsdienst of overtuigingen, politieke of andere denkbeelden, het behoren tot een nationale minderheid, vermogen, geboorte, een handicap, leeftijd of seksuele geaardheid, is verboden’.

Aangezien cyberpesten vele vormen kan aannemen, kan het zijn dat je het gevoel hebt het slachtoffer te zijn van cyberpesten die niet specifiek discriminerend zijn. In dergelijke gevallen **zijn enkele suggesties:**

Meld het cyberpesten op school/werk (als je wordt gepest door iemand op je school/werkplek)

Stop Online Pesters is een Nederlands interventieschema op maat voor laagopgeleide slachtoffers van cyberpesten, bedoeld om slachtoffers te leren omgaan met cyberpesten en de negatieve gevolgen ervan.

Blokkeer en meld de cyberpester op je social media kanalen

Blokkeer en meld het nummer van de pester

Informatie opvragen bij de plaatselijke politie

Doe aangifte bij de politie (als dit na overleg met de politie de beste manier van handelen wordt geacht)

Bulgarije

Cybermisdrijven, waaronder cyberpesten, privacy- en veiligheidsrisico's online, worden gemeld bij de afdeling cybercriminaliteit van het ministerie van Binnenlandse Zaken van Bulgarije. Het is een algemeen meldingsmechanisme voor niet-dringende signalen van cybercriminaliteit (voornamelijk gericht op cyberfraude en kinderpornografie). Het programma wordt gecoördineerd door de afdeling cybercriminaliteit van het directoraat-generaal voor de bestrijding van de georganiseerde misdaad van het ministerie van Binnenlandse Zaken.
Via een onlineformulier kunnen cyberpesten, cyberfraude en kinderpornografie worden gemeld. Voor dringende gevallen wordt mensen aangeraden zich te melden via het algemene alarmnummer 112.
Website: www.cybercrime.bg
Telefoon: 112 (in geval van nood en dringende zaken)

Er is ook een door de overheid beheerd mechanisme voor steun en advies aan kinderen en jongeren over verschillende zaken, waaronder cyberpesten, haatzaaien en privacy- en veiligheidsrisico's online. Dit mechanisme is de nationale telefoonlijn voor kinderen 116 111, die wordt beheerd door het staatsagentschap voor kinderbescherming en tot doel heeft alle kinderen en hun families in Bulgarije te helpen. De telefonisten die de oproepen beantwoorden zijn opgeleide psychologen die 24 uur per dag, 7 dagen per week, anoniem en volledig gratis klaar staan om te luisteren, te steunen, te overleggen en de bellers te begeleiden bij alle kwesties die hen bezighouden.


2. Haatdragende Taal

2.1 Wat is haatdragende taal?

Er is geen universeel aanvaarde definitie van haatzaaien. In deze paragraaf zullen we een paar definities schetsen die zowel in de EU-wetgeving als door toonaangevende organisaties die haatzaaien bestrijden, worden gegeven.

‘(Illegale) haatzaaiende meningsuiting wordt in de EU-wetgeving gedefinieerd als "het publiekelijk aanzetten tot geweld of haat op grond van bepaalde kenmerken, zoals ras, huidskleur, godsdienst, afstamming en 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.’

INACH (het leidende netwerk in de EU en wereldwijd ter bestrijding van cyberhaat) definieert haatdragende taal als:

"De opzettelijke of onopzettelijke openbare discriminerende en/of lasterlijke uitspraken; het opzettelijk aanzetten tot haat en/ of geweld en/ of segregatie op grond van iemands of een groep mensen werkelijke of vermeende ras, etniciteit, taal, nationaliteit, huidskleur, geloofsovertuiging of het ontbreken daarvan, geslacht, geslachtsidentiteit, geslacht, seksuele geaardheid, politieke overtuiging, sociale status, geboorte, leeftijd, geestelijke gezondheid, handicap, ziekte.’

In de EU-wetgeving worden de vrijheid van meningsuiting beschermd, waardoor sommigen menen dat er een conflict bestaat tussen de bescherming van de vrijheid van meningsuiting en de strafbaarstelling van haatzaaien. Veel deskundigen stellen dat dit vermeende "belangenconflict" tussen de strafbaarstelling van haatzaaien en de bescherming van de vrijheid van meningsuiting verkeerd wordt begrepen. In feite verbiedt het Internationaal Verdrag inzake burgerrechten en politieke rechten (IVBPR) "het aanzetten tot nationale, raciale of religieuze haat, dat aanzet tot discriminatie, vijandigheid of geweld". In deze korte video wordt dit misverstand verder toegelicht en wordt uitgelegd waarom vrijheid van meningsuiting niet absoluut is.

De "piramide van haat" (hieronder afgebeeld) geeft het gevaar aan van alle vormen van haatzaaiende taal:

De piramide van haat wordt gebruikt om te illustreren hoe haatdragende taal in het verleden (en ook nu nog) een voorloper is van extreem geweld. Het is de bedoeling te benadrukken hoe haatdragende taal een bedreiging kan vormen voor anderen door bij te dragen tot de piramide van haat en geweld. Het aanpakken van haatzaaiende taal is dan ook essentieel voor het creëren van een vreedzamere en tolerantere wereld.

2.2 Hoe haatzaaien te voorkomen

Haatzaaien wordt op EU-niveau aangepakt door de richtlijn audiovisuele mediadiensten (AMSD), die de nationale autoriteiten in elk EU-land verplicht ervoor te zorgen dat audiovisuele mediadiensten niet aanzetten tot haat.

Daarnaast is de Commissie op EU-niveau met Facebook, Microsoft, Twitter en Youtube een "gedragscode voor het bestrijden van illegale haatzaaiende uitlatingen online" overeengekomen. De toepassing van deze gedragscode wordt regelmatig gecontroleerd met een netwerk van organisaties in de hele EU.

Hoe kun je op individueel niveau haatzaaien voorkomen?

Eén manier om haatzaaien te bestrijden is het blokkeren en melden van haatzaaiende uitlatingen die u online tegenkomt (zie de volgende paragraaf over tips voor het melden van haatzaaiende uitlatingen). De Verenigde Naties bevelen de volgende praktijken aan om haatzaaien te voorkomen:

- Pauzeer - weerhoud uzelf ervan haatdragende opmerkingen te maken en/of dergelijke inhoud te delen
- Fact check - zorg ervoor dat je valse en bevooroordeelde informatie opspoort voordat je verkeerde informatie verspreidt
- Uitdagen - verspreid je eigen tegenspraak en daag haatdragende taal waar mogelijk uit
- Ondersteunen- neem een publiek standpunt in en betuig je solidariteit aan slachtoffers van haatdragende taal
- Melden- bekijk de gemeenschapsrichtlijnen van de sociale-mediaplatforms die je gebruikt en meld gevallen van haatdragende taal die deze richtlijnen schenden. Voor ernstigere gevallen kun je een klacht indienen bij de politie (bv. wanneer er wordt aangezet tot geweld).
- Opvoeden - deel voorlichtingsmateriaal en publieke campagnes of ga in gesprek met je vrienden en familie
- Zet je in - overweeg je aan te sluiten bij een NGO of een initiatief dat zich inzet om haatzaaien in jouw gemeenschap aan te pakken.

Om meer te weten te komen over haatzaaien en manieren om haat te voorkomen, kun je jezelf testen door deze quiz van de Verenigde Naties te doen.

2.3 Hoe kan ik haatzaaien melden?

INACH is een toonaangevend netwerk binnen de EU en wereldwijd dat zich inzet voor de bestrijding van cyberhaat. Het is een stichting naar Nederlands recht en is gevestigd in Amsterdam, maar heeft 32 leden uit 28 landen. De website van INACH biedt een online meldplatform waar incidenten van cyberhaat kunnen worden gemeld. Naast het aanbieden van een klachten- en meldpunt tegen cyberhaat, gebruikt INACH de gegevens van alle ontvangen klachten om rapporten en analyses te schrijven. Op deze manier probeert INACH invloed uit te oefenen op het publiek, sociale mediabedrijven en internationale instellingen, wat hen helpt bij het lobbyen voor internationale wetgeving tegen cyberhaat.

Naast het melden van gevallen van cyberhaat via INACH, kunnen gebruikers ook rechtstreeks melding maken van gevallen van haatzaaien via het socialemediakanaal waarin zij dit tegenkomen. Op de website van de Raad van Europa staat informatie over hoe je aangifte kunt doen op sociale mediakanalen. In sommige gevallen hoeft u geen account te hebben om een melding te kunnen doen. Op Facebook bijvoorbeeld kunt u dit online formulier invullen zonder een Facebookaccount te hebben of daarop ingelogd te zijn.

Sommige Europese landen hebben nationale meldingsprocedures en -mechanismen voor haatdragende taal, haatmisdrijven en cyberpesten ingevoerd als onderdeel van de "No Hate Speech Youth Campaign" van de Europese Raad. De lijst van landen en hun meldingsprocedures is te vinden op de website van de Raad van Europa.

Andere suggesties voor het melden van haatdragende taal zijn

Meld de haatzaaiende uitlatingen bij de politie
Doe aangifte bij een gezaghebbend orgaan, bijvoorbeeld een civiele of administratieve rechtbank
Doe aangifte bij een NGO, bijvoorbeeld MiND is het nationale meldpunt in Nederland voor haatzaaiende en discriminerende inhoud.
Praat met iemand die je vertrouwt - bijvoorbeeld een ouder, vriend, leraar

3. CYBERVEILIGHEID EN PRIVACY

3.1. Waarom is de bescherming van persoonsgegevens belangrijk?

De term bescherming van persoonsgegevens is gedefinieerd in art. 4, lid 1, van de Algemene verordening gegevensbescherming: persoonsgegevens zijn alle informatie die betrekking heeft op 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 nader in op de soorten gegevens die bescherming behoeven.

Gegevensbescherming is belangrijk, omdat het misbruik van de informatie van een individu of een organisatie voorkomt, en verschillende privacy- en veiligheidsrisico's beoogt te voorkomen, zoals frauduleuze activiteiten, hacking, phishing en identiteitsdiefstal (beschreven in de volgende paragraaf).

Het soort gegevens dat moet worden beschermd

Vitale informatie, zoals namen, adressen, e-mailadressen, telefoonnummers, gezondheidsinformatie of bankgegevens zijn allemaal gegevens die zorgvuldig moeten worden opgeslagen en beschermd. Als dergelijke informatie in verkeerde handen terechtkomt, kan dit de veiligheid van mensen in vele vormen in gevaar brengen, waaronder persoonlijke integriteit, fysieke veiligheid en financiële zekerheid. Gestolen informatie kan ook worden gebruikt om valse profielen aan te maken en fraude te plegen.

Voorbeelden van persoonsgegevens zijn

- een naam en achternaam;
- een huisadres
- een e-mailadres, zoals name.surname@company.com;
- een identiteitskaartnummer
- locatiegegevens (bijvoorbeeld de locatiegegevensfunctie op een mobiele telefoon)*;
- een Internet Protocol (IP)-adres
- een cookie-ID*;
- de reclame-identificatie van uw telefoon
- gegevens van een ziekenhuis of een arts, bijvoorbeeld een symbool dat een persoon op unieke wijze identificeert.
- Voorbeelden van gegevens die niet als persoonsgegevens worden beschouwd, zijn
- een registratienummer van een bedrijf
- een e-mailadres, zoals info@company.com;
- geanonimiseerde gegevens - persoonsgegevens die zodanig zijn geanonimiseerd dat de betrokkene niet of niet meer identificeerbaar is, worden niet langer als persoonsgegevens beschouwd. Om echt anoniem te zijn, moet de anonimisering onomkeerbaar zijn.

Wie is verantwoordelijk voor de bescherming van onze gegevens?

Gegevensbescherming is het proces waarbij belangrijke informatie wordt beschermd tegen corruptie, compromittering of verlies. Het belang van gegevensbescherming neemt toe naarmate de hoeveelheid gegevens die wordt gecreëerd en opgeslagen ongekend snel blijft toenemen. Daarom moeten organisaties die persoonlijke informatie opslaan en beheren, ervoor zorgen dat die informatie gevrijwaard blijft van corruptie, compromittering of verlies. In de Europese Unie beschermt de General Data Protection Regulation (GDPR) de persoonsgegevens van de EU-burgers. Het is de strengste privacy- en beveiligingswet ter wereld. Hoewel de GDPR is opgesteld en aangenomen door de Europese Unie (EU), legt deze verplichtingen op aan organisaties overal ter wereld, zolang zij zich richten op of gegevens verzamelen over mensen in de EU. De verordening is op 25 mei 2018 in werking getreden.

Belangrijkste elementen van gegevensbescherming

Een zeer belangrijk model voor gegevensbescherming is de CIA-triade, waarbij de drie letters van de naam staan voor de drie elementen van gegevensbescherming: vertrouwelijkheid, integriteit en beschikbaarheid. Dit model is ontwikkeld om personen en organisaties te helpen een holistische benadering van gegevensbescherming te ontwikkelen. De drie elementen worden als volgt gedefinieerd:

- Vertrouwelijkheid: De gegevens worden alleen opgevraagd door geautoriseerde operators met de juiste geloofsbrieven.
- Integriteit: Alle gegevens die binnen een organisatie zijn opgeslagen, zijn betrouwbaar, nauwkeurig en niet onderhevig aan ongerechtvaardigde wijzigingen.
- Beschikbaarheid: De opgeslagen gegevens zijn veilig en direct beschikbaar wanneer dat nodig is.

Volgens de GDPR zijn er ook verschillende beginselen van de bescherming van persoonsgegevens waaraan organisaties die deze verzamelen en beheren moeten voldoen:

- Rechtmatigheid, billijkheid en transparantie - De verwerking moet rechtmatig, billijk en transparant zijn voor de betrokkene.
- Beperking van het doel - De voor de verwerking verantwoordelijke moet de gegevens verwerken voor de legitieme doeleinden die uitdrukkelijk aan de betrokkene zijn aangegeven toen hij ze verzamelde.
- Gegevensminimalisering - De voor de verwerking verantwoordelijke mag slechts zoveel gegevens verzamelen en verwerken als absoluut noodzakelijk is voor de gespecificeerde doeleinden.
- Nauwkeurigheid - De verantwoordelijke voor de verwerking moet de persoonsgegevens nauwkeurig en actueel houden.
- Opslagbeperking - De verantwoordelijke voor de verwerking mag persoonlijk identificeerbare gegevens slechts zo lang opslaan als voor het gespecificeerde doel noodzakelijk is.
- Integriteit en vertrouwelijkheid - De verwerking moet op zodanige wijze geschieden dat passende beveiliging, integriteit en vertrouwelijkheid worden gewaarborgd (bijvoorbeeld door gebruikmaking van encryptie).
- Verantwoordingsplicht - De voor de verwerking verantwoordelijke is verantwoordelijk voor het kunnen aantonen van de naleving van al deze GDPR-beginselen.

Het belang van gegevensbescherming neemt toe naarmate de hoeveelheid gecreëerde en opgeslagen gegevens met ongekende snelheid blijft toenemen. Er is ook weinig tolerantie voor downtime die het onmogelijk kan maken om toegang te krijgen tot belangrijke informatie. Zoals hierboven uiteengezet, zijn organisaties die persoonsgegevens verzamelen, opslaan en beheren verantwoordelijk voor het garanderen dat deze gegevens niet worden misbruikt en op elk moment beschikbaar zijn voor geautoriseerd personeel. De GDPR garandeert dit door middel van concrete wettelijke voorschriften en sancties voor de organisaties die zich daar niet aan houden. Aan de andere kant kunnen personen zich beveiligen tegen ongewenste pogingen van externe partijen om toegang te krijgen tot hun gegevens, en hun privacy beschermen tegen degenen met wie zij geen toestemming geven om hun persoonlijke informatie te delen.

3.2 Soorten bedreigingen en misdrijven in verband met persoonsgegevens en privacy.

- Identiteitsdiefstal

Identiteitsdiefstal is het misdrijf waarbij de persoonlijke of financiële informatie van een andere persoon wordt verkregen om diens identiteit te gebruiken voor het plegen van fraude, zoals het doen van ongeoorloofde transacties of aankopen. Identiteitsdiefstal kan op verschillende manieren worden gepleegd en de slachtoffers lopen meestal schade op aan hun krediet, financiën en reputatie. De identiteitsdief kan uw informatie gebruiken om krediet aan te vragen, belasting in te dienen of medische hulp te krijgen. Deze handelingen kunnen uw kredietstatus schaden en u tijd en geld kosten om uw goede naam te herstellen.

Identiteitsdiefstal vindt plaats wanneer iemand uw persoonlijke gegevens steelt, zoals uw burgerservicenummer, bankrekeningnummer en creditcardgegevens. Identiteitsdiefstal kan op veel verschillende manieren worden gepleegd. Sommige identiteitsdieven doorzoeken vuilnisbakken op zoek naar bankrekeningafschriften en creditcardafschriften. Bij meer hightech methoden wordt toegang verkregen tot bedrijfsdatabases om lijsten met klantgegevens te stelen. Zodra identiteitsdieven de informatie hebben die zij zoeken, kunnen zij iemands kredietwaardigheid en de status van andere persoonlijke informatie ruïneren.

Identiteitsdieven maken steeds meer gebruik van computertechnologie om de persoonlijke informatie van anderen te verkrijgen voor identiteitsfraude. Om dergelijke informatie te vinden, kunnen zij de harde schijven van gestolen of afgedankte computers doorzoeken; computers of computernetwerken hacken; toegang krijgen tot computergebaseerde openbare registers; malware voor het verzamelen van informatie gebruiken om computers te infecteren; surfen op sociale netwerksites; of misleidende e-mails of sms-berichten gebruiken.

Soorten identiteitsdiefstal

Financiële identiteitsdiefstal

Bij financiële identiteitsdiefstal gebruikt iemand de identiteit of informatie van een andere persoon om krediet, goederen, diensten of voordelen te verkrijgen. Dit is de meest voorkomende vorm van identiteitsdiefstal.

Identiteitsdiefstal van de sociale zekerheid

Als identiteitsdieven uw burgerservicenummer bemachtigen, kunnen zij dit gebruiken om creditcards en leningen aan te vragen en vervolgens uitstaande saldi niet te betalen. Fraudeurs kunnen uw nummer ook gebruiken om medische, arbeidsongeschiktheids- en andere uitkeringen

Diefstal van medische identiteit

Bij medische identiteitsdiefstal doet iemand zich voor als een andere persoon om gratis medische zorg te krijgen.

Synthetische identiteitsdiefstal

Synthetische identiteitsdiefstal is een vorm van fraude waarbij een crimineel echte (meestal gestolen) en valse informatie combineert om een nieuwe identiteit te creëren, die wordt gebruikt om frauduleuze rekeningen te openen en frauduleuze aankopen te doen. Met synthetische identiteitsdiefstal kan de crimineel geld stelen van creditcardmaatschappijen of kredietverstrekkers die krediet verlenen op basis van de valse identiteit.

Identiteitsdiefstal van kinderen

Bij identiteitsdiefstal van kinderen gebruikt iemand de identiteit van een kind voor verschillende vormen van persoonlijk gewin. Dit komt vaak voor, omdat kinderen doorgaans niet over informatie beschikken die de dader in de weg zou kunnen staan. De fraudeur kan de naam en het sofi-nummer van het kind gebruiken om een woning te verkrijgen, werk te vinden, een lening af te sluiten of te voorkomen dat hij wordt gearresteerd wegens een uitstaande aanhoudingsbevel. Vaak is het slachtoffer een familielid, het kind van een vriend, of iemand anders die dicht bij de dader staat. Sommige mensen stelen zelfs de persoonlijke gegevens van overleden dierbaren.

Diefstal van fiscale identiteit

Van fiscale identiteitsdiefstal is sprake wanneer iemand uw persoonlijke gegevens, waaronder uw burgerservicenummer, gebruikt om op uw naam een valse belastingaangifte in te dienen en een terugbetaling te innen.

Criminele identiteitsdiefstal

Bij criminele identiteitsdiefstal doet een crimineel zich tijdens een arrestatie voor als iemand anders om te proberen een dagvaarding te ontlopen, de ontdekking van een arrestatiebevel op zijn echte naam te voorkomen of een arrestatie- of veroordelingsdossier te vermijden.

Identiteitsdiefstal bij werkloosheid

Iemand gebruikt uw persoonlijke gegevens om een werkloosheidsuitkering aan te vragen (en te ontvangen).

- Online seksuele intimidatie

Online seksuele intimidatie wordt gedefinieerd als ongewenst seksueel gedrag op een digitaal platform en wordt erkend als een vorm van seksueel geweld.

Online seksuele intimidatie omvat een breed scala van gedragingen waarbij gebruik wordt gemaakt van digitale inhoud (afbeeldingen, video's, posts, berichten, pagina's) op een verscheidenheid van verschillende platforms (privé of openbaar). Het kan iemand het gevoel geven dat hij of zij wordt bedreigd, uitgebuit, gedwongen, vernederd, overstuur, geseksualiseerd of gediscrimineerd.

Soorten online seksuele intimidatie
Niet-consensueel delen van intieme beelden en video's
Seksuele beelden en video's van een persoon worden zonder hun toestemming gedeeld of zonder hun toestemming genomen. Dit omvat een reeks gedragingen, zoals:
- Seksuele beelden/video's die zonder toestemming zijn gemaakt ('creep shots' of 'upskirting')
- Seksuele beelden/video's die met toestemming zijn genomen, maar zonder toestemming zijn gedeeld ("wraakporno")
- seksuele handelingen zonder toestemming (bv. verkrachting) die digitaal zijn vastgelegd (en mogelijk worden gedeeld)

Uitbuiting, dwang en bedreigingen
Een persoon die seksueel wordt bedreigd, wordt gedwongen deel te nemen aan seksueel gedrag online, of wordt gechanteerd met seksuele inhoud. Dit omvat een reeks gedragingen, zoals:

- Iemand online lastigvallen of onder druk zetten om seksuele beelden van zichzelf te delen of deel te nemen aan seksueel gedrag online (of offline)
- De dreiging van het publiceren van seksuele inhoud (beelden, video's, geruchten) gebruiken om iemand te bedreigen, te dwingen of te chanteren ("sextortion")
- Online bedreigingen van seksuele aard (bv. bedreigingen met verkrachting)
- Anderen er online toe aanzetten seksueel geweld te plegen
- Iemand aanzetten tot seksueel gedrag en vervolgens bewijzen daarvan delen

Seksueel getint pesten
Een persoon wordt het doelwit van een groep of gemeenschap en wordt daar systematisch buiten gehouden door het gebruik van seksuele inhoud die hem of haar vernedert, van streek maakt of discrimineert. Dit omvat een reeks gedragingen, zoals:

- Roddels, geruchten of leugens over seksueel gedrag die online worden geplaatst, hetzij door iemand direct bij naam te noemen, hetzij door indirect op iemand te zinspelen
- beledigend of discriminerend seksueel taalgebruik en scheldpartijen online

- Zich voordoen als iemand en zijn reputatie schaden door seksuele inhoud te delen of anderen seksueel lastig te vallen
- Persoonlijke informatie online delen zonder medelijden om seksuele intimidatie aan te moedigen ("doxing")
- Gepest worden op grond van het werkelijke of vermeende geslacht en/of seksuele geaardheid
- Lichaam aan de schandpaal nagelen
- Iemand "outen", waarbij zijn of haar seksualiteit of genderidentiteit zonder zijn of haar toestemming online openbaar wordt gemaakt

Ongewenste seksualisering

Een persoon ontvangt ongewenste seksuele verzoeken, opmerkingen en inhoud. Dit omvat een reeks gedragingen, zoals

- Geseksualiseerde opmerkingen (bijv. op foto's)
- geseksualiseerde virale campagnes die mensen onder druk zetten om deel te nemen
- iemand seksuele inhoud sturen (afbeeldingen, emoji's, berichten) zonder dat hij/zij daarvoor toestemming heeft gegeven
- ongewenste seksuele avances of verzoeken om seksuele gunsten
- Grappen' van seksuele aard
- Beoordelen van leeftijdsgenoten op aantrekkelijkheid/seksuele activiteit
- Het veranderen van afbeeldingen van een persoon om ze seksueel te maken

Bij dit soort seksuele intimidatie kan iemand zich een van de volgende dingen voelen:

- Bedreigd of bang
- Uitgebuit
- Gedwongen
- Dat hun waardigheid wordt geschonden
- Vernederd of vernederd
- Beschaamd of veroordeeld
- In de war gebracht
- Geseksualiseerd
- Gediscrimineerd worden op grond van hun geslacht of seksuele geaardheid
- Schuldig voelen of denken dat het hun schuld is

De ervaring en de gevolgen van online seksuele intimidatie zijn uniek voor het individu en kunnen zowel op korte termijn als op lange termijn gevolgen hebben voor de geestelijke gezondheid en het welzijn. De gevolgen op lange termijn kunnen worden versterkt door nieuwe slachtoffers als de inhoud opnieuw online wordt gedeeld, of omdat het initiële trauma van het incident veel later opnieuw opduikt. Het is belangrijk te erkennen dat er geen eenduidige manier is waarop een jongere online seksuele intimidatie kan ervaren en dat het ook gevolgen kan hebben voor anderen die er getuige van zijn.

- Phishing

Bij phishing wordt frauduleuze communicatie verzonden die afkomstig lijkt te zijn van een betrouwbare bron. Meestal gebeurt dit via e-mail. Het doel is gevoelige gegevens te stelen, zoals creditcard- en inloggegevens, of malware te installeren op de computer van het slachtoffer. Phishing is een veel voorkomende vorm van cyberaanval die iedereen zou moeten leren kennen om zichzelf te beschermen.

Soms zijn hackers tevreden met het verkrijgen van uw persoonlijke gegevens en creditcardinformatie voor financieel gewin. In andere gevallen worden phishing-e-mails verzonden om inloggegevens van werknemers of andere details te verzamelen voor gebruik in meer kwaadaardige aanvallen tegen een paar personen of een specifiek bedrijf.

Phishing begint met een frauduleuze e-mail of andere communicatie die is ontworpen om een slachtoffer te lokken. Het bericht wordt zo opgemaakt dat het lijkt alsof het van een betrouwbare afzender komt. Als het slachtoffer wordt misleid, wordt hij of zij overgehaald vertrouwelijke informatie te verstrekken - vaak op een frauduleuze website. Soms wordt er ook malware gedownload op de computer van het doelwit.

Cybercriminelen beginnen met het identificeren van een groep personen die ze willen bereiken. Vervolgens creëren ze e-mail- en sms-berichten die legitiem lijken, maar in werkelijkheid gevaarlijke koppelingen, bijlagen of lokmiddelen bevatten waarmee ze hun doelwitten verleiden tot het uitvoeren van een onbekende, riskante actie.

Phishing-risico's omvatten:

- Geld dat van uw bankrekening wordt gestolen
- Frauduleuze afboekingen van creditcards
- Verlies van toegang tot foto's, video's en bestanden
- Valse berichten in sociale media die op uw accounts zijn geplaatst
- Cybercriminelen die zich voordoen als u tegenover een vriend of familielid, waardoor zij in gevaar komen

In het kort:

- Phishers maken vaak gebruik van emoties zoals angst, nieuwsgierigheid, urgentie en hebzucht om ontvangers te dwingen bijlagen te openen of op links te klikken.
- Phishing-aanvallen zijn zo ontworpen dat het lijkt alsof ze van legitieme bedrijven en personen afkomstig zijn.
- Cybercriminelen innoveren voortdurend en worden steeds geraffineerder.
- Er is maar één succesvolle phishingaanval nodig om uw netwerk te compromitteren en uw gegevens te stelen, en daarom is het altijd belangrijk om "na te denken voordat u klikt".

Om phishing te voorkomen, geeft CISCO de volgende tips:
Vermijd onbekende afzenders. Controleer namen en e-mailadressen voordat u reageert.
Vertrouw geen links of bijlagen in ongevraagde e-mails.
Wees achterdochtig bij e-mails met de vermelding "dringend".
Pas op voor berichten met fouten in spelling of grammatica.
Laat u niet verleiden door "aanbiedingen". Die zijn meestal te mooi om waar te zijn.
Overweeg het gebruik van een beveiligde e-mailprovider.
Geef nooit persoonlijke of financiële informatie op basis van een e-mailverzoek.
Wanneer u e-mail ontvangt van bekende instellingen (overheid, banken, uw huisarts), ga dan direct naar de bron in plaats van te klikken op links in de e-mail.
Wees op uw hoede voor algemene begroetingen, zoals "Geachte heer of mevrouw".
Begrijp het beleid van uw serviceprovider voor het opsporen en stoppen van phishing.
Geef een onbekende of ongevraagde hulp geen toegang tot uw computer.

- Internetfraude en oplichting

Internetfraude is het gebruik van onlinediensten en -software met toegang tot het internet om slachtoffers te bedriegen of te bestelen. De term "internetfraude" heeft in het algemeen betrekking op cybercriminele activiteiten die plaatsvinden via internet of e-mail, waaronder misdrijven als identiteitsdiefstal, phishing en andere hackingactiviteiten die bedoeld zijn om mensen op te lichten.

Elk jaar wordt voor miljoenen dollars aan frauduleuze activiteiten gepleegd via internetzwendel die via onlinediensten op slachtoffers is gericht, en de cijfers blijven stijgen naarmate het internetgebruik toeneemt en de technieken van cybercriminelen geavanceerder worden.

Cybercriminelen maken gebruik van verschillende aanvalsvectoren en -strategieën om internetfraude te plegen. Het gaat onder meer om kwaadaardige software, e-mail en instant messaging om malware te verspreiden, spoofed websites die gebruikersgegevens stelen en uitgebreide, wijdverspreide phishing-zwendel.

Internetfraude kan worden onderverdeeld in verschillende belangrijke soorten aanvallen, waaronder

- Phishing (hierboven in detail uitgelegd): Het gebruik van e-mail en online berichtendiensten om slachtoffers te misleiden tot het delen van persoonlijke gegevens, inloggegevens en financiële gegevens.
- Datalekken: Het stelen van vertrouwelijke, beschermde of gevoelige gegevens van een beveiligde locatie en het verplaatsen ervan naar een niet-vertrouwde omgeving. Hieronder valt ook het stelen van gegevens van gebruikers en organisaties.
- Denial of service (DoS): Het onderbreken van de toegang van verkeer tot een online dienst, systeem of netwerk om kwaadwillenden te veroorzaken.
- Malware: Het gebruik van kwaadaardige software om apparaten van gebruikers te beschadigen of onbruikbaar te maken of om persoonlijke en gevoelige gegevens te stelen.
- Ransomware: Een type malware dat gebruikers de toegang tot kritieke gegevens ontzegt en vervolgens betaling eist in de belofte van herstel van de toegang. Ransomware wordt meestal geleverd via phishing-aanvallen.
- Compromittering van zakelijke e-mail (BEC): Een geraffineerde vorm van aanval die gericht is op bedrijven die vaak overschrijvingen doen.

Hierbij worden legitieme e-mailaccounts gecompromitteerd door middel van social engineeringtechnieken om ongeoorloofde betalingen te doen.

Enkele voorbeelden:

- Zwendel met wenskaarten

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

- Kredietkaartfraude

Creditcardfraude doet zich meestal voor wanneer hackers frauduleus aan de creditcard- of debetkaartgegevens van mensen komen 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 kredietkaart- of bankleningdeals om slachtoffers te lokken. Een slachtoffer kan bijvoorbeeld een bericht van zijn bank ontvangen waarin staat dat hij in aanmerking komt voor een speciale lening of dat hem een enorm geldbedrag als lening ter beschikking is gesteld. Deze zwendel blijft mensen bedriegen ondanks het wijdverbreide besef dat dergelijke aanbiedingen niet voor niets te mooi zijn om waar te zijn.

- Oplichting bij online daten

Een ander typisch voorbeeld van internetfraude is gericht op de overvloed aan online datingtoepassingen en websites. Hackers richten zich op deze apps om slachtoffers te verleiden geld te sturen en persoonlijke gegevens te delen met nieuwe liefdesgeïnteresseerden. 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.

- Loterijgeldfraude

Een andere veel voorkomende vorm van internetfraude is e-mailfraude 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 klein bedrag hebben betaald.

Loterijfraudeurs stellen hun e-mails zo op dat ze geloofwaardig overkomen, maar toch trappen veel mensen in deze oplichterij. De zwendel is gericht op de dromen van mensen om grote sommen geld te winnen, ook al hebben ze misschien nog nooit een lot gekocht. Bovendien zal geen enkel legitiem loterijprogramma de winnaars vragen te betalen om hun prijs op te eisen.

- De Nigeriaanse prins

Een klassieke internetfraude tactiek, de Nigeriaanse Prins oplichting aanpak blijft gemeenschappelijk en bloeiend ondanks wijdverspreide bewustwording.

De zwendel gaat uit van een rijke Nigeriaanse familie of persoon die zijn rijkdom wil delen in ruil voor hulp bij het verkrijgen van hun erfenis. Het gebruikt phishing tactieken om e-mails te sturen die een emotionele achtergrondverhaal, dan lokt slachtoffers in een belofte van 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.

De oplichter zal onvermijdelijk vragen om meer uitgebreide vergoedingen om verdere administratieve taken en transactiekosten te dekken, ondersteund door legitiem ogende bevestigingsdocumenten. De beloofde opbrengst van de investering komt echter nooit.

Tips om internetfraude en oplichting te vermijden:
Het is van vitaal belang om nooit geld te sturen naar iemand die men via internet heeft ontmoet, nooit persoonlijke of financiële gegevens te delen met personen die niet legitiem of betrouwbaar zijn, en nooit te klikken op hyperlinks of bijlagen in e-mails of instant messages. Zodra ze het doelwit zijn, moeten internetgebruikers online scammeractiviteiten en phishing-e-mails bij de autoriteiten melden.

Creditcardfraude kan ook worden voorkomen door bankrekeningen goed in de gaten te houden, meldingen over creditcardactiviteiten in te stellen, zich aan te melden voor kredietbewaking en gebruik te maken van diensten voor consumentenbescherming. Als gebruikers te maken krijgen met creditcardfraude, moeten zij dit melden bij de relevante wettelijke autoriteiten en kredietbureaus.

- Spam

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

Spam is geen acroniem voor een computerbedreiging, hoewel er wel enkele zijn voorgesteld (domme zinloze irritante malware, bijvoorbeeld). De inspiratie voor het gebruik van de term "spam" om massaal ongewenste berichten te beschrijven is een Monty Python sketch waarin de acteurs verklaren dat iedereen het voedsel Spam moet eten, of ze het nu willen of niet. Op dezelfde manier moet iedereen met een e-mailadres helaas last hebben van spamberichten, of we dat nu willen of niet.

Spammers gebruiken vele vormen van communicatie om hun ongewenste berichten in bulk te versturen. Sommige van deze berichten zijn marketingberichten waarin ongevraagd goederen worden aangeboden. Andere soorten spamberichten kunnen malware verspreiden, u persoonlijke informatie ontfutselen of u bang maken door u te laten denken dat u moet betalen om uit de problemen te komen.

Spamfilters voor e-mail vangen veel van dit soort berichten op, en telefoonmaatschappijen waarschuwen u vaak voor een "spamrisico" van onbekende bellers. Of het nu via e-mail, sms, telefoon of sociale media is, sommige spamberichten komen er toch doorheen, en u wilt ze kunnen herkennen en deze bedreigingen vermijden. Hieronder staan verschillende soorten spam waar u op moet letten:

- Phishing-e-mails (hierboven al beschreven)
- E-mail spoofing - in spoofed e-mails wordt een e-mail van een legitieme afzender nagebootst of nagebootst, en wordt u gevraagd actie te ondernemen. Goed uitgevoerde spoofs zullen bekende merknamen en inhoud bevatten, vaak van een groot bekend bedrijf zoals PayPal of Apple.

- Technische ondersteuning - bij technische ondersteuning wordt in het spambericht aangegeven dat u een technisch probleem hebt en dat u contact moet opnemen met de technische ondersteuning door het telefoonnummer te bellen of op een link in het bericht te klikken.
- Malspam - kort voor "malware spam" of "kwaadaardige spam", malspam is een spambericht dat malware op uw apparaat aflevert. Nietsvermoedende lezers die op een koppeling klikken of een e-mailbijlage openen, komen terecht in een soort malware, waaronder ransomware, Trojaanse paarden, bots, infostealers, cryptominers, spyware en keyloggers. Een veelgebruikte methode is het opnemen van kwaadaardige scripts in een bijlage van een bekend type, zoals een Word-document,
PDF-bestand of PowerPoint-presentatie. Zodra de bijlage wordt geopend, worden de scripts uitgevoerd en wordt de payload van de malware opgehaald.
- Spam telefoontjes en spam sms'jes - heeft u wel eens een robocall ontvangen? Dat is call spam. Een sms-bericht van een onbekende afzender waarin u dringend wordt verzocht op een onbekende link te klikken? Dat wordt sms-spam genoemd of "smishing", een combinatie van sms en phishing.
Als je spamoproepen en -sms'jes ontvangt op je Android of iPhone, bieden de meeste grote providers je een optie om spam te melden. Het blokkeren van nummers is een andere manier om mobiele spam te bestrijden.

- Cyberhacking

Iedereen die gebruik maakt van een computer met internetverbinding is vatbaar voor de bedreigingen van hackers en online roofdieren. Deze online schurken maken meestal gebruik van phishing scams, spam e-mail of instant messages en nepwebsites om gevaarlijke malware op uw computer af te leveren en uw computerbeveiliging in gevaar te brengen.

Computerhackers kunnen ook proberen rechtstreeks toegang te krijgen tot uw computer en tot uw privégegevens als u niet door een firewall wordt beschermd. Ze kunnen uw gesprekken afluisteren of de back-end van uw persoonlijke website doorzoeken. Meestal vermomd met een valse identiteit, kunnen roofdieren u verleiden tot het onthullen van gevoelige persoonlijke en financiële informatie, of nog veel erger.
Terwijl uw computer met het internet is verbonden, verstuurt de malware die een hacker op uw pc heeft geïnstalleerd stilletjes uw persoonlijke en financiële gegevens zonder uw medeweten of toestemming. Of een computerroofdier kan zich vergrijpen aan de privégegevens die u onbewust hebt onthuld. In beide gevallen zullen ze in staat zijn om:

- Uw gebruikersnamen en wachtwoorden te stelen
- Uw geld stelen en op uw naam creditcards en bankrekeningen openen
- Uw krediet te ruïneren
- nieuwe PIN-codes (Personal Identification Numbers) of extra creditcards aanvragen
- aankopen doen
- Zichzelf of een alias die zij controleren toevoegen als geautoriseerde gebruiker zodat het gemakkelijker is om uw krediet te gebruiken
- Contante voorschotten krijgen
- Uw socialezekerheidsnummer gebruiken en misbruiken
- uw informatie verkopen aan andere partijen die ze voor illegale doeleinden gebruiken

Om uzelf tegen deze bedreigingen te beschermen, kunt u het volgende doen:
- Voortdurend de juistheid van persoonlijke rekeningen controleren en eventuele afwijkingen meteen aanpakken
- Wees uiterst voorzichtig wanneer u chatrooms binnengaat of persoonlijke webpagina's plaatst
- Beperk de persoonlijke informatie die u op een persoonlijke webpagina plaatst
- Controleer verzoeken van online "vrienden" of kennissen zorgvuldig op roofzuchtig gedrag
- Houd persoonlijke en financiële informatie buiten online gesprekken
- Wees uiterst voorzichtig wanneer u een online "vriend" of kennis in levende lijve wilt ontmoeten
- Gebruik een 2-weg firewall
- Update uw besturingssysteem regelmatig
- Verhoog de beveiligingsinstellingen van uw browser
- Vermijd twijfelachtige websites
- Download alleen software van sites die u vertrouwt. Beoordeel gratis software en toepassingen voor het delen van bestanden zorgvuldig voordat u ze downloadt.
- Open geen berichten van onbekende afzenders
- Verwijder berichten waarvan u vermoedt dat het spam is onmiddellijk
- Zorg ervoor dat u de beste beveiligingssoftwareproducten op uw pc hebt geïnstalleerd:
- Gebruik antivirusbescherming
- Zorg voor bescherming met antispyware software

- Cyberstalken

Cyberstalking is het gebruik van internet en andere technologieën om iemand online lastig te vallen of te stalken. Dit online lastigvallen, dat in het verlengde ligt van cyberpesten en persoonlijk stalken, kan de vorm aannemen van e-mails, sms-berichten, berichten op sociale media en meer, en is vaak methodisch, opzettelijk en aanhoudend.

Meestal houden de interacties niet op, zelfs niet als de ontvanger zijn ongenoegen uit of de persoon vraagt om te stoppen. De inhoud die aan het doelwit wordt gericht is vaak ongepast en soms zelfs verontrustend, waardoor de persoon zich angstig, verontrust, angstig en bezorgd kan voelen.

Bij cyberstalken gebruiken cyberstalkers verschillende tactieken en technieken om hun doelwit lastig te vallen, te vernederen, te intimideren en te controleren. In feite zijn veel cyberstalkers technologisch onderlegd en creatief en bedenken een groot aantal manieren om hun doelwitten te kwellen en lastig te vallen. Hier zijn enkele voorbeelden van dingen die mensen die cyberstalken kunnen doen:

- onbeleefd, beledigend of suggestief commentaar online zetten
- Het doelwit online volgen door lid te worden van dezelfde groepen en forums
- Bedreigende, controlerende of onzedelijke berichten of e-mails sturen naar het doelwit

- Technologie gebruiken om het doelwit te bedreigen of te chanteren
- Het doelwit overmatig taggen in berichten, zelfs als ze niets met hem te maken hebben
- Commentaar geven op of liken van alles wat het doelwit online plaatst
- Valse accounts aanmaken om het doelwit te volgen op sociale media
- Het doelwit herhaaldelijk berichten sturen
- De online accounts van het doelwit hacken of kapen
- Proberen seks of expliciete foto's af te persen
- Ongewenste cadeaus of voorwerpen naar het doelwit sturen
- Vertrouwelijke informatie online vrijgeven
- Echte of valse foto's van het doelwit plaatsen of verspreiden
- Het doelwit bombarderen met seksueel getinte foto's van zichzelf
- Nepberichten maken om het slachtoffer te schande te maken
- De online bewegingen van het doelwit volgen door traceerapparatuur te installeren
- De camera van het doelwit op zijn laptop of smartphone hacken om hem stiekem op te nemen
- Doorgaan met het lastig vallen van het slachtoffer, zelfs nadat hem is gevraagd te stoppen

Net als stalking kan cyberstalking een breed scala aan fysieke en emotionele gevolgen hebben voor degenen die het doelwit zijn. Het is bijvoorbeeld niet ongewoon dat degenen die online worden lastiggevallen, last hebben van woede, angst en verwarring. Ze kunnen ook problemen hebben met slapen en zelfs klagen over maagklachten.

De manieren om cyberstalking te voorkomen lijken sterk op de manieren die worden aanbevolen voor het voorkomen van andere cyberbedreigingen, omdat ze allemaal met elkaar verband houden en op dezelfde manier werken. Enkele van de tips zijn:
- Creëer sterke wachtwoorden. Zorg ervoor dat je sterke wachtwoorden hebt voor al je online accounts en ook sterke wachtwoorden voor je apparaten. Stel vervolgens een herinnering in op uw telefoon om uw wachtwoorden regelmatig te wijzigen. Kies wachtwoorden die moeilijk te raden zijn, maar die u gemakkelijk kunt onthouden.

- Zorg ervoor dat u elke keer uitlogt. Het lijkt misschien lastig, maar zorg ervoor dat u uitlogt uit e-mail, social media-accounts en andere online accounts nadat u ze hebt gebruikt. Op deze manier heeft iemand die op uw apparaat kan komen, geen gemakkelijke toegang tot uw accounts.
- Houd uw apparaten in de gaten. Laat uw telefoon niet op uw bureau op het werk liggen of loop niet weg van een open laptop. Het kost iemand maar een minuut of twee om een volgapparaat te installeren of uw apparaat te hacken. Zorg er dus voor dat u deze dingen in uw bezit houdt of dat u ze op een of andere manier beveiligt.
- Wees voorzichtig op openbare wifi. Erken het feit dat als je openbare wifi gebruikt in hotels of in de plaatselijke coffeeshop, je jezelf in gevaar brengt voor hacking. Probeer af te zien van het gebruik van openbare wifi of investeer in VPN.
- Oefen online veiligheidsgewoonten. Met andere woorden, maak er een prioriteit van om alleen vriendverzoeken te accepteren van mensen die u kent en houd uw berichten privé. Overweeg ook om één e-mailadres te hebben dat specifiek bestemd is voor uw online activiteiten. Gebruik dit e-mailadres wanneer u online inkopen doet of deelneemt aan loyaliteitsprogramma's.
- Maak gebruik van de beveiligingsinstellingen. Loop al uw online accounts na, met name uw sociale media-accounts, en zorg ervoor dat u de sterkst mogelijke privacy-instellingen gebruikt. U kunt zelfs instellen dat mensen u niet kunnen taggen of geen foto's van u kunnen plaatsen zonder eerst uw toestemming te vragen.

- Maak algemene schermnamen. In plaats van uw volledige naam online te gebruiken, kunt u overwegen een geslachtsneutrale schermnaam of pseudoniem te gebruiken. Op die manier maakt u het mensen moeilijker om u online te vinden. Laat ook de optionele secties, zoals uw geboortedatum of uw woonplaats, leeg.
- Houd locaties veilig. Overweeg de geolocatie-instellingen op foto's uit te schakelen. Plaats ook geen foto's van uw locatie in real time, maar plaats foto's die achteraf laten zien waar u bent geweest.
- Wees voorzichtig met online datingsites. Gebruik niet je volledige naam op online datingsites. Geef ook geen persoonlijke informatie zoals je achternaam, adres, e-mail en telefoonnummer totdat je elkaar persoonlijk hebt ontmoet en een vertrouwensband hebt opgebouwd.
- Voer een social media audit uit. Het is altijd een goed idee om uw social media-accounts door te nemen en foto's of posts te verwijderen die te veel informatie over u bevatten of die een beeld oproepen dat u niet wilt verspreiden. Houd er ook rekening mee dat zelfs als u iemand op sociale media hebt geblokkeerd, hij uw account nog steeds kan zien door de account van een ander te gebruiken of door een nepprofiel aan te maken.

De manieren om met cyberstalking om te gaan, in het geval het al gebeurt, zijn onder meer:
- Zeg de persoon te stoppen. Reageer slechts één keer op de persoon die je cyberstalkt en zeg dat hij/zij moet stoppen met contact met je op te nemen. Je hoeft niets specifieks te zeggen of je antwoord uit te leggen, vraag hem gewoon om nooit meer contact met je op te nemen.
- Blokkeer de persoon. Zorg ervoor dat je de persoon die je cyberstalkt blokkeert van al je accounts. Je moet ze blokkeren op sociale media en op je smartphone.
- Weiger op elk contact te reageren. Als de persoon die je cyberstalkt manieren blijft vinden om contact met je op te nemen, reageer dan niet op wat hij post of naar je stuurt.
- Verander van e-mailadres en schermnaam. Overweeg een nieuw e-mailadres en een andere schuilnaam om het voor de cyberstalker moeilijker te maken je te bereiken.

Als je de persoon die je cyberstalkt hebt gevraagd te stoppen en zijn of haar gedrag gaat door, is het belangrijk om actie tegen hem of haar te ondernemen. Dit houdt in dat je contact opneemt met de juiste autoriteiten en bewijs verzamelt van hun daden. U kunt ook overwegen om met een advocaat te praten.

Dit zijn de belangrijkste punten die aan de orde moeten komen als u actie onderneemt. Uw plaatselijke politie kan u laten weten of er nog iets is dat u kunt doen om veilig te blijven.

- Bewaar bewijsmateriaal van alles. Ook al heb je misschien zin om alles te vernietigen, toch is het belangrijk om kopieën te bewaren van alles wat de persoon die je cyberstalkte, heeft gestuurd. Maak een kopie voor jezelf en een kopie voor de politie.
- Breng de plaatselijke politie op de hoogte. Het is belangrijk om de politie in te lichten en een officiële klacht in te dienen als je wordt gecyberstalked. Zelfs als ze niet meteen iets kunnen doen, is het belangrijk om een officiële klacht in te dienen als het gedrag aanhoudt of escaleert.
- Meld ze bij de site of dienst die ze hebben gebruikt. Als de persoon die je cyberstalkte je lastigviel via Facebook, Instagram, Twitter, Snapchat, YouTube, Gmail, of een andere methode, laat dan de juiste instanties weten wat je meemaakt. Vaak nemen deze organisaties klachten over cyberstalking serieus en zullen ze de zaak aanpakken.

3.3 Hoe kunnen bedreigingen voor de cyberveiligheid op sociale media/instellingen worden gemeld?

Alle sociale netwerken hebben mechanismen opgezet voor het melden van verschillende soorten bedreigingen voor de cyberveiligheid, waaronder online haatzaaien, identiteitsdiefstal, seksuele intimidatie, cyberpesten, enz. Hieronder vindt u informatie over enkele van de populairste sociale netwerken:

- Facebook

De veiligheidskwesties van Facebook omvatten meerdere categorieën. Er kan sprake zijn van beledigende inhoud of haatpagina's die u wilt melden of misschien doet iemand zich voor als u op Facebook, enz. De beste manier om beledigende inhoud of spam op Facebook te rapporteren is door de link Rapporteren te gebruiken in de buurt van de inhoud zelf.

Om een profiel te melden:

- Ga naar het profiel dat je wilt rapporteren door op de naam ervan te klikken in je Feed of door ernaar te zoeken.
- Klik op "..." aan de rechterkant en selecteer Ondersteuning zoeken of profiel rapporteren.
- Om feedback te geven, klik je op de optie die het beste beschrijft hoe dit profiel ingaat tegen hun Community Standaarden, klik dan op Volgende.
- Afhankelijk van uw feedback kunt u vervolgens mogelijk een rapport indienen bij Meta. Voor sommige typen inhoud vraagt Facebook je niet om een rapport in te dienen, maar gebruikt het je feedback om hun systemen te helpen leren. Klik op Gereed.

Een foto of video rapporteren

- Klik op de foto of video om deze uit te vouwen. Als het profiel is vergrendeld en u de foto op volledige grootte niet kunt bekijken, klikt u op Ondersteuning zoeken of Foto rapporteren.
- Klik op "..." rechts van de foto of video.
- Klik op Ondersteuning zoeken of Foto melden voor foto's of Video melden voor video's.
- Selecteer de optie die het probleem het beste omschrijft en volg de instructies op het scherm.

Om een bericht te melden:

- Om een bericht te melden dat tegen de Community Standards van Facebook ingaat:
- Klik vanaf elke pagina op Facebook op het Messenger-pictogram in de rechterbovenhoek.
- Open het Bericht.
- Als u het bericht als pop-upvenster hebt geopend, klikt u op het instellingenpictogram.
- Klik op Er klopt iets niet.
- Om feedback te geven, klik je op de optie die het beste beschrijft hoe dit bericht ingaat tegen de communitystandaarden van Facebook.
- Afhankelijk van uw feedback kunt u vervolgens mogelijk een rapport indienen bij Meta. Voor sommige typen inhoud vraagt Facebook je niet om een rapport in te dienen, maar gebruiken ze je feedback om hun systemen te helpen leren.

Zo rapporteer je een pagina:

- Ga naar de Pagina die je wilt rapporteren door op de naam ervan te klikken in je Feed of door ernaar te zoeken.
- Klik op Meer onder de omslagfoto van de pagina.
- Selecteer Ondersteuning zoeken of Pagina rapporteren.

- Als u feedback wilt geven, klikt u op de optie die het beste beschrijft hoe deze pagina ingaat tegen de communitystandaarden van Facebook.
- Afhankelijk van uw feedback kunt u vervolgens mogelijk een rapport indienen bij Meta. Voor sommige typen inhoud vraagt Facebook je niet om een rapport in te dienen, maar gebruiken ze je feedback om hun systemen te helpen leren.

Om een groep te rapporteren:
- Ga naar de groep die je wilt rapporteren door op de naam ervan in je Feed te klikken of ernaar te zoeken.
- Klik op Meer onder de omslagfoto van de groep.
- Selecteer Groep rapporteren.
Zo rapporteer je een gebeurtenis:
- Klik vanuit uw Feed op Gebeurtenissen in het linkermenu.
- Ga naar het evenement dat u wilt melden.
- Klik op "..." en selecteer Gebeurtenis melden.
- Als u feedback wilt geven, klikt u op de optie die het beste beschrijft hoe dit profiel ingaat tegen de communitystandaarden van Facebook.
- Afhankelijk van uw feedback kunt u vervolgens mogelijk een rapport indienen bij Meta. Voor sommige typen inhoud vraagt Facebook je niet om een rapport in te dienen, maar gebruiken ze je feedback om hun systemen te helpen leren.

Zo rapporteer je een opmerking:
- Ga naar de opmerking die je wilt rapporteren.
- Klik op "..." naast de opmerking.
- Klik op Geef feedback of Meld deze opmerking.
- Als u feedback wilt geven, klikt u op de optie die het beste beschrijft hoe deze opmerking in strijd is met de communitystandaarden van Facebook. Als u geen geschikte opties ziet, klikt u op Iets anders om er meer te zoeken.

- Afhankelijk van uw feedback kunt u vervolgens mogelijk een rapport indienen bij Meta. Voor sommige soorten inhoud vraagt Facebook je niet om een rapport in te dienen, maar gebruiken ze je feedback om hun systemen te helpen leren.
Zo rapporteer je een advertentie op Facebook:
- Ga naar de advertentie die je wilt rapporteren door op de naam ervan te klikken in je Feed of door ernaar te zoeken.
- Klik op "..." naast de advertentie die u wilt rapporteren
- Klik op Advertentie melden en volg de instructies op het scherm.

- Instagram

Berichten rapporteren
- 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 afzonderlijke stukjes inhoud rapporteren door op de drie puntjes boven een post te tikken, een bericht vast te houden of door een account te bezoeken en rechtstreeks vanaf het profiel te rapporteren. Ga voor meer informatie hier naar het Helpcentrum van Instagram.

Accounts rapporteren

- Accounts die in strijd zijn met de Community Guidelines van Instagram kunnen in-app of via een webformulier worden gemeld. Voor meer informatie kun je terecht in het Helpcentrum.

Opmerkingen melden

- Als je een opmerking ziet die spam is of bedoeld is om jou of iemand anders te pesten of lastig te vallen, meld deze dan.
- Open het gesprek in de Instagram-app.
- Tik op het individuele bericht dat je wilt melden en houd het vast.
- Tik op melden.
- Selecteer een reden waarom je het bericht wilt melden en tik vervolgens op Melden verzenden.
- Ga voor meer informatie naar het Helpcentrum.

Berichten melden

- Als u een bericht ontvangt dat u ongepast vindt, blijft u het afzonderlijke bericht aanraken om het te melden. Ga voor meer informatie naar het Helpcentrum.

Verhalen melden

- Als je een verhaal van iemand ziet en denkt dat het in strijd is met de communityrichtlijnen van Instagram, kun je het melden.
- Open het verhaal.
- Tik op de drie stippen onder aan de foto of video die je wilt melden.
- Tik op Rapporteren en volg de instructies op het scherm.
- Ga voor meer informatie naar het Helpcentrum.

- Tik Tok

- Voor vragen, problemen of problemen met je profiel kun je hier informatie en ondersteuning vinden. In de sectie Veiligheid kun je naar Meld een probleem gaan en een LIVE-video, een LIVE-commentaar, een video, een comment, een direct message, een geluid, een hashtag melden, en je kunt ook iemand melden. De stappen zijn heel eenvoudig te volgen, je hoeft alleen maar de optie Melden te vinden en de instructies te volgen.
- Voor vragen, zorgen of problemen met het privacybeleid of fraude van TikTok, kun je hier ondersteuning vinden. Je wordt doorgestuurd naar een online formulier waar je informatie over je gegevens kunt opvragen, een privacyschending kunt melden of vragen kunt stellen over een bepaalde privacykwestie.

- Twitter

In het Helpcentrum van Twitter kunt u informatie en ondersteuning vinden in geval van gecompromitteerde en gehackte accounts, over privacy, spam en nepaccounts, gevoelige en aanstootgevende inhoud, grof gedrag en het melden daarvan.

Om een Tweet te rapporteren:

- Navigeer naar de Tweet die je wilt rapporteren op twitter.com of vanuit de Twitter voor iOS of Twitter voor Android app.
- Selecteer het pictogram "...".
- Selecteer Rapporteren.
- Selecteer voor wie het rapport is: Ikzelf, Iemand anders of een specifieke groep mensen, of Iedereen op Twitter.

- Twitter zal je vervolgens vragen om meer informatie te geven over het probleem dat je wilt rapporteren. Twitter kan je ook vragen om extra Tweets te selecteren van het account dat je rapporteert, zodat ze een betere context hebben om je rapport te evalueren.
- Twitter zal er dan voor zorgen dat ze je informatie correct hebben door te bevestigen wat je rapporteert en welke extra context je hebt gedeeld, en welke regel het mogelijk heeft overtreden.
- Twitter zal de tekst van de Tweets die je hebt gemeld opnemen in follow-up e-mails en meldingen aan jou. Om deze informatie niet te ontvangen, kun je het vinkje weghalen uit het vakje naast Updates over dit rapport kunnen deze Tweets tonen.
- Zodra je je rapport hebt ingediend, zal Twitter aanbevelingen doen voor extra acties die je kunt ondernemen om je Twitter-ervaring te verbeteren.

Zo rapporteer je een account:
- Ga naar het accountprofiel en selecteer het pictogram "...".
- Selecteer Rapporteren.
- Selecteer voor wie het rapport is: Ikzelf, Iemand anders of een specifieke groep mensen, of Iedereen op Twitter.
- Twitter zal je vervolgens vragen om aanvullende informatie te verstrekken over het probleem dat je rapporteert. Ze kunnen je ook vragen om Tweets van dat account te selecteren zodat ze een betere context hebben om je rapport te evalueren.
- Twitter zal er dan voor zorgen dat ze je informatie correct hebben door te bevestigen wat je rapporteert, alsook de extra context die je hebt gedeeld, en welke regel het mogelijk heeft overtreden.
- Twitter zal de tekst van de Tweets die je hebt gemeld opnemen in follow-up e-mails en meldingen aan jou. Om deze informatie niet te ontvangen, kun je het vinkje weghalen uit het vakje naast Updates over dit rapport kunnen deze Tweets tonen.
- Zodra je je rapport hebt ingediend, zal Twitter aanbevelingen doen voor extra acties die je kunt ondernemen om je Twitter-ervaring te verbeteren.

Zo rapporteer je een individueel bericht of gesprek:
- Selecteer de Direct Message conversatie en zoek het bericht dat je wilt rapporteren. (Als u het hele gesprek wilt rapporteren, klikt u op het pictogram "...").
- Selecteer het pictogram met de informatie "i" en selecteer @gebruikersnaam rapporteren.
- Als u It's abusive or harmful (Het is beledigend of schadelijk) selecteert, zal Twitter u vragen om aanvullende informatie te verstrekken over het probleem dat u rapporteert. Ze kunnen je ook vragen om extra berichten te selecteren van het account dat je rapporteert, zodat ze een betere context hebben om je melding te beoordelen.
- Zodra u uw rapport hebt ingediend, zal Twitter aanbevelingen doen voor extra acties die u kunt ondernemen om uw Twitter-ervaring te verbeteren.
Wanneer wordt het beschouwd als een misdrijf?

Spanje:
In Spanje lopen de gevolgen van cybermisdrijven op van vijf jaar gevangenisstraf tot boetes tot 2.700 €.
Stalking wordt een misdrijf wanneer iemand herhaaldelijk iemands gevoel van veiligheid inperkt en wanneer hij of zij het slachtoffer het gevoel geeft vernederd, beledigd of bedreigd te worden. Het hoeft geen verbazing te wekken dat iemand die zich hieraan schuldig maakt, te maken krijgt met verschillende consequenties die variëren van drie maanden tot twee jaar gevangenisstraf of de betaling van een boete aan het slachtoffer, een dagelijks bedrag dat rechters bepalen. Een dagelijkse boete van 15 euro gedurende zes maanden komt neer op een totaalbedrag van 2.700 euro.

Het openbaar maken van geheimen heeft ook in Spanje gevolgen aangezien het een ernstig misdrijf is. Eenieder die "zonder toestemming van de betrokkene audiovisuele beelden of opnamen verspreidt, bekendmaakt of aan derden overdraagt" kan eveneens een gevangenisstraf of een geldboete tegemoet zien. De verspreiding van seksuele beelden is nog ernstiger en kan nog meer gevolgen hebben. Bovendien moet worden gesproken over identiteitsdiefstal. Dat is het zich toe-eigenen van de identiteit van een persoon. Met andere woorden, zich voordoen als die persoon, zijn identiteit aannemen tegenover anderen. Een voorbeeld hiervan is het aanmaken van een account op een sociaal netwerk om zich voor te doen als een andere persoon om informatie te verzamelen of voor een ander doel. Hierop staat een gevangenisstraf van zes maanden tot drie jaar.

Aan deze bedreigingen van de cyberveiligheid moet een einde komen. Daarom is er in Spanje een manier om het op een legaal niveau te brengen. Allereerst moet een slachtoffer dat actie wil ondernemen, eerst bewijs verzamelen van wat er aan de hand is en vervolgens zo snel mogelijk aangifte doen bij het politiebureau. Na controle zullen zij contact met u opnemen en de situatie beoordelen. Als zij vinden dat het in orde is, zal de aangifte een nieuw proces starten en zullen er juridische stappen worden ondernomen.

België

Cyberbeveiliging is het resultaat van een reeks beveiligingsmaatregelen die het risico op verstoring van of ongeoorloofde toegang tot informatie- en communicatiesystemen (ICT) tot een minimum beperken. Het omvat alle redelijke en aanvaardbare maatregelen om de ICT van burgers, bedrijven, organisaties en de overheid te beschermen tegen cyberdreigingen. Cyberbeveiliging omvat de bescherming van systemen (zoals hardware, software en bijbehorende infrastructuur) en netwerken, alsook van de gegevens die zij bevatten.

In de Belgische Nationale Risicobeoordeling 2018-2023 van het Nationaal Crisiscentrum wordt cyberveiligheid beschouwd als een van de belangrijkste risico's waarmee België de komende jaren zal worden geconfronteerd. Binnen deze cluster worden cybercriminaliteit en hacktivisme geïdentificeerd als nationale prioritaire risico's.

Deze definitie is afkomstig van het "Centrum voor Cyberveiligheid in België, de nationale autoriteit voor cyberveiligheid in België, die ook de 4 belangrijkste dreigingen specificeert waarop cyberveiligheid een antwoord moet bieden: buitenlandse militaire en inlichtingendiensten, terrorisme, hacktivisme en cybercriminaliteit. In dit verslag zal de cyberveiligheid waar we ons op zullen richten voornamelijk betrekking hebben op hacktivisme en cybercriminaliteit vanwege hun meest gebruikte aanvalsmethoden, sociale media, en vanwege de directe impact die ze hebben op de algemene veiligheid van elke burger, inclusief jongeren.

In juli 2016 is de richtlijn beveiliging van netwerk- en informatiesystemen (NIB) vastgesteld, die op 7 april 2019 in Belgisch recht is omgezet: Wet tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid. Artikel 7 van deze richtlijn (overgenomen in artikel 10 van de Belgische NIB-wet) verplicht de lidstaten om een nationale strategie voor de beveiliging van netwerk- en informatiesystemen op te stellen. Tot de publicatie van de Belgische Wet op de Netwerk- en Informatiesystemen (NIB) in mei 2019 beschikte het land niet over een volledige wetgeving inzake cyberbeveiliging. Deze grote stap werd gezet dankzij het Agentschap voor cyberbeveiliging van de Europese Unie (ENISA), dat bijdraagt aan het cyberbeleid van de EU, de betrouwbaarheid van ICT-producten, -diensten en -processen verhoogt met certificeringsregelingen voor cyberbeveiliging, samenwerkt met de lidstaten en EU-organen, en Europa helpt zich voor te bereiden op de cyberuitdagingen van morgen. Afgezien daarvan kunnen we wijzen op de volgende wetgeving die afhankelijk van de cybercriminaliteit zal worden gebruikt:

- Belgisch wetboek van strafrecht: art. 550 (b) "Hacking", art. 210bis "IT-fraude";
- Wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren
-Richtlijn (EU) 2016/1148 van 6 juli 2016 betreffende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de gehele Unie
-Wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid
- Koninklijk besluit van 12 juli 2019 tot uitvoering van de wet van 7 april 2019 tot vaststelling van het kader voor het beveiligingsnetwerk en de informatiesystemen van algemeen belang voor de openbare veiligheid
- Verordening (EU) 2019/881 van 17 april 2019 inzake ENISA
- Uitvoeringsverordening (EU)2018/ 151 van de Commissie van 30 januari 2018 tot vaststelling van regels voor de toepassing van Richtlijn EU 2016/1148 van het Europees Parlement en de Raad wat betreft de nadere specificatie van de elementen waarmee digitale dienstverleners rekening moeten houden bij het beheer van beveiligingsrisico's.

Nederland:

In 2021 meldden bijna 2,5 miljoen Nederlanders van 15 jaar of ouder dat zij slachtoffer waren geworden van cybercriminaliteit - dit komt neer op bijna 17% van de bevolking!

Het Nederlandse parlement heeft wetgeving over cybercriminaliteit uitgevaardigd die het volgende voorkomt:

Artikel 138a: Een ieder die zich opzettelijk en wederrechtelijk toegang verschaft tot een geautomatiseerd systeem voor de opslag of verwerking van gegevens, of een deel van een dergelijk systeem;
Artikel 138 ter: het wederrechtelijk ernstig hinderen van gegevensverwerking;
artikel 232: vervalsing van een elektronisch token met bewijskracht en het gebruik van een dergelijk token alsof het een echt token was.

Cybercriminaliteit wordt gedefinieerd als "criminaliteit waarbij sprake is van digitale vormen van identiteitsfraude, fraude bij het online kopen of verkopen, hacking en cyberpesten (laster, stalken, chantage en bedreiging met geweld die online wordt gepleegd)".

Cyberdelicten met betrekking tot de persoonlijke levenssfeer van individuen, organisaties en overheden zijn in de Nederlandse wetgeving strafbaar gesteld (conform de artikelen hierboven). Veel voorkomende cyberdelicten die in Nederland worden gemeld zijn:

Hacken
Fraude met online winkelen
Cyberpesten

Veel voorkomende cyberdelicten, zoals vastgesteld door de Nederlandse overheid, zijn de volgende

Phishing: het gebruik van valse e-mailberichten om persoonlijke informatie van internetgebruikers te verkrijgen
Misbruik maken van persoonlijke informatie (identiteitsdiefstal)
Hacken: het platleggen of misbruiken van websites of computernetwerken
Verspreiden van haat en aanzetten tot terreur
Kinderpornografie verspreiden
Grooming: seksuele avances maken naar minderjarigen

Het Nationaal Cyber Security (NCSC) is verantwoordelijk voor het toezicht op de digitale veiligheid in Nederland. Dit doet het NCSC door:
Het continu monitoren van alle verdachte bronnen op het internet
Organisaties te adviseren over hoe zij zich kunnen beschermen tegen online dreigingen
Ontwikkelingen op het gebied van digitale technologie te volgen en beveiligingssystemen bij te werken

Bulgarije

"Cybercriminaliteit" (ook wel "computercriminaliteit" of "hightech-criminaliteit" genoemd) moet worden opgevat als "criminele handelingen die worden gepleegd door gebruik te maken van elektronische communicatienetwerken en informatiesystemen, of tegen dergelijke netwerken en systemen". In feite verwijst de term naar drie categorieën van criminele handelingen. De eerste omvat traditionele soorten criminaliteit zoals fraude of namaak, hoewel deze categorie in de context van cybercriminaliteit in het bijzonder betrekking heeft op strafbare feiten die worden gepleegd via elektronische communicatienetwerken en informatiesystemen ("elektronische netwerken"). De tweede categorie betreft de publicatie in elektronische media van illegale inhoud (zoals kinderpornografie of inhoud die aanzet tot geweld en verband houdt met haatzaaien en discriminatie). De derde omvat misdrijven die specifiek zijn voor elektronische netwerken, zoals aanvallen op informatiesystemen, denial of service en hacking.
Bulgarije heeft het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, dat in 2001 door de Raad van Europa is goedgekeurd, en de bijbehorende protocollen geratificeerd. Op basis hiervan bevat het Bulgaarse wetboek van strafrecht definities en sancties met betrekking tot cybercriminaliteit.

In het wetboek van strafrecht worden verschillende soorten cybermisdrijven omschreven:
-Cyberfraude wordt gedefinieerd in Art. 212a
-Een bijzondere vorm van vernieling en beschadiging met gebruikmaking van digitale instrumenten wordt gedefinieerd in art. 216, lid 2. 216, lid 2
-Een specifieke vorm van schending van het briefgeheim wordt gedefinieerd in art. 171. 171.
-Kinderpornografie wordt ook specifiek strafbaar gesteld.
-De cyberdelicten van hoofdstuk 9 van het strafwetboek (art. 319a tot en met art. 319f van het strafwetboek). Zij tasten de openbare relaties aan die zorgen voor de goede werking van computers, computersystemen, computerbronnen en computernetwerken, alsmede de rechtmatige totstandbrenging en het rechtmatige gebruik van informatie. Het gaat onder meer om ongeoorloofde toegang, wijziging, beschadiging of vernietiging van gegevens of programma's, de introductie van een virus of de verspreiding van wachtwoorden.

-Het eerste betreft het zonder toestemming kopiëren of gebruiken van computergegevens door middel van het verkrijgen van ongeoorloofde toegang tot computerbronnen (artikel 319 bis).
-De volgende vorm van computercriminaliteit is het namaken of vernietigen van een computerprogramma of van computergegevens (artikel 319 ter). Dit omvat het toevoegen, wijzigen of verwijderen van een computerprogramma of computergegevens, waardoor deze niet-authentiek worden of niet meer in overeenstemming zijn met de oorspronkelijke programma's en gegevens.
-Het inbrengen van een computervirus in een computer of informatienetwerk wordt bedoeld in art. 319d, lid 1, van het wetboek van strafrecht.
Artikel 319 sexies, lid 1, van het strafwetboek, omvat de verspreiding van computer- of systeemwachtwoorden, wanneer dit leidt tot de onthulling van persoonsgegevens of persoonlijke geheimen. De straf kan oplopen tot één jaar gevangenisstraf.

Wat online privacy en veiligheid betreft, is het belangrijk te vermelden dat de Bulgaarse regelgeving verband houdt met de GDPR, die wordt geregeld door de Commissie voor de bescherming van persoonsgegevens. Het is een onafhankelijk staatsorgaan dat personen beschermt bij de verwerking van hun persoonsgegevens en bij de toegang tot die gegevens, en dat toeziet op de naleving van de wet op de bescherming van persoonsgegevens. Het is een onafhankelijk, collegiaal orgaan en bestaat uit een voorzitter en vier leden. De leden van de commissie en haar voorzitter worden op voordracht van de Raad van Ministers door de Nationale Assemblee verkozen voor een termijn van vijf jaar en kunnen voor een volgende termijn worden herkozen. Een van de belangrijkste taken van de commissie is het doorverwijzen van zaken in verband met inbreuken op de GDPR naar het Hof van Justitie in Bulgarije.

3.4 Hoe veiligheidsrisico's voor gegevens te vermijden

Een van de belangrijkste dingen die we moeten doen om onze gegevens te beschermen, is het hebben van een sterk wachtwoord. Dat is erg nuttig omdat cybercriminelen tegenwoordig steeds nieuwe en innovatieve manieren bedenken om accounts te hacken en persoonlijke gegevens in handen te krijgen. Enkele mogelijke gevolgen van zwakke wachtwoorden zijn datalekken, identiteitsdiefstal, computerkaping, chantage en verlies van privacy.

Om te voorkomen dat mensen deze gevolgen ondervinden, volgen hier instructies over hoe u een sterk wachtwoord kunt maken waarop u kunt vertrouwen.
- Gebruik nooit persoonlijke informatie. Het lijkt misschien voor de hand liggend, maar veel mensen gebruiken hun eigen persoonlijke informatie bij het maken van hun wachtwoord. Het wordt aanbevolen om geen namen, verjaardagen, adressen of telefoonnummers te gebruiken.
- Gebruik een combinatie van letters, cijfers en symbolen. Hoe meer willekeurige tekens u gebruikt, hoe complexer uw wachtwoord zal zijn.
- Geef prioriteit aan de lengte van uw wachtwoord. Dit verkleint de kans dat u het slachtoffer wordt van een cyberaanval.
- Herhaal nooit wachtwoorden. Mensen zijn gewend om altijd hetzelfde wachtwoord te kiezen. Dit is een grote fout omdat het hen in gevaar brengt voor credential stuffing aanvallen.
- Vermijd het gebruik van echte woorden. Hackers gebruiken kwaadaardige programma's die elk woord uit een woordenboek kunnen verwerken om wachtwoorden te kraken. Daarom kan het gebruik van verzonnen woorden helpen om een sterk en veilig wachtwoord te maken.

Om uw informatie te beschermen is het bovendien aan te raden om alleen websites te gebruiken die u vertrouwt. Veel mensen weten niet hoe ze moeten controleren of een website veilig is of niet, daarom zullen enkele tips worden gegeven.

Controleer allereerst of de URL de juiste spelling heeft, beveiligd is met "https" en een soort indicator heeft dat het geverifieerd is, zoals een slotje.
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. Daarom zijn deze sites vatbaar voor malware, wat een bedreiging kan vormen voor uw veiligheid.
Ten derde moet u kunnen controleren of er contactinformatie beschikbaar is, evenals een toegankelijk privacybeleid. Deze zijn meestal helemaal onderaan de homepage te vinden. Een andere nuttige tip is om te lezen een aantal getuigenissen en recensies voor de site van andere mensen, zodat u kunt krijgen om te weten ervaringen die andere mensen hadden met behulp 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 bieden gratis is, maar het heeft wel een prijs. Deze gratis WIFI-hotspots stellen hackers in staat zich tussen de persoon die er gebruik van maakt en het verbindingspunt te plaatsen, dus in plaats van rechtstreeks met de hotspot te praten, sturen mensen hun informatie naar de hacker, die zich er vervolgens op baseert. Hackers hebben dan toegang tot elk stukje informatie dat mensen over het internet versturen: belangrijke e-mails, kredietkaartinformatie en beveiligingsgegevens. Als hackers die informatie eenmaal hebben, kunnen ze toegang krijgen tot uw systemen alsof ze u zijn. Om te voorkomen dat u op deze manier wordt gehackt, is het raadzaam WIFI uit te schakelen wanneer u het niet nodig hebt en wanneer u dit soort verbindingen toch moet gebruiken, dit te doen met een VPN. Een VPN is een virtueel privénetwerk aangezien het zal helpen uw informatie sterk te versleutelen. Als u echt gebruik moet maken van deze gratis WIFI, probeer dan niet online te bankieren, te winkelen of te werken. Wat ook kan helpen is Bluetooth en het delen van bestanden uit te schakelen.
Hoe kunnen personen hun persoonlijke gegevens beschermen?

1. Beveilig uw accounts
In het afgelopen decennium hebben datalekken en wachtwoordlekken grote bedrijven getroffen, zoals Facebook, Home Depot, Marriott, Yahoo, enzovoort, en ook overheidsinstellingen hebben te lijden gehad onder cyberaanvallen waardoor derde onbevoegden toegang hebben gekregen tot persoonlijke gegevens van burgers (bijvoorbeeld de aanval op de Bulgaarse nationale belastingdienst in 2019). Als u online accounts hebt, is het mogelijk dat hackers gegevens van ten minste een daarvan hebben gelekt. Om dat te controleren, kunt u uw e-mailadres zoeken op Have I Been Pwned? om uw e-mailadres te vergelijken met honderden datalekken (een "inbreuk" is een incident waarbij gegevens onopzettelijk worden blootgesteld in een kwetsbaar systeem, meestal als gevolg van onvoldoende toegangscontroles of beveiligingszwakheden in de software).

Er zijn andere manieren om mogelijke aanwijzingen te identificeren dat een account is gehackt, uw identiteit is gestolen of uw gegevens op een andere manier zijn geschonden. Leer uzelf de waarschuwingssignalen van een mogelijke inbreuk kennen en creëer positieve gewoonten voor het bewaken van uw persoonlijke gegevensbeveiliging om mogelijke aanvallen of inbreuken te identificeren voordat ze escaleren tot verwoesting. Lees tips over gegevensbescherming en informatie over de waarschuwingssignalen van een datalek of hack, zoals deze lijst met "15 tekenen dat u bent gehackt - en hoe u kunt terugvechten".

Als uw account is gehackt, uw gegevens verloren zijn gegaan of uw apparaat is gestolen, beschouw dit dan als een leermoment. Zoek uit wat er precies is misgegaan en hoe u uw gegevens had kunnen beschermen door betere voorzorgsmaatregelen te nemen. Terwijl u dingen repareert, is het een goed moment om een stap terug te doen en uzelf een meer fundamentele vraag te stellen: Wat was de reden voor de inbreuk? Als het om uw bankrekening ging, ligt het antwoord misschien voor de hand. In andere gevallen, zoals bij e-mail, kan het om allerlei redenen zijn - van het versturen van spam tot het vragen van geld aan uw contactpersonen of het resetten van wachtwoorden bij andere diensten. Een aanvaller kan zelfs proberen toegang tot uw bedrijf te krijgen. Als u weet waarom u het doelwit was, kunt u soms ook beter begrijpen hoe u werd aangevallen.

Een manier om het niveau van digitale beveiliging te verhogen en onze persoonlijke gegevens te beschermen is het gebruik van een wachtwoordmanager om verschillende, complexe wachtwoorden voor elke account te genereren en te onthouden - dit is een van de belangrijkste dingen die mensen kunnen doen om hun privacy en veiligheid vandaag de dag te beschermen. LastPass en 1password kunnen u hierbij helpen door wachtwoorden te genereren, accounts te controleren op beveiligingsinbreuken, voor te stellen zwakke wachtwoorden te wijzigen en uw wachtwoorden te synchroniseren tussen uw computer en telefoon. Gebruik geen burgerservicenummers, telefoonnummers, adressen of andere persoonlijk identificeerbare informatie als wachtwoorden.

Een andere suggestie is om waar mogelijk tweestapsverificatie te gebruiken voor uw online accounts. De meeste banken en grote sociale netwerken bieden deze optie. Zoals de naam al zegt, vereist authenticatie in twee stappen twee stappen: het invoeren van uw wachtwoord en het invoeren van een nummer waartoe alleen u toegang heeft. Stap één is bijvoorbeeld het inloggen bij Facebook met uw gebruikersnaam en wachtwoord. In stap twee stuurt Facebook u een tijdelijke code in een sms of, nog beter, via een app als Google Authenticator, en u voert die code in om in te loggen.

2. Bescherm uw surfen op het web

Bedrijven en websites volgen alles wat we online doen. Elke advertentie, knop op een sociaal netwerk en website verzamelt informatie over uw locatie, surfgewoonten en meer. De verzamelde gegevens onthullen meer over u dan u zou verwachten. Zelfs als u uw persoonlijke informatie niet openbaar deelt op sociale media, is de kans groot dat de websites die u regelmatig bezoekt alle gegevens leveren die adverteerders nodig hebben om vast te stellen wat voor soort persoon u bent. Dit is een van de redenen waarom gerichte advertenties een van de meest verontrustende innovaties van het internet blijven.

Een browserextensie zoals uBlock Origin blokkeert advertenties en de gegevens die ze verzamelen. De uBlock Origin-extensie voorkomt ook dat malware in je browser wordt uitgevoerd en biedt je een eenvoudige manier om de advertentieblokkering uit te schakelen wanneer je sites wilt ondersteunen waarvan je weet dat ze veilig zijn. Je kunt uBlock combineren met Privacy Badger, dat trackers blokkeert, en advertenties zullen niet overal verschijnen. Om stalkeradvertenties nog meer te vertragen, schakelt u op interesses gebaseerde advertenties van Apple, Facebook, Google en Twitter uit. Veel websites bieden de mogelijkheid om je af te melden voor het verzamelen van gegevens, maar je moet dit handmatig doen. Dit zal het probleem niet volledig elimineren, maar het zal de hoeveelheid verzamelde gegevens aanzienlijk verminderen.

Het installeren van de HTTPS Everywhere-extensie helpt ook bij het beschermen van uw persoonlijke gegevens. Het leidt je automatisch naar de beveiligde versie van een site als de site dat ondersteunt, waardoor het voor een aanvaller - vooral als je op openbare wifi zit in een koffietent, op een vliegveld of in een hotel - moeilijk wordt om digitaal af te luisteren wat je aan het doen bent.

3. Gebruik antivirussoftware op uw computer

Virussen lijken misschien niet meer zo vaak voor te komen als tien jaar geleden, maar ze bestaan nog steeds. Kwaadaardige software op uw computer kan allerlei soorten schade aanrichten, van vervelende pop-ups tot het heimelijk delven van bitcoin tot het scannen naar persoonlijke informatie. Als u het risico loopt op gevaarlijke koppelingen te klikken, of als u een computer deelt met meerdere mensen in een huishouden, is het de moeite waard om antivirussoftware in te stellen, vooral op Windows-computers. Als uw computer Windows 10 gebruikt, moet u de ingebouwde software van Microsoft, Windows Defender, gebruiken. U kunt ook een extra beschermingslaag hebben als u een antivirusprogramma installeert.

4. Werk uw software en apparaten bij

Besturingssystemen van telefoons en computers, webbrowsers, populaire apps en zelfs smart-home-apparaten krijgen regelmatig updates met nieuwe functies en beveiligingsverbeteringen. Deze beveiligingsupdates zijn doorgaans veel beter in het tegengaan van hackers dan antivirussoftware. Alle drie grote besturingssystemen kunnen automatisch worden bijgewerkt, maar u moet wel even controleren of automatische updates zijn ingeschakeld voor het besturingssysteem van uw keuze: Windows, MacOS of Chrome OS. Hoewel het frustrerend is om uw computer aan te zetten en te moeten wachten op een update die de software die u gebruikt mogelijk kapotmaakt, zijn de veiligheidsvoordelen de moeite waard. Uw telefoon heeft ook opties voor automatische updates, maar soms moet u de installatie van updates handmatig goedkeuren.

5. Installeer geen software die u niet volledig kent en vertrouwt

Elke vreemde app die je op je telefoon installeert en elke browserextensie of elk stukje software dat je van een vage website downloadt, is weer een potentieel privacy- en veiligheidslek. Talloze mobiele apps traceren je locatie overal waar je gaat en oogsten je gegevens zonder toestemming te vragen, zelfs in apps voor kinderen. blijf bij het rechtstreeks downloaden van programma's en browserextensies van hun makers en officiële app stores.

Hier kun je zien welke apps toegang hebben tot je locatie, contacten, microfoon en andere gegevens. Schakel machtigingen uit als ze niet zinvol zijn - Google Maps heeft bijvoorbeeld uw locatie nodig om te kunnen werken, maar uw notitie-app niet. Denk in de toekomst na over app-machtigingen wanneer u nieuwe software installeert; als een app gratis is, verzamelt en verkoopt deze mogelijk uw gegevens.

6. Schakel Bluetooth uit als u het niet gebruikt

Bluetooth-technologie heeft de mobiele wereld ongelooflijk veel gemakken gebracht, maar het opent ook de deur voor kwetsbaarheden. De meeste bedreigingen die gebruik maken van Bluetooth-verbindingen zijn afhankelijk van de actieve Bluetooth-verbinding, en hoewel ze meestal niet verwoestend of gevaarlijk zijn, zijn ze zeker ongemakkelijk en kunnen ze ernstig zijn. "Bluetooth-aanvallen zijn afhankelijk van het misbruiken van het proces voor het aanvragen en verlenen van toestemming, dat de ruggengraat van Bluetooth-verbindingen vormt. Ongeacht de beveiligingsfuncties op uw apparaat, is de enige manier om volledig te voorkomen dat aanvallers misbruik maken van dat proces van toestemming vragen/verlenen, de Bluetooth-functie van uw apparaat uit te schakelen wanneer u het niet gebruikt - niet in een onzichtbare of ondetecteerbare modus, maar volledig uitschakelen.

7. Wees overdreven voorzichtig bij het delen van persoonlijke informatie

Deze tip geldt zowel voor de online als de offline wereld: Wie vraagt om uw persoonlijke informatie, zoals uw burgerservicenummer of creditcardgegevens? Waarom hebben ze die nodig? Hoe gaan ze die gebruiken? Welke veiligheidsmaatregelen hebben ze genomen om ervoor te zorgen dat uw privé-informatie privé blijft? Al deze belangrijke vragen moeten duidelijk worden beantwoord voordat u uw persoonlijke gegevens aan iemand verstrekt.

8. Kijk uit voor imitators

In verband met de vorige tip zijn er veel bedriegers die nietsvermoedende consumenten proberen te verleiden tot het verstrekken van hun gevoelige persoonlijke informatie door zich voor te doen als de bank, creditcardmaatschappij of andere entiteit van de persoon. Dit kan telefonisch of online gebeuren, via phishing-e-mails of websites die zijn ontworpen om het uiterlijk en het gevoel van het authentieke bedrijf na te bootsen. Zorg ervoor dat u weet wie uw persoonlijke of financiële informatie krijgt. Geef geen persoonlijke informatie via de telefoon, per post of via internet tenzij u het initiatief hebt genomen tot het contact of weet met wie u te maken hebt. Als een bedrijf dat beweert een rekening bij u te hebben een e-mail stuurt waarin om persoonlijke informatie wordt gevraagd, klik dan niet op de links in de e-mail. Typ in plaats daarvan de naam van het bedrijf in uw webbrowser, ga naar hun site en neem contact met hen op via de klantenservice. Of bel het nummer van de klantenservice dat op uw rekeningafschrift staat. Vraag of het bedrijf echt een verzoek heeft gestuurd.

9. Deel niet te veel informatie op sociale netwerkplatforms

Sociale netwerken zijn voor veel mensen een manier van leven geworden, maar het delen van te veel persoonlijke informatie op uw sociale media-profielen kan gevaarlijk zijn. Veel hackers zijn er bijvoorbeeld in geslaagd om wachtwoorden te raden door middel van trial-and-error-methoden, door combinaties te gebruiken van veelvoorkomende informatie (zoals de namen van kinderen, adressen en andere details) die gemakkelijk te vinden zijn op de sociale-mediaprofielen van gebruikers. Post geen informatie die u kwetsbaar maakt, zoals uw adres of informatie over uw agenda of routine. Als uw connecties informatie over u posten, zorg er dan voor dat de gecombineerde informatie niet meer is dan u comfortabel vindt dat vreemden weten. Wees ook attent bij het posten van informatie, inclusief foto's, over je connecties.

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

Sociale netwerken zoals Facebook bieden gebruikers de mogelijkheid om hun privacyinstellingen aan te passen. Op Facebook kunt u bijvoorbeeld kiezen wie de inhoud kan zien die u post en wie informatie op uw profiel kan zien, zoals uw plaats van tewerkstelling, geboortedatum en woonplaats. Kies altijd het hoogst mogelijke privacyniveau om ervoor te zorgen dat uw persoonlijke gegevens niet in handen komen van iemand met kwade bedoelingen. De inhoud die u online plaatst, zal lang blijven bestaan, maar u kunt de privacyinstellingen op de meeste sociale mediasites aanpassen. Dit heeft invloed op wie contact met u kan opnemen en wie de informatie kan zien die u plaatst. Wees kieskeurig: hoewel het leuk is om informatie te delen, moet u uw online reputatie niet uit het oog verliezen. En als u te veel informatie openbaar maakt, kan dit door identiteitsdieven worden gebruikt om uw identiteit te kapen.

11. Vergeet niet uit te loggen

Aanmelden bij online diensten is nodig wanneer u toegang wilt tot uw persoonlijke accounts, maar veel gebruikers vergeten zich af te melden wanneer ze klaar zijn met een dienst. Wanneer u toegang hebt tot accountgebaseerde websites via een openbare computer (of een gedeeld apparaat), moet u ervoor zorgen dat u zich afmeldt bij de service wanneer een sessie is beëindigd. Het feit dat een nieuwe website wordt geopend na een bezoek aan een site waarop u bent aangemeld, betekent niet dat de volgende gebruiker niet op de back-knop kan drukken en toegang kan krijgen tot uw aangemelde account. Sommige systemen zijn zo ingesteld dat informatie ook automatisch wordt opgeslagen, dus controleer of deze functie kan worden uitgeschakeld.

12. Open geen e-mails van mensen die u niet kent

Als u een e-mail ontvangt van een bron of persoon die u niet herkent, open hem dan niet, en vermijd zeker het klikken op links of bestandsbijlagen. Er is een gouden regel voor het omgaan met spam e-mails: als het eruit ziet als een spambericht, is het dat waarschijnlijk ook - dus verwijder het bericht zonder erop te klikken of iets te downloaden. Dergelijke berichten kunnen software bevatten die de afzender vertelt dat u de e-mail hebt geopend, waarmee wordt bevestigd dat u een actieve account hebt, wat kan leiden tot nog meer spamberichten. Sommige malwareprogramma's kunnen uw e-mailadres stelen en het gebruiken om opnieuw spamberichten te verzenden onder het mom van een legitiem adres. Bedriegers kunnen zich bijvoorbeeld voordoen als iemand die u kent, zoals een vriend, familielid of collega. Als het bericht in kwestie afkomstig lijkt te zijn van iemand die u kent, neem dan buiten uw e-mail om contact met hem op.

13. Sla geen wachtwoorden op in uw browser

Het is een gevaarlijke gewoonte om wachtwoorden in browsers te 'onthouden'. Als iemand toegang krijgt tot uw computer of mobiele apparaat, kan hij gemakkelijk toegang krijgen tot alle accounts waarvoor u inloggegevens in uw browser hebt opgeslagen. Het maakt inloggen misschien gemakkelijker, maar het is een riskante gewoonte als het gaat om gegevensbescherming. Houd deze pop-ups in de gaten en zorg ervoor dat u ze weigert.

14. Gebruik geen sociale media-inloggegevens om u te registreren voor of aan te melden bij sites van derden

Het lijkt een handige optie: Registreer u gewoon voor een website of online dienst met uw Facebook- of LinkedIn-account, en zolang u bent aangemeld bij dat sociale netwerk, is aanmelden bij de site van derden snel en eenvoudig. Dit kan echter uw privacy in gevaar brengen. Hoewel het een handige optie is, kan het aanmelden bij een andere account met uw Facebook-gebruikersnaam en -wachtwoord betekenen dat u de andere site alle informatie geeft die Facebook over u heeft verzameld. Erger nog, als iemand uw sociale inloggegevens kaapt, kunnen ze ook toegang krijgen tot deze accounts van derden.

15. Kies een veilige, gerenommeerde e-mailprovider

Zorg ervoor dat uw e-mailprovider een goede beveiliging garandeert. U moet er zeker van zijn dat uw e-mailprovider technologie zoals DMARC gebruikt om phishing tegen te gaan en risico's te minimaliseren. Het goede nieuws is dat Google het doet, Yahoo doet het, Microsoft ondersteunt het, AOL ondersteunt het, dus als je een van deze gebruikt, ben je op weg om privacy- en veiligheidsrisico's te minimaliseren.

5. Niet-formele educatie

Er zijn andere niet-formele manieren waarop mensen zich meer bewust zijn geworden van problemen in verband met veilig online gaan. Niet alleen in het formele of specifieke onderwijs wordt over cyberbeveiliging gesproken, maar ook via nieuwsberichten, online beïnvloeders, ouders en leerkrachten, en slachtoffers die hun mond open doen, wordt op verschillende manieren aan bewustwording gedaan.

Cyberbeveiliging en privacy:

Het aanpakken of reguleren van cyberbeveiliging en privacy wordt vaak geassocieerd met officiële instellingen en instanties of formeel onderwijs. Niet-formele educatie op dit gebied heeft echter ook een impact.

Chantal Stekelenburg maakt deel uit van de Women in Cybersecurity Community Association en heeft een grote online aanhang opgebouwd. Ze heeft zich uitgesproken over cybersecurity en richt zich vooral op het aanmoedigen van vrouwen om beveiligingsenthousiastelingen en -deskundigen te worden.

Cyberpesten

Beïnvloeders en andere personen die zich over cyberpesten hebben uitgesproken, hebben een belangrijk effect gehad op de manier waarop mensen tegen deze kwestie aankijken en op de mate waarin mensen hierover zijn voorgelicht. Veel jongeren schamen zich vaak om zich op een formele of officiële manier uit te spreken, door aangifte te doen of personeel op school of binnen andere instellingen te waarschuwen. Niet-formele benaderingen zijn dus nuttig omdat zij mensen die cyberpesten hebben meegemaakt, in staat stellen zich met anderen in verbinding te stellen, zich minder alleen te voelen en eerder geneigd zijn zich uit te spreken.

Een nieuwsartikel in 2018 meldde dat een Nederlands hof van beroep een gevangenisstraf bevestigde voor een man die was veroordeeld voor het cyberpesten van vele jonge mannen en vrouwen, velen uit Nederland. Hij had meisjes onder druk gezet om seksuele handelingen te verrichten voor webcams. Dit verhaal kreeg veel aandacht in de media en kan worden gezien als een duidelijk voorbeeld van niet-formele educatie met betrekking tot cyberpesten en cybercriminaliteit. Hoe meer aandacht aan dit soort zaken wordt besteed, hoe meer mensen zich ervan bewust worden dat cyberpesten en cybercriminaliteit voorkomen en gerapporteerd kunnen worden.

4. Non-formal Education

Haatdragende taal

Het belang van niet-formeel onderwijs strekt zich uit tot haatzaaiende taal, aangezien het van vitaal belang is dat mensen zich hiertegen uitspreken. Er zijn belangrijke campagnes over dit onderwerp geweest.

In Nederland is er een nationale campagne, als onderdeel van de bredere No Hate Speech Youth Campaign van de Raad van Europa, die tot doel heeft jongeren te mobiliseren om haatzaaiende taal te bestrijden en de mensenrechten te bevorderen. Dit moedigt mensen aan om haatzaaiende taal te melden en direct aan te pakken. Online activisten beschikken zo over een platform en een gemeenschap waar zij ideeën kunnen uitwisselen en zich kunnen verenigen tegen deze kwestie, waardoor mensen in staat worden gesteld haatzaaien aan de kaak te stellen.

Spanje

Als we het hebben over niet-formele educatieve manieren om mensen bewust te maken van cyberpesten en haatzaaien in Spanje, kunnen we niet heen om de belangrijke rol van cultuur, beïnvloeders en grote marketingcampagnes.

Cyberpesten

Influencers zijn inderdaad een potentiële referentie voor mensen. Met miljoenen volgers is dit nieuwe beroep in staat een hoger doel te bereiken via sociale media en online platforms. De methodologie is eenvoudig en doeltreffend: terwijl mensen in hun vrije tijd sociale media consumeren, ontvangen zij ook al deze informatie die door de influencers wordt doorgegeven zonder dat zij daarvoor extra moeite hoeven te doen.

In Spanje zijn er veel voorbeelden van influencers die hun spotlights hebben gebruikt om mensen bewust te maken van cyberpesten. Y luego ganas tú (Nube de Tinta) bijvoorbeeld is een boek met korte verhalen waarin de auteurs (5 Spaanse influencers) door middel van hun eigen verhalen en ficties die putten uit de realiteit, het probleem van pesten op school vertellen. Een probleem dat als samenleving uit de hand loopt: één op de twee scholieren in Spanje beweert te maken te hebben gehad met een vorm van pesten of cyberpesten. Deze influencers zijn Javier Ruescas, Manu Carbajo, Jedet Sánchez, María Herrejón y Andrea Compton en zij zijn populair in Spanje vanwege hun strijd voor sociale rechten en zichtbaarheid.

Een ander voorbeeld van een poging om cyberpesten te bestrijden is de podcast Estirando el chicle van Carolina Iglesias en Victoria Martín. In deze podcast worden verschillende bekende mensen geïnterviewd over onderwerpen als cyberpesten en de zichtbaarheid van LGBT. De podcast heeft veel erkenning gekregen met prijzen zoals de Ondas Award voor de beste podcast of het beste digitale omroepprogramma, omdat het "een baanbrekend programma is in termen van taal en aanpak dat humor, interviews en sociale inhoud zonder vooroordelen mengt". Daarnaast is het ook relevant te vermelden hoe het bekende shampoomerk H&S heeft bijgedragen aan de strijd tegen pesten. In de campagne "Stop het pesten" proberen vele Spaanse publieke figuren, zoals Marta Pompo of Ebai, het bewustzijn te vergroten door hun eigen ervaringen met haatzaaien in de sociale media te vertellen. Daarnaast zal op de H&S-website een educatieve microsite worden geactiveerd met adviezen voor leerlingen, leerkrachten en ouders om hen een actieve rol te laten spelen in pestsituaties. Evenals voorlichtingspillen om de verschillende betrokken partijen bewuster te maken.

BELGIË (CONEXX-EU)

Uit België willen we de aandacht vestigen op een communicatiecampagne tegen cyberpesten door jongeren en een van de belangrijkste beïnvloeders onder de aandacht brengen:

WAT TEGEN WAT PESTEN Campagne

Jongerenplatform WAT WAT werkt samen met influencers en jongeren om pesten onder jongeren bespreekbaar te maken aan de hand van tips en ervaringen. Met een Facebook messenger dilemma spel, wakkert WAT WAT het gesprek over pesten aan. Pesten of gepest worden, trollen of liken, pester of pukkelhoofd: de keuze is aan jou.

Ze ontwikkelden een campagne tijdens de Vlaamse "Week tegen pesten" om kinderen en jongeren bewust te maken van wat pesten is, wat je ertegen kan doen en welke gevolgen pesten heeft.

Waargebeurde verhalen werden publiekelijk gedeeld: Angel (16) werd door haar pesters gedwongen gft-afval te eten. In de week tegen pesten deelt zij - samen met Yasmien Naciri (27), Margot (22) en Jorrit (23) - haar verhaal en laat ze haar littekens zien van jarenlang pesten. Deze moedige verhalen zetten jongeren aan tot nadenken, tot praten en tot het helpen van elkaar.

WAT WAT roept iedereen op om meer te doen tegen pesten. Maak een statement door de campagneposters op te hangen in klaslokalen of jeugdlokalen en maak pesten bespreekbaar in je groep met de spelmethodiek met de hashtag #tegenpesten

Angèle, de meest succesvolle Belgische zangeres van het moment, is met 3,6 miljoen ook de meest gevolgde influencer op Instagram in het land (Statista, 2019). Niet alleen dat, de artieste zet zich behoorlijk in voor gelijke educatie en het einde van haatzaaien tegen vrouwen en de LGTBI+ gemeenschap, en dat is terug te horen in haar liedjes.

5. Conclusions

5. Conclusie

In dit handboek zijn cyberpesten en haatdragende taal uitgelegd en in een context geplaatst. Hun definities kunnen verschillen van land tot land, maar beide worden beschouwd als agressie tegen andere mensen. In het geval van cyberpesten zijn er gewoonlijk drie actoren (de dader, het slachtoffer en omstanders), in het geval van haatdragende taal is het moeilijker om een gemeenschappelijk scenario vast te stellen, maar het gaat evenzeer om een persoon die discrimineert en de receptor die wordt gediscrimineerd.

Dit handboek bevat verschillende manieren om cyberpesten en haatdragende taal 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 rechtskader van het land. In Spanje bijvoorbeeld kun je aangifte doen bij de politie, terwijl er in Nederland een nationale hulplijn voor discriminatie bestaat. Bovendien wordt aangetoond waarom begrippen als gegevensbescherming of CIAD-triade belangrijk zijn en welke soorten privacybedreigingen er zijn, zoals identiteitsdiefstal, online seksuele intimidatie, phising of fraude.

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

6. References

101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Online Safe in 2022. (2022, May 26). Digital Guardian. https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe

A, D. (2020). *Cyberbullying (for Parents) - Nemours KidsHealth*. Nemours KidsHealth. https://kidshealth.org/en/parents/cyberbullying.html

A, D. (2020). *Cyberbullying (for Parents) - Nemours KidsHealth*. Nemours KidsHealth. https://kidshealth.org/en/parents/cyberbullying.html

A. (2018). *Report security vulnerabilities | TikTok Help Center*. TikTok. https://support.tiktok.com/en/safety-hc/reporting-security-vulnerabilities/reporting-the-security-vulnerabilities.

Assistant Secretary for Public Affairs (ASPA). (2019b, December 4). *Report Cyberbullying*. StopBullying.Gov. https://www.stopbullying.gov/cyberbullying/how-to-report

Assistant Secretary for Public Affairs (ASPA). (2021, May 21). *Tips for Teachers*. StopBullying.Gov. https://www.stopbullying.gov/cyberbullying/tips-for-teachers

C, S. (2021). *Password security: How to create strong passwords in 5 steps.* Norton. https://us.norton.com/internetsecurity-privacy-password-security.html.

Caroline Rizza. (2013). *Social networks and Cyber-bullying among teenagers: EU Scientific e political report*. https://doi.org/10.2788/41784

Celine Chateau. (2016). *Policy department Citizen¡s rights and constitutional affairs*. https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

Center, C. R. (2021, October 18). Preventing Cyberbullying: Top Ten Tips for Adults Who Are Being Harassed Online. Cyberbullying Research Center. https://cyberbullying.org/preventing-cyberbullying-adults

CISCO. (2021). Think Before You Click [Slides]. CISCO. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/phishing-program-infographic.pdf

Commission for Personal Data Protection, available. (2019). FOLD. https://www.cpdp.bg/?p=element&aid=12

Convention on Cybercrim (No. 185). (2001, November). Convention on Cybercrime. https://rm.coe.int/1680081561

Cyberbullying Research Center. (2022). Cyberbullying Fact Sheet: Identification, Prevention, and Response. https://cyberbullying.org/cyberbullying-fact-sheet-identification-prevention-and-response

Defining online sexual harassment. (2021, December 15). Childnet. https://www.childnet.com/what-we-do/our-projects/project-deshame/defining-online-sexual-harassment/

Digital Guardian. (22–05-26). 101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Online Safe in 2022. https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe.

Facebook - Meld je aan of registreer je. (2018). Facebook. https://www.facebook.com/unsupportedbrowser

Griffin, M. (2020, March 5). Advice on what to do if your child is a victim of cyber bullying. Laya Healthcare. https://www.layahealthcare.ie/thrive/family/what-to-do-if-your-child-is-victim-of-cyber-bullyi/.

How to Protect Your Digital Privacy. (2019). The Privacy Project Guides - The New York Times. https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy

Identity Theft. (2022, June 12). Investopedia. https://www.investopedia.com/terms/i/identitytheft.asp

Instagram Help Center. (2018). Instagram. https://help.instagram.com/192435014247952?helpref=uf_permalink

J. (2013). Social Networks and Cyber-bullying among Teenagers. JRC Publications Repository. https://publications.jrc.ec.europa.eu/repository/handle/JRC80157

L. (2021, 28 enero). Ciberdelincuencia en el código penal - Letslaw. LetsLaw. https://letslaw.es/ciberdelincuencia/

L.J. (2022, June 2). Delitos en redes: de cinco años de cárcel a multas de hasta 2.700 euros. Diario Noticias de Álava. https://www.noticiasdealava.eus/vivir-on/internet-y-ciencia/2022/04/24/delitos-redes-consecuencias/1183252.html.

Lex.bg - Р—РºРєРѕРЅРёР»РЅРёС†Рё, РїРЂРºРІРёР»РЅРёС†Рё, РєРѕРЅСЃС‚РёС‚СѓС†РёСЏ, РєРѕРґРµРєСЃРё, РґРЂР¶РєРІРµРЅ РІРµСЂСЃРёСЏ РїРѕ РїРёРЂР»РєРѕРІРѕ. (2017). Lex.Bg. https://www.lex.bg/laws/ldoc/1589654529

P. (2020). *Why is Data Protection Important?* PECB. https://pecb.com/article/why-is-data-protection-important

S, G. Cyberstalking: Prevention, Consequences, and Coping. (2021, August 17). Verywell Mind. https://www.verywellmind.com/what-is-cyberstalking-5181466

Safety and security. (2018). Twitter. https://help.twitter.com/en/safety-and-security

W, The Dangers of Hacking and What a Hacker. (2020). © Copyright 2004 - 2022 Webroot Inc. All Rights Reserved. https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-hackers

What Is Internet Fraud? Types of Internet Fraud. (2019). Fortinet. https://www.fortinet.com/resources/cyberglossary/internet-fraud

What is personal data? (2018, August 1). European Commission - European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

What Is Phishing? (2022, May 5). Cisco. https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#%7Ehow-phishing-works

Wilkey Oh, E. (2020, March 15). Teachers' Essential Guide to Cyberbullying Prevention. Common Sense Education. https://www.commonsense.org/education/articles/teachers-essential-guide-to-cyberbullying-prevention

Ф. (2009). Киберсигурност. Фондация. https://www.netlaw.bg/bg/a/kiber-sigurnost


www.digit-safe.com
info@digit-safe.com