Digitale Veiligheid & Criminaliteit 2018

Digitale Veiligheid & Criminaliteit 2018

Verklaring van tekens

Niets (blanco)	Een cijfer kan op logische gronden niet voorkomen
.	Het cijfer is onbekend, onvoldoende betrouwbaar of geheim
*	Voorlopige cijfers
**	Nader voorlopige cijfers
2018–2019	2018 tot en met 2019
2018/2019	Het gemiddelde over de jaren 2018 tot en met 2019
2018/'19	Oogstjaar, boekjaar, schooljaar enz., beginnend in 2018 en eindigend in 2019
2016/'17–2018/'19	Oogstjaar, boekjaar, enz., 2016/'17 tot en met 2018/'19

In geval van afronding kan het voorkomen dat het weergegeven totaal niet overeenstemt met de som van de getallen.

Colofon

Uitgever
Centraal Bureau voor de Statistiek
Henri Faasdreef 312, 2492 JP Den Haag
www.cbs.nl

Prepress
Centraal Bureau voor de Statistiek

Ontwerp
Edenspiekermann

Inlichtingen
Tel. 088 570 70 70
Via contactformulier: www.cbs.nl/infoservice

© Centraal Bureau voor de Statistiek, Den Haag/Heerlen/Bonaire, 2019.
Verveelvoudigen is toegestaan, mits het CBS als bron wordt vermeld.

Voorwoord

De steeds verdergaande digitalisering zorgt voortdurend voor nieuwe mogelijkheden in onze maatschappij. Mensen, bedrijven, organisaties, apparaten... iedereen en alles maakt steeds intensiever gebruik van het internet. Daarmee samenhangend wordt de digitale veiligheid steeds belangrijker en uitdagender. Dit blijkt ook uit de toenemende vraag naar betere informatie over de omvang en de aard van de digitale criminaliteit, ten behoeve van beleid en wetgeving. Het is immers belangrijk voor alle partijen dat burgers vertrouwen hebben en houden in de veiligheid rondom internetgebruik.

In 2018 is door het Centraal Bureau voor de Statistiek in samenwerking met de politie een nieuw onderzoek naar Digitale Veiligheid & Criminaliteit uitgevoerd. Het onderzoek heeft als doel om het thema cybercrime bij burgers zo nauwkeurig mogelijk in beeld te brengen. Aan het onderzoek hebben ruim 38 duizend personen van 12 jaar en ouder deelgenomen. De uitkomsten zijn daarmee representatief voor de Nederlandse bevolking.

In de voorliggende publicatie worden de belangrijkste resultaten van het onderzoek gepresenteerd. Aan bod komen de diverse vormen van digitale criminaliteit waar burgers in hun privéleven slachtoffer van kunnen worden. Ook de gevolgen voor het slachtoffer en de motieven voor het al dan niet doen van melding en aangifte worden beschreven. Deze publicatie gaat daarnaast in op het bewustzijn van burgers over de gevaren van het gebruik van internet.

De publicatie Digitale Veiligheid & Criminaliteit 2018 wordt in pdf-vorm uitgebracht via de website van het CBS.

Directeur-Generaal CBS
Dr. T.B.P.M. Tjin-A-Tsoi

Den Haag/Heerlen/Bonaire, juli 2019

Inhoud

1. Inleiding

Digitale veiligheid en digitale criminaliteit zijn thema's die nadrukkelijk op de politieke en maatschappelijke agenda staan. Beleidsmakers van het ministerie van Justitie en Veiligheid en vele andere departementen, politie en tal van andere maatschappelijke organisaties houden zich met deze onderwerpen bezig. Het ligt dus voor de hand dat de vraag naar meer en betere informatie over zowel digitale veiligheid als digitale criminaliteit alleen maar groeit. Het CBS publiceert jaarlijks een overzicht van de door het CBS verzamelde informatie in de Cybersecuritymonitor (CBS, 2018a), waarin onder andere gebruik wordt gemaakt van de Veiligheidsmonitor (VM) (CBS, 2018b) en het onderzoek ICT-gebruik bij huishoudens en personen (CBS, 2019a). Deze bronnen geven echter geen volledig beeld van het totale scala aan veiligheidsmaatregelen en slachtofferschap van digitale criminaliteit. Naast cijfers over de omvang van slachtofferschap van digitale criminaliteit is er ook behoefte aan informatie over de impact ervan op slachtoffers, zowel financieel als emotioneel. Ook is inzicht in het meld-, en aangiftegedrag van burgers noodzakelijk voor het maken van beleid. Daarnaast is er behoefte aan meer gegevens rondom cybersecurity; wat doet men er zelf aan om te voorkomen dat men slachtoffer wordt van digitale criminaliteit?

Het CBS heeft in samenwerking met de politie het pilotonderzoek naar Digitale Veiligheid & Criminaliteit (DVC) opgezet, waarbij de vraagstellingen zoals die nu in de reguliere Veiligheidsmonitor zijn opgenomen, zijn uitgebreid en verbeterd. Daarnaast wordt het internetgebruik en preventie van online criminaliteit door burgers in het pilotonderzoek uitgebreider onderzocht dan in het onderzoek ICT-gebruik bij huishoudens en personen.

1.1 Het belang van het meten van digitale criminaliteit

Binnen een tijdsbestek van twee à drie decennia heeft het fenomeen internet zich geworteld in de samenleving. Door het massale gebruik hiervan worden zeer grote hoeveelheden aan informatie, vaak persoonlijk van aard, vastgelegd. Deze stroom van (persoonlijke) informatie is daarmee zeer aantrekkelijk voor mensen met minder goede bedoelingen. Jaarlijks komen er veel burgers in aanraking met een of meerdere vormen van digitale criminaliteit. Een deel wordt daadwerkelijk slachtoffer, met eventueel financiële en/of emotionele gevolgen. Net als bij de traditionele 'offline' criminaliteit zijn er veel verschillende vormen van online criminaliteit. Voor dit rapport zijn een aantal hoofdgroepen van digitale criminaliteit onderscheiden, namelijk 'hacken', 'vermogensdelicten', 'interpersoonlijke incidenten', en identiteitsfraude zonder financiële schade (zie verder paragraaf 1.4 van dit hoofdstuk). De internetcriminaliteit is echter continu in beweging. Het is daarom van belang om de omvang en ontwikkeling hierin periodiek zo goed mogelijk te meten, en daarbij de onderzoeksvraagstellingen waar nodig aan te passen aan de nieuwste ontwikkelingen.

1.2 Veiligheidsmonitor en cybercrime

In 2012 heeft er voor het laatst een doorontwikkeling plaatsgevonden in zowel design als vragenlijst van de VM (CBS, 2019b). Sindsdien zijn er jaarlijks een aantal vragen opgenomen over cybercrime, waarbij de ondervraagde personen kunnen aangeven of ze in de voorgaande 12 maanden slachtoffer zijn geweest van online identiteitsfraude, aan- en verkoopfraude, hacken of cyberpesten. Daarmee was Nederland voorloper in Europa op dit gebied (Reep en Junger, 2018). De vraagstelling is grotendeels gebaseerd op een onderzoek naar cybercrime van de Noordelijke Hogeschool Leeuwarden in 2011 waarbij is samengewerkt met het CBS (Domenie et al., 2013).

De laatste uitvoering van de VM waarin hierover is gepubliceerd was in 2017 (CBS, 2018b). Als gevolg van bezuinigingen bij het ministerie van Justitie en Veiligheid heeft de Raad voor de Veiligheidsmonitor begin 2018 besloten de enquêtefrequentie van de VM te verlagen naar 1 keer per twee jaar. De eerstvolgende uitvoering is eind dit jaar (2019) en zal nog dezelfde vraagstellingen over cybercrime als in de jaren 2012–2017 bevatten, zodat trends in slachtofferschap kunnen worden gecontinueerd. Voor de uitvoering van 2021 zullen de vraagstellingen over cybercrime naar verwachting worden aangepast op basis van de leerpunten uit dit pilotonderzoek.

De uitkomsten van het pilotonderzoek zoals beschreven in dit rapport verschillen echter inhoudelijk en methodologisch van de Veiligheidsmonitor, waardoor vergelijking van uitkomsten niet mogelijk is. Dit geldt ook voor overeenkomstige cijfers over internetgebruik en internetveiligheid uit het onderzoek ICT gebruik bij huishoudens en personen dat het CBS jaarlijks uitvoert. De belangrijkste onderzoeksverschillen met beide bestaande CBS-onderzoeken worden weergegeven in dit rapport (zie bijlage).

1.3 Doel en opzet van het pilotonderzoek Digitale Veiligheid & Criminaliteit

Doel

Een van de belangrijkste doelen van het onderzoek Digitale Veiligheid & Criminaliteit is een beter totaalbeeld te krijgen van de incidentie en impact van digitale criminaliteit bij de Nederlandse bevolking van 12 jaar of ouder. Hiervoor was het nodig om nieuwe vraagstellingen te ontwikkelen. Als vertrekpunt hiervoor is na een eerste interne consultatie binnen het CBS ook gesproken met verschillende afdelingen van het ministerie van Justitie en Veiligheid (preventie, fraude), het WODC en de politie om de informatiebehoefte verder in kaart te brengen. Op basis hiervan is er een concept vragenlijst ontwikkeld. Vervolgens is deze vragenlijst ook ter beoordeling voorgelegd aan experts op het terrein van digitale criminaliteit, zoals dr. Rutger Leukfeldt en prof. dr. Marianne Junger.

Een ander belangrijk doel van het pilotonderzoek is inzicht te verkrijgen in hoe veilig men zich gedraagt op het internet. Hoe staat het met de kennis op dit terrein en welke preventiemaatregelen worden er genomen?
De vragenlijst van het pilotonderzoek Digitale Veiligheid & Criminaliteit is beschikbaar via de website van het CBS (CBS, 2019c).

Bij de analyse van de verzamelde gegevens bleek dat een aantal vragen in de enquête wellicht niet duidelijk genoeg gesteld zijn. In de methodologische verantwoording in bijlage A is beschreven hoe hiermee is omgegaan en wat mogelijke consequenties zijn voor enkele uitkomsten van dit onderzoek. Dit zijn leerpunten voor een volgende editie.

Opzet

Om ook betrouwbare detailinformatie te kunnen geven over het slachtofferschap van minder voorkomende digitale criminaliteit was een grote steekproef wenselijk. Door de samenwerking met de politie werd het uit financieel oogpunt mogelijk om een steekproef van 100 000 personen te benaderen voor dit pilotonderzoek. Hierbij is gekozen voor een internetenquête (CAWI-only). Aangezien in Nederland vrijwel alle personen toegang hebben tot het internet is hiermee een goede afspiegeling van de bevolking bereikt. Uit het onderzoek ICT-gebruik huishoudens en personen is bekend dat jongeren van 12 jaar al veel tijd doorbrengen op internet. Voor dit pilotonderzoek is daarom deze leeftijdsgrens van 12 jaar aangehouden. Het veldwerk voor het onderzoek vond plaats van begin oktober tot half december 2018. Van de 100 000 benaderde personen hebben ruim 38 000 personen meegedaan. Meer gedetailleerde informatie over de uitvoering van het onderzoek is opgenomen in de Onderzoeksverantwoording achterin deze publicatie.

1.4 Gehanteerde indeling voor slachtofers van digitale criminaliteit

In dit pilotonderzoek is slachtofferschap van digitale criminaliteit uitgebreider en gedetailleerder bevraagd dan in de VM. Door te vragen wat er precies is voorgevallen, is een beter en gedetailleerder onderscheid mogelijk binnen de verschillende hoofdvormen van digitale criminaliteit.

In dit onderzoek is slachtofferschap ingedeeld in de volgende hoofdgroepen.
- Hacken. Dit betreft alle delicten waarbij er is ingebroken op een computer(netwerk), e-mailaccount of website en waarbij gegevens verstoord, geblokkeerd of gestolen zijn, maar die niet hebben geleid tot een van de delicten in de andere hoofdgroepen.
- Vermogensdelicten. Dit betreft alle delicten waarbij de dader handelde met een financieel motief, en ook geld heeft verdiend.
- Interpersoonlijke incidenten. Dit zijn incidenten in de persoonlijke sfeer, waarbij de dader het slachtoffer heeft beledigd, gekwetst of bedreigd. Hierbij is een extra onderscheid gemaakt in interpersoonlijke incidenten zonder en met een seksuele (bij) bedoeling. Deze incidenten kunnen een grote impact hebben op het slachtoffer, maar het kan ook om roddels binnen vriendengroepen gaan.

– De categorie identiteitsfraude zonder financiële schade omvat delicten waarbij de dader de (persoons)gegevens van het slachtoffer heeft misbruikt, maar er financieel niet direct op vooruit is gegaan.

1.4.1 Indeling van delicten en incidenten voor slachto ers van digitale criminaliteit

1			**Hacken totaal inclusief modus operandi**
	1.1		Hacken[1)]
	1.2		Hacken als modus operandi[2)]
		1.2.1	Voorafgaand aan een vermogensdelict
		1.2.2	Voorafgaand aan een interpersoonlijk incident
		1.2.3	Voorafgaand aan identiteitsfraude zonder financiële schade
2			**Vermogensdelicten**
	2.1		Fraude via het betalingsverkeer
		2.1.1	Geld van rekening gehaald en/of betalingen gedaan
		2.1.2	Lening, abonnement, goederen of diensten verkregen op naam van het slachtoffer
	2.2		Fraude bij online handel
		2.2.1	Aankoopfraude
		2.2.2	Verkoopfraude
	2.3		Vermogensdelicten, anders dan via betalingsverkeer of online handel
		2.3.1	Nepboete/nepfactuur of nepactie
		2.3.2	Voorschotfraude
		2.3.3	Frauduleuze factuurwijziging
		2.3.4	Microsoftscam
		2.3.5	Wangirifraude
		2.3.6	Afpersing, bedreiging zonder geweld
		2.3.7	Ransomware of cryptoware
		2.3.8	Whaling[3)]
		2.3.9	Overige identiteitsfraude
3			**Interpersoonlijke incidenten, niet seksueel**
	3.1		Stalking
	3.2		Bedreiging met geweld
	3.3		Laster
		3.3.1	Verhalen of roddels verspreid
		3.3.2	Foto's of filmpjes verspreid
		3.3.3	Overig laster (bv. gepest, gênante website gemaakt of berichten gepost onder naam slachtoffer)
4			**Interpersoonlijke incidenten, seksueel**
	4.1		Stalking
	4.2		Bedreiging met geweld
	4.3		Laster
		4.3.1	Verhalen of roddels verspreid
		4.3.2	Foto's of filmpjes verspreid
		4.3.3	Overig laster (bv. gepest, gênante website gemaakt of berichten gepost onder naam slachtoffer)
5			**Identiteitsfraude zonder financiële schade**
	5.1		Poging geld van de rekening te halen en/of betalingen te doen
	5.2		Poging tot verkrijgen van lening, abonnement, goederen of diensten op naam van het slachtoffer
	5.3		Overige identiteitsfraude

[1)] Hiertoe behoren hackdelicten waarbij gegevens zijn verstoord, geblokkeerd of gestolen.
[2)] Hacken als modus operandi (werkwijze) omvat hackdelicten die zijn gepleegd voorafgaand aan vermogensdelicten (2), interpersoonlijke incidenten (3,4) en bij identiteitsfraude zonder financiële schade (5). Deze hackdelicten zijn bij deze andere hoofdgroepen opgenomen en meegeteld.

1.5 Leeswijzer

Hoofdstuk 2 beschrijft het totaal aan slachtofferschap van digitale criminaliteit zoals dit door burgers is gerapporteerd en gaat op hoofdniveau in op slachtofferschap van hacken, vermogensdelicten, interpersoonlijke incidenten en identiteitsfraude zonder financiële schade. Het hoofdstuk gaat van start met een korte intro van het internetgebruik in Nederland.

Hoofdstuk 3 geeft meer informatie over de hackdelicten. Wat deed het met de slachtoffers, en hebben slachtoffers het ergens gemeld? In hoofdstuk 4 worden de digitale vermogensdelicten nader besproken, waaronder fraude via het betalingsverkeer, fraude bij online handel en enkele overige vermogensdelicten die veelal het gevolg zijn van phishing. De hoofdstukken 5 en 6 richten zich op de interpersoonlijke incidenten, waarbij in hoofdstuk 5 de niet-seksuele incidenten worden beschreven en in hoofdstuk 6 de incidenten waarbij de dader een seksuele (bij)bedoeling had. Vormen van identiteitsfraude waaraan de dader géén geld heeft verdiend komen in hoofdstuk 7 aan de orde. Internetgebruikers krijgen over het algemeen vaak te maken met verschillende vormen van phishing. Hoewel het grootste deel er geen slachtoffer van wordt, kan het wel als lastig worden ervaren. Hoofdstuk 8 geeft hier inzicht in.
Naast slachtofferschap zijn in dit onderzoek ook diverse aspecten van internetveiligheid en preventieve activiteiten gemeten. In hoofdstuk 9 wordt op verschillenden aspecten van deze 'cybersecurity' ingegaan.

In de Tabellenbijlage zijn alle cijfers uit dit rapport, voorzien van betrouwbaarheidsintervallen, opgenomen. Daarna volgen de Onderzoeksverantwoording, een methodologische toelichting op slachtofferschap van digitale criminaliteit, en een toelichting op de verschillen tussen het nieuwe pilotonderzoek Digitale Veiligheid & Criminaliteit en de Veiligheidsmonitor en het ICT-onderzoek. Afgesloten wordt met een literatuurlijst en een lijst van medewerkers die aan deze publicatie hebben bijgedragen.

Samenvatting

Deze samenvatting laat op hoofdlijnen de onderzoeksresultaten zien van het pilotonderzoek Digitale Veiligheid & Criminaliteit 2018. Er wordt een overzicht gegeven van de meest belangrijke landelijke uitkomsten over het slachtofferschap van digitale criminaliteit onder internetgebruikers en cybersecurity. Deze uitkomsten worden beschreven voor het jaar 2018. Door het karakter van dit pilotonderzoek zijn er geen vergelijkbare cijfers over eerdere jaren beschikbaar.

Landelijke uitkomsten

Internetgebruik

- In 2018 telde Nederland bijna 14,5 miljoen internetgebruikers waarvan 93 procent aangaf het internet dagelijks te gebruiken.
- Ruim een derde (35 procent) van de internetgebruikers maakte gebruik van het internet op openbare plekken met behulp van WIFI zonder wachtwoord.
- Ruim 4 op de 10 internetgebruikers (41 procent) maakten nooit gebruik van Wi-Fi op openbare plekken.

Internetactiviteiten

- Bijna alle internetgebruikers (90 procent of meer) zoeken informatie, sturen berichten, en doen aan internetbanken.
- Ruim 80 procent koopt goederen of diensten.
- Bijna 70 procent gebruikt sociale media.
- Bijna de helft verkoopt goederen of diensten.

Totale slachtofferschap digitale criminaliteit

- In 2018 is bijna 1 op de 12 internetgebruikers (8,5 procent) slachtoffer geweest van digitale criminaliteit. Dit betreft 1,2 miljoen inwoners van 12 jaar of ouder.
- Mannen en vrouwen die het internet gebruiken zijn in vrijwel gelijke mate slachtoffer geweest van digitale criminaliteit. Mannen worden wel iets vaker slachtoffer van vermogensdelicten dan vrouwen (5 tegen 4 procent).
- Jongere internetgebruikers worden vaker slachtoffer van digitale criminaliteit dan oudere internetgebruikers. Van de 12- tot 18-jarigen en 18- tot 25 jarigen is in 2018 12 à 13 procent slachtoffer geweest. Van de 65-plussers was dit 3 à 4 procent.
- Vanaf het 25e levensjaar is er een lichte daling te zien in het slachtofferschap van digitale criminaliteit, en vanaf 55 jaar een grotere daling.

Hacken

- In 2018 is bijna 1 op de 50 internetgebruikers (1,8 procent) slachtoffer geweest van een of meer gevallen van hacken, waarbij gegevens zijn verstoord, geblokkeerd of gestolen.
- Bij ruim de helft (56 procent) was ingebroken op hun sociale media account; bij bijna 3 op de 10 werd het email-account gehackt.
- Inbraak gebeurt het meest doordat iemand aan de wachtwoorden komt. Iets minder dan de helft (45 procent) van de slachtoffers geeft dit aan.
- Misbruik van een email-account of profielsite is met bijna een kwart van de slachtoffers (27 procent) het meest genoemde gevolg.
- Bijna een kwart van de slachtoffers van hacken (24 procent) heeft te maken met emotionele gevolgen en bijna 4 op 10 hebben door het hacken minder vertrouwen in de digitale veiligheid.
- Melding en aangifte van hacken vindt nauwelijks plaats: 5 procent van de slachtoffers meldde dit ergens; minder dan 3 procent deed aangifte bij de politie. Belangrijkste redenen voor het slachtoffer om niet te melden en geen aangifte te doen, waren dat zij van mening waren dat het niet helpt, het niet belangrijk genoeg was, of dat het niet mogelijk was.

Vermogensdelicten

- In 2018 is bijna 1 op de 20 twintig internetgebruikers (4,6 procent) slachtoffer geweest van een of meer vermogensdelicten.

Fraude via het betalingsverkeer

- Van fraude via het betalingsverkeer werd 0,7 procent van de internetgebruikers in 2018 slachtoffer. Bij 0,5 procent werd geld van de rekening gehaald en/of betalingen gedaan; bij 0,2 procent werden op naam van het slachtoffer een lening, abonnement, goederen of diensten verkregen.
- Bij slachtoffers waarbij geld van de rekening werd gehaald, gebeurde dit vooral door phishing (30 procent) en hacken (12 procent).
- Bijna 9 op de 10 slachtoffers van wie geld van de rekening verdween (86 procent) maakten hiervan melding, vooral bij de bank of financiële instellingen. Bij de politie deden 2 op de 10 (19 procent) een melding en vrijwel evenveel deden aangifte (18 procent).

- Ruim de helft van de slachtoffers (54 procent) waarbij geld van de rekening werd gehaald heeft dit wel ergens gemeld maar geen aangifte gedaan. Belangrijkste redenen hiervoor waren dat het niet belangrijk genoeg was (15 procent) en dat de bank of creditcardmaatschappij het verder zou afhandelen (12 procent).
- Bijna 8 op de 10 slachtoffers die door betalingsfraude geld kwijt raakten van hun rekening kregen de financiële schade vergoed (78 procent). Een derde (34 procent) kreeg te maken met emotionele gevolgen. Meer dan de helft (52 procent) heeft minder vertrouwen in de digitale veiligheid.

Fraude online handel

- Van fraude bij online handel werd 2,9 procent van de internetgebruikers slachtoffer, waarvan het grootste deel van aankoopfraude (2,7 procent).
- Ruim 4 op de 10 slachtoffers van aankoopfraude (42 procent) in 2018 deden hun aankoop via een tweedehands verkoopsite. Producten waarbij vaak gefraudeerd werd zijn kleding, schoeisel en accessoires (30 procent) en mobiele telefoons (20 procent).
- Bijna 4 op de 10 slachtoffers van aankoopfraude (39 procent) meldden dit. Een kwart deed dit bij de politie. Minder dan een kwart van de slachtoffers (23 procent|) deed aangifte.
- Belangrijkste redenen om aankoopfraude niet te melden zijn dat het niet belangrijk genoeg is (30 procent) en het toch niet helpt (22 procent).
- Een op de tien slachtoffers van aankoopfraude in 2018 gaf aan de schade vergoed te hebben gekregen. Ruim 4 op de 10 zeiden dat ze kampten met emotionele gevolgen. Ruim een op de drie (35 procent) heeft door het gebeurde minder vertrouwen in de digitale veiligheid.

Andere vermogensdelicten

- Van andere vermogensdelicten waarbij slachtoffers geld kwijtraakten, was 1,2 procent van de internetgebruikers slachtoffer. Het meest voorkomend waren Wangirifraude (0,5 procent) en nepboetes/-facturen of nepacties (0,3 procent).
- Van Wangirifraude maakte 15 procent van de slachtoffers melding bij een of meerdere instanties; 6 procent deed dit bij de politie. Slechts 2 procent deed aangifte bij de politie.
- Van nepboetes/-facturen of nepacties maakte ruim 40 procent melding, waarvan 26 procent bij de politie. Een vergelijkbaar deel (24 procent) deed aangifte.

Interpersoonlijke incidenten, niet seksueel

- Van een of meer interpersoonlijke incidenten zonder seksuele (bij)bedoeling zoals stalking, bedreiging met geweld, en laster werd 1,4 procent van de internetgebruikers in 2018 slachtoffer.
- Jongeren van 12 tot 18 jaar hebben met 5 procent het vaakst last van niet-seksuele interpersoonlijke incidenten. Meisjes in die leeftijdsklasse worden er vaker mee geconfronteerd dan jongens van die leeftijd (7 tegen 4 procent).
- Het meest voorkomende niet-seksuele interpersoonlijke incident is laster (0,9 procent). Het gaat dan onder andere om roddels, foto's of filmpjes verspreiden en pesten. Stalking en bedreiging met geweld komen met 0,4 en 0,3 procent minder voor.
- Niet-seksuele interpersoonlijke incidenten vinden vooral via sociale media plaats, namelijk bij 65 procent van de slachtoffers van laster, en bij 57 procent van de slachtoffers van stalking en bedreiging met geweld.

– Slachtoffers van niet-seksuele interpersoonlijke incidenten kennen vaak de dader(s). Bij laster weet bijna driekwart (73 procent) wie dit is/zijn; bij stalking en bedreiging respectievelijk 67 en 57 procent.
– Bij bijna de helft van de slachtoffers van niet-seksuele laster en stalking (resp. 47 en 48 procent) is sprake van emotionele gevolgen, vooral boosheid. Bij bedreiging is dit bij 4 op de 10 slachtoffers het geval.
– Niet-seksuele bedreiging met geweld wordt door de slachtoffers het vaakst gezien als een strafbaar misdrijf; 27 procent geeft dit aan. De meeste slachtoffers van stalking (50 procent), bedreiging met geweld (44 procent) en laster (46 procent) beoordelen deze incidenten weliswaar als verkeerd, maar zien ze niet als een strafbaar misdrijf.
– Van de niet-seksuele interpersoonlijke delicten wordt stalking het vaakst door de slachtoffers gemeld (52 procent). Daarna volgen laster (42 procent) en bedreiging (34 procent). De aangiftepercentages bedragen respectievelijk 11, 11 en 6 procent.
– Belangrijkste reden om niet te melden of geen aangifte te doen is dat het niet helpt, waarbij vaak wordt aangegeven dat het geen zaak voor de politie is.

Interpersoonlijke incidenten, seksueel

– Van een of meer interpersoonlijke incidenten met een seksuele (bij)bedoeling zoals stalking, bedreiging met geweld en laster werd 0,7 procent in 2018 slachtoffer.
– Jongvolwassenen van 18 tot 25 jaar hebben het vaakst te maken met seksuele interpersoonlijke incidenten. Vrouwen in deze leeftijdsklasse werden met 3 procent veel vaker slachtoffer hiervan dan mannen van die leeftijd (0,8 procent).
– Seksueel getinte stalking en laster komen ongeveer evenveel voor: respectievelijk 0,4 en 0,3 procent van de internetgebruikers wordt hiervan slachtoffer. Seksuele bedreiging met geweld komt met 0,1 procent minder vaak voor.
– Seksuele interpersoonlijke incidenten vinden vooral via sociale media plaats, namelijk bij 70 procent van de slachtoffers van laster en bij 66 procent van de slachtoffers van stalking.
– Slachtoffers van seksuele interpersoonlijke incidenten weten in meer dan de helft van de gevallen wie de dader(s) is/zijn. Bij laster kent 55 procent de dader en bij stalking 52 procent.
– Ongeveer de helft van de slachtoffers van seksueel getinte stalking (51 procent) ondervindt emotionele gevolgen, vooral boosheid. Bij laster met seksuele (bij) bedoelingen is dit bij ruim 4 op de 10 slachtoffers het geval (44 procent).
– Seksuele laster wordt door ruim 2 op de 10 slachtoffers als een strafbaar misdrijf gezien. Voor seksuele stalking ligt dit met 16 procent iets lager. De grootste groep slachtoffers van laster (35 procent) en stalking (52 procent) vonden het incident weliswaar verkeerd, maar zagen dit niet als een strafbaar misdrijf.
– Seksuele stalking wordt door 50 procent gemeld bij instantie(s); seksuele laster door 45 procent. De aangiftepercentages liggen voor beide soorten incidenten rond de 10 procent.
– Belangrijkste redenen voor het niet melden van seksuele laster zijn dat het niet helpt (18 procent), dat het niet belangrijk is (10 procent), schaamte (9 procent) of dat het al is opgelost (8 procent). Bij seksuele stalking zijn dit ook de belangrijkste redenen om niet te melden. Voor beide interpersoonlijke incidenten zijn de meeste van deze redenen ook de belangrijkste om geen aangifte bij de politie te doen. Alleen speelt angst voor de gevolgen hier een grotere rol dan schaamte.

Identiteitsfraude zonder financiële schade

- Van identiteitsfraude zonder financiële schade werd in 2018 1 procent van de internetgebruikers slachtoffer.
- Bij 0,2 procent van de internetgebruikers werd een poging gedaan om geld van de rekening te halen of betalingen te doen. Bij 0,5 procent werd gepoogd om een lening, abonnement, goederen of diensten aan te vragen op naam van het slachtoffer. Bij 0,3 procent werden persoonsgegevens misbruikt voor bijvoorbeeld het aanvragen van een zorgvergoeding of voor het plegen van misdrijven.

Phishing

- In 2018 gaf 35 procent van de internetgebruikers aan dat ze in aanraking kwamen met phishing, voornamelijk via nepmails. Het gaat dan om bijvoorbeeld voorschotfraude, microsoftscam, wangirifraude of pogingen tot afpersing.
- Naar schatting 1 à 1,5 procent van de internetgebruikers heeft daadwerkelijk geld verloren door phishing.
- Vooral afperspogingen hebben een grote impact: van degenen die er niet intrapten, ondervond 1 op de 3 emotionele gevolgen, vooral boosheid, en een vergelijkbaar aandeel heeft minder vertrouwen in de digitale veiligheid.

Cybersecurity

- In 2018 zeiden 9 op de 10 internetgebruikers bekend te zijn met begrippen als back-ups, antivirusprogramma's of hacken. Met firewall en phishing zijn minstens 7 op de 10 bekend. Veel minder bekend zijn begrippen als pharming (16 procent), cryptoware (27 procent) en wangirifraude (34 procent).
- Bij het doorgeven van persoonlijke gegevens zijn internetgebruikers vooral terughoudend als het gaat om het burgerservicenummer, bank- of creditcardgegevens, of informatie over gezondheid en werk. Ongeveer de helft geeft aan deze informatie niet te delen via het internet.
- Internetgebruikers zijn dan ook het meest bezorgd over misbruik van hun bank- en persoonsgegevens. In 2018 zei 42 procent hier zeer bezorgd over te zijn.
- Vanwege de bezorgdheid over de veiligheid laten internetgebruikers bepaalde activiteiten op het web achterwege. In 2018 zei 45 procent om die reden wel eens af te zien van het doen van online aankopen, een vergelijkbaar aandeel (42 procent) vermeed het downloaden van zaken als apps, software, muziek etc.
- In 2018 gaf 1 op de 5 internetgebruikers aan nooit backups te maken; 1 op de 10 zei nooit computerprogramma's (bijvoorbeeld besturingssysteem, virusscanner of internetbrowser) te updaten of vernieuwen. Eveneens 1 op de 10 beschermde de toegang tot de apparatuur nooit met toegangscodes, wachtwoorden en dergelijke.

2. Internetgebruik en slachtoerschap van digitale criminaliteit

We leven in een maatschappij waar het internet niet meer weg te denken is in het dagelijks leven. De opkomst van internet biedt naast veel positieve kanten echter ook negatieve: het wereldwijde web is een nieuwe vrijplaats waar ook mensen met minder goede bedoelingen hun slag proberen te slaan.
In dit hoofdstuk wordt op hoofdlijnen beschreven welk deel van de Nederlandse internetgebruikers van 12 jaar of ouder in 2018 slachtoffer is geweest van digitale criminaliteit (paragraaf 2.2). Hierbij wordt het slachtofferschap ook verbijzonderd naar de in dit onderzoek onderscheiden hoofdgroepen hacken, vermogensdelicten, persoonlijke delicten en identiteitsfraude zonder financiële schade. In de volgende hoofdstukken worden deze hoofdgroepen verder in detail beschreven. Om het slachtofferschap van digitale criminaliteit in perspectief te plaatsen, zal eerst in paragraaf 2.1 een beeld worden gegeven van het internetgebruik in Nederland.

2.1 Internetgebruik

In 2018 telde Nederland bijna 14,9 miljoen mensen van 12 jaar of ouder en de meesten van hen (97,7 procent ofwel 14,5 miljoen) gaven aan gebruik te maken van het internet. Van alle internetgebruikers zei 92,6 procent (bijna 13,5 miljoen) dagelijks voor privédoeleinden van het internet gebruik te maken.

Internet is, met name sinds de intrede van de smartphone, inmiddels al lang niet meer gebonden aan een vaste plek thuis, maar is vrijwel overal in Nederland beschikbaar. Maar liefst 85 procent van de internetters gebruikt het internet op openbare plaatsen.

De wijze waarop toegang tot het internet wordt verkregen op openbare plekken kan ook nog verschillen. Met 64 procent deed de grootste groep internetgebruikers dat via een eigen mobiel internetabonnement. Daarnaast maakte bijna de helft (48 procent) gebruik van een openbaar WiFi-netwerk dat was beveiligd met een wachtwoord en ruim een derde (35 procent) gebruikte in 2018 weleens een openbare WiFi-verbinding zonder wachtwoord.

2.1.1 Internetgebruik, 2018[1)]

	% internetgebruikers
Gebruikt dagelijks internet	92,6
Gebruikt internet op openbare plekken	84,5
Gebruikt internet op openbare plekken via Wi-Fi met wachtwoord	48,2
Gebruikt internet op openbare plekken via Wi-Fi zonder wachtwoord	34,9
Gebruikt internet op openbare plekken via eigen 3g/4g abonnement	64,1
Gebruikt dagelijks Wi-Fi op openbare plekken	14,9
Gebruikt nooit Wi-Fi op openbare plekken	41,4

[1)] Personen van 12 jaar of ouder met internetgebruik.

Anno 2018 wordt het internet ingezet voor tal van activiteiten. Het internet werd het vaakst gebruikt voor het opzoeken van informatie: bijna alle internetgebruikers (98 procent) gaven aan dit te hebben gedaan. Ook het versturen van berichten werd door het leeuwendeel van de internetgebruikers (95 procent) genoemd. Daarnaast is ook het online bankieren niet meer weg te denken; 9 op de 10 internetgebruikers geven aan hiervan gebruik te maken.

Een van de andere grote gemakken van het internet is het online bestellen van diensten of goederen. Internetters kunnen op elk moment op zoek naar producten van hun gading en hoeven hiervoor niet persé naar de winkel. Daarnaast zijn er volop mogelijkheden om de prijzen en andere informatie van de producten te vergelijken. Ook zijn de kopers niet meer gebonden aan het lokale aanbod, maar kan landelijk en zelfs wereldwijd worden gekocht. In 2018 gaven meer dan 8 op de 10 (82 procent) van de internetgebruikers aan online aankopen te doen.

Andere veelgenoemde online activiteiten zijn het downloaden van applicaties (77 procent) en het gebruiken van sociale media (69 procent). In het onderzoek is ook gevraagd naar enkele specifieke online activiteiten van internetgebruikers. Zo zeiden bijna 2 op de 10 internetgebruikers erotische sites te bezoeken (19 procent), terwijl 6 procent datingsites bezocht. Online gokken werd door 4 procent van de internetgebruikers genoemd.

2.1.2 Internetactiviteiten, 2018[1)]

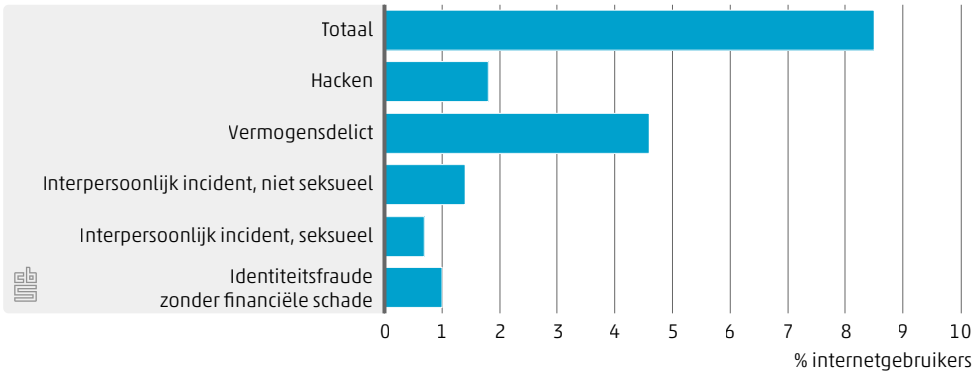
	% internetgebruikers
Zoeken van informatie	98,2
Berichten versturen	94,7
Internetbankieren	89,5
Kopen van goederen of diensten	81,9
Downloaden van apps, games, afbeeldingen of software	76,8
Sociale media	68,5
Foto's, documenten of bestanden op het internet opslaan (cloud)	61,5
Streamen van films of muziek	60,0
Gamen	54,6
Verkopen van goederen of diensten	47,3
Professionele netwerksites	41,5
Downloaden van muziek of films	39,6
Erotische sites bezoeken	18,7
Datingsites bezoeken	5,8
Gokken	3,8

[1)] Personen 12 jaar of ouder met internetgebruik.

2.2 Slachtoerschap van digitale criminaliteit

Van alle internetgebruikers van 12 jaar en ouder rapporteerde 8,5 procent in 2018 dat ze in de afgelopen 12 maanden het slachtoffer waren van één of meerdere vormen van digitale criminaliteit. Het gaat hierbij om ruim 1,2 miljoen personen. Digitale vermogensdelicten waarbij door criminelen geld werd buitgemaakt kwamen het meeste voor: 4,6 procent van de internetgebruikers werd hiervan slachtoffer. Daarnaast zei 1,8 procent slachtoffer te zijn geworden van hacken, waarbij bijvoorbeeld gegevens werden gestolen of misbruik werd gemaakt van online accounts. Van interpersoonlijke incidenten, waaronder online laster, stalking of bedreiging met geweld (niet seksueel getint), werd 1,4 procent van de internetgebruikers slachtoffer. Van interpersoonlijke incidenten met een seksuele (bij) bedoeling was dat 0,7 procent. Verder werd 1 procent slachtoffer van identiteitsfraude zonder dat daarbij financiële schade werd geleden. Hieronder valt bijvoorbeeld een mislukte poging om diensten of goederen op iemand anders' naam te bestellen.

2.2.1 Slachtoerschap digitale criminaliteit, 2018[1)]



[1)] Personen van 12 jaar of ouder met internetgebruik.

Wanneer het slachtofferschap van deze soorten digitale criminaliteit wordt vergeleken tussen mannen en vrouwen, blijkt dat ze wat betreft het totaalcijfer niet significant van elkaar verschillen. Mannen waren wel vaker dan vrouwen slachtoffer van vermogensdelicten (5,1 procent tegen 4 procent), terwijl meer vrouwen dan mannen te maken kregen met online seksueel getinte persoonlijke delicten (1 procent tegen 0,3 procent).

2.2.2 Slachtoerschap van digitale criminaliteit naar geslacht, 2018[1)]

	Totaal	Mannen	Vrouwen
	% internetgebruikers		
Totaal	8,5	8,7	8,3
Hacken	1,8	1,6	1,9
Vermogensdelict	4,6	5,1	4,0
Interpersoonlijk incident, niet seksueel	1,4	1,2	1,6
Interpersoonlijk incident, seksueel	0,7	0,3	1,0
Identiteitsfraude zonder financiële schade	1,0	1,2	0,8

1) Personen van 12 jaar of ouder met internetgebruik.

Jongere internetgebruikers werden in 2018 vaker slachtoffer van digitale criminaliteit dan ouderen. Vanaf de groep 18- tot 25-jarigen neemt het slachtofferschap van digitale criminaliteit af naarmate de leeftijd toeneemt. Vooral vanaf 55 jaar is een daling te zien. In de leeftijd van 12 tot 18 jaar werden internetgebruikers met 5,3 procent het vaakst slachtoffer van de niet-seksueel getinte interpersoonlijke incidenten. Zo kregen deze jongeren relatief vaak te maken met online bedreigingen met geweld, pesten, roddelen of stalking. Ook in de leeftijdsgroep van 18 tot 25 jaar is er sprake van een relatief hoger aandeel interpersoonlijke incidenten, zowel voor niet seksueel getint als seksueel getint. Bij de oudere leeftijdsgroepen kwamen vermogensdelicten weer wat meer voor en persoonlijke incidenten verhoudingsgewijs wat minder.

2.2.3 Slachtoerschap van digitale criminaliteit naar leeftijd, 2018[1)]

	Totaal	Hacken	Vermogens-delict	Interpersoonlijk incident, niet seksueel	Interpersoonlijk incident, seksueel	Identiteitsfraude zonder financiële schade
	% internetgebruikers					
12 tot 18 jaar	12,0	2,4	3,8	5,3	1,3	0,9
18 tot 25 jaar	12,7	2,5	5,9	3,0	1,9	1,1
25 tot 35 jaar	11,1	2,5	6,0	1,7	0,9	1,5
35 tot 45 jaar	9,8	2,0	6,2	1,0	0,5	1,1
45 tot 55 jaar	9,3	2,1	5,5	0,8	0,4	1,1
55 tot 65 jaar	5,4	1,1	3,2	0,5	0,3	0,7
65 tot 75 jaar	3,9	0,9	2,2	0,4	0,1	0,7
75 jaar of ouder	3,3	0,5	2,2	0,1	0,1	0,5

1) Personen van 12 jaar of ouder met internetgebruik.

3. Hacken

In 2018 geeft 1,8 procent van de internetgebruikers aan in de afgelopen 12 maanden slachtoffer te zijn geweest van hacken, in de wet ook wel computervredebreuk genoemd. Bij hacken is er onrechtmatig ingebroken of ingelogd op iemands computer, mobiele telefoon, e-mailaccount, sociale netwerksite (bijvoorbeeld Facebook of Twitter) of een andersoortig online account waarbij gegevens zijn verstoord, geblokkeerd of gestolen. Hacken is een zuiver ICT-delict. Een dergelijk delict kenmerkt zich doordat het enkel kan plaatsvinden in een ICT-omgeving, in tegenstelling tot delicten zoals het plegen van fraude die ook daarbuiten mogelijk zijn.

Van alle internetgebruikers die in 2018 slachtoffer werden van hacken gaf met 56 procent ruim meer dan de helft aan dat er was ingebroken op hun sociale media. Ook een inbraak op een e-mailaccount kwam met 28 procent naar verhouding vaak voor. Bij 12 procent van de slachtoffers werd er ingebroken op een desktop, laptop of tablet, en bij eveneens 12 procent werd ingebroken op een ander apparaat. Een inbraak op een mobiele telefoon of andere huishoudelijke apparaten (zoals beveiligingsapparatuur of babyfoon) kwam met 6 en 0,1 procent minder vaak voor.

3.1 Hacken – soort hack[1)], 2018

	% slachtoffers
Ingebroken op computer (desktop, laptop of tablet)	11,5
Ingebroken op e-mailaccount	27,9
Ingebroken op mobiele telefoon	6,1
Ingebroken op sociale media	56,4
Ingebroken op andere huishoudelijke apparatuur	0,1
Ingebroken op ander apparaat	12,1

[1)] Meerdere antwoorden mogelijk.

Voor het grootste deel van de gehackte internetgebruikers (40 procent) had deze hack verder gelukkig geen gevolgen. Wanneer de hack wel gevolgen had, kwam misbruik van een e-mailaccount of een internetprofiel met 27 procent veruit het vaakst voor. Andere gevolgen die voorkwamen waren bijvoorbeeld het misbruik van persoonlijke gegevens op internet (9 procent), een virus met verlies van gegevens (7 procent) en het blokkeren, verstoren of vasthouden van computergegevens als gevolg van ransomware (6 procent).

3.2 Hacken – gevolgen[1)], 2018

	% slachtoffers
Virus met verlies van gegevens	6,6
Misbruik van persoonlijke gegevens op het internet	9,3
Ransomware	5,7
Gegevens gestolen via trojan horse	2,9
Cryptoware	2,2
Malware	4,8
Misbruik van computer (bv. in botnet of DDos-aanval)	0,7
Misbruik van emailaccount of profielsite	26,9
Pharming (omleiden van internetverkeer)	0,3
Andere gevolgen	11,1
Geen gevolgen	39,3
Account geblokkeerd[2)]	5,2
Ongewenste items verstuurd[2)]	4,2

[1)] Meerdere antwoorden mogelijk.
[2)] Genoemd bij de open antwoordcategorie.

Hacken als doel, niet als middel

In deze cijfers zijn alleen de incidenten meegenomen waarbij het hacken, behalve de bovengenoemde gevolgen, geen verdere, achterliggende oogmerken had. Zo kan het zijn dat door middel van de hack ook geld is buitgemaakt. In dat geval wordt het incident niet tot hacken maar tot de vermogensdelicten gerekend (hoofdstuk 4). Ook wanneer persoonlijke delicten (hoofdstukken 5 en 6) en identiteitsfraude (hoofdstuk 7) zijn gepleegd door middel van een hack, worden deze tot de desbetreffende delictscategorie gerekend en niet tot hacken. Zouden deze echter ook bij hacken worden meegerekend, dan werd in 2018 in totaal 2,1 procent slachtoffer van hacken.

Wijze van inbraak

Het grootste deel van de slachtoffers van hacken (45 procent) gaf aan dat er is ingebroken op hun computer, mobiele telefoon of account doordat iemand aan hun wachtwoorden is gekomen. Ongeveer een derde wist niet hoe de dader toegang had verkregen. In maar 3 procent van de gevallen ging het om een hack waarbij iemand fysiek toegang verkreeg tot de computer.

3.3 Hacken – oorzaak van inbraak[1], 2018

	% slachtoffers
Zelf (bewust of per ongeluk) installeren van een programma	7,1
Installeren van een programma door iemand anders	4,8
Iemand aan wachtwoorden gekomen	44,7
Fysieke toegang tot computer verkregen	2,7
Onbekend hoe toegang is verkregen	33,7
Gehackt[2]	3,6
Op een link, bericht, bijlage of filmpje geklikt[2]	3,9
Andere wijze[2]	5,3

[1] Meerdere antwoorden mogelijk.
[2] Genoemd bij de open antwoordcategorie.

Gevolgen voor slachto er

Ongeveer een kwart van de slachtoffers van hacken (24 procent) ondervond in 2018 emotionele gevolgen van hetgeen hen is overkomen. Dit uitte zich vooral in boosheid (21 procent). Verder had bijna 40 procent na het incident minder vertrouwen in de digitale veiligheid en 15 procent minder vertrouwen in de eigen digitale vaardigheden. Bijna 3 op de 10 slachtoffers waren bang dat het hacken in de toekomst vaker zal gebeuren.

3.4 Hacken – gevolgen voor slachtoffer[1], 2018

	% slachtoffers
Emotionele gevolgen	24,3
Blijft eraan denken	6,3
Erg boos	20,7
Sliep slechter	3,9
Minder vertrouwen in digitale veiligheid	38,7
Minder vertrouwen in eigen digitale vaardigheid	14,7
Bang dat het vaker zal gebeuren	28,9

[1] Meerdere antwoorden mogelijk.

Melding en aangifte

In 2018 heeft 5 procent van de slachtoffers van hacken bij een instantie melding gedaan van de hack. In verreweg de meeste gevallen is deze melding gedaan bij de politie, maar ook bij het Centraal Meldpunt Nederland en Meld Misdaad Anoniem werden incidenten gemeld. Van alle hackslachtoffers deed uiteindelijk 3 procent aangifte bij de politie.

3.5 Hacken – melding[1] en aangifte, 2018

	% slachtoffers
Gemeld bij minstens één van de volgende instanties	5,1
Politie	4,8
Centraal Meldpunt Nederland (meld.nl)	0,3
Meld Misdaad Anoniem	0,2
Aangifte bij de politie	2,8

[1] Meerdere antwoorden mogelijk.

Bijna 95 procent van de slachtoffers van hacken deed dus geen melding bij de politie of een andere instantie. In 16 procent van de gevallen deden slachtoffers van hacken geen melding, omdat ze er vanuit gingen dat dit toch niet zou helpen. Zij gaven vooral aan niet te verwachten dat de dader bij een melding zal worden gepakt. Andere redenen om niet te melden die naar verhouding vaak worden genoemd, zijn dat het teveel moeite kost (9 procent) en dat het kwam door een eigen fout (8 procent). Daarnaast gaf 13 procent aan dat het niet mogelijk was om melding te doen van het incident. Verder is van ruim een vijfde van de hackslachtoffers onbekend waarom zij geen melding hebben gedaan.

3.6 Hacken – belangrijkste reden niet melden, 2018

	% slachtoffers
Niet gemeld	94,9
Helpt niet, totaal	15,6
Krijg geld toch niet terug	1,1
Ontmoedigende houding van de politie	1,6
Dader wordt toch niet gepakt	12,4
Er wordt toch niets mee gedaan[1)]	0,5
Niet belangrijk genoeg, totaal	13,5
Ging om een klein bedrag	1,5
Te veel moeite	8,8
Niet in me opgekomen[1)]	0,8
Er was geen schade[1)]	2,4
Overige redenen of onbekend, totaal	65,8
Dader is bekende	2,0
Was mijn eigen fout	8,2
Wegens schaamte	1,2
Was niet mogelijk voor dit incident	13,0
Andere reden	18,7
Onbekend	22,7

[1)] Genoemd bij de open antwoordcategorie.

Van alle slachtoffers van hacken gaf 0,5 procent aan het incident niet aangegeven te hebben bij de politie, omdat ze er vanuit gingen dat dat toch niet zou helpen. Bovendien was dat ook meestal op advies van de politie. Voor 0,4 procent van de slachtoffers was het niet belangrijk genoeg om aan te geven. Met 0,7 procent werd ook relatief vaak genoemd dat het niet mogelijk was om aangifte te doen voor het incident.

3.7 Hacken - belangrijkste reden geen aangifte, 2018

	% slachtoffers
Wel ergens gemeld, maar geen aangifte	2,3
Helpt niet, totaal	0,5
Advies van de politie	0,4
Afwijzende houding van de politie	0,1
Niet belangrijk genoeg, totaal	0,4
Te veel moeite	0,4
Overige redenen of onbekend, totaal	1,5
Was mijn eigen fout	0,2
Dader is bekende	0,3
Was niet mogeijk voor dit incident	0,7
Andere reden	0,1
Onbekend	0,2

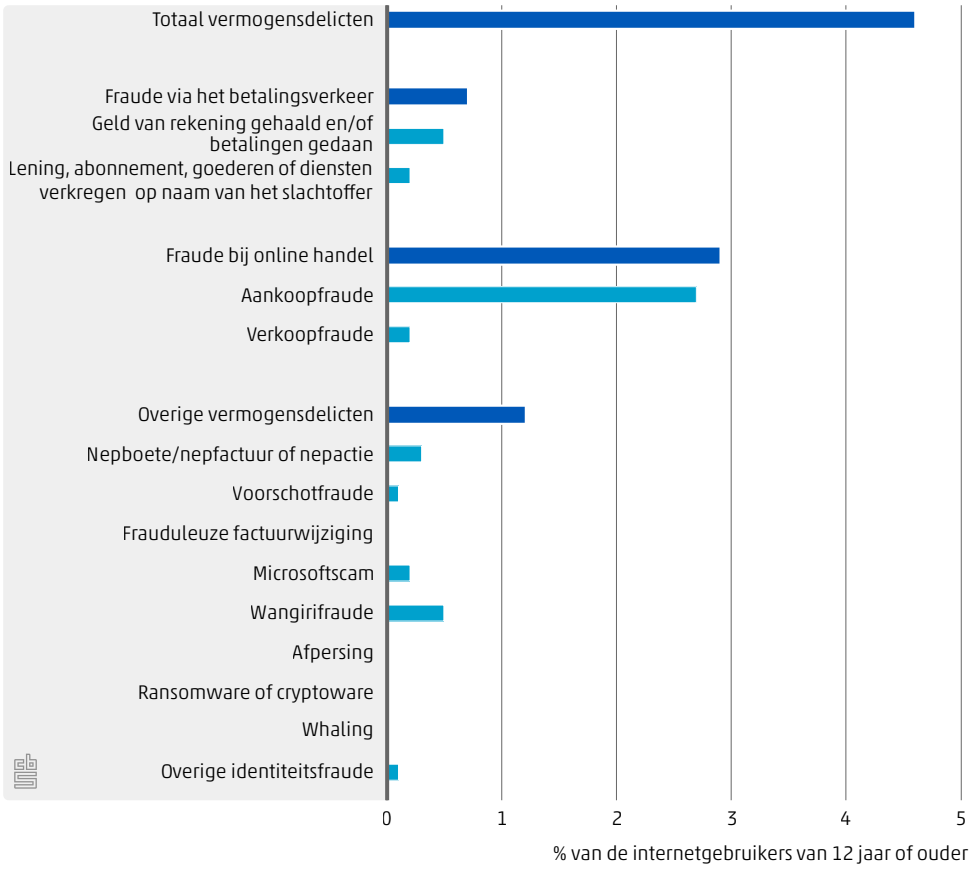
4.

Vermogensdelicten

In 2018 is 4,6 procent van de internetgebruikers slachtoffer geweest van een of meer vermogensdelicten die via internet zijn gepleegd. Oplichting bij online handel, en dan met name bij het doen van aankopen, kwam het vaakst voor: van alle internetgebruikers heeft 2,7 procent weleens betaald voor een product of dienst die nooit geleverd werd. Maar er is een heel scala aan andere criminele activiteiten met een financieel motief. Zo werd 0,7 procent slachtoffer van fraude via het betalingsverkeer. Daarnaast verloor 1,2 procent geld aan overige vormen van fraude. Deze delicten betreffen vaak een vorm van phishing.

Dit hoofdstuk gaat dieper in op slachtofferschap van deze vermogensdelicten. In paragraaf 4.1 komt fraude via het betalingsverkeer aan bod. Paragraaf 4.2 gaat in op oplichting bij online handel. En in paragraaf 4.3 komen overige vormen van fraude aan de orde.

4.1 Slachto erschap online vermogensdelicten, 2018



In dit rapport wordt phishing breder gezien dan de traditionele nepmails van banken. Onder phishing vallen alle activiteiten waarbij massaal personen worden benaderd met nepberichten/nepacties in de veronderstelling dat er altijd wel een aantal personen zijn die hier nietsvermoedend op ingaan. Veelal gebeurt dit nog via de e-mail, maar ook worden steeds vaker andere media ingezet. De berichten zijn meestal niet persoonlijk. Spear-phishing is een subvorm met een meer persoonlijke en gerichte benadering, waarbij de dader vooraf ook informatie over het potentiële slachtoffer heeft gezocht.

Tot de slachtoffers van vermogensdelicten rekenen we iedereen aan wie de dader geld heeft verdiend. Hiertoe behoren dus ook degenen die de schade vergoed kregen door een andere instantie en daardoor er zelf financieel niet op achteruit zijn gegaan.

4.1 Fraude via het betalingsverkeer

0,7 procent van de internetgebruikers gaf aan in 2018 financiële schade te hebben geleden door fraude via het betalingsverkeer. Deze vorm van identiteitsfraude[1)] is onder te verdelen in twee hoofdgroepen. Bij de eerste heeft de dader directe toegang tot de rekening van het slachtoffer en heeft hij/zij er geld vanaf gehaald of er betalingen mee gedaan. Dit is 0,5 procent van de internetgebruikers overkomen. De tweede is niet gericht op betalingsaccounts maar op accounts waarmee bestellingen worden gedaan waarbij de rekening voor het slachtoffer komt. De dader heeft dus een lening, abonnement, goederen of diensten verkregen op naam van het slachtoffer. Dit overkwam 0,2 procent van de internetgebruikers.

In de enquête zijn 187 slachtoffers van fraude via het betalingsverkeer nader bevraagd over dit delict. Deze detailinformatie volgt hieronder. Over het verkrijgen van een lening, abonnement, goederen of diensten door de dader is informatie van slechts 68 slachtoffers beschikbaar. Dit aantal is te gering om betrouwbare detailinformatie over dit delict te kunnen geven (zie ook tabel 4 in de tabellenbijlage).

Manier waarop de gegevens zijn verkregen

Ruim 3 op de 10 slachtoffers van wie geld van de rekening is verdwenen wisten niet hoe de dader aan de gegevens is gekomen. Door 13 procent van de slachtoffers werd aangegeven dat ze zelf de gegevens hebben doorgegeven aan een webshop of via de telefoon. Naar schatting werd 30 procent van de incidenten in eerste instantie veroorzaakt door een vorm van phishing. Minstens 12 procent werd voorafgegaan door een hack.

1) In enkele gevallen betreft het geen identiteitsfraude, bijvoorbeeld als een gezinslid de 'dader' is.

4.1.1 Geld van rekening gehaald en/of betalingen gedaan – manier waarop dader aan de gegevens is gekomen, 2018

	% slachtoffers
Zelf bankpas in goed vertrouwen ter beschikking gesteld	5,1
Zelf persoonlijke gegevens in goed vertrouwen aan een bekende ter beschikking gesteld	1,4
Zelf gegevens doorgegeven op een webshop of via de telefoon	13,2
Niet online, maar door kopiëren creditcard of bijv. dumpster diving[1)]	0,7
Diefstal van paspoort of ID-kaart waarbij identiteit overgenomen werd	1,7
Diefstal van bankpas/creditcard	6,8
Skimmen van bankpas/creditcard	11,2
Scannen van mobiele telefoon, bijv door contactloos betalen (shimming)	0,0
Phishing of pharming	11,3
Hacken van computer/tablet/telefoon	3,5
Malware (bv. een computervirus of trojan horse)	2,4
Keylogging	0,0
Hacken van bedrijf of bank waar persoonlijke gegevens bekend zijn	6,3
Andere wijze	4,3
Onbekend	32,2
Totaal door phishing[2)]	30,2
Totaal door hacken als modus operandi[2)]	12,2

1) Genoemd bij de open antwoordcategorie.
2) Aan meerdere vormen van gegevensdiefstal ging een vorm van phishing vooraf. Zie de methodologische toelichting in de onderzoeksverantwoording voor de berekening van 'totaal door phishing' en 'totaal door hacken'.

Melding en aangifte

De meeste slachtoffers van betalingsverkeerfraude meldden dit bij een instantie (86 procent). Ruim drie kwart (77 procent) had contact met hun bank of andere financiële instelling. Daarnaast meldde 19 procent het (ook) bij de politie en 11 procent bij de Fraudehelpdesk. Zo'n 3 procent van de slachtoffers gaf aan dat ze het bij het bedrijf hebben gemeld waar het geld naar was overgeschreven, en 2 procent bij het Centraal Meldpunt Identiteitsfraude en -fouten.

4.1.2 Geld van rekening gehaald en/of betalingen gedaan – melding[1)] en aangifte, 2018

	% slachtoffers
Gemeld bij minstens één van de volgende instanties	86,4
Politie	18,9
Bank of financiële instelling	77,4
Fraudehelpdesk	10,7
Centraal Meldpunt Identiteitsfraude en -fouten	2,0
Autoriteit Consument en Markt	0,0
Bedrijf of webshop waar betaling, aanvraag of bestelling is gedaan[2)]	3,0
Aangifte bij de politie	18,3
Weet niet of er aangifte is gedaan	13,8

1) Meerdere antwoorden mogelijk.
2) Genoemd bij de open antwoordcategorie.

Bijna een op de vijf slachtoffers (18 procent) deed aangifte bij de politie.
Er zijn verschillende redenen waarom slachtoffers het delict niet meldden. De belangrijkste reden was dat het niet belangrijk genoeg was, voornamelijk omdat het om een klein bedrag ging. Dit werd door 5 procent van de slachtoffers genoemd.

4.1.3 Geld van rekening gehaald en/of betalingen gedaan – belangrijkste reden niet melden, 2018

	% slachtoffers
Niet gemeld	13,6
Helpt niet, totaal	2,2
Krijg geld toch niet terug	1,3
Ontmoedigende houding van de politie	0,6
Dader wordt toch niet gepakt	0,3
Niet belangrijk genoeg, totaal	4,7
Ging om een klein bedrag	3,9
Te veel moeite	0,4
Niet in me opgekomen[1)]	0,4
Overige redenen of onbekend, totaal	6,7
Dader is bekende	0,0
Was mijn eigen fout	0,5
Was niet mogelijk voor dit incident	0,0
Andere reden	2,9
Onbekend	3,3

[1)] Genoemd bij de open antwoordcategorie.

Indien een slachtoffer het voorval bij iemand of bij een instantie heeft gemeld, hoeft daar nog geen aangifte bij de politie op te volgen. Het delict was volgens 15 procent van de slachtoffers niet ernstig genoeg voor een aangifte, omdat het bijvoorbeeld om een klein bedrag ging of voor dit delict te veel moeite was. Daarnaast deed 12 procent van de slachtoffers geen aangifte omdat de financiële instelling het verder zou afhandelen.

4.1.4 Geld van rekening gehaald en/of betalingen gedaan – belangrijkste reden geen aangifte, 2018

	% slachtoffers
Wel ergens gemeld, maar geen aangifte	54,2
Helpt niet, totaal	8,0
Krijg geld toch niet terug	0,0
Ontmoedigende houding van de politie	0,6
Er wordt toch niets mee gedaan[1)]	0,5
Dader wordt toch niet gepakt	6,9
Niet belangrijk genoeg, totaal	15,4
Ging om een klein bedrag	6,7
Te veel moeite	6,7
Niet in me opgekomen[1)]	2,0
Overige redenen of onbekend	30,8
Bank of creditcardmaatschappij zou het verder afhandelen[1)]	12,0
Dader is bekende	0,4
Was mijn eigen fout	1,8
Wegens schaamte	0,7
Was niet mogelijk voor dit incident	2,5
Andere reden	6,4
Onbekend	7,0

[1)] Genoemd bij de open antwoordcategorie.

Gevolgen voor het slachto er

Bijna 8 op de 10 slachtoffers (78 procent) kreeg de financiële schade helemaal vergoed. Het feit dat iemand toegang heeft gehad tot de rekening kan echter ook niet-materiële schade veroorzaken. Zo ondervond 34 procent van de slachtoffers emotionele gevolgen, voornamelijk boosheid. Ook voelt ruim de helft van de slachtoffers zich sindsdien minder veilig in de digitale wereld. 29 procent is bang voor herhaling.

4.1.5 Geld van rekening gehaald en/of betalingen gedaan – gevolgen voor het slachto er[1)], 2018

	% slachtoffers
Aanvankelijke financiële schade	
Helemaal vergoed	78,0
Deels vergoed	6,3
Niets vergoed	15,7
Emotionele gevolgen	33,7
Blijft eraan denken	12,5
Erg boos	25,7
Sliep slechter	7,4
Minder vertrouwen in de digitale veiligheid	52,3
Minder vertrouwen in de eigen digitale vaardigheid	10,0
Bang dat het vaker zal gebeuren	29,2

[1)] Meerdere antwoorden mogelijk.

4.2 Fraude bij online handel

Zo'n 2,9 procent van de Nederlanders is in 2018 weleens opgelicht bij de online aan- of verkoop van goederen of diensten. Van hen werd 2,7 procent slachtoffer van aankoopfraude: men heeft iets gekocht maar niet ontvangen (en ook het geld niet terug gekregen). Verkoopfraude komt in de privésetting niet veel voor: slechts 0,2 procent van de burgers werd in 2018 niet betaald voor een door hen geleverd product of een geleverde dienst.

In de enquête zijn 901 slachtoffers van aankoopfraude nader bevraagd over dit delict. Deze detailinformatie volgt hieronder. Over verkoopfraude is informatie van slechts 75 slachtoffers voorhanden. Dit aantal is te gering om betrouwbare detailinformatie over dit delict te geven (zie ook tabel 5 in de tabellenbijlage).

Gebruikte website

De grootste groep slachtoffers van aankoopfraude, namelijk 42 procent, had hun aankoop bij een tweedehands verkoopsite gedaan, 16 procent had bij verkoopsites als Amazon, Alibaba gekocht. Een kwart van de slachtoffers had bij een webshop gekocht, waarbij veelal bleek dat het een nepwebshop was. Slechts 7 procent van de aankopen gingen via sociale media.

4.2.1 Aankoopfraude – gebruikte website, 2018

	% slachtoffers
Tweedehands verkoopsite	41,5
Verkoopsite als Amazon, Alibaba	16,3
Veilingsite	3,5
Social media	6,5
Nederlandstalige nepwebshop	10,9
Niet-Nederlandstalige nepwebshop	8,0
Bestaande webshop[1)]	5,5
Anders	5,7
Onbekend	2,1

[1)] Genoemd bij de open antwoordcategorie.

Gekochte producten

Bij de meeste gevallen van aankoopfraude ging het om de aanschaf van kleding, schoenen of accessoires (30 procent). Ook behoorden relatief veel aankopen tot de categorie 'mobiele telefoons, audio, tv of computer' (20 procent).

4.2.2 Aankoopfraude – gekochte producten, 2018

	% slachtoffers
Tickets en kaartjes	5,3
Mobiele telefoons, audio, tv, computer, etc.	19,7
Kleding, sportartikelen, schoenen, accessoires	29,6
Duurzame consumptiegoederen	7,5
Films, muziek, boeken, spellen of speelgoed	9,7
Vakanties, vervoer of reizen	1,4
Levensmiddelen en producten voor persoonlijke verzorging	6,2
Overig	19,3
Onbekend	1,4

Melding en aangifte

Ruim een derde van de kopers heeft de oplichting bij een instantie gemeld; 6 procent deed dit zelfs bij twee instanties. De meeste slachtoffers (25 procent) meldden zich bij de politie, maar ook werd relatief veel contact opgenomen met de bank/financiële instelling (9 procent), de Fraudehelpdesk of Marktplaats (beide 5 procent).
Zo'n 23 procent van de slachtoffers deed aangifte bij de politie.

4.2.3 Aankoopfraude – melding[1] en aangifte, 2018

	% slachtoffers
Gemeld bij minstens één van de volgende instanties	38,9
Politie/LMIO	24,9
Fraudehelpdesk	4,6
Consumentenprogramma zoals Kassa, Radar of Opgelicht	2,2
Consuwijzer (vermoeden van fraude via webwinkels)	1,2
Bank, financiële instelling, creditcardmaatschappij of PayPal[2]	8,5
Marktplaats[2]	4,6
Aangifte bij de politie	22,6
Weet niet of er aangifte is gedaan	2,6

[1] Meerdere antwoorden mogelijk.
[2] Genoemd bij de open antwoordcategorie.

3 op de 10 slachtoffers hebben het delict nergens gemeld omdat het niet zo belangrijk was, veelal omdat het om een klein bedrag ging. Nog eens 22 procent dacht dat het toch niet helpt, vooral omdat ze verwachtten hun geld toch niet meer terug te krijgen.

4.2.4 Aankoopfraude – belangrijkste reden niet melden, 2018

	% slachtoffers
Niet gemeld	61,1
Helpt niet, totaal	22,1
Krijg geld toch niet terug	16,9
Dader wordt toch niet gepakt	4,2
Ontmoedigende houding van de politie	1,0
Niet belangrijk genoeg, totaal	29,7
Ging om een klein bedrag	23,5
Te veel moeite	5,8
Niet in me opgekomen[1]	0,4
Overige redenen of onbekend, totaal	9,2
Was mijn eigen fout	2,1
Wegens schaamte	1,2
Was niet mogelijk voor dit incident	0,9
Andere reden	2,7
Onbekend	2,3

[1] Genoemd bij de open antwoordcategorie.

Van de slachtoffers had 14 procent het delict dus wel bij een instantie gemeld, maar had er geen aangifte van gedaan bij de politie. Meestal omdat ze dachten dat het toch niet zou helpen.

4.2.5 Aankoopfraude – belangrijkste reden geen aangifte, 2018

	% slachtoffers
Wel ergens gemeld, maar geen aangifte	13,7
Helpt niet, totaal	5,7
Krijg geld toch niet terug	3,1
Dader wordt toch niet gepakt	1,9
Ontmoedigende houding van de politie	0,6
Politie doet er toch niets mee	0,1
Niet belangrijk genoeg, totaal	2,2
Ging om een klein bedrag	1,6
Te veel moeite	0,6
Niet in me opgekomen[1)]	0,0
Overige redenen of onbekend	5,8
Bank zou het verder afhandelen	2,7
Was mijn eigen fout	0,7
Uit schaamte	0,2
Was niet mogelijk voor dit incident	0,7
Andere reden	0,8
Onbekend	0,7

[1)] Genoemd bij de open antwoordcategorie.

Gevolgen voor het slachto er

Bijna alle slachtoffers van aankoopfraude hebben hiervan financieel nadeel gehad. Slechts 1 op de 10 slachtoffers kreeg de financiële schade vergoed, omdat ze bijvoorbeeld met een creditcard of via PayPal hadden betaald. Daarnaast riep het delict bij 42 procent van de slachtoffers bepaalde emoties op. Dit uitte zich voornamelijk in erge boosheid (39 procent) en het 'niet los kunnen laten' (12 procent). Ruim 1 op de 3 slachtoffers (35 procent) voelt zich sindsdien minder veilig in de digitale wereld, 23 procent is bang dat het hen nog eens zal overkomen.

4.2.6 Aankoopfraude – gevolgen voor het slachto er[1)], 2018

	% slachtoffers
Kreeg de financiële schade vergoed	10,0
Emotionele gevolgen	42,4
Blijft eraan denken	11,7
Erg boos	38,6
Sliep slechter	3,2
Minder vertrouwen in de digitale veiligheid	35,3
Minder vertrouwen in de eigen digitale vaardigheid	8,9
Bang dat het vaker zal gebeuren	23,4

[1)] Meerdere antwoorden mogelijk.

Bijna de helft van de slachtoffers (46 procent) heeft achteraf nog informatie opgezocht over de dader. In de meeste gevallen gebeurde dit via media als Google, fora, Opgelicht, Kassa, Radar (29 procent). Van de checkfunctie op politie.nl maakte 12 procent gebruik.

4.2.7 Aankoopfraude – achteraf nog informatie opgezocht over de dader[1)], 2018

	% slachtoffers
Geen informatie over de dader meer opgezocht	46,2
Controlefunctie op Politie.nl	12,1
Google, fora, Opgelicht, Kassa, Radar	28,6
Kamer van Koophandel	2,1
Anders	10,8

1) Meerdere antwoorden mogelijk.

4.3 Overige vermogensdelicten

Naast fraude via het betalingsverkeer en bij online handel zijn er veel andere soorten digitale criminaliteit waarbij het de dader puur om het geld gaat. In de enquête is er een aantal uitgevraagd die nu bekend zijn, maar er worden telkens weer nieuwe varianten bedacht. Aan veel van deze delicten gaat een vorm van phishing vooraf. Tot de slachtoffers worden alleen degenen gerekend die erin zijn getrapt, oftewel: de dader heeft geld aan hen verdiend[2)]. Daarbij moet opgemerkt worden dat niet iedereen weet dat hij of zij is opgelicht. Dit verborgen slachtofferschap kan echter niet worden gemeten in een slachtofferenquête en is dus niet meegenomen in de cijfers.

In 2018 is 1 procent van de internetgebruikers naar eigen zeggen slachtoffer geweest van een 'overig' vermogensdelict. Hieronder volgt een beschrijving van slachtofferschap van de afzonderlijke delicten die hiertoe worden gerekend (zie tabel 4.3.1 en tabel 6 in de tabellenbijlage voor een uitgebreidere verantwoording).

Nepboete/nepfactuur of nepactie

In 2018 heeft 0,3 procent van de internetgebruikers een nepboete of nepfactuur betaald, of geld verloren aan een nepactie[3)]. Bij nepacties kan gedacht worden aan nepacties voor donatie als om nep-winacties van bekende supermarkten, doe-het-zelf-, en elektronicazaken.

2) Bij een aantal van deze delicten was de vraagstelling niet toereikend om te kunnen onderscheiden of de respondent 'geen geld is kwijtgeraakt' omdat hij/zij er niet intrapte of omdat de schade volledig vergoed werd. De werkelijke slachtofferprevalenties kunnen daarom in feite iets hoger liggen, met name bij delicten waarbij de schade vaak vergoed wordt.

3) Het is niet mogelijk een goede schatting te geven van het aantal personen dat deze specifieke nepberichten heeft ontvangen (zie de methodologische toelichting in de onderzoeksverantwoording voor verdere uitleg).

Voorschotfraude

Bijna 4 procent van de internetgebruikers is in 2018 benaderd voor een vorm van voorschotfraude. Slechts 0,1 procent is ingegaan op het aanbod en heeft hier financiële schade door geleden. Voorschotfraude kent vele verschijningsvormen. De benadering van het slachtoffer gebeurt via verschillende kanalen en de 'gouden bergen' die in het vooruitzicht worden gesteld variëren van een deel van de winst, een erfenis, goederen, een relatie of huisdier tot het ontvangen van een lening.

Frauduleuze factuurwijziging

Weinig internetgebruikers (0,1 procent) geven aan dat in 2018 een oplichter het rekeningnummer van een bestaande factuur heeft gewijzigd. Nagenoeg niemand is hierdoor geld kwijtgeraakt.

Microsoftscam

'Hello, I am calling from Microsoft about a problem with your computer.' Circa 15 procent van de Nederlanders ontving in 2018 een telefoontje van die strekking met het aanbod het probleem op te lossen. Ondanks de bekendheid van deze helpdeskfraude ging toch nog 0,2 procent van de internetgebruikers hierop in en leed financieel verlies.

Wangirifraude

Het is voor criminelen relatief eenvoudig om met software naar honderdduizenden telefoonnummers te bellen, en de mensen die terugbellen door te schakelen naar een duur betaalnummer. Minstens 4 procent van de Nederlanders gaf aan in 2018 te zijn benaderd door middel van deze zogeheten 'Wangiri'telefoontjes, 0,5 procent had naar het dure betaalnummer teruggebeld en ontving een hoge telefoonrekening.

Afpersingsmails

In 2018 zijn massaal en in verschillende varianten zeer intimiderende seksueel getinte afpersmails uitgezet. Hierin werd gedreigd met het verspreiden van videobeelden waarop de ontvanger naar porno zou kijken, tenzij deze zeer snel een aanzienlijk bedrag (vaak honderden euro's) naar een bitcoinrekening zou overschrijven. Minstens 2 procent van de internetgebruikers had in 2018 te maken gehad met afpersing, waarbij het in de meeste gevallen ging om dit soort porno-afpersmails. Vrijwel niemand gaf aan betaald te hebben.

Whaling

In de periode dat het onderzoek liep (het laatste kwartaal van 2018) is volgens de media een vorm van spear-phishing sterk in opkomst geraakt (NOS, 2018; NRC, 2019). Hierbij wordt om geld gevraagd door de fraudeur die zich als een familielid, bekende of werkgever 'in geldnood' voordoet. Deze vorm van fraude wordt 'whaling' genoemd. De meest voorkomende vorm van whaling is 'whatsappfraude', maar de oplichting gebeurt ook via andere sociale media, e-mail of SMS. In de enquête is hier niet specifiek naar gevraagd, maar dit soort incidenten werd door 14 respondenten (minder dan 0,1 procent van de internetgebruikers) genoemd bij de open vragen. Slechts 1 respondent gaf aan hier financiële schade door te hebben geleden.

Ransomware of cryptoware

Een vermogensdelict waar – in tegenstelling tot de hierboven genoemde – meestal geen phishing aan ten grondslag ligt, is ransomware of cryptoware (zie ook hoofdstuk 3 over hacken). Hierbij is een computer geblokkeerd of zijn computergegevens versleuteld. Dit is 0,2 procent van de internetgebruikers naar eigen zeggen in 2018 overkomen. Een kwart van hen , dit komt neer op 0,04 procent van de internetgebruikers, heeft geld aan de dader betaald voor het herstellen daarvan. Dit delict komt als vermogensdelict dus vrijwel niet voor.

Overige identiteitsfraude

Er is specifiek naar twee vormen van identiteitsfraude gevraagd die niet direct betrekking hebben op fraude in het betalingsverkeer, te weten het misbruik van persoonsgegevens voor het aanvragen van een zorgvergoeding en het misbruik van persoonsgegevens voor het plegen van misdrijven[4]. 0,4 procent van de internetgebruikers zei dat hun persoonsgegevens voor deze doeleinden in 2018 zijn misbruikt; 0,1 procent is er geld aan kwijtgeraakt (zie ook hoofdstuk 7 over identiteitsfraude zonder financiële schade).

Hieronder volgt meer gedetailleerde informatie over slachtofferschap van twee delicten, te weten nepboetes/nepfacturen/nepacties en Wangirifraude. Alleen voor deze delicten is het aantal slachtoffers in het onderzoek voldoende (respectievelijk 103 en 167) om dit op een betrouwbare wijze te kunnen doen (zie ook tabel 6 in de tabellenbijlage). In hoofdstuk 8 wordt meer in detail ingegaan op enkele van de hierboven beschreven vormen van phishing waarbij de ontvanger géén financieel verlies leed.

4.3.1 Slachto erschap van enkele andere vermogensdelicten, 2018

	% van de internetgebruikers van 12 jaar of ouder
Nepboete/nepfactuur of nepactie	0,3
Voorschotfraude	0,1
Frauduleuze factuurwijziging	0,0
Microsoftscam	0,2
Wangirifraude	0,5
Afpersing	0,0
Whaling'[1)]	0,0
Ransomware of cryptoware	0,0
Overige identiteitsfraude	0,1

[1)] Genoemd bij de open antwoordcategorie.

Nepboetes/nepfacturen/nepacties en Wangirifraude

Melding en aangifte

Ruim 4 op de 10 slachtoffers van nepboetes, nepfacturen of nepacties hebben het delict gemeld, voornamelijk bij de politie (26 procent). Ook werden deze nepberichten nogal eens bij een bank (15 procent) en/of de Fraudehelpdesk (12 procent) gemeld. Bijna een kwart van de slachtoffers (24 procent) deed aangifte bij de politie.

[4)] Uit de open vragen blijkt dat enkele respondenten dit wat ruimer hebben geïnterpreteerd en het gebruik van de persoonsgegevens an sich al als misdrijf hebben gezien.

Wangirifraude werd door 15 procent van de slachtoffers bij een instantie gemeld, veelal bij de politie en/of de telefoon- of internetprovider[5]. Slechts 2 procent deed aangifte.

4.3.2 Nepboete/nepfactuur of nepactie en wangirifraude – melding[1] en aangifte, 2018

	Nepboete/nepfactuur of nepactie	Wangirifraude
	% slachtoffers	
Gemeld bij minstens één van de volgende instanties	41,3	15,1
Politie	25,7	5,6
Bank of financiële instelling	15,4	2,5
Fraudehelpdesk	11,6	1,9
Echte bedrijf[2]	5,5	
Telefoon of internetprovider		6,7
Centraal Meldpunt Identiteitsfraude en -fouten	4,2	0,0
Aangifte bij de politie	23,8	2,0
Weet niet of er aangifte is gedaan	5,1	3,3

[1] Meerdere antwoorden mogelijk.
[2] Genoemd bij de open antwoordcategorie.

Voor slachtoffers van nepboetes, nepfacturen of nepacties is de belangrijkste reden om niet te melden dat het niet belangrijk genoeg was (21 procent). Het ging in de meeste gevallen om een klein bedrag.

4.3.3 Nepboete/nepfactuur of nepactie en wangirifraude – belangrijkste reden niet melden, 2018

	Nepboete/nepfactuur of nepactie	Wangirifraude
	% slachtoffers	
Niet gemeld	*58,7*	*84,9*
Helpt niet, totaal	13,4	28,6
Krijg geld toch niet terug	9,1	13,8
Ontmoedigende houding van de politie	2,5	2,3
Dader wordt toch niet gepakt	1,7	12,5
Niet belangrijk genoeg, totaal	21,2	38,1
Ging om een klein bedrag	17,5	29,0
Te veel moeite	3,6	8,6
Niet in me opgekomen[1]	0,0	0,5
Overige redenen of onbekend, totaal	24,1	18,1
Was mijn eigen fout	5,8	5,5
Wegens schaamte	2,3	1,1
Was niet mogelijk voor dit incident	6,0	3,7
Andere reden	5,9	2,1
Onbekend	4,1	5,8

[1] Genoemd bij de open antwoordcategorie.

[5] Waarschijnlijk ligt dit percentage veel hoger. Niet alle slachtoffers die de schade volledig vergoed kregen door de telecomprovider zullen in de enquête hebben opgegeven dat ze geld zijn kwijtgeraakt (zie ook noot 2). Zij zijn niet als slachtoffer gerekend en kregen de vraag over melding niet.

Dit was ook voor slachtoffers van Wangirifraude de belangrijkste reden om het niet te melden (38 procent). Daarnaast verwachtten ook relatief veel slachtoffers dat het niet zou helpen (29 procent), bijvoorbeeld omdat men het geld toch niet terugkrijgt of de dader niet wordt gepakt.

De belangrijkste reden om geen aangifte bij de politie te doen was voor slachtoffers van nepboetes, nepfacturen of nepacties dat het toch niet helpt (4 procent). Dit was ook de belangrijkste reden voor slachtoffers van Wangirifraude (3 procent), evenals de reden dat het delict niet belangrijk genoeg werd bevonden (eveneens 3 procent).

4.3.4 Nepboete/nepfactuur of nepactie en wangirifraude – belangrijkste reden geen aangifte, 2018

	Nepboete/nepfactuur of nepactie	Wangirifraude
	% slachtoffers	
Wel ergens gemeld, maar geen aangifte	12,4	9,8
Helpt niet, totaal	4,0	2,6
Krijg geld toch niet terug	0,6	1,4
Ontmoedigende houding van de politie	1,4	0,0
Dader wordt toch niet gepakt	1,1	1,3
Advies van de politie	0,8	0,0
Niet belangrijk genoeg, totaal	1,6	2,5
Ging om een klein bedrag	0,0	2,5
Te veel moeite	1,6	0,0
Overige redenen of onbekend	6,7	4,7
Was mijn eigen fout	0,9	0,6
Was niet mogelijk voor dit incident	2,6	0,0
Bank zou het verder afhandelen[1)]	0,5	0,0
Andere reden	2,1	1,0
Onbekend	0,7	3,1

[1)] Genoemd bij de open antwoordcategorie.

Gevolgen voor het slachto er

Van de slachtoffers van nepboetes, nepfacturen of nepacties kreeg 12 procent de financiële schade volledig vergoed. Ruim 40 procent ondervond emotionele gevolgen. Dit uitte zich voornamelijk in boosheid (bij 35 procent). Bijna 4 op de 10 slachtoffers (39 procent) hebben sinds het delict plaatsvond minder vertrouwen in de digitale veiligheid.

Van de slachtoffers van Wangirifraude kreeg 4 procent de financiële schade volledig vergoed[6)]. Een derde van hen (32 procent) ondervond emotionele gevolgen, voornamelijk boosheid. Eveneens een derde (33 procent) heeft sindsdien minder vertrouwen in de digitale veiligheid.

[6)] Waarschijnlijk ligt dit percentage hoger. Niet alle slachtoffers die de schade volledig vergoed kregen door de telecomprovider zullen in de enquête hebben opgegeven dat ze geld zijn kwijtgeraakt (zie ook noot 2). Zij zijn niet als slachtoffer gerekend en kregen de vraag over vergoeding niet.

4.3.5 Nepboete/nepfactuur of nepactie en wangirifraude – gevolgen voor het slachto er[1], 2018

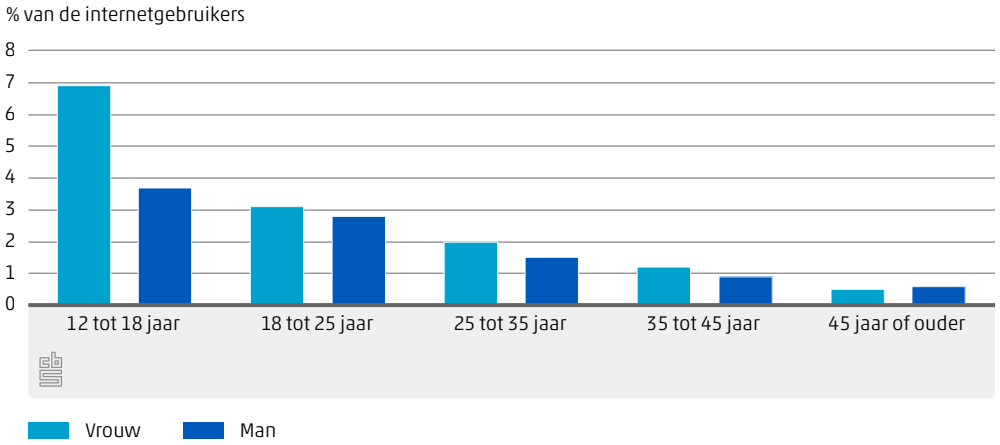
	Nepboete/nepfactuur of nepactie	Wangirifraude
	% slachtoffers	
Financiële schade		
Helemaal vergoed	12,2	4,3
Deels vergoed	2,3	2,0
Niets vergoed	77,9	79,8
Onbekend	7,6	14,0
Emotionele gevolgen	41,6	32,4
Blijft eraan denken	18,4	8,1
Erg boos	35,0	25,4
Sliep slechter	13,0	2,6
Minder vertrouwen in de digitale veiligheid	38,8	33,3
Minder vertrouwen in de eigen digitale vaardigheid	15,7	11,5

[1] Meerdere antwoorden mogelijk.

5. Interpersoonlijke incidenten, niet seksueel

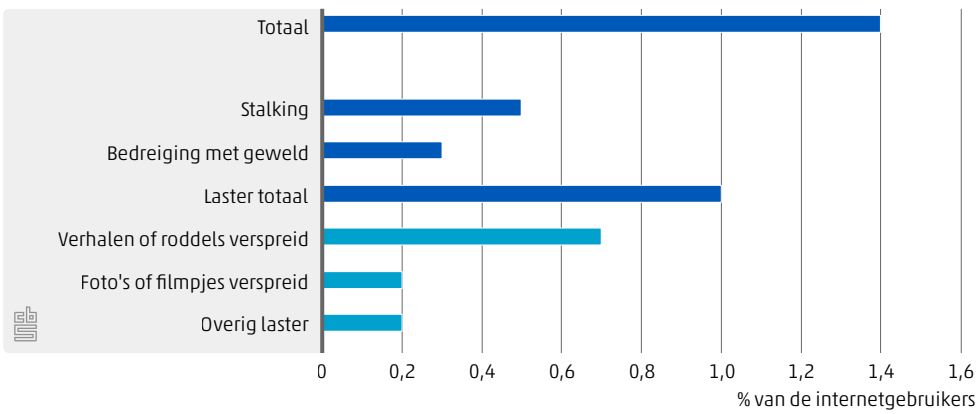
In 2018 heeft 1,4 procent van de internetgebruikers weleens last gehad van interpersoonlijke niet-seksuele cyberincidenten. Het gaat dan om incidenten in de persoonlijke sfeer, zoals roddel, pesten, stalken of bedreiging, zonder dat daarbij sprake is van seksuele bedoelingen. Tieners, en dan vooral meisjes, ondervonden dit soort incidenten het vaakst: 5 procent van alle 12- tot 18-jarigen zei hiervan weleens last te hebben gehad; 7 procent van de meisjes tegen 4 procent van de jongens.

5.1 Last gehad van niet-seksuele interpersoonlijke incidenten naar leeftijd en geslacht, 2018



Laster werd het meest genoemd (door 0,9 procent). Het ging dan met name om het rondgaan van verhalen of roddels (0,7 procent), maar ook om het verspreiden van foto's of filmpjes (0,2 procent) en andere vormen van laster, zoals het maken van een gênante website of profiel over het slachtoffer of het posten van berichten uit naam van het slachtoffer (0,2 procent). Stalking en bedreiging met geweld kwamen minder vaak voor en werden door respectievelijk 0,5 en 0,3 procent van de internetgebruikers genoemd.

5.2 Last gehad van interpersoonlijke niet-seksuele incidenten, 2018



In de enquête zijn 327 slachtoffers van niet-seksuele laster, 129 slachtoffers van stalking en 96 slachtoffers van bedreiging met geweld nader ondervraagd over hetgeen hen is overkomen. Deze detailinformatie volgt hieronder (zie ook tabel 7 in tabellenbijlage).

Gebruikte medium

De meeste incidenten gebeurden via sociale media: bij 65 procent van de slachtoffers van laster en bij 57 procent van de slachtoffers van stalking en bedreiging. Daarnaast werd WhatsApp vaak gebruikt (bij 3 à 4 op de 10 slachtoffers). E-mail werd slechts bij ongeveer 10 procent van de slachtoffers gebruikt. Tevens kwam het voor dat combinaties van deze media werden ingezet. Daarnaast werden ook andere media gebruikt, zoals gamefora of datingsites.

5.3 Interpersoonlijke niet-seksuele incidenten – gebruikte medium[1], 2018

	Laster	Stalking	Bedreiging
	% slachtoffers		
Via e-mail	7,2	16,2	9,0
Via sociale media	65,2	56,9	57,4
Via WhatsApp of sms[2]	41,0	38,6	35,4
Anders of onbekend	7,1	14,1	20,0

[1] Meerdere antwoorden mogelijk.
[2] Genoemd bij de open antwoordcategorie.

De dader

De meeste slachtoffers wisten wie de dader(s) waren. Bij 73 procent van de slachtoffers van laster, 67 procent van de gestalkten en 57 procent van de bedreigden was de dader c.q. waren de daders bekend. Dit hoeft overigens niet altijd iemand te zijn die het slachtoffer in het echte leven, dus buiten de digitale wereld kent.

Laster werd vaak gepleegd door vrienden en/of iemand van school. Beide werden door ruim een vijfde van de slachtoffers als dader genoemd, maar er zal sprake zijn van overlap, bijvoorbeeld in geval van een schoolvriend. Bij 13 procent van de lasterslachtoffers behoorde een ex-partner tot de dader(s).

Stalking en bedreiging gebeurde in de meeste gevallen door een ex-partner, namelijk bij respectievelijk 17 procent en 14 procent van de slachtoffers.

5.4 Interpersoonlijke niet-seksuele incidenten – informatie over de dader(s)[1], 2018

	Laster	Stalking	Bedreiging
	% slachtoffers		
Dader is bekend	73,0	66,6	57,1
Partner	0,3	2,9	1,2
Ex-partner	13,0	16,5	14,3
Ander familielid	2,9	1,9	0,0
Buurtgenoot	3,1	2,8	5,3
Vriend/vriendin	20,7	11,4	8,7
Iemand van school	22,6	9,4	9,8
Collega	1,6	1,1	1,0

[1] Meerdere antwoorden mogelijk.

Gevolgen voor het slachto er

Bijna de helft van de slachtoffers van laster (47 procent) ondervond hiervan emotionele gevolgen: de meesten waren erg boos (38 procent). Bijna een kwart (23 procent) van de slachtoffers voelt zich hierdoor minder veilig in de digitale wereld, een vijfde van de slachtoffers is bang voor herhaling.

Ook van stalking ondervond bijna de helft (48 procent) emotionele gevolgen, voornamelijk boosheid (43 procent). Ongeveer een kwart sliep er slechter door. Ruim een vijfde (21 procent) van de gestalkten heeft sindsdien minder vertrouwen in de digitale veiligheid. Eenzelfde deel is bang voor herhaling.

Van degenen die met geweld bedreigd zijn, rapporteerden 40 procent emotionele gevolgen, boosheid kwam wederom het vaakst voor (28 procent). Bedreiging heeft minder impact op het vertrouwen in de toekomst dan laster en stalking: bij minder dan 1 op de 10 slachtoffers heeft het een negatief effect op het vertrouwen in de digitale veiligheid of bestaat er angst voor herhaling.

5.5 Interpersoonlijke niet-seksuele incidenten – gevolgen voor het slachto er[1], 2018

	Laster	Stalking	Bedreiging
	% slachtoffers		
Emotionele gevolgen	46,5	48,4	39,7
Blijft eraan denken	15,6	18,1	16,7
Erg boos	37,9	42,8	28,4
Sliep slechter	17,4	25,9	15,0
Minder vertrouwen in de digitale veiligheid	23,0	20,6	8,8
Minder vertrouwen in de eigen digitale vaardigheid	7,3	3,7	0,9
Bang dat het vaker zal gebeuren	19,7	21,4	7,7
Financiële schade, niets vergoed	2,2	0,9	4,1

[1] Meerdere antwoorden mogelijk.

Aard van de incidenten

Volgens 9 procent van de slachtoffers van laster betrof het incident een strafbaar misdrijf. Bijna de helft van de slachtoffers (46 procent) vond de laster wel verkeerd, maar zou het niet als misdrijf omschrijven. Zo'n 4 procent vond het aan zichzelf te wijten; 10 procent beschreef het incident als iets dat toevallig gebeurde.

Stalking werd vaker als een strafbaar misdrijf beschouwd, namelijk door 17 procent van de slachtoffers. Maar ook hier vindt de helft van de slachtoffers het wel verkeerd, maar niet echt een misdrijf. Door 7 procent werd het slechts als een toevallige gebeurtenis beschouwd; 2 procent vond het zijn of haar eigen schuld.

Bedreigingen werden het vaakst als een strafbaar misdrijf gezien, namelijk door ruim een kwart van de slachtoffers (27 procent). Daarnaast vond 44 procent het verkeerd, maar geen misdrijf. Bedreiging werd niet vaak als toeval of eigen schuld beschouwd.

5.6 Interpersoonlijke niet-seksuele incidenten – aard van de incidenten volgens de slachtoffers, 2018

	Laster	Stalking	Bedreiging
	% slachtoffers		
Strafbaar misdrijf	9,1	16,5	26,8
Verkeerd, maar geen misdrijf	46,3	50,1	43,6
Toevallige gebeurtenis	9,9	6,9	2,5
Niet strafbaar, was eigen schuld	4,3	2,2	2,7
Kan het niet plaatsen	20,0	14,4	11,0
Wil niet antwoorden	10,3	9,8	13,5

Melding en aangifte

Ruim 4 op de 10 slachtoffers van laster (42 procent) hadden dit ergens gemeld. Een derde vertelde het aan mensen uit de persoonlijke kring, met name familie of vrienden (32 procent). Daarnaast meldde 14 procent het bij een instantie, meestal bij de politie (12 procent), 6 procent deed aangifte bij de politie.

Ruim de helft van de slachtoffers van stalking (52 procent) heeft dit bij iemand gemeld. Het meest werd het verteld aan familie of vrienden (37 procent). Bij een instantie werd het stalken door een kwart van de slachtoffers gemeld, waarvan verreweg het grootste deel bij de politie (23 procent). Ruim 1 op de 10 slachtoffers (11 procent) deed aangifte bij de politie.

Van de slachtoffers van bedreiging ondernam twee derde geen actie. Een kwart (26 procent) vertelde dit aan familie of vrienden. Een op de vijf meldde het bij een instantie, waarvan ook hier bijna altijd bij de politie (19 procent). Net als bij stalking deed bij bedreiging ruim 1 op de 10 aangifte bij de politie.

5.7 Interpersoonlijke niet-seksuele incidenten – melding[1] en aangifte, 2018

	Laster	Stalking	Bedreiging
	% slachtoffers		
Gemeld	42,1	51,5	34,4
Verteld aan familie, vrienden of leerkracht	33,4	38,9	26,4
Familie of vrienden	31,7	36,9	26,4
Leerkracht	6,4	6,6	3,9
Gemeld bij minstens één van de volgende instanties:	14,2	24,7	19,6
Politie	12,3	23,0	18,6
Pesten.nl	0,0	0,0	0,0
Meldpunt huiselijk geweld	0,0	1,1	1,0
Via sociale media[2]	0,4	1,7	1,0
Werkgever[2]	1,5	1,6	0,0
Aangifte bij de politie	6,4	11,1	11,4

[1] Meerdere antwoorden mogelijk.
[2] Genoemd bij de open antwoordcategorie.

Er zijn verschillende redenen waarom slachtoffers het incident nergens hebben gemeld. De belangrijkste reden was dat dat toch niet zou helpen. Dit werd door 24 procent van de slachtoffers van laster en bedreiging opgegeven en door 15 procent van de slachtoffers van stalking. Slachtoffers van stalking en bedreiging gaven hiervoor relatief vaak geen reden op.

5.8 Interpersoonlijke niet-seksuele incidenten – belangrijkste reden niet melden, 2018

	Laster	Stalking	Bedreiging
	% slachtoffers		
Niet gemeld	57,9	48,5	65,6
Helpt niet, totaal	24,3	14,9	24,3
Helpt toch niets	10,7	8,0	11,5
Afwijzende houding van de politie	0,0	0,0	1,9
Geen zaak voor de politie	12,3	5,7	7,4
Dader wordt toch niet gepakt	1,4	1,2	3,5
Niet belangrijk genoeg, totaal	13,8	8,1	11,1
Was niet zo belangrijk	12,2	6,0	9,4
Te veel moeite	1,6	2,1	1,7
Overige redenen of onbekend, totaal	19,8	25,4	30,2
Is al opgelost	8,4	6,1	5,8
Dader is bekende	2,8	1,5	2,2
Angst voor de gevolgen	0,3	3,3	2,5
Wegens schaamte	0,6	0,9	2,2
Was mijn eigen schuld[1]	0,2	0,0	0,0
Weet niet waar dat zou kunnen	0,8	0,6	0,0
Andere reden	2,2	1,9	6,1
Onbekend	4,4	11,2	11,5

[1] Genoemd bij de open antwoordcategorie.

Indien een slachtoffer het voorval bij iemand of bij een instantie heeft gemeld, hoeft daar nog geen aangifte bij de politie op te volgen. Redenen om dit niet te doen zijn hier ook vaak dat het toch niet zal helpen. Dit werd door 16 procent van de slachtoffers van laster en stalking genoemd en door 10 procent van de bedreigden. Ongeveer 9 procent van de slachtoffers van laster en stalking deed geen aangifte bij de politie omdat het al was opgelost.

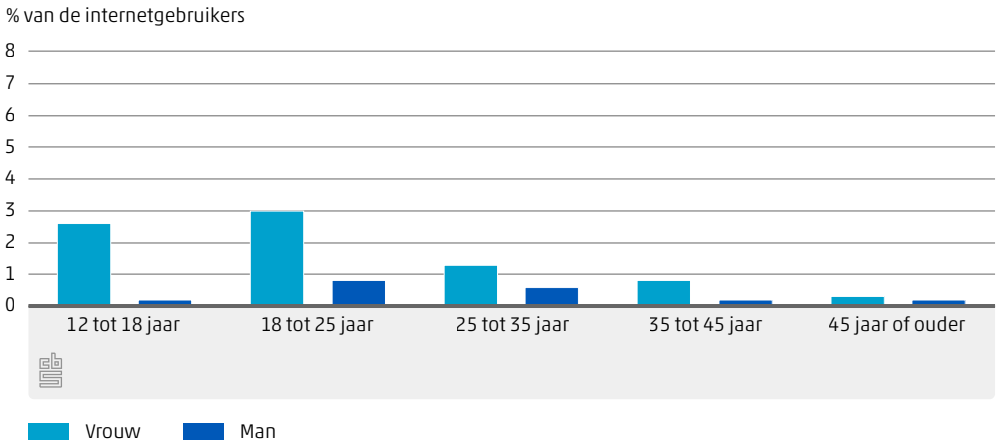
5.9 Interpersoonlijke niet-seksuele incidenten – belangrijkste reden geen aangifte, 2018

	Laster	Stalking	Bedreiging
	% slachtoffers		
Wel ergens gemeld maar geen aangifte	35,7	40,4	23,0
Helpt niet, totaal	15,9	15,6	10,4
Helpt toch niets	5,4	5,7	7,9
Advies van de politie	1,0	1,0	0,0
Afwijzende houding van de politie	1,4	2,2	0,6
Geen zaak voor de politie	7,0	4,6	1,9
Dader wordt toch niet gepakt	0,8	2,2	0,0
Niet belangrijk genoeg, totaal	4,7	6,6	5,5
Was niet zo belangrijk	3,7	6,0	5,5
Te veel moeite	1,0	0,7	0,0
Overige redenen of onbekend	15,1	18,2	7,1
Is al opgelost	8,4	9,4	2,6
Dader is bekende	1,1	0,0	0,7
Angst voor de gevolgen	1,1	3,0	1,1
Uit schaamte	0,2	0,0	0,0
Weet niet waar dat zou kunnen	0,0	0,6	0,0
Andere reden	2,2	3,5	0,8
Onbekend	2,2	1,6	1,9

6. Interpersoonlijke incidenten, seksueel

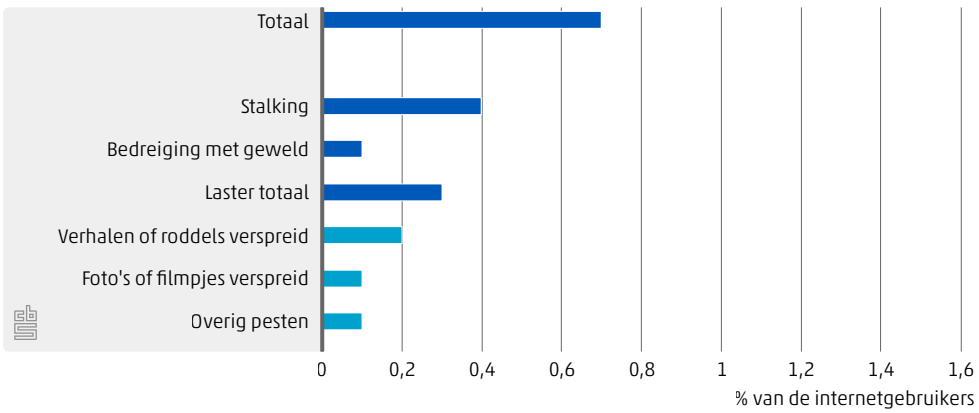
In 2018 had 0,7 procent van de internetgebruikers weleens last gehad van cyberincidenten in de persoonlijke sfeer waarbij sprake was van een seksuele (bij-)bedoeling. Het gaat dan om incidenten als roddel, pesten, stalken of bedreiging met geweld. Jonge vrouwen ondervonden dit soort incidenten het vaakst: zo geeft 3 procent van de 18- tot 25-jarige vrouwen aan hiervan weleens last te hebben gehad, tegen 0,8 procent van de mannen in deze leeftijdscategorie.

6.1 Last gehad van seksuele interpersoonlijke incidenten naar leeftijd en geslacht, 2018



Stalking en laster met een seksuele (bij-)bedoeling kwamen ongeveer even vaak voor, te weten bij respectievelijk 0,4 en 0,3 procent van de internetgebruikers. Stalking wordt iets vaker gerapporteerd door jongvolwassen vrouwen, laster iets meer door tienermeisjes. Bedreiging met geweld vond minder vaak plaats; dit wordt genoemd door 0,1 procent van de internetgebruikers.

6.2 Last gehad van seksuele interpersoonlijke incidenten, 2018



Behalve met op de persoon gerichte incidenten worden jonge vrouwen ook relatief vaak geconfronteerd met massaal verzonden 'seksuele spam', zoals naaktfoto's/ filmpjes of datingverzoeken. Ongeveer 3 procent van de jonge vrouwen in de leeftijd van 12 tot 25 jaar meldden dit in de enquête. Bij hun mannelijke leeftijdsgenoten was dit ongeveer 1 procent. Seksuele spam wordt nauwelijks ontvangen door ouderen.

In de enquête werden 106 slachtoffers van seksueel getinte laster en 115 slachtoffers van seksueel getinte stalking nader ondervraagd over dit incident. Deze detailinformatie volgt hieronder. Over bedreiging met geweld is informatie van slechts 16 slachtoffers beschikbaar. Dit aantal is te gering om betrouwbare detailinformatie over dit incident te geven (zie ook tabel 8 tabellenbijlage).

Seksueel getinte laster en stalking

Gebruikte medium

Verreweg de meeste laster en stalking met seksuele bedoeling gebeurde via sociale media: bij 69 procent van de slachtoffers van laster en 66 procent van de slachtoffers van stalking. Bij 1 op de 3 slachtoffers werd WhatsApp gebruikt en bij ongeveer 1 op de 6 à 7 e-mail. Soms werden combinaties van deze media gebruikt, en soms ook andere media zoals datingsites.

6.3 Seksuele interpersoonlijke incidenten – gebruikte medium, 2018

	Laster	Stalking
	% slachtoffers	
E-mail	12,5	17,3
Social media	69,3	65,8
What's App of sms[1)]	31,5	34,5
Anders	10,2	9,1

[1)] Werd genoemd bij de open antwoordcategorie.

De dader

Iets meer dan de helft van de slachtoffers wist wie de dader(s) waren: bij 55 procent van de slachtoffers van laster en 52 procent van de gestalkten was/waren de dader(s) bekend. Dit hoeft niet altijd iemand te zijn die het slachtoffer in het echte leven kent.

Bij seksuele laster gaf 11 procent van de slachtoffers aan dat de dader de ex-partner was, 9 procent zei iemand van school. Bij stalking noemde 16 procent van de slachtoffers de ex-partner als dader.

6.4 Seksuele interpersoonlijke incidenten – informatie over de dader(s)[1)], 2018

	Laster	Stalking
	% slachtoffers	
Dader is bekend	55,1	52,3
Partner	1,2	0,0
Ex-partner	10,9	15,6
Buurtgenoot	1,5	2,5
Vriend/vriendin	5,3	2,1
Iemand van school	8,5	3,6
Collega	1,3	1,2

[1)] Meerdere antwoorden mogelijk.

Gevolgen voor het slachtoffer

Zo'n 44 procent van de slachtoffers van laster en 51 procent van de gestalkten ondervond emotionele gevolgen. Dit uitte zich voornamelijk in boosheid (bij bijna 40 procent van de slachtoffers). Daarnaast kon bijna 1 op de 5 slachtoffers het niet loslaten, of sliep er slechter door.

Ruim een kwart van de slachtoffers heeft minder vertrouwen in de digitale veiligheid door deze incidenten. Ongeveer een vijfde van de slachtoffers is bang dat het vaker zal gebeuren.

6.5 Seksuele interpersoonlijke incidenten – gevolgen voor het slachtoffer[1)], 2018

	Laster	Stalking
	% slachtoffers	
Emotionele gevolgen	43,6	50,5
Blijft eraan denken	19,1	18,4
Erg boos	39,5	37,2
Sliep slechter	18,0	20,9
Minder vertrouwen in de digitale veiligheid	28,5	27,9
Minder vertrouwen in de eigen digitale vaardigheid	17,4	15,8
Bang dat het vaker zal gebeuren	21,9	19,2
Financiële schade, niet vergoed	2,3	2,9

[1)] Meerdere antwoorden mogelijk.

Aard van de incidenten

Volgens ruim 1 op de 5 slachtoffers van seksueel getinte laster (22 procent) betrof het incident een strafbaar misdrijf. Ruim een derde (35 procent) vond het incident wel verkeerd, maar zou het niet als misdrijf omschrijven. Ongeveer 1 op de 10 slachtoffers van laster vond het aan zichzelf te wijten, eenzelfde deel beschreef het incident als iets dat toevallig gebeurde.

Seksueel getinte stalking wordt minder vaak als een misdrijf beschouwd, namelijk door 16 procent van de slachtoffers. Ruim de helft van de gestalkten (52 procent) vond het wel verkeerd, maar geen misdrijf.

6.6 Seksuele interpersoonlijke incidenten – aard van de incidenten volgens de slachto ers, 2018

	Laster	Stalking
	% slachtoffers	
Strafbaar misdrijf	21,9	16,1
Verkeerd, maar geen misdrijf	34,8	52,3
Toevallige gebeurtenis	8,7	5,2
Niet strafbaar, was eigen schuld	9,2	2,5
Kan het niet plaatsen	13,3	19,1
Wil niet antwoorden	12,1	4,7

Melding en aangifte

Bijna de helft van de slachtoffers van seksueel getinte laster (45 procent) heeft dit ergens gemeld. Bijna een derde vertelde het aan familie of vrienden. Daarnaast meldde 16 procent het bij een instantie, verreweg het vaakst bij de politie (15 procent). 10 procent deed aangifte.

6.7 Seksuele interpersoonlijke incidenten – melding en aangifte, 2018

	Laster	Stalking
	% slachtoffers	
Gemeld	44,7	49,7
Verteld aan familie/vrienden/leerkracht	33,0	38,9
Familie of vrienden	31,0	38,9
Leerkracht	4,4	0,4
Gemeld bij een instantie	16,1	19,5
Politie	15,2	16,5
Pesten.nl	0,0	0,0
Meldpunt huiselijk geweld	0,0	0,9
Social media[1)]	0,9	2,1
Werkgever[1)]	.	.
Aangifte bij de politie	9,6	9,8

[1)] Werden genoemd bij de open antwoordcategorie.

De helft van de slachtoffers van stalking heeft dit ergens gemeld. Bijna 40 procent vertelde het aan familie of vrienden en bijna 20 procent van de slachtoffers meldde het (daarnaast) bij een instantie, voornamelijk bij de politie (17 procent). 1 op de 10 deed aangifte.

Er zijn verschillende redenen waarom slachtoffers het incident nergens hebben gemeld. Bij laster kwamen deze vaak erop neer dat het niet zou helpen (18 procent). Daarnaast vond 10 procent het niet belangrijk genoeg, zei 8 procent dat het al snel was opgelost en noemde 9 procent schaamte als reden om niet te melden.
Seksueel getinte stalking werd meestal niet gemeld omdat het niet belangrijk genoeg gevonden werd (17 procent). Daarnaast zei 11 procent van de slachtoffers dat het al was opgelost en 12 procent dat het niet zou helpen.

6.8 Seksuele interpersoonlijke incidenten – belangrijkste reden niet melden, 2018

	Laster	Stalking
	% slachtoffers	
Niet gemeld	*55,3*	*50,3*
Helpt niet, totaal	17,5	11,8
Helpt toch niets	9,5	7,6
Geen zaak voor de politie	7,0	2,8
Dader wordt toch niet gepakt	1,0	1,5
Niet belangrijk genoeg, totaal	10,2	17,1
Was niet zo belangrijk	10,2	16,1
Te veel moeite	0,0	1,0
Overige redenen of onbekend	27,6	21,4
Is al opgelost	8,3	10,6
Dader is bekende	0,3	1,1
Angst voor de gevolgen	3,1	1,5
Uit schaamte	8,6	3,8
Was mijn eigen schuld[1)]	0,8	0,0
Weet niet waar dat zou kunnen	3,2	2,0
Andere reden	1,8	1,2
Onbekend	1,5	1,2

[1)] Werd genoemd bij de open antwoordcategorie.

Indien een slachtoffer het voorval ergens heeft gemeld, hoeft daar nog geen aangifte bij de politie op te volgen. Ook hier wordt als belangrijkste reden om dit achterwege te laten het vaakst opgegeven dat het toch niet zal helpen (door 12 procent van de slachtoffers). Daarnaast vond 8 procent van de slachtoffers van seksueel getinte laster en 6 procent van de gestalkten het niet belangrijk genoeg. Zo'n 3 procent van de slachtoffers van laster kreeg het advies van de politie om geen aangifte te doen.

6.9 Seksuele interpersoonlijke incidenten – belangrijkste reden geen aangifte, 2018

	Laster	Stalking
	% slachtoffers	
Wel ergens gemeld maar geen aangifte	35,1	39,8
Helpt niet, totaal	11,7	11,6
Helpt toch niets	6,5	7,1
Advies van de politie	2,7	0,8
Afwijzende houding van de politie	0,0	0,0
Geen zaak voor de politie	1,7	1,9
Dader wordt toch niet gepakt	0,7	1,3
Niet belangrijk genoeg, totaal	8,3	6,4
Was niet zo belangrijk	6,7	6,4
Te veel moeite	1,6	0,0
Overige redenen of onbekend	15,2	21,8
Is al opgelost	3,3	6,0
Dader is bekende	1,5	1,0
Dader was niet bekend[1)]	0,0	0,5
Angst voor de gevolgen	1,7	3,2
Uit schaamte	0,0	0,6
Weet niet waar dat zou kunnen	0,5	2,2
Andere reden	4,1	5,3
Onbekend	4,0	3,5

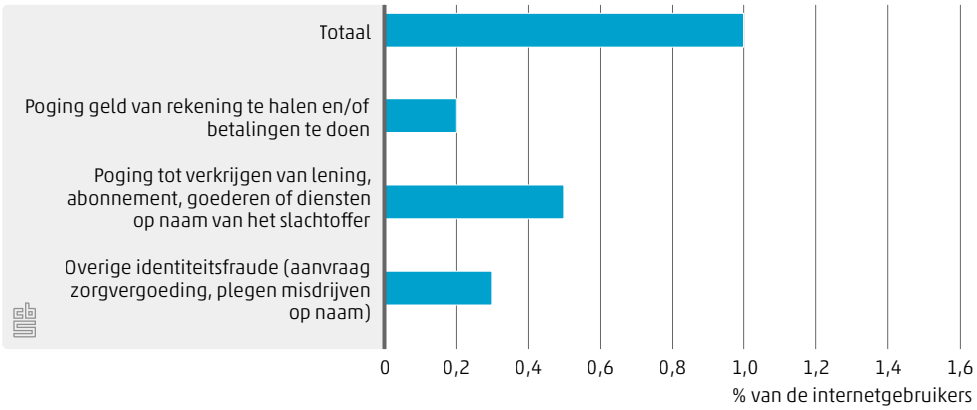
[1)] Werd genoemd bij de open antwoordcategorie.

7. Identiteitsfraude zonder nanciële schade

Naast vermogensdelicten waarbij de persoon geld is verloren (hoofdstuk 4), zijn er ook delicten waarbij weliswaar geen financiële schade is opgetreden, maar die wel degelijk grote impact kunnen hebben, omdat de dader in naam van het slachtoffer handelde. Tot deze categorie behoren twee vormen van financieel 'mislukte' fraude via het betalingsverkeer en andere identiteitsfraude, waarbij in dit onderzoek specifiek is gevraagd naar het misbruik van persoonsgegevens voor het aanvragen van een zorgvergoeding of voor het plegen van een misdrijf.

Eén procent van de internetgebruikers werd in 2018 slachtoffer van identiteitsfraude zonder financieel verlies. Bij 0,2 procent probeerde de dader geld van de rekening af te halen of er betalingen mee te doen en bij 0,5 procent werd getracht een lening, abonnement, goederen of diensten aan te vragen. Daarnaast werden bij 0,3 procent persoonsgegevens misbruikt voor het aanvragen van een zorgvergoeding of het plegen van misdrijven.

7.1 Slachto erschap identiteitsfraude zonder nanciële schade, 2018



Uit de enquête bleken er 175 slachtoffers te zijn op wiens naam de dader een lening, abonnement, goederen of diensten aanvroeg en 107 slachtoffers van identiteitsfraude anders dan via het betalingsverkeer. Deze personen zijn nader ondervraagd over dit delict, en de detailinformatie volgt hieronder. Het aantal respondenten dat aangaf dat een dader toegang tot de rekening probeerde te krijgen, was 74. Dit aantal is te gering om betrouwbare detailinformatie over dit delict te geven (zie ook tabel 9 in tabellenbijlage).

Misbruik persoonsgegevens voor lening/abonnement/ goederen en andere identiteitsfraude

Manier waarop de gegevens zijn verkregen

Slachtoffers op wiens naam een lening, abonnement, goederen of diensten werden aangevraagd weten vaak niet hoe de dader aan de gegevens is gekomen. Dit was bij bijna 4 op de 10 slachtoffers (39 procent) het geval. Door 28 procent van de slachtoffers werd aangegeven dat het door een vorm van hacken is gebeurd. Naar schatting werd bij 17 procent van de slachtoffers de gegevens verkregen door een vorm van phishing.

Ook degenen op wiens naam een zorgvergoeding is aangevraagd of een misdrijf is gepleegd wisten in 4 van de 10 gevallen niet hoe de gegevens waren verkregen. Ruim 20 procent dacht dat ze via hacken zijn verkregen en dan meestal via een hack bij een bedrijf waar de persoonlijke gegevens bekend zijn.

7.2 Identiteitsfraude zonder financiële schade – manier waarop de gegevens zijn verkregen, 2018

	Poging tot verkrijgen van lening, abonnement, goederen of diensten op naam van het slachtoffer	Overige identiteitsfraude (aanvraag zorgvergoeding, plegen misdrijf op naam)
	% slachtoffers	
Zelf bankpas in goed vertrouwen ter beschikking gesteld	1,6	.
Zelf persoonlijke gegevens in goed vertrouwen aan een bekende ter beschikking gesteld	1,5	.
Zelf gegevens doorgegeven op een webshop of via de telefoon	7,5	9,0
Niet online, maar door copiëren creditcard of bijv. dumpster diving[1)]	1,8	.
Diefstal van paspoort of ID-kaart waarbij identiteit overgenomen werd	0,8	3,1
Diefstal van bankpas/creditcard	0,8	.
Skimmen van bankpas/creditcard	1,5	.
Scannen van mobiele telefoon, bijv door contactloos betalen (shimming)	0,0	1,0
Phishing of pharming	8,2	6,9
Hacken van device of account	17,0	2,7
Via malware (bv. een computervirus of trojan horse)	2,0	2,9
Keylogging	0,0	1,2
Hacken van bedrijf of bank waar persoonlijke gegevens bekend zijn	8,7	14,3
Andere wijze	9,2	18,6
Weet het niet	39,4	40,5
Totaal door phishing[2)]	17,2	.
Totaal door hacken[2)]	27,7	21,0

1) Werd genoemd bij de open antwoordcategorie.
2) Aan meerdere vormen van gegevensdiefstal ging een vorm van phishing vooraf. Zie de methodologische toelichting in de onderzoeksverantwoording voor de berekening van 'totaal door phishing' en 'totaal door hacken'.

Gevolgen voor het slachtoffer

Het misbruik van persoonsgegevens voor de aanvraag van een lening, abonnement, goederen of diensten zorgde bij ruim een derde (36 procent) van de slachtoffers voor emotionele gevolgen, voornamelijk boosheid. 4 op de 10 slachtoffers heeft minder vertrouwen in de digitale veiligheid sinds het incident.

Ook van de slachtoffers op wiens naam een zorgvergoeding is aangevraagd of een misdrijf is gepleegd heeft een derde er emotioneel onder geleden. Dit uitte zich ook hier voornamelijk in boosheid. Bijna de helft (45 procent) van de slachtoffers heeft sindsdien minder vertrouwen in de digitale veiligheid. Ruim een kwart van de slachtoffers (27 procent) is bang dat het vaker zal gebeuren.

7.3 Identiteitsfraude zonder financiële schade – gevolgen voor het slachtoffer[1], 2018

	Poging tot verkrijgen van lening, abonnement, goederen of diensten op naam van het slachtoffer	Overige identiteitsfraude (aanvraag zorgvergoeding, plegen misdrijven op naam)
	% slachtoffers	
Emotionele gevolgen	35,5	33,6
Blijft eraan denken	11,8	9,9
Erg boos	30,4	27,8
Sliep slechter	7,4	10,1
Minder vertrouwen in de digitale veiligheid	40,1	44,7
Minder vertrouwen in de eigen digitale vaardigheid	11,6	18,2
Bang dat het vaker zal gebeuren	34,7	27,2

[1] Meerdere antwoorden mogelijk.

Melding en aangifte

Ruim de helft van de slachtoffers (51 procent) heeft de fraudeleuze aanvraag van een lening, abonnement, goederen of diensten gemeld, voornamelijk bij de politie (25 procent) en/of bij de bank (22 procent). 1 op de 10 slachtoffers gaf aan contact op te hebben genomen met het bedrijf waar de aanvraag of bestelling was gedaan, 16 procent deed aangifte bij de politie.

De frauduleuze aanvraag van een zorgvergoeding of het misdrijf dat door iemand anders was gepleegd werd door 39 procent van de slachtoffers gemeld. Een derde deed dit bij de politie en 12 procent (ook) bij de bank of andere financiële instelling. Bijna een kwart (24 procent) deed aangifte.

7.4 Identiteitsfraude zonder financiële schade – melding[1] en aangifte, 2018

	Poging tot verkrijgen van lening, abonnement, goederen of diensten op naam van het slachtoffer	Overige identiteitsfraude (aanvraag zorgvergoeding, plegen misdrijven op naam)
	% slachtoffers	
Gemeld bij minstens één van de volgende instanties	50,9	39,0
Politie	24,5	32,9
Bank, financiële instelling of creditcardmaatschappij[2]	21,5	12,3
Fraudehelpdesk	4,3	8,4
Centraal Meldpunt Identiteitsfraude en -fouten	4,4	1,4
Bedrijf of webshop waar de aanvraag of bestelling was gedaan[3]	10,0	
Aangifte bij de politie	15,7	23,5
Weet niet of er aangifte is gedaan	8,4	0,0

[1] Meerdere antwoorden mogelijk.
[2] Deze signaleerden het soms eerder dan het slachtoffer.
[3] Werd genoemd bij de open antwoordcategorie.

De slachtoffers die de frauduleuze aanvraag van een lening, abonnement, goederen of diensten niet hebben gemeld deden dit vooral omdat ze dachten dat het toch niet zou helpen (11 procent). Volgens 9 procent van de slachtoffers was het delict niet belangrijk genoeg.

Als redenen om het misbruik van persoonsgegevens voor de aanvraag van een zorg-vergoeding of voor het plegen van het misdrijf niet te melden werden relatief vaak genoemd dat de dader toch niet wordt gepakt (8 procent), het te veel moeite kost (8 procent), het door een eigen fout was gebeurd (7 procent) en dat het niet mogelijk was voor dit incident (6 procent).

7.5 Identiteitsfraude zonder financiële schade – belangrijkste reden niet melden, 2018

	Poging tot verkrijgen van lening, abonnement, goederen of diensten op naam van het slachtoffer	Overige identiteitsfraude (aanvraag zorg-vergoeding, plegen misdrijven op naam)
	% slachtoffers	
Niet gemeld	*49,1*	*61,0*
Helpt niet, totaal	10,8	12,3
Ontmoedigende houding van de politie	0,0	3,5
Advies van de politie	1,0	0,0
Dader wordt toch niet gepakt	8,6	7,5
Er wordt toch niets mee gedaan[1)]	1,2	1,2
Niet belangrijk genoeg, totaal	8,5	7,7
Ging om een klein bedrag, was geen belangrijk incident	1,9	0,0
Te veel moeite	3,7	7,7
Er was geen financiële schade[1)]	2,9	0,0
Overige redenen of onbekend	29,8	41,1
Dader is bekende	0,4	0,0
Was mijn eigen fout	5,2	7,3
Wegens schaamte	0,2	0,0
Was niet mogelijk voor dit incident	2,8	6,3
Andere reden	9,4	8,8
Onbekend	11,7	18,7

[1)] Werden genoemd bij de open antwoordcategorie.

Slachtoffers van een frauduleuze aanvraag van een lening, abonnement, goederen of diensten op hun naam lieten een aangifte vooral achterwege omdat het niet mogelijk was voor dit incident (5 procent), het toch niet helpt (4 procent) of niet belangrijk genoeg was (3 procent).

Ook door slachtoffers op wiens naam een zorgvergoeding is aangevraagd of misdrijf is gepleegd werd het vaakst genoemd dat een aangifte niet mogelijk was.

7.6 Identiteitsfraude zonder financiële schade – belangrijkste reden geen aangifte, 2018

	Poging tot verkrijgen van lening, abonnement, goederen of diensten op naam van het slachtoffer	Overige identiteitsfraude (aanvraag zorgvergoeding, plegen misdrijven op naam)
	% slachtoffers	
Wel ergens gemeld, maar geen aangifte	26,8	15,5
Helpt niet, totaal	4,0	2,8
Ontmoedigende houding van de politie	1,0	1,1
Op advies van de politie	1,3	1,6
Dader wordt toch niet gepakt	1,6	0,0
Niet belangrijk genoeg, totaal	3,4	1,1
Ging om een klein bedrag, was geen belangrijk incident	0,0	1,1
Te veel moeite	1,5	0,0
Niet in me opgekomen[1)]	0,8	0,0
Er was geen financiële schade[1)]	1,2	0,0
Overige redenen of onbekend	19,4	11,6
Bank, of creditcardmaatschappij zou het verder afhandelen[1)]	2,8	0,7
Was mijn eigen fout	0,7	0,0
Was niet mogelijk voor dit incident	4,5	3,5
Andere reden	6,8	6,1
Onbekend	4,5	1,4

1) Werden genoemd bij de open antwoordcategorie.

8. Phishing

De digitale wereld biedt een ruime mogelijkheid om snel en gemakkelijk veel geld te verdienen. Fraudeurs kunnen voor hun kwalijke praktijken honderdduizenden mensen tegelijk benaderen en daarmee in een grote vijver vissen waar altijd wel een paar vissen aanbijten. Het enige dat oplichters moeten doen is af en toe iets nieuws verzinnen.

Vroeger handelden de fraudeurs voornamelijk uit naam van een bekende of vertrouwde instantie en visten ze via e-mail. De e-mail is nog steeds verreweg het populairst, maar ze gebruiken ook steeds vaker sociale media, zoals Facebook en WhatsApp, en de telefoon. Ook vinden fraudeurs het niet altijd meer noodzakelijk om te handelen vanuit een vertrouwde instantie. Phishing wordt steeds geraffineerder, de fraudeurs steeds professioneler.

Een vorm van phishing is spear-phishing. Hierbij doet de fraudeur eerst wat moeite om (online) het potentiële slachtoffer te leren kennen. Daarmee kan hij of zij weliswaar minder mensen benaderen, maar de benadering is persoonlijker en de slaagkans daardoor groter.

In de enquête is naar een aantal specifieke vormen van phishing gevraagd, te weten het ontvangen van nepboetes/-facturen/-acties, Microsoftbellers, Wangiritelefoontjes, en voorschotfraude. Daarmee wordt in dit onderzoek phishing breder gezien dan gebruikelijk is bij de politie. Het aantal mensen dat hiermee geconfronteerd werd en er slachtoffer van werd is per vorm al besproken in hoofdstuk 4. Hieronder wordt nog kort ingegaan op (slachtofferschap van) phishing in totaliteit.

Phishing totaal

In de enquête heeft in totaal 35 procent van de respondenten opgegeven dat ze in 2018 in aanraking kwamen met phishing, voornamelijk via nepmails. Hierbij zijn ook de vormen van phishing meegeteld waar in de vragenlijst niet specifiek naar gevraagd is maar die door de respondenten genoemd zijn bij de open antwoordmogelijkheden van de vragenlijst, zoals mails van nepbanken. Naar alle waarschijnlijkheid zal het percentage personen dat geconfronteerd wordt met phishing in de praktijk hoger liggen. Er wordt namelijk verwacht dat veel respondenten hun ervaring met phishing niet in het onderzoek hebben aangegeven omdat met name nepmails vaak weinig indruk meer maken.

Phishing met nanciële schade

Naar schatting heeft 1 à 1,5 procent van de internetgebruikers daadwerkelijk geld verloren door phishing. Wangirifraude zorgde voor de meeste slachtoffers en had waarschijnlijk de hoogste slaagkans. Ook nepmails (nepboetes, acties, facturen, bankmails, enzovoort) zorgden voor veel slachtoffers, maar die worden dan ook massaal ontvangen. De impact die dit had op deze slachtoffers is besproken in hoofdstuk 4.

Phishing zonder nanciële schade

Maar ook bij degenen die er niet intrappen en geen geld verliezen wekt het slechts ontvangen van phishing al irritaties op. De Microsoftbellers en Wangiritelefoontjes riepen emoties op bij 17 respectievelijk 19 procent van de ontvangers. Bij de voorschotmails was dit iets minder. Ongeveer een kwart van de ontvangers van deze vormen van phishing hebben hierdoor minder vertrouwen in de digitale veiligheid.

Afperspogingen hebben nog meer impact. Een derde deel van degenen die ermee geconfronteerd werden rapporteerde emotionele gevolgen, voornamelijk boosheid (27 procent). Ook werden slaapproblemen (10 procent) of het niet los kunnen laten (10 procent) relatief veel gemeld[1].

8.1 Enkele vormen van phishing – gevolgen voor de ontvanger, 2018

	Voorschotfraude	Microsoftscam	Wangirifraude	Poging tot afpersing[1]
	% van de ontvangers die er niet zijn ingetrapt			
Emotionele gevolgen	11,6	16,6	18,6	33,2
Blijft eraan denken	2,7	2,8	3,9	9,8
Erg boos	9,6	14,9	16,3	26,5
Sliep slechter	1,6	0,8	1,2	9,7
Minder vertrouwen in de digitale veiligheid	26,8	21,7	24,6	32,4
Minder vertrouwen in de eigen digitale vaardigheid	9,3	6,1	8,4	10,2

1) Poging afpersing betreft voor een onbekend deel geen phishing.
2) Meerdere antwoorden mogelijken.

Phishing wordt relatief weinig gemeld door degenen die er niet zijn ingetrapt. Poging tot afpersing wordt het meest gemeld (12 procent), vooral bij de politie (9 procent) en daarnaast ook bij de Fraudehelpdesk (3 procent). Voorschotmails en Microsoft- en Wangiritelefoontjes worden door minder dan 10 procent van de ontvangers bij een officiële instantie gemeld, meestal bij de politie en/of de Fraudehelpdesk (beide rond de 2,5 procent). Wangiritelefoontjes worden daarnaast ook weleens bij de telefoon- of internetprovider gemeld.

8.2 Enkele vormen van phishing – melding, 2018

	Voorschotfraude	Microsoftscam	Wangirifraude	Poging tot afpersing[1]
	% van de ontvangers die er niet zijn ingetrapt			
Gemeld bij minstens één van de volgende instanties	8,4	7,1	8,4	11,8
Politie	2,6	2,4	2,7	9,3
Bank, financiële instelling of creditcardmaatschappij	3,5	1,9	1,9	.
Fraudehelpdesk[2]	2,7	2,4	1,5	3,0
Echte bedrijf[2]	.	0,4	.	0,2
Telefoon/internetprovider[2]	.	0,5	2,5	.
Centraal Meldpunt Identiteitsfraude en -fouten	0,4	0,5	0,9	.
Sociale media[2]	.	.	.	0,2
Eigen werkgever[2]	.	.	.	0,8

1) Poging tot afpersing betreft voor een onbekend deel geen phishing.
2) Opgegeven in de open antwoordcategorie.

1) De meeste afperspogingen in 2018 betroffen de pornomail, maar er zit ook een (onbekend) aantal afpersingen tussen die niet tot phishing gerekend kunnen worden. Deze cijfers moeten daarom voorzichtig geïnterpreteerd worden.

9.

Cybersecurity

In de voorgaande hoofdstukken werd ingegaan op de verschillende vormen van slachtofferschap van digitale criminaliteit onder internetgebruikers. In dit hoofdstuk staat vooral de veiligheid op het internet, de cybersecurity, die gebruikers van het internet betrachten, centraal.
Tijdens de Landelijke Veiligheidsdag dit jaar trapte minister Grapperhaus van het ministerie van Justitie en Veiligheid de publiekscampagne 'Eerst checken, dan klikken' af. De campagne roept mensen op zich beter te beschermen tegen internetcriminaliteit. Ook tekenden minister Grapperhaus, staatssecretaris Keijzer van het ministerie van Economische Zaken en Klimaat, en een groot aantal bedrijven en brancheorganisaties het convenant 'Preventie cybercriminaliteit'. Daarin spreken zij met elkaar af zich in te zetten om mensen te stimuleren preventieve maatregelen tegen internetcriminaliteit te nemen. Hierbij kan gedacht worden aan onder andere het gebruik van een virusscanner en verschillende sterke wachtwoorden, software-updates direct uitvoeren en het regelmatig maken van back-ups.

In dit hoofdstuk worden een aantal aspecten van internetveiligheid besproken. Paragraaf 9.1 gaat over de kennis van burgers over internetveiligheid. In paragraaf 9.2 komt de bereidheid om persoonlijke informatie over het internet door te geven aan de orde. In paragraaf 9.3 gaat het om de bezorgdheid over internetveiligheid. Paragraaf 9.4 tenslotte bespreekt de bescherming van internetapparatuur door internetgebruikers en het gebruik van wachtwoorden.

Bij het weergeven van onderzoeksuitkomsten in dit hoofdstuk zijn soms antwoordcategorieën uit de vragenlijst samengevoegd en worden niet altijd alle gevraagde antwoorditems getoond. Deze zijn wel beschikbaar in de tabellenbijlage elders in dit rapport.

9.1 Kennis internetveiligheid

In 2018 gaven ongeveer 9 op de 10 internetgebruikers aan dat ze van back-ups maken, een antivirusprogramma, spam en hacken hadden gehoord en dat ze wisten wat ermee wordt bedoeld. Ruim 7 op de 10 internetgebruikers hadden van een firewall en phishing gehoord en wisten wat ermee wordt bedoeld. De relatief nieuwere begrippen met betrekking tot internetveiligheid zijn minder bekend bij de internetgebruikers. Slechts een kwart gaf aan dat ze van cryptoware had gehoord en wist wat er mee werd bedoeld. Voor pharming was dit met minder dan 2 op de 10 (16 procent) mensen nog lager.

9.1.1 Kennis internetveiligheid, 2018[1)]

	Heeft ervan gehoord en weet (ongeveer) wat ermee wordt bedoeld
	% internetgebruikers
Begrippen	
Back-ups maken	89,5
Een antivirusprogramma	92,9
Een firewall	73,8
Spam	90,1
Een DDos aanval	55,6
Hacken	89,2
Phishing	71,7
Pharming	15,6
Ransomware	38,1
Spyware	53,2
Cryptoware	26,8
Malware	42,1
Belfraude of wangiri	34,1
Microsoft helpdeskfraude	45,3

[1)] Personen van 12 jaar of ouder met internetgebruik.

9.2 Bereidheid doorgeven persoonlijke informatie via internet

Internetgebruikers blijken in het algemeen terughoudend om gevoelige persoonlijke gegevens zoals Burgerservicenummer, betalingsgegevens en informatie over gezondheid en werk online te delen. Ruim de helft van de internetgebruikers gaf aan dat ze hun Burgerservicenummer (54 procent) en informatie over hun gezondheid (51 procent) niet online deelden. Iets minder dan de helft (47 procent) deelden geen betalingsgegevens zoals banknummer of creditcardnummer via het internet en 43 procent deelde geen informatie over hun werk online.

Ook met het online delen van foto's is men relatief terughoudend, vooral met het delen van foto's van iemand anders zonder toestemming. Bijna 1 op de 3 internetgebruikers deelde geen foto's van zichzelf via internet. Maar liefst ruim drie kwart gaf aan geen foto's van iemand anders te delen als ze geen toestemming hadden van die persoon.

Met persoonsgegevens zoals naam en geboortedatum heeft men minder problemen om dit online te delen. Slechts ongeveer 1 op de 10 zei deze niet via internet te delen.

9.2.1 Geneigdheid doorgeven persoonlijke informatie via internet, 2018[1)]

In hoeverre bent u geneigd de volgende persoonlijke informatie door te geven via internet?	Ik deel dit niet via internet % internetgebruikers
Uw naam	7,4
Uw geboortedatum	10,0
Uw adresgegevens	16,1
Uw Burgerservicenummer	53,7
Contactgegevens zoals telefoonnummer of e-mailadres	10,6
Betalingsgegevens zoals banknummer of creditcardnummer	43,5
Informatie over uw gezondheid	51,0
Informatie over uw werk	47,2
Een foto van uzelf	31,0
Een foto van iemand anders, zonder toestemming van diegene	78,2

1) Personen van 12 jaar of ouder met internetgebruik.

9.3 Bezorgdheid over internet-veiligheid

Met 42 procent zijn internetgebruikers het vaakst zeer bezorgd over het misbruik van hun bank- of persoonsgegevens. Ongeveer 30 procent van de internetgebruikers was zeer bezorgd over het hacken van één van hun apparaten, over ransomware en over phishing/pharming. Tegelijkertijd gaf een even groot aandeel aan hier (bijna) niet bezorgd over te zijn.

Over een computervirus of -infectie en vooral over ongewenste e-mail maakt men zich minder vaak zorgen. Over ongewenste e-mail gaf 19 procent van de internetgebruikers aan zeer bezorgd te zijn en 24 procent was zeer bezorgd over een computervirus of -infectie.

9.3.1 Bezorgdheid over internetveiligheid, 2018[1)]

In hoeverre bent u bezorgd dat de volgende zaken u kunnen overkomen?	Zeer bezorgd % internetgebruikers	(bijna) Niet bezorgd
Computervirus of -infectie	24,4	28,3
Ongewenste e-mail, ook wel spam genoemd	18,6	43,8
Het hacken van een apparaat, bv. computer, tablet, telefoon, social media of e-mailaccount	30,2	27,5
Software die de computer blokkeert of bestanden versleutelt (ransomware)	30,3	31,0
Misleidende e-mails of vervalste websites waarmee geprobeerd wordt persoonlijke informatie te verkrijgen (phishing/pharming)	30,7	31,7
Misbruik van uw bank- of persoonsgegevens	42,2	23,7

1) Personen van 12 jaar of ouder met internetgebruik.

De afgelopen jaren zijn de mogelijkheden om persoonsgegevens online veilig op te slaan steeds groter geworden. Er zijn bijvoorbeeld veel ontwikkelingen op het gebied van antispyware en wordt inloggen met een wachtwoord en verificatie op je smartphone steeds normaler. Toch zorgen deze maatregelen er niet voor dat mensen bepaalde online activiteiten wel eens vermijden vanwege hun bezorgdheid over internetveiligheid. Naar dit vermijdingsgedrag is in het onderzoek gevraagd, waarbij het gaat om internetgebruik voor privédoeleinden, ongedacht waar het internet werd gebruikt of op welk apparaat. Bijna de helft (45 procent) van de internetgebruikers gaf aan wel eens afgezien te hebben van het bestellen van goederen of diensten en 42 procent van het downloaden van apps, software, muziek, video's, spelletjes of andere databestanden. Van internetbankieren werd het minst vaak afgezien vanwege bezorgdheid over de veiligheid: ruim een kwart heeft dit omwille daarvan wel eens achterwege gelaten.

9.3.2 Vermijden internetactiviteiten wegens bezorgdheid internetveiligheid, 2018[1)]

	% Internetgebruikers
Wel eens afzien van uitvoeren activiteiten[2)]	
Heeft wegens bezorgdheid over veiligheid weleens afgezien van het bestellen van goederen of diensten	45,1
Heeft wegens bezorgdheid over veiligheid weleens afgezien van het plaatsen van persoonlijke informatie op social media	34,9
Heeft wegens bezorgdheid over veiligheid weleens afgezien van het downloaden van apps, software, muziek, videos, spelletjes of andere databestanden	41,8
Heeft wegens bezorgdheid over veiligheid weleens afgezien van het gebruik van draadloos internet ergens anders dan thuis of op het werk	32,0
Heeft wegens bezorgdheid over veiligheid weleens afgezien van internetbankieren	26,4

1) Personen van 12 jaar of ouder met internetgebruik.
2) Meerdere antwoorden mogelijk.

9.4 Bescherming internetapparatuur en persoonlijke gegevens

Het is belangrijk dat internetgebruikers zichzelf online beschermen. Anders kan men bijvoorbeeld slachtoffer worden van identiteitsfraude of van een webwinkel die nep blijkt te zijn. De Rijksoverheid geeft consumenten basistips om zich online te beschermen, bijvoorbeeld: geen wachtwoord gebruiken dat voor de hand ligt, het wachtwoord niet doorgeven aan vreemden, de computer regelmatig updaten en een virusscanner installeren. Daarnaast verwijst de Rijksoverheid naar andere websites voor meer informatie over onder andere online veiligheid, privacy en sociale media.

In 2018 gaven bijna 3 op de 10 internetgebruikers (28 procent) aan dat ze altijd de website waarop ze persoonlijke informatie moeten verstrekken controleren door bijvoorbeeld te letten op de https-beveiliging. Bijna 2 op de 10 (17 procent) zeiden altijd de toegang tot hun persoonlijke gegevens en informatie te beperken op sociale media, zoals Facebook en Twitter. Ruim 1 op de 10 (12 procent) weigert altijd toegang tot de geografische locatie, foto's of contacten op mobiele internetapparatuur en eenzelfde aandeel (11 procent) verwijdert altijd cookies.

9.4.1 Activiteiten ter bescherming persoonlijke gegevens, 2018[1)]

	Altijd	Nooit
	% internetgebruikers	
Bescherming van persoonlijke gegevens		
Lezen of raadplegen van privacyregels vóór het invullen van persoonlijke informatie	8,0	21,0
Het invullen van verzonnen persoonsgegevens	0,9	56,5
Toegang weigeren tot uw geografische locatie, foto's of contacten op uw mobiele internet apparatuur	12,3	14,1
Beperkte toegang geven tot uw persoonlijke gegevens en informatie op sociale netwerksites zoals Facebook en Twitter	17,4	21,3
Toestaan dat persoonlijke informatie wordt gebruikt voor commerciële doeleinden (denk aan cookies)	7,9	19,4
Cookies verwijderen	11,2	18,4
Controleren of de website waarop u persoonlijke informatie moet verstrekken veilig is, bijvoorbeeld door te letten op https-beveiliging	27,8	14,1
Nagaan welke persoonlijke informatie van u beschikbaar is op websites of via zoekmachines als Google met het doel deze aan te vullen of te verwijderen	4,5	31,2

1) Personen van 12 jaar of ouder met internetgebruik.

Er bestaan ook nog andere maatregelen om internetapparatuur en/of persoonlijke informatie op het internet beter te beschermen tegen misbruik door anderen. Bijna de helft (45 procent) gaf aan vaak de computerprogramma's up-to-date te houden of te vernieuwen, 10 procent van de internetgebruikers deed dit nooit. Ongeveer 1 op de 4 internetgebruikers zei vaak gegevens op te slaan in de cloud en 1 op de 5 maakte vaak back-ups op een andere computer of op een externe harde schijf. Van de internetgebruikers gaf 18 procent aan de firewall en de spamfilter vaak te onderhouden.

9.4.2 Maatregelen ter bescherming van internetapparatuur en/of persoonlijke informatie op internet, 2018[1)]

	Vaak	Nooit
	% internetgebruikers	
Mate bescherming apparatuur en persoonlijke informatie		
Maken van back-ups op een andere computer of op een externe harde schijf	21,4	22,1
Opslaan van gegevens in de cloud	24,3	32,4
Up-to-date houden of vernieuwen van computerprogramma's (bv. besturingssysteem, virusscanner of internetbrowser)	45,2	10,2
Tussentijds zelf controleren op virussen zonder dat de scanner hierom vraagt	16,6	28,6
Onderhouden van een firewall	18,1	33,5
Onderhouden van een spamfilter	17,9	32,9

1) Personen van 12 jaar of ouder met internetgebruik.

Om in te kunnen loggen op online diensten of websites is ter verificatie bijna altijd een wachtwoord vereist. Een goed gekozen wachtwoord verkleint de kans om ten prooi te vallen aan internetcriminelen aanzienlijk, maar in de praktijk blijkt dat toch nog vaak lastig te zijn. Door het toenemende internetgebruik in de afgelopen jaren is het aantal online accounts toegenomen, wat het moeilijk maakt om voor iedere online dienst of website een sterk wachtwoord te bedenken en dat ook nog eens te onthouden. Een oplossing hiervoor is het gebruik van een wachtwoordmanager, waarbij maar één wachtwoord onthouden hoeft te worden om toegang te krijgen tot de andere wachtwoorden die worden bewaard in een digitale kluis.

In 2018 gaven bijna 2 op de 3 (64 procent) internetgebruikers aan dat ze vaak de toegang tot hun digitale apparaten beschermen met een toegangscode, wachtwoord of

vingerafdruk; 10 procent deed dat nooit. Van de internetgebruikers zei 60 procent vaak gebruik te maken van sterke wachtwoorden die voldoende en verschillende letters en tekens bevatten, terwijl 5 procent dit nooit deed. Bijna 41 procent gebruikte vaak verschillende wachtwoorden voor hun digitale accounts. Van de internetgebruikers veranderde 15 procent regelmatig hun wachtwoorden. Een wachtwoordmanager werd in 2018 door slechts 9 procent van de internetters vaak gebruikt. Ook het zelf instellen of wijzigen van het wachtwoord van het Wi-Fi netwerk thuis gebeurde door minder dan 1 op de 10 internetgebruikers regelmatig.

9.4.3 Beheer van wachtwoorden, 2018[1)]

	Vaak	Nooit
	% internetgebruikers	
Mate van beheer wachtwoorden		
Toegang tot apparaten beschermen met een toegangscode, wachtwoord, vingerafdruk	63,6	10,2
Zelf regelmatig wachtwoorden veranderen	14,6	17,8
Sterke wachtwoorden gebruiken (voldoende en verschillende letters/tekens)	59,9	5,3
Gebruik maken van een wachtwoordmanager	8,6	66,9
Verschillende wachtwoorden gebruiken	40,6	8,7
Instellen of wijzigen van het wachtwoord van uw Wi-Fi netwerk	8,6	47,2

1) Personen van 12 jaar of ouder met internetgebruik.

Twee derde van de internetgebruikers (67 procent) zei (bijna) altijd zelf de eigen internet-apparatuur en persoonlijke gegevens te beschermen. Ruim een kwart (27 procent) gaf aan dat iemand anders dat (bijna) altijd voor hen doet.

Tabellenbijlage

Deze bijlage bevat uitgebreide tabellen waarin alle cijfers uit de hoofdstukken 2 tot en met 9 zijn opgenomen.

Het onderzoek 'Digitale veiligheid en criminaliteit' is uitgevoerd bij een steekproef. Dit betekent dat de weergegeven percentages schattingen betreffen. Om een indicatie te geven van de precisie van deze schattingen worden in deze tabellen ook de 95%-betrouwbaarheidsintervallen weergegeven. Deze intervallen bevatten met 95% zekerheid de werkelijke (onbekende) waarde. De betrouwbaarheidsintervallen zijn berekend met Complex Samples (SPSS).

Indien een schatting 0 procent is, heeft geen enkele respondent in het onderzoek dit antwoord gegeven. Dit betekent niet dat dit helemaal niet voorkomt in de populatie.

In de tabellen over slachtofferschap is detailinformatie opgenomen over de verschillende delicten. In de hoofdstukken is alleen detailinformatie gegeven over de delicten waarbij minstens 100 slachtoffers ondervraagd zijn. Voor de bijlagetabellen hebben we een lagere grens van 50 waarnemingen aangehouden om toch een zo volledig mogelijk beeld te geven van de delicten. Dit betekent wel dat de betrouwbaarheidsmarges rondom de schatting groter zijn.

Overzicht van de tabellen

1. Slachtofferschap van digitale criminaliteit
2. Gebruik en activiteiten op het internet
3. Slachtofferschap van hacken en nadere delictinformatie
4. Slachtofferschap van fraude via het betalingsverkeer en nadere delictinformatie
5. Slachtofferschap van fraude bij online handel en nadere delictinformatie
6. Slachtofferschap van overige vermogensdelicten en nadere delictinformatie

7a. Slachtofferschap van niet-seksuele interpersoonlijke incidenten en nadere delictinformatie

7b. Slachtofferschap van seksuele interpersoonlijke incidenten en nadere delictinformatie

8. Interpersoonlijke incidenten en seksueel getinte spam, naar geslacht en leeftijd
9. Slachtofferschap van identiteitsfraude zonder financiële schade en nadere delictinformatie
10. Enkele gerapporteerde vormen van phishing, gevolgen voor de ontvangers en melding
11. Het verstrekken van persoonlijke informatie via internet
12. Activiteiten ter bescherming van persoonlijke gegevens op het internet
13. Algemene kennis over digitale veiligheid
14. Bezorgdheid over de digitale veiligheid
15. Bescherming van internetapparatuur en persoonlijke informatie op het internet
16. Andere vormen van internetveiligheid

1. Slachtofferschap van digitale criminaliteit, 2018[1)]

	Schatting	Ondergrens	Bovengrens
	% internetgebruikers		
Slachtofferschap totaal	8,5	8,2	8,8
Hacken	1,8	1,6	1,9
Hacken totaal inclusief modus operandi[2)]	2,1	2,0	2,3
Hacken als modus operandi	0,4	0,4	0,5
Voorafgaande aan een vermogensdelict	0,2	0,1	0,2
Voorafgaande aan een persoonlijk delict	0,1	0,1	0,1
Voorafgaande aan een overig delict	0,2	0,2	0,3
Vermogensdelicten	4,6	4,3	4,8
Fraude via het betalingsverkeer	0,7	0,6	0,8
Geld van rekening gehaald en/of betalingen gedaan	0,5	0,4	0,6
Lening, abonnement, goederen of diensten verkregen op naam van het slachtoffer	0,2	0,2	0,3
Fraude bij online aankoop	2,9	2,7	3,1
Aankoopfraude	2,7	2,5	2,9
Verkoopfraude	0,2	0,2	0,3
Vermogensdelicten, anders dan via betalingsverkeer of online handel	1,2	1,1	1,3
Nepboete/nepfactuur of nepactie	0,3	0,3	0,4
Voorschotfraude	0,1	0,1	0,1
Frauduleuze factuurwijziging	0,0	0,0	0,1
Microsoftscam	0,2	0,1	0,2
Wangirifraude	0,5	0,4	0,6
Afpersing, bedreiging zonder geweld	0,0	0,0	0,1
Ransomware of cryptoware	0,0	0,0	0,1
Whaling'[3)]	0,0	0,0	0,0
Overige identiteitsfraude	0,1	0,1	0,1
Interpersoonlijke incidenten, niet seksueel	1,4	1,3	1,5
Stalking	0,5	0,4	0,5
Bedreiging met geweld	0,3	0,3	0,4
Laster	1,0	0,9	1,1
Verhalen of roddels verspreid	0,7	0,6	0,8
Foto's of filmpjes verspreid	0,2	0,1	0,2
Overig (bv. gepest, genante website gemaakt of berichten gepost onder naam slachtoffer)	0,2	0,2	0,3
Interpersoonlijke incidenten, seksueel	0,7	0,6	0,8
Stalking	0,4	0,3	0,4
Bedreiging met geweld	0,1	0,0	0,1
Laster	0,3	0,3	0,4
Verhalen of roddels verspreid	0,2	0,2	0,3
Foto's of filmpjes verspreid	0,1	0,1	0,2
Overig (bv. gepest, gênante website gemaakt of berichten gepost onder naam slachtoffer)	0,1	0,1	0,1
Identiteitsfraude zonder financiële schade	1,0	0,9	1,1
Poging geld van rekening te halen en/of betalingen te doen	0,2	0,2	0,3
Poging tot verkrijgen van lening, abonnement, goederen of diensten op naam van het slachtoffer	0,5	0,4	0,6
Overige identiteitsfraude	0,3	0,3	0,4

1) Personen van 12 jaar of ouder met internetgebruik.
2) Zie het tekstkader in hoofdstuk 3.
3) Naar dit delict is niet expliciet gevraagd.
Bron: CBS; pilot onderzoek naar Digitale Veiligheid & Criminaliteit, 2018.

2. Gebruik en activiteiten op het internet, 2018[1]

	Schatting	Ondergrens	Bovengrens
	% internetgebruikers		
Internetgebruik[2]			
Gebruikt dagelijks internet	92,6	92,3	92,9
Gebruikt internet op openbare plekken	84,5	84,1	84,9
Gebruikt internet op openbare plekken via Wi-Fi met wachtwoord	48,2	47,6	48,7
Gebruikt internet op openbare plekken via Wi-Fi zonder wachtwoord	34,9	34,4	35,4
Gebruikt internet op openbare plekken via eigen 3g/4g abonnement	64,1	63,5	64,6
Gebruikt dagelijks Wi-Fi op openbare plekken	14,9	14,5	15,3
Gebruikt nooit Wi-Fi op openbare plekken	41,4	40,9	42,0
Internetactiviteiten[2]			
Berichten sturen	94,7	94,4	94,9
Zoeken van informatie	98,2	98,0	98,3
Internetbankieren	89,5	89,2	89,8
Sociale media	68,5	68,0	69,0
Professionele netwerksites	41,5	40,9	42,0
Foto's, documenten of bestanden op het internet opslaan (cloud)	61,5	61,0	62,0
Downloaden van muziek of films	39,6	39,0	40,1
Streamen van muziek of films	60,0	59,5	60,5
Downloaden van apps, games, afbeeldingen of software	76,8	76,3	77,2
Gamen	54,6	54,0	55,1
Gokken	3,8	3,6	4,0
Datingsites bezoeken	5,8	5,6	6,1
Erotische sites bezoeken	18,7	18,3	19,1
Kopen van goederen of diensten	81,9	81,4	82,3
Verkopen van goederen of diensten	47,3	46,7	47,8
Aanwezigheid Wi-Fi en aangesloten apparatuur[2]			
Heeft thuis een Wi-Fi netwerk	98,0	97,8	98,1
Heeft thuis een computer verbonden met Wi-Fi	40,5	40,0	41,0
Heeft thuis een laptop verbonden met Wi-Fi	79,2	78,7	79,6
Heeft thuis een tablet verbonden met Wi-Fi	64,6	64,1	65,1
Heeft thuis een smartphone verbonden met Wi-Fi	90,9	90,5	91,2
Heeft thuis een smart-tv verbonden met Wi-Fi	47,1	46,5	47,6
Heeft thuis een camerasysteem verbonden met Wi-Fi	6,3	6,1	6,6
Heeft thuis een alarmsysteem verbonden met Wi-Fi	4,1	3,9	4,3
Heeft thuis een verwarmingssysteem verbonden met Wi-Fi	12,1	11,7	12,4
Heeft thuis medische apparaten verbonden met Wi-Fi	1,1	1,0	1,2
Heeft thuis een spelcomputer of ander speelgoed verbonden met Wi-Fi	25,8	25,3	26,3
Heeft thuis apparatuur voor woongemak (rolluiken, verlichting, muziek etc.) verbonden met Wi-Fi	18,6	18,2	19,0
Heeft thuis een streaming device, raspberry-pi of fototoestel verbonden met Wi-Fi[3]	0,8	0,7	0,9
Heeft thuis zonnepanelen verbonden met Wi-Fi[3]	0,7	0,6	0,8
Heeft thuis een smartwatch of fitnesstracker verbonden met Wi-Fi[3]	0,2	0,1	0,2

[1] Personen van 12 jaar of ouder met internetgebruik.
[2] Meerdere antwoorden mogelijk.
[3] Genoemd bij de open antwoordcategorie.
Bron: CBS; pilot onderzoek naar Digitale Veiligheid & Criminaliteit, 2018.

3. Slachto erschap van hacken en nadere delictinformatie, 2018[1)]

	Schatting	Ondergrens	Bovengrens
	% internetgebruikers		
Slachtoffer van hacken geweest	1,8	1,6	1,9
	% slachtoffers		
Soort hack[2)]			
Computer (desktop, laptop of tablet)	11,5	9,1	14,5
E-mailaccount	27,9	24,2	31,8
Mobiele telefoon	6,1	4,2	8,6
Sociale media	56,4	52,2	60,5
Andere huishoudelijke apparatuur	0,1	0,0	0,7
Ander apparaat	12,1	9,7	15,0
Gevolgen[2)]			
Virus met verlies van gegevens	6,6	4,7	9,2
Misbruik van persoonlijke gegevens op het internet	9,3	7,1	12,2
Ransomware	5,7	4,0	8,0
Gegevens gestolen via trojan horse	2,9	1,9	4,5
Cryptoware	2,2	1,3	3,9
Malware	4,8	3,3	6,9
Misbruik van computer (bv. in botnet of Ddos-aanval)	0,7	0,2	1,9
Misbruik van emailaccount of profielsite	26,9	23,4	30,8
Pharming (omleiden van internetverkeer)	0,3	0,1	1,5
Andere gevolgen	11,1	8,8	14,0
Geen gevolgen	39,3	35,3	43,5
Account geblokkeerd[3)]	5,2	3,7	7,3
Ongewenste items verstuurd[3)]	4,2	2,8	6,3
Wijze van inbraak[2)]			
Zelf (bewust of per ongeluk) installeren van een programma	7,1	5,3	9,5
Installeren van een programma door iemand anders	4,8	3,4	6,9
Iemand aan wachtwoorden gekomen	44,7	40,6	48,9
Fysieke toegang tot computer verkregen	2,7	1,7	4,4
Onbekend hoe toegang is verkregen	33,7	29,9	37,7
Op een link, bericht, bijlage of filmpje geklikt[3)]	3,9	2,6	5,8
Andere wijze	9,0	6,9	11,5
Gevolgen voor het slachtoffer[2)]			
Emotionele gevolgen	24,3	20,9	28,0
Blijft eraan denken	6,3	4,6	8,6
Erg boos	20,7	17,5	24,2
Sliep slechter	3,9	2,6	5,8
Minder vertrouwen in digitale veiligheid	38,7	34,7	42,9
Minder vertrouwen in eigen digitale vaardigheid	14,7	12,0	17,9
Bang dat het vaker zal gebeuren	28,9	25,3	32,8
Melding[2)] en aangifte			
Gemeld bij minstens één van de volgende instanties	5,1	3,6	7,3
Politie	4,8	3,3	7,0
Centraal Meldpunt Nederland (meld.nl)	0,3	0,1	0,9
Meld Misdaad Anoniem	0,2	0,0	1,2
Aangifte bij de politie	2,8	1,7	4,7
Belangrijkste reden delict niet gemeld			
Helpt niet, totaal	15,6	12,8	18,8
Krijg geld toch niet terug	1,1	0,5	2,7
Ontmoedigende houding van de politie	1,6	0,8	3,1
Dader wordt toch niet gepakt	12,4	10,0	15,3
Er wordt toch niets mee gedaan[3)]	0,5	0,2	1,3

3. Slachtoerschap van hacken en nadere delictinformatie, 2018[1] (slot)

	Schatting	Ondergrens	Bovengrens
	% slachtoffers		
Niet belangrijk genoeg, totaal	13,5	10,9	16,7
Ging om een klein bedrag	1,5	0,7	3,1
Te veel moeite	8,8	6,7	11,6
Niet in me opgekomen[3]	0,8	0,3	1,8
Er was geen schade[3]	2,4	1,5	4,0
Overige redenen of onbekend, totaal	65,8	61,8	69,7
Dader is bekende	2,0	1,1	3,7
Was mijn eigen fout	8,2	6,2	10,7
Wegens schaamte	1,2	0,5	2,8
Was niet mogelijk voor dit incident	13,0	10,4	16,2
Andere reden	18,7	15,7	22,2
Onbekend	22,7	19,3	26,4
Belangrijkste reden delict niet aangegeven			
Helpt niet, totaal	0,5	0,2	1,2
Advies van de politie	0,4	0,1	1,1
Afwijzende houding van de politie	0,1	0,0	0,6
Niet belangrijk genoeg, totaal	0,4	0,1	1,3
Te veel moeite	0,4	0,1	1,3
Overige redenen of onbekend, totaal	1,5	0,7	2,9
Was mijn eigen fout	0,2	0,0	1,1
Dader is bekende	0,3	0,0	1,8
Was niet mogelijk voor dit incident	0,7	0,2	1,9
Andere reden	0,1	0,0	0,9
Onbekend	0,2	0,0	1,1

1) Personen van 12 jaar of ouder met internetgebruik.
2) Meerdere antwoorden mogelijk.
3) Genoemd bij de open antwoordcategorie.
Bron: CBS; pilot onderzoek naar Digitale Veiligheid & Criminaliteit, 2018.

4. Slachtoerschap van fraude via het betalingsverkeer en nadere delictinformatie, 2018[1)]

	Geld van rekening gehaald en/of betalingen gedaan			Lening, abonnement, goederen of diensten verkregen op naam		
	Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens
	% internetgebruikers					
Slachtoffer geweest	0,5	0,4	0,6	0,2	0,2	0,3
	% slachtoffers					
Manier waarop men aan de gegevens is gekomen						
Zelf bankpas in goed vertrouwen ter beschikking gesteld	5,1	2,3	10,9	1,1	0,1	7,2
Zelf persoonlijke gegevens in goed vertrouwen aan een bekende ter beschikking gesteld	1,4	0,4	4,5	4,6	1,4	14,4
Zelf gegevens doorgegeven aan een webshop of via de telefoon	13,2	8,9	19,1	13,0	6,8	23,7
Niet online, maar door kopiëren creditcard of bijv. dumpster diving[2)]	0,7	0,1	4,9	3,4	0,8	12,8
Diefstal van paspoort of ID-kaart waarbij identiteit overgenomen werd	1,7	0,5	5,2	2,6	0,6	10,1
Diefstal van bankpas/creditcard	6,8	3,7	12,2	2,8	0,4	17,0
Skimmen van bankpas/creditcard	11,2	7,1	17,3	2,5	0,6	9,5
Scannen van mobiele telefoon, bijv door contactloos betalen (skimming)	0,0	0,0	0,0	0,0	0,0	0,0
Phishing of pharming	11,3	7,2	17,3	5,7	1,9	15,4
Hacken van computer/tablet/telefoon	3,5	1,6	7,5	9,0	3,7	20,5
Malware (bv. een computervirus of trojan horse)	2,4	0,7	7,4	1,4	0,2	9,0
Keylogging	0,0	0,0	0,0	0,0	0,0	0,0
Hacken van bedrijf of bank waar persoonlijke gegevens bekend zijn	6,3	3,6	10,8	6,9	3,0	15,0
Andere wijze	4,3	2,3	7,8	9,0	3,8	20,0
Onbekend	32,2	25,4	39,9	38,0	26,6	50,9
Totaal door phishing[3)]	30,2	23,6	37,7	19,8	11,7	31,4
Totaal door hacken[3)]	12,2	8,0	18,1	17,3	9,7	28,9
Gevolgen voor het slachtoffer[4)]						
Financiële schade helemaal vergoed	78,0	70,9	83,8	55,1	42,2	67,3
Financiële schade deels vergoed	6,3	3,3	11,4	9,0	3,7	20,0
Financiële schade niets vergoed	15,7	10,9	22,1	35,9	24,5	49,2
Emotionele gevolgen	33,7	26,9	41,3	39,8	28,2	52,6
Blijft eraan denken	12,5	8,4	18,1	13,6	6,9	25,0
Erg boos	25,7	19,6	33,0	38,0	26,6	50,9
Sliep slechter	7,4	4,4	12,2	11,3	5,2	22,7
Minder vertrouwen in digitale veiligheid	52,3	44,5	59,9	45,3	33,2	58,0
Minder vertrouwen in eigen digitale vaardigheid	10,0	6,3	15,4	8,6	3,9	17,7
Bang dat het vaker zal gebeuren	29,2	22,8	36,6	37,9	26,5	50,7
Melding[4)] en aangifte						
Gemeld bij minstens één van de volgende instanties	86,4	79,5	91,2	66,3	53,3	77,3
Politie	18,9	13,8	25,5	16,9	9,4	28,5
Bank of financiële instelling	77,4	69,9	83,4	52,6	40,0	64,9
Fraudehelpdesk	10,7	7,0	16,2	9,1	4,6	17,2
Centraal Meldpunt Identiteitsfraude en -fouten	2,0	0,7	5,5	4,0	1,0	14,5
Autoriteit Consument en Markt	0,0	0,0	0,0	1,3	0,2	8,5
Bedrijf of webshop waar betaling, aanvraag of bestelling is gedaan[2)]	3,0	1,1	7,9	6,9	3,1	15,0
Aangifte bij de politie	18,3	13,3	24,8	13,4	6,9	24,5
Weet niet of er aangifte is gedaan	13,8	9,4	19,8	11,4	5,8	21,2
Belangrijkste reden delict niet gemeld						
Helpt niet, totaal	2,2	0,9	5,6	4,6	1,4	14,1
Krijg geld toch niet terug	1,3	0,4	4,4	3,8	1,0	14,0
Ontmoedigende houding van de politie	0,6	0,1	4,3	0,8	0,1	5,7
Dader wordt toch niet gepakt	0,3	0,0	1,9	0,0	0,0	0,0
Niet belangrijk genoeg, totaal	4,7	2,2	9,9	8,7	3,5	20,1
Ging om een klein bedrag	3,9	1,6	9,1	6,8	2,4	17,8

4. Slachtoerschap van fraude via het betalingsverkeer en nadere delictinformatie, 2018[1] (slot)

	Geld van rekening gehaald en/of betalingen gedaan			Lening, abonnement, goederen of diensten verkregen op naam		
	Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens
	% internetgebruikers					
Te veel moeite	0,4	0,1	2,9	2,0	0,3	12,7
Niet in me opgekomen[2]	0,4	0,1	3,0	0,0	0,0	0,0
Overige redenen of onbekend, totaal	6,7	3,4	12,8	20,3	11,9	32,5
Dader is bekende	0,0	0,0	0,0	3,9	1,0	14,3
Was mijn eigen fout	0,5	0,1	3,2	1,2	0,2	8,2
Wegens schaamte	0,0	0,0	0,0	0,0	0,0	0,0
Was niet mogelijk voor dit incident	0,0	0,0	0,0	1,5	0,2	9,8
Andere reden	2,9	1,1	7,7	10,1	4,6	20,8
Onbekend	3,3	1,2	9,2	3,6	0,9	13,3
Belangrijkste reden delict niet aangegeven						
Helpt niet, totaal	8,0	4,8	12,9	8,7	3,3	21,3
Krijg geld toch niet terug	0,0	0,0	0,0	4,7	1,1	17,8
Ontmoedigende houding van de politie	0,6	0,1	2,4	1,9	0,3	12,4
Er wordt toch niets mee gedaan[2]	0,5	0,1	3,4	0,0	0,0	0,0
Dader wordt toch niet gepakt	6,9	4,0	11,7	2,1	0,3	13,2
Niet belangrijk genoeg, totaal	15,4	10,3	22,4	7,5	3,0	17,3
Ging om een klein bedrag	6,7	3,7	11,8	6,1	2,2	15,9
Te veel moeite	6,7	3,3	13,1	0,0	0,0	0,0
Niet in me opgekomen[2]	2,0	0,8	4,9	1,3	0,2	8,8
Overige redenen of onbekend, totaal	30,8	24,2	38,4	25,2	16,1	37,2
Bank of creditcardmaatschappij zou het verder afhandelen[2]	12,0	7,9	17,9	18,1	10,5	29,5
Dader is bekende	0,4	0,1	2,9	0,0	0,0	0,0
Was mijn eigen fout	1,8	0,6	5,0	3,3	0,8	12,7
Wegens schaamte	0,7	0,1	4,6	0,0	0,0	0,0
Was niet mogelijk voor dit incident	2,5	1,0	6,2	0,0	0,0	0,0
Andere reden	6,4	3,3	11,8	3,8	1,3	10,3
Onbekend	7,0	4,0	12,1	0,0	0,0	0,0

1) Personen van 12 jaar of ouder met internetgebruik.
2) Genoemd bij de open antwoordcategorie.
3) Aan meerdere vormen van gegevensdiefstal ging een vorm van phishing vooraf. Zie de methodologische toelichting in de onderzoeksverantwoording voor de berekening van 'totaal door phishing' en 'totaal door hacken'.
4) Meerdere antwoorden mogelijk.

Bron: CBS; pilot onderzoek naar Digitale Veiligheid & Criminaliteit, 2018.

5. Slachtoerschap van fraude bij online handel en nadere delictinformatie, 2018[1)]

	Aankoopfraude			Verkoopfraude		
	Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens
	% internetgebruikers					
Slachtofferschap geweest	2,7	2,5	2,9	0,2	0,2	0,3
	% slachtoffers					
Website die is gebruikt						
Tweedehands verkoopsite	41,5	38,1	45,0	71,7	59,0	81,6
Verkoopsite als Amazon, Alibaba	16,3	13,9	19,0	4,8	1,5	14,2
Veilingsite	3,5	2,4	5,1	3,1	0,4	18,7
Social media	6,5	4,9	8,6	2,7	0,7	10,3
Nederlandstalige nepwebshop	10,9	9,0	13,2	.	.	.
Niet-Nederlandstalige nepwebshop	8,0	6,3	10,1	.	.	.
Bestaande webshop[2)]	5,5	4,1	7,2	.	.	.
Eigen webshop of website[2)]				9,4	4,3	19,2
Anders	5,7	4,3	7,5			
Onbekend	2,1	1,3	3,3	8,4	3,4	19,1
Soort aankoop						
Tickets en kaartjes	5,3	3,9	7,2	14,9	8,3	25,4
Bobiele telefoons, audio, tv, computer, etc.	19,7	17,1	22,6	27,9	18,4	40,0
Kleding, sportartikelen, schoenen, accessoires	29,6	26,4	32,9	15,7	8,9	26,4
Duurzame consumptiegoederen	7,5	5,8	9,5	6,3	2,6	14,5
Films, muziek, boeken, spellen of speelgoed	9,7	7,8	12,1	7,8	3,1	18,4
Vakanties, vervoer of reizen	1,4	0,8	2,4	0,0	0,0	0,0
Levensmiddelen en producten voor persoonlijke verzorging	6,2	4,7	8,1	6,7	2,1	19,6
Overig	19,3	16,8	22,1	13,7	8,0	22,4
Onbekend	1,4	0,7	2,6	6,9	2,5	17,4
Gevolgen voor het slachtoffer[3)]						
Kreeg de financiële schade vergoed	10,0	8,1	12,3			
Emotionele gevolgen	42,4	38,9	45,9	55,1	43,0	66,6
Blijft eraan denken	11,7	9,5	14,2	19,5	11,1	31,9
Erg boos	38,6	35,2	42,0	43,2	31,9	55,4
Sliep slechter	3,2	2,1	4,7	5,1	1,5	15,6
Minder vertrouwen in digitale veiligheid	35,3	32,0	38,7	33,9	23,6	46,0
Minder vertrouwen in eigen digitale vaardigheid	8,9	7,0	11,1	6,2	2,3	15,7
Bang dat het vaker zal gebeuren	23,4	20,5	26,5	28,3	18,7	40,5
Melding[3)] en aangifte						
Gemeld bij minstens één van de volgende instanties[3)]	38,9	35,5	42,4	43,9	32,4	56,0
Gemeld bij minstens twee van de volgende instanties[3)]	5,7	4,3	7,6	7,2	3,3	14,9
Politie/LMIO	24,9	22,0	28,1	27,2	17,9	39,1
Fraudehelpdesk	4,6	3,3	6,3	5,8	2,4	13,0
Consumentenprogramma zoals Kassa, Radar of Opgelicht	2,2	1,3	3,6	0,9	0,1	6,4
Consuwijzer (vermoeden van fraude via webwinkels)	1,2	0,7	2,4	3,1	0,4	18,7
Bank, financiële instelling, creditcardmaatschappij of PayPal[2)]	8,5	6,8	10,6	7,1	3,0	15,5
Marktplaats[2)]	4,6	3,4	6,2	6,9	2,9	15,6
Aangifte bij de politie	22,6	19,8	25,6	20,5	12,5	31,9
Weet niet of er aangifte is gedaan	2,6	1,6	4,0	4,5	1,1	17,5
Controle achteraf door slachtoffer[3)]						
Controlefunctie op Politie.nl	12,1	9,9	14,7	.	.	.
Google, fora, Opgelicht, Kassa, Radar	28,6	25,6	31,8	.	.	.
Kamer van Koophandel	2,1	1,3	3,4	.	.	.
Anders	10,8	8,8	13,1	.	.	.
Geen informatie over de dader meer opgezocht	46,2	42,7	49,7			

5. Slachtoerschap van fraude bij online handel en nadere delictinformatie, 2018[1] (slot)

	Aankoopfraude			Verkoopfraude		
	Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens
	% slachtoffers					
Belangrijkste reden delict niet gemeld						
Helpt niet, totaal	22,1	19,3	25,2	20,0	11,9	31,6
Krijg geld toch niet terug	16,9	14,4	19,7	11,1	5,5	21,0
Dader wordt toch niet gepakt	4,2	3,0	6,0	9,0	3,9	19,5
Ontmoedigende houding van de politie	1,0	0,5	2,0	0,0	0,0	0,0
Niet belangrijk genoeg, totaal	29,7	26,7	33,0	14,5	8,1	24,6
Ging om een klein bedrag	23,5	20,7	26,6	12,5	6,6	22,4
Te veel moeite	5,8	4,4	7,7	1,1	0,2	7,4
Niet in me opgekomen[2]	0,4	0,2	1,1	0,9	0,1	6,1
Overige redenen of onbekend, totaal	9,2	7,4	11,4	21,6	13,1	33,4
Was mijn eigen fout	2,1	1,3	3,4	1,5	0,4	6,1
Wegens schaamte	1,2	0,6	2,3	0,0	0,0	0,0
Was niet mogelijk voor dit incident	0,9	0,5	1,9	4,6	1,6	12,3
Andere reden	2,7	1,8	4,1	3,3	0,7	13,4
Onbekend	2,3	1,5	3,6	12,2	5,9	23,3
Belangrijkste reden delict niet aangegeven						
Helpt niet, totaal	5,7	4,3	7,6	4,0	1,5	10,5
Krijg geld toch niet terug	3,1	2,1	4,6	2,1	0,5	8,0
Dader wordt toch niet gepakt	1,9	1,1	3,2	0,0	0,0	0,0
Ontmoedigende houding van de politie	0,6	0,2	1,5	1,9	0,4	7,9
Politie doet er toch niets mee	0,1	0,0	0,9	0,0	0,0	0,0
Niet belangrijk genoeg, totaal	2,2	1,4	3,3	6,9	2,6	17,1
Ging om een klein bedrag, was geen belangrijk incident	1,6	1,0	2,7	3,4	0,8	12,9
Te veel moeite	0,6	0,3	1,3	3,5	0,9	13,1
Niet in me opgekomen[2]	0,0	0,0	0,0	0,0	0,0	0,0
Overige redenen of onbekend, totaal	5,8	4,3	7,8	7,9	3,8	15,6
Bank zou het verder afhandelen	2,7	1,8	4,3	1,8	0,4	7,3
Was mijn eigen fout	0,7	0,3	1,5	0,0	0,0	0,0
Uit schaamte	0,2	0,0	1,2	0,0	0,0	0,0
Was niet mogelijk voor dit incident	0,7	0,3	2,0	2,0	0,4	8,9
Andere reden	0,8	0,4	1,7	3,1	1,0	9,4
Onbekend	0,7	0,3	1,6	1,0	0,1	6,7

[1] Personen van 12 jaar of ouder met internetgebruik.
[2] Genoemd bij de open antwoordcategorie.
[3] Meerdere antwoorden mogelijk.
Bron: CBS; pilot onderzoek naar Digitale Veiligheid & Criminaliteit, 2018.

6. Slachto erschap van overige vermogensdelicten en nadere delictinformatie, 2018[1)]

	Nepboete/nepfactuur of nepactie			Microsoftscam			Wangirifraude		
	Schatting	Onder-grens	Boven-grens	Schatting	Onder-grens	Boven-grens	Schatting	Onder-grens	Boven-grens
	% internetgebruikers								
Slachtoffer geweest	0,3	0,3	0,4	0,2	0,1	0,2	0,5	0,4	0,6
Gevolgen voor het slachtoffer[2)]	% slachtoffers								
Financiële schade									
Helemaal vergoed	12,2	6,4	21,8	7,0	2,5	18,3	4,3	2,1	8,6
Deels vergoed	2,3	0,7	7,1	3,1	0,9	9,5	2,0	0,7	5,5
Niets vergoed	77,9	67,7	85,5	70,7	57,0	81,4	79,8	72,3	85,7
Onbekend	7,6	3,7	15,0	19,2	10,6	32,4	14,0	9,0	21,1
Emotionele gevolgen	41,6	31,4	52,5	27,1	17,4	39,7	32,4	25,2	40,5
Blijft eraan denken	18,4	11,4	28,4	11,1	5,6	20,8	8,1	4,7	13,7
Erg boos	35,0	25,4	46,0	24,2	14,9	36,6	25,4	19,0	33,1
Sliep slechter	13,0	7,3	22,0	9,0	4,0	19,1	2,6	0,9	7,4
Minder vertrouwen in digitale veiligheid	38,8	29,1	49,5	34,8	23,2	48,5	33,3	26,0	41,6
Minder vertrouwen in eigen digitale vaardigheid	15,7	9,3	25,2	19,6	10,6	33,3	11,5	7,0	18,4
Melding[2)] en aangifte									
Gemeld bij minstens één van de volgende instanties	41,3	31,2	52,2	28,7	18,3	42,1	15,1	10,1	22,1
Politie	25,7	16,8	37,1	24,3	14,9	37,0	5,6	2,5	11,9
Bank of financiële instelling	15,4	9,2	24,6	13,9	7,5	24,3	2,5	0,8	8,1
Fraudehelpdesk	11,6	5,9	21,7	9,2	3,6	21,5	1,9	0,6	5,7
Echte bedrijf[3)]	5,5	2,6	11,4	0,0	0,0	0,0			
Telefoon of internetprovider				0,0	0,0	0,0	6,7	3,8	11,7
Centraal Meldpunt Identiteitsfraude en -fouten	4,2	1,1	15,0	4,7	1,2	17,2	0,0	0,0	0,0
Aangifte bij de politie	23,8	15,2	35,3	21,7	12,8	34,3	2,0	0,5	7,0
Weet niet of er aangifte is gedaan	5,1	2,3	11,2	1,2	0,2	8,2	3,3	1,2	9,2
Belangrijkste reden delict niet gemeld									
Helpt niet, totaal	13,4	7,4	22,8	25,0	15,0	38,8	28,6	21,8	36,6
Krijg geld toch niet terug	9,1	4,3	18,1	12,0	5,7	23,6	13,8	9,1	20,3
Ontmoedigende houding van de politie	2,5	0,6	9,6	2,7	0,4	16,8	2,3	0,7	7,0
Dader wordt toch niet gepakt	1,7	0,4	7,1	10,3	4,3	22,7	12,5	7,9	19,3
Niet belangrijk genoeg, totaal	21,2	14,0	30,8	9,8	4,2	21,0	38,1	30,6	46,3
Ging om een klein bedrag	17,5	11,0	26,7	4,2	1,0	16,6	29,0	22,1	37,1
Te veel moeite	3,6	1,3	10,0	5,5	2,0	14,1	8,6	5,1	14,0
Niet in me opgekomen[3)]	0,0	0,0	0,0	0,0	0,0	0,0	0,5	0,1	3,7
Overige redenen of onbekend, totaal	24,1	16,2	34,3	36,5	24,6	50,2	18,1	12,7	25,2
Was mijn eigen fout	5,8	2,2	14,6	0,7	0,1	5,0	5,5	2,9	10,0
Wegens schaamte	2,3	0,6	8,9	1,6	0,2	10,6	1,1	0,2	7,7
Was niet mogelijk voor dit incident	6,0	2,8	12,5	7,7	2,6	20,2	3,7	1,6	8,1
Andere reden	5,9	2,6	13,0	12,4	6,1	23,5	2,1	0,8	5,0
Onbekend	4,1	1,5	10,7	14,1	6,9	26,8	5,8	2,8	11,3
Belangrijkste reden delict niet aangegeven									
Helpt niet, totaal	4,0	1,5	9,9	1,3	0,2	8,9	2,6	1,0	6,8
Krijg geld toch niet terug	0,6	0,1	4,0	1,3	0,2	8,9	1,4	0,3	5,4
Ontmoedigende houding van de politie	1,4	0,2	9,4	0,0	0,0	0,0	0,0	0,0	0,0
Dader wordt toch niet gepakt	1,1	0,3	4,5	0,0	0,0	0,0	1,3	0,3	4,9
Advies van de politie	0,8	0,1	5,6	0,0	0,0	0,0	0,0	0,0	0,0
Niet belangrijk genoeg, totaal	1,6	0,4	6,4	0,0	0,0	0,0	2,5	1,0	6,3
Ging om een klein bedrag	0,0	0,0	0,0	0,0	0,0	0,0	2,5	1,0	6,3
Te veel moeite	1,6	0,4	6,4	0,0	0,0	0,0	0,0	0,0	0,0
Overige redenen of onbekend, totaal	6,7	3,5	12,6	4,5	1,0	17,8	4,7	2,3	9,2
Was mijn eigen fout	0,9	0,2	3,8	4,5	1,0	17,8	0,6	0,1	3,9

6. Slachto erschap van overige vermogensdelicten en nadere delictinformatie, 2018[1] (slot)

	Nepboete/nepfactuur of nepactie			Microsoftscam			Wangirifraude		
	Schatting	Onder-grens	Boven-grens	Schatting	Onder-grens	Boven-grens	Schatting	Onder-grens	Boven-grens
	% slachtoffers								
Was niet mogelijk voor dit incident	2,6	0,8	8,1	0,0	0,0	0,0	0,0	0,0	0,0
Bank zou het verder afhandelen[3]	0,5	0,1	3,3	0,0	0,0	0,0	0,0	0,0	0,0
Andere reden	2,1	0,7	6,4	0,0	0,0	0,0	1,0	0,2	3,8
Onbekend	0,7	0,1	5,0	0,0	0,0	0,0	3,1	1,3	7,5

1) Personen van 12 jaar of ouder met internetgebruik.
2) Meerdere antwoorden mogelijk.
3) Genoemd bij de open antwoordcategorie.
Bron: CBS; pilot onderzoek naar Digitale Veiligheid & Criminaliteit, 2018.

7a. Slachtoerschap van niet-seksuele interpersoonlijke incidenten en nadere informatie, 2018[1)]

	Laster			Stalking			Bedreiging met geweld		
	Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens
	% internetgebruikers								
Slachtoffer geweest	1,0	0,9	1,1	0,5	0,4	0,5	0,3	0,3	0,4
	% slachtoffers								
Gebruikte medium[2)]									
E-mail	7,2	4,7	11,1	16,2	10,6	23,9	9,0	4,6	16,6
Sociale media	65,2	59,3	70,7	56,9	47,5	65,8	57,4	46,4	67,7
WhatsApp of sms[3)]	41,0	35,3	47,0	38,6	29,9	48,0	35,4	26,0	46,1
Anders of onbekend	7,1	4,4	11,2	14,1	8,8	21,8	20,0	12,1	31,2
Een datingapp, datingsite	0,4	0,1	2,9	0,0	0,0	0,0	0,0	0,0	0,0
Een gameplatform	1,6	0,5	5,1	2,7	0,6	10,4	7,9	3,5	17,2
Anders	5,1	3,0	8,6	11,4	7,0	18,1	12,1	6,1	22,5
Informatie over de dader(s)									
Dader is bekend	73,0	67,2	78,1	66,6	57,0	75,1	57,1	46,2	67,3
Dader is[2)]:									
Partner	0,3	0,0	2,4	2,9	0,7	11,3	1,2	0,2	7,8
Ex-partner	13,0	9,3	17,8	16,5	10,9	24,2	14,3	8,0	24,2
Ender familielid	2,9	1,5	5,7	1,9	0,6	5,8	0,0	0,0	0,0
Buurtgenoot	3,1	1,6	5,9	2,8	0,9	8,3	5,3	2,2	12,4
Vriend/vriendin	20,7	16,3	25,9	11,4	6,7	18,9	8,7	4,0	17,9
Iemand van school	22,6	18,2	27,6	9,4	5,4	15,8	9,8	5,5	16,9
Collega	1,6	0,6	4,2	1,1	0,3	4,6	1,0	0,1	6,9
Gevolgen voor het slachtoffer[2)]									
Emotionele gevolgen	46,5	40,5	52,5	48,4	39,2	57,7	39,7	29,9	50,4
Blijft eraan denken	15,6	11,7	20,4	18,1	12,1	26,2	16,7	10,5	25,7
Erg boos	37,9	32,3	43,8	42,8	34,0	52,1	28,4	20,0	38,6
Sliep slechter	17,4	13,1	22,7	25,9	18,6	34,7	15,0	8,7	24,6
Minder vertrouwen in digitale veiligheid	23,0	18,3	28,5	20,6	13,6	30,0	8,8	4,4	16,9
Minder vertrouwen in eigen digitale vaardigheid	7,3	4,6	11,2	3,7	1,5	8,8	0,9	0,1	5,9
Bang dat het vaker zal gebeuren	19,7	15,3	25,0	21,4	14,8	29,9	7,7	3,8	14,6
Financiële schade niets vergoed	2,2	1,0	4,9	0,9	0,1	6,0	4,1	1,3	12,5
Aard van de incidenten volgens de slachtoffers									
Strafbaar misdrijf	9,1	6,0	13,4	16,5	10,5	24,9	26,8	18,1	37,6
Verkeerd, maar geen misdrijf	46,3	40,4	52,3	50,1	40,8	59,4	43,6	33,3	54,5
Toevallige gebeurtenis	9,9	7,1	13,6	6,9	3,4	13,5	2,5	0,7	8,1
Niet strafbaar, was eigen schuld	4,3	2,4	7,5	2,2	0,8	6,0	2,7	0,8	8,3
Kan het niet plaatsen	20,0	15,7	25,2	14,4	9,3	21,8	11,0	6,3	18,7
Wil niet antwoorden	10,3	7,2	14,7	9,8	5,1	18,1	13,5	7,9	22,1
Melding[2)] en aangifte									
Niet gemeld	57,9	51,9	63,6	48,5	39,2	57,8	65,6	54,9	74,9
Verteld aan familie, vrienden of leerkracht	33,4	28,1	39,2	38,9	30,2	48,3	26,4	18,0	36,8
Familie of vrienden	31,7	26,4	37,4	36,9	28,4	46,3	26,4	18,0	36,8
Leerkracht	6,4	4,3	9,2	6,6	3,5	12,1	3,9	1,7	8,6
Gemeld bij minstens één van de volgende instanties:	14,2	10,4	19,1	24,7	17,4	33,9	19,6	12,4	29,5
Politie	12,3	8,8	17,0	23,0	15,9	32,1	18,6	11,6	28,5
Meldpunt huiselijk geweld	0,0	0,0	0,0	1,1	0,1	7,1	1,0	0,1	7,0
Via sociale media[3)]	0,4	0,1	2,9	1,7	0,4	6,7	1,0	0,1	6,6
Werkgever[3)]	1,5	0,5	4,0	1,6	0,4	6,3	0,0	0,0	0,0
Aangifte bij de politie	6,4	3,9	10,3	11,1	6,5	18,3	11,4	6,4	19,6
Weet niet of er aangifte is gedaan	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0

7a. Slachtoerschap van niet-seksuele interpersoonlijke incidenten en nadere informatie, 2018[1] (slot)

	Laster			Stalking			Bedreiging met geweld		
	Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens
	% slachtoffers								
Belangrijkste reden niet melden									
Helpt niet, totaal	24,3	19,3	30,2	14,9	9,4	22,7	24,3	15,9	35,2
Helpt toch niets	10,7	7,1	15,7	8,0	4,1	15,1	11,5	6,0	20,8
Afwijzende houding van de politie	0,0	0,0	0,0	0,0	0,0	0,0	1,9	0,3	12,4
Geen zaak voor de politie	12,3	8,7	17,0	5,7	2,7	11,4	7,4	3,2	16,2
Dader wordt toch niet gepakt	1,4	0,5	3,8	1,2	0,3	5,0	3,5	1,1	10,5
Niet belangrijk genoeg, totaal	13,8	10,2	18,2	8,1	4,1	15,5	11,1	6,2	19,2
Was niet zo belangrijk	12,2	8,9	16,4	6,0	2,7	12,7	9,4	4,9	17,3
Te veel moeite	1,6	0,6	4,1	2,1	0,5	8,6	1,7	0,4	6,5
Overige redenen of onbekend, totaal	19,8	15,6	24,9	25,4	18,1	34,5	30,2	21,3	40,9
Is al opgelost	8,4	5,8	12,1	6,1	3,1	11,7	5,8	2,5	12,7
Dader is bekende	2,8	1,4	5,4	1,5	0,5	4,7	2,2	0,5	8,6
Angst voor de gevolgen	0,3	0,1	1,3	3,3	1,2	8,6	2,5	0,8	8,0
Wegens schaamte	0,6	0,1	2,6	0,9	0,1	5,8	2,2	0,5	8,3
Was mijn eigen schuld[3]	0,2	0,0	1,6	0,0	0,0	0,0	0,0	0,0	0,0
Weet niet waar dat zou kunnen	0,8	0,2	3,4	0,6	0,1	4,1	0,0	0,0	0,0
Andere reden	2,2	0,9	4,9	1,9	0,5	6,3	6,1	2,7	13,2
Onbekend	4,4	2,5	7,7	11,2	6,1	19,7	11,5	5,9	21,2
Belangrijkste reden geen aangifte									
Helpt niet, totaal	15,9	12,0	20,7	15,6	9,9	23,8	10,4	5,0	20,2
Helpt toch niets	5,4	3,1	9,1	5,7	2,4	12,9	7,9	3,2	18,0
Advies van de politie	1,0	0,4	2,9	1,0	0,1	6,5	0,0	0,0	0,0
Afwijzende houding van de politie	1,4	0,5	3,8	2,2	0,7	6,9	0,6	0,1	3,9
Geen zaak voor de politie	7,0	4,6	10,5	4,6	2,0	10,1	1,9	0,5	7,5
Dader wordt toch niet gepakt	0,8	0,2	2,7	2,2	0,7	6,9	0,0	0,0	0,0
Niet belangrijk genoeg, totaal	4,7	2,8	7,7	6,6	3,5	12,2	5,5	2,4	12,3
Was niet zo belangrijk	3,7	2,1	6,4	6,0	3,0	11,4	5,5	2,4	12,3
Te veel moeite	1,0	0,3	3,1	0,7	0,1	4,5	0,0	0,0	0,0
Overige redenen of onbekend, totaal	15,1	11,5	19,7	18,2	11,9	26,7	7,1	3,5	13,7
Is al opgelost	8,4	5,7	12,1	9,4	5,1	16,6	2,6	0,9	6,9
Dader is bekende	1,1	0,4	3,1	0,0	0,0	0,0	0,7	0,1	4,6
Dader was niet bekend[3]	0,3	0,0	2,1	0,0	0,0	0,0	0,0	0,0	0,0
Angst voor de gevolgen	1,1	0,4	2,9	3,0	0,9	9,5	1,1	0,2	7,7
Uit schaamte	0,2	0,0	1,5	0,0	0,0	0,0	0,0	0,0	0,0
Weet niet waar dat zou kunnen	0,0	0,0	0,0	0,6	0,1	4,1	0,0	0,0	0,0
Andere reden	2,2	1,1	4,4	3,5	1,3	9,0	0,8	0,1	5,4
Onbekend	2,2	1,1	4,7	1,6	0,4	7,3	1,9	0,4	8,6

1) Personen van 12 jaar of ouder met internetgebruik.
2) Meerdere antwoorden mogelijk.
3) Genoemd bij de open antwoordcategorie.
Bron: CBS; pilot onderzoek naar Digitale Veiligheid & Criminaliteit, 2018.

7b. Slachtoerschap van seksuele interpersoonlijke incidenten en nadere informatie, 2018[1)]

	Laster			Stalking		
	Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens
	% internetgebruikers					
Slachtoffer geweest	0,3	0,3	0,4	0,4	0,3	0,4
	% slachtoffers					
Gebruikte medium[2)]						
E-mail	12,5	7,4	20,1	17,3	11,4	25,4
Sociale media	69,3	58,9	78,1	65,8	56,0	74,4
WhatsApp of sms[3)]	31,5	22,5	42,1	34,5	25,7	44,5
Anders of onbekend	10,2	5,5	18,3	9,1	4,9	16,2
Een datingapp, datingsite	2,0	0,5	8,0	3,9	1,4	10,1
Een gameplatform	0,0	0,0	0,0	1,6	0,4	6,0
Anders	8,2	4,0	15,9	3,6	1,4	9,3
Informatie over de dader(s)						
Dader is bekend	55,1	44,5	65,2	52,3	42,6	61,7
Dader is[2)]:						
Partner	1,2	0,2	8,3	0,0	0,0	0,0
Ex-partner	10,9	6,1	18,7	15,6	9,7	24,1
Ender familielid	0,0	0,0	0,0	0,0	0,0	0,0
Buurtgenoot	1,5	0,3	5,9	2,5	0,6	9,5
Vriend/vriendin	5,3	2,4	11,4	2,1	0,7	6,7
Iemand van school	8,5	4,4	15,9	3,6	1,3	9,5
Collega	1,3	0,2	8,7	1,2	0,2	8,1
Gevolgen voor het slachtoffer[2)]						
Emotionele gevolgen	43,6	33,7	53,9	50,5	40,9	60,1
Blijft eraan denken	19,1	12,6	27,9	18,4	11,9	27,5
Erg boos	39,5	30,1	49,8	37,2	28,3	47,1
Sliep slechter	18,0	11,7	26,7	20,9	13,9	30,1
Minder vertrouwen in digitale veiligheid	28,5	19,9	39,0	27,9	20,0	37,4
Minder vertrouwen in eigen digitale vaardigheid	17,4	10,7	27,1	15,8	9,6	24,9
Bang dat het vaker zal gebeuren	21,9	14,5	31,5	19,2	12,6	28,1
Financiële schade niets vergoed	2,3	0,6	8,8	2,9	0,9	8,9
Aard van de incidenten volgens de slachtoffers						
Strafbaar misdrijf	21,9	14,8	31,1	16,1	10,2	24,6
Verkeerd, maar geen misdrijf	34,8	25,8	45,2	52,3	42,7	61,9
Toevallige gebeurtenis	8,7	3,6	19,5	5,2	2,5	10,3
Niet strafbaar, was eigen schuld	9,2	4,7	17,3	2,5	0,8	7,7
Kan het niet plaatsen	13,3	7,9	21,3	19,1	12,4	28,2
Wil niet antwoorden	12,1	6,1	22,6	4,7	1,8	11,9
Melding[2)] en aangifte						
Niet gemeld	55,3	44,8	65,4	50,3	40,7	59,9
Verteld aan familie, vrienden of leerkracht	33,0	24,0	43,5	38,9	29,8	48,8
Familie of vrienden	31,0	22,2	41,4	38,9	29,8	48,8
Leerkracht	4,4	2,1	8,9	0,4	0,1	3,1
Gemeld bij minstens één van de volgende instanties:	16,1	10,0	24,8	19,5	12,5	29,2
Politie	15,2	9,3	23,9	16,5	10,3	25,5
Meldpunt huiselijk geweld	0,0	0,0	0,0	0,0	0,0	0,0
Via sociale media[3)]	0,0	0,0	0,0	0,9	0,1	6,0
Werkgever[3)]	0,9	0,1	6,0	2,1	0,3	13,5
Aangifte bij de politie	9,6	5,0	17,5	9,8	5,2	17,9
Weet niet of er aangifte is gedaan	0,0	0,0	0,0	0,0	0,0	0,0

7b. Slachtoerschap van seksuele interpersoonlijke incidenten en nadere informatie, 2018[1] (slot)

	Laster			Stalking		
	Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens
	% slachtoffers					
Belangrijkste reden niet melden						
Helpt niet, totaal	17,5	10,7	27,3	11,8	7,1	19,1
Helpt toch niets	9,5	4,8	17,9	7,6	3,9	14,1
Geen zaak voor de politie	7,0	3,0	15,5	2,8	1,0	7,7
Dader wordt toch niet gepakt	1,0	0,1	6,8	1,5	0,4	6,0
Niet belangrijk genoeg, totaal	10,2	5,2	19,3	17,1	11,1	25,4
Was niet zo belangrijk	10,2	5,2	19,3	16,1	10,4	24,2
Te veel moeite	0,0	0,0	0,0	1,0	0,1	6,7
Overige redenen of onbekend, totaal	27,6	19,2	37,9	21,4	14,7	30,0
Is al opgelost	8,3	4,1	16,1	10,6	6,0	18,0
Dader is bekende	0,3	0,0	1,9	1,1	0,1	7,1
Angst voor de gevolgen	3,1	0,8	11,6	1,5	0,4	5,9
Wegens schaamte	8,6	4,1	17,3	3,8	1,4	10,1
Was mijn eigen schuld[3]	0,8	0,1	5,4	0,0	0,0	0,0
Weet niet waar dat zou kunnen	3,2	1,0	10,1	2,0	0,6	6,2
Andere reden	1,8	0,5	5,7	1,2	0,3	4,6
Onbekend	1,5	0,4	6,5	1,2	0,4	3,9
Belangrijkste reden geen aangifte						
Helpt niet, totaal	11,7	6,6	19,8	11,6	6,7	19,5
Helpt toch niets	6,5	2,9	13,9	7,1	3,3	14,5
Advies van de politie	2,7	0,8	8,4	0,8	0,1	5,6
Afwijzende houding van de politie	0,0	0,0	0,0	0,0	0,0	0,0
Geen zaak voor de politie	1,7	0,4	7,4	1,9	0,5	7,4
Dader wordt toch niet gepakt	0,7	0,1	5,0	1,3	0,3	5,5
Niet belangrijk genoeg, totaal	8,3	4,5	15,0	6,4	2,8	13,7
Was niet zo belangrijk	6,7	3,3	13,1	6,4	2,8	13,7
Te veel moeite	1,6	0,4	6,2	0,0	0,0	0,0
Overige redenen of onbekend, totaal	15,2	8,9	24,6	21,8	14,6	31,4
Is al opgelost	3,3	0,9	11,4	6,0	2,8	12,2
Dader is bekende	1,5	0,4	6,2	1,0	0,2	4,8
Dader was niet bekend[3]	0,0	0,0	0,0	0,5	0,1	3,2
Angst voor de gevolgen	1,7	0,4	7,8	3,2	1,0	9,4
Uit schaamte	0,0	0,0	0,0	0,6	0,1	3,8
Weet niet waar dat zou kunnen	0,5	0,1	3,3	2,2	0,4	10,5
Andere reden	4,1	1,8	9,2	5,3	1,9	14,1
Onbekend	4,0	1,1	13,8	3,5	1,3	9,2

1) Personen van 12 jaar of ouder met internetgebruik.
2) Meerdere antwoorden mogelijk.
3) Genoemd bij de open antwoordcategorie.
Bron: CBS; pilot onderzoek naar Digitale Veiligheid & Criminaliteit, 2018.

8. Interpersoonlijke incidenten en seksueel getinte spam, naar geslacht en leeftijd, 2018[1)]

		Interpersoonlijke niet-seksuele incidenten			Interpersoonlijke seksuele incidenten			Seksuele spam		
		Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens
		% internetgebruikers								
Geslacht	*Leeftijd*									
Man	12 tot 18 jaar	3,7	2,9	4,8	0,2	0,1	0,4	1,0	0,7	1,6
Man	18 tot 25 jaar	2,8	2,0	3,9	0,8	0,4	1,5	1,1	0,7	1,9
Man	25 tot 35 jaar	1,5	1,0	2,2	0,6	0,3	1,1	0,6	0,3	1,0
Man	35 tot 45 jaar	0,9	0,5	1,4	0,2	0,1	0,6	0,4	0,2	0,8
Man	45 jaar of ouder	0,6	0,4	0,7	0,2	0,1	0,3	0,3	0,2	0,4
Vrouw	12 tot 18 jaar	6,9	5,8	8,3	2,6	1,9	3,5	3,2	2,4	4,1
Vrouw	18 tot 25 jaar	3,1	2,3	4,3	3,0	2,2	4,1	2,8	2,1	3,9
Vrouw	25 tot 35 jaar	2,0	1,4	2,8	1,3	0,8	1,9	1,3	0,9	2,0
Vrouw	35 tot 45 jaar	1,2	0,8	1,8	0,8	0,5	1,4	0,6	0,4	1,0
Vrouw	45 jaar of ouder	0,5	0,3	0,6	0,3	0,2	0,5	0,6	0,5	0,8

[1)] Personen van 12 jaar of ouder met internetgebruik.
Bron: CBS; pilot onderzoek naar Digitale Veiligheid & Criminaliteit, 2018.

9. Slachtoerschap van identiteitsfraude zonder nanciële schade en nadere delictinformatie, 2018[1)]

	Poging geld van rekening te halen en/ of betalingen te doen			Poging tot verkrijgen van lening, abonnement, goederen of diensten op naam van het slachtoffer			Overige identiteitsfraude		
	Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens
	% internetgebruikers								
Slachtoffer geweest	0,2	0,2	0,3	0,5	0,4	0,6	0,3	0,3	0,4
	% slachtoffers								
Manier waarop de gegevens zijn verkregen									
Zelf bankpas in goed vertrouwen ter beschikking gesteld	12,9	6,4	24,3	1,6	0,4	6,3	.	.	.
Zelf persoonlijke gegevens in goed vertrouwen aan een bekende ter beschikking gesteld	2,6	0,6	10,1	1,5	0,4	5,4	.	.	.
Zelf gegevens doorgegeven op een webshop of via de telefoon	9,7	4,5	19,6	7,5	4,3	12,9	9,0	4,1	18,6
Niet online, maar door kopiëren creditcard of bijv. dumpster diving[2)]	0,9	0,1	6,2	1,8	0,5	5,6	.	.	.
Diefstal van paspoort of ID-kaart waarbij identiteit overgenomen werd	4,5	1,1	16,4	0,8	0,1	5,7	3,1	1,1	8,0
Diefstal van bankpas of creditcard	1,4	0,2	9,2	0,8	0,1	5,2	.	.	.
Skimmen van bankpas of creditcard	8,2	3,7	17,5	1,5	0,4	5,0	.	.	.
Shimmen, scannen van mobiele telefoon	0,0	0,0	0,0	0,0	0,0	0,0	1,0	0,1	6,5
Phishing of pharming	11,0	4,9	22,5	8,2	4,9	13,3	6,9	3,5	13,1
Hacken van device of account	7,5	3,0	17,4	17,0	11,9	23,8	2,7	0,9	7,5
Via malware (bv. een computervirus of trojan horse)	0,0	0,0	0,0	2,0	0,6	6,4	2,9	0,9	8,9
Keylogging	0,0	0,0	0,0	0,0	0,0	0,0	1,2	0,2	7,9
Hacken van bedrijf of bank waar persoonlijke gegevens bekend zijn	1,8	0,3	11,8	8,7	5,1	14,4	14,3	8,5	23,0
Andere wijze	4,0	1,5	10,5	9,2	5,6	15,0	18,6	11,6	28,4
Weet het niet	35,5	24,8	48,0	39,4	31,9	47,4	40,5	30,8	50,9
Totaal door phishing[3)]	33,7	23,0	46,5	17,2	12,2	23,8	.	.	.
Totaal door hacken[3)]	9,3	4,1	19,7	27,7	21,1	35,4	21,0	14,0	30,4
Gevolgen voor het slachtoffer[4)]									
Emotionele gevolgen	25,8	16,3	38,4	35,5	28,2	43,4	33,6	24,6	44,1
Blijft eraan denken	10,4	4,4	22,7	11,8	7,5	18,1	9,9	5,3	17,8
Erg boos	17,4	10,1	28,1	30,4	23,6	38,3	27,8	19,5	38,0
Sliep slechter	3,1	0,8	11,8	7,4	4,1	12,9	10,1	5,4	18,3
Minder vertrouwen in digitale veiligheid	35,3	24,1	48,5	40,1	32,8	48,0	44,7	34,7	55,2
Minder vertrouwen in eigen digitale vaardigheid	7,4	3,6	14,5	11,6	7,5	17,4	18,2	11,0	28,6
Bang dat het vaker zal gebeuren	24,4	15,6	36,1	34,7	27,7	42,4	27,2	19,1	37,0
Melding[4)] en aangifte									
Gemeld bij minstens één van de volgende instanties[4)]	60,0	47,3	71,5	50,9	43,0	58,8	39,0	29,3	49,6
Politie	23,6	14,7	35,6	24,5	18,2	32,2	32,9	23,7	43,6
Bank of financiële instelling	38,0	27,1	50,2	21,5	15,9	28,5	12,3	6,5	22,1
Fraudehelpdesk	3,0	0,7	11,3	4,3	2,1	8,7	8,4	4,1	16,5
Centraal Meldpunt Identiteitsfraude en -fouten	0,0	0,0	0,0	4,4	1,8	10,1	1,4	0,3	5,4
Autoriteit Consument en Markt	0,0	0,0	0,0	0,0	0,0	0,0	.	.	.
Bedrijf of webshop waar betaling, aanvraag of bestelling was gedaan[2)]	5,5	1,4	19,6	10,0	6,1	15,9	.	.	.
Aangifte bij de politie	15,0	8,3	25,6	15,7	10,6	22,6	23,5	15,6	33,7
Weet niet of er aangifte is gedaan	11,4	6,0	20,6	8,4	4,9	14,0	0,0	0,0	0,0
Belangrijkste reden niet melden									
Helpt niet, totaal	2,1	0,5	8,3	10,8	6,6	17,0	12,3	7,2	20,1
Ontmoedigende houding van de politie	0,0	0,0	0,0	0,0	0,0	0,0	3,5	1,3	9,0

9. Slachtoerschap van identiteitsfraude zonder nanciële schade en nadere delictinformatie, 2018[1] (slot)

	Poging geld van rekening te halen en/ of betalingen te doen			Poging tot verkrijgen van lening, abonnement, goederen of diensten op naam van het slachtoffer			Overige identiteitsfraude		
	Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens
	% slachtoffers								
Advies van de politie	0,0	0,0	0,0	1,0	0,1	7,0	0,0	0,0	0,0
Dader wordt toch niet gepakt	2,1	0,5	8,3	8,6	5,1	14,1	7,5	3,8	14,3
Er wordt toch niets mee gedaan[2]	0,0	0,0	0,0	1,2	0,2	6,1	1,2	0,2	8,2
Niet belangrijk genoeg, totaal	4,9	1,3	16,1	8,5	4,9	14,4	7,7	3,9	14,7
Ging om een klein bedrag, was geen belangrijk incident	4,9	1,3	16,1	1,9	0,7	5,3	0,0	0,0	0,0
Te veel moeite	0,0	0,0	0,0	3,7	1,6	8,3	7,7	3,9	14,7
Er was geen financiële schade[2]	0,0	0,0	0,0	2,9	1,0	8,0	0,0	0,0	0,0
Overige redenen of onbekend, totaal	33,0	22,3	45,8	29,8	23,1	37,5	41,1	31,4	51,5
Dader is bekende	1,1	0,2	7,3	0,4	0,1	2,9	0,0	0,0	0,0
Was mijn eigen fout	3,7	0,8	15,8	5,2	2,6	10,3	7,3	3,0	16,6
Wegens schaamte	1,5	0,2	10,0	0,2	0,0	1,7	0,0	0,0	0,0
Was niet mogelijk voor dit incident	0,0	0,0	0,0	2,8	1,1	6,7	6,3	3,2	12,0
Andere reden	6,3	2,7	13,8	9,4	5,8	14,8	8,8	4,7	15,9
Onbekend	20,4	11,9	32,9	11,7	7,4	18,2	18,7	11,8	28,4
Belangrijkste reden geen aangifte									
Helpt niet, totaal	4,9	1,0	20,1	4,0	1,9	8,1	2,8	0,9	8,4
Ontmoedigende houding van de politie	0,0	0,0	0,0	1,0	0,2	4,3	1,1	0,2	7,7
Op advies van de politie	1,1	0,2	7,6	1,3	0,3	5,2	1,6	0,4	6,4
Dader wordt toch niet gepakt	3,7	0,5	21,9	1,6	0,6	4,5	0,0	0,0	0,0
Niet belangrijk genoeg, totaal	3,5	1,3	9,4	3,4	1,6	7,3	1,1	0,2	7,4
Ging om een klein bedrag, was geen belangrijk incident	1,1	0,1	7,2	0,0	0,0	0,0	1,1	0,2	7,4
Te veel moeite	1,4	0,3	5,8	1,5	0,5	4,6	0,0	0,0	0,0
Niet in me opgekomen[2]	0,0	0,0	0,0	0,8	0,1	5,3	0,0	0,0	0,0
Er was geen financiële schade[2]	1,0	0,1	7,0	1,2	0,4	3,6	0,0	0,0	0,0
Overige redenen of onbekend, totaal	25,2	16,0	37,2	19,4	13,9	26,3	11,6	6,2	20,9
Bank, of creditcardmaatschappij zou het verder afhandelen[2]	3,3	1,2	8,7	2,8	1,0	7,4	0,7	0,1	4,7
Dader is bekende	2,2	0,3	13,8	0,0	0,0	0,0	0,0	0,0	0,0
Was mijn eigen fout	2,1	0,5	9,0	0,7	0,1	4,6	0,0	0,0	0,0
Uit schaamte	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Was niet mogelijk voor dit incident	7,5	3,0	17,9	4,5	2,2	9,2	3,5	1,3	9,1
Andere reden	3,8	1,2	11,3	6,8	4,0	11,4	6,1	2,3	15,4
Onbekend	6,2	2,3	15,9	4,5	2,1	9,4	1,4	0,2	9,0

1) Personen van 12 jaar of ouder met internetgebruik.
2) Werden genoemd bij open antwoordcategorieën.
3) Aan meerdere vormen van gegevensdiefstal ging een vorm van phishing vooraf. Zie de methodologische toelichting in de onderzoeksverantwoording voor de berekening van 'totaal door phishing' en 'totaal door hacken'.
4) Meerdere antwoorden mogelijk.
Bron: CBS; pilot onderzoek naar Digitale Veiligheid & Criminaliteit, 2018.

10. Enkele gerapporteerde vormen van phishing, emotionele gevolgen en melding, 2018[1)]

	Voorschotfraude			Microsoftscam			Wangirifraude			Poging tot afpersing		
	Schatting	Onder-grens	Boven-grens	Schatting	Onder-grens	Boven-grens	Schatting	Onder-grens	Boven-grens	Schatting	Onder-grens	Boven-grens
	% van de internetgebruikers											
Phishing ontvangen	3,7	3,5	3,9	14,7	14,3	15,1	3,7	3,4	3,9	2,3	2,2	2,5
Slachtoffer geweest	0,1	0,1	0,1	0,2	0,1	0,2	0,5	0,4	0,6	0,0	0,0	0,1
	% van de ontvangers die er niet zijn ingetrapt											
Gevolgen voor de ontvanger[2)]												
Emotionele gevolgen	11,6	9,9	13,6	16,6	15,6	17,7	18,6	16,2	21,3	33,2	29,7	36,9
Blijft eraan denken	2,7	1,9	3,9	2,8	2,3	3,3	3,9	2,8	5,4	9,8	7,7	12,4
Erg boos	9,6	8,0	11,4	14,9	14,0	15,9	16,3	14,1	18,9	26,5	23,3	30,0
Sliep slechter	1,6	1,0	2,5	0,8	0,5	1,0	1,2	0,7	2,1	9,7	7,6	12,4
Minder vertrouwen in digitale veiligheid	26,8	24,3	29,4	21,7	20,6	22,9	24,6	22,0	27,6	32,4	29,0	36,0
Minder vertrouwen in eigen digitale vaardigheid	9,3	7,8	11,2	6,1	5,4	6,7	8,4	6,8	10,5	10,2	8,1	12,7
Melding van de incidenten[2)]												
Gemeld bij minstens één van de volgende instanties	8,4	7,0	10,1	7,1	6,4	7,8	8,4	6,7	10,3	11,8	9,5	14,5
Polite	2,6	1,8	3,7	2,4	2,0	2,8	2,7	1,8	4,1	9,3	7,3	11,9
Bank, financiële instelling of creditcardmaatschappij	3,5	2,6	4,6	1,9	1,6	2,3	1,9	1,3	2,9			
Fraudehelpdesk[3)]	2,7	1,9	3,7	2,4	2,0	2,9	1,5	0,9	2,3	3,0	2,0	4,5
Echte bedrijf[3)]				0,4	0,3	0,6				0,2	0,0	1,7
Telefoonprovider, internetprovider[3)]				0,5	0,4	0,8	2,5	1,6	3,7	.	.	.
Centraal Meldpunt Identiteitsfraude en -fouten	0,4	0,2	0,9	0,5	0,3	0,7	0,9	0,4	1,8	.	.	.
Sociale media[3)]	.	.	.	.	.	.	.	.	.	0,2	0,0	1,2
Eigen werkgever[3)]	.	.	.	.	.	.	.	.	.	0,8	0,3	1,7

1) Personen van 12 jaar of ouder met internetgebruik.
2) Meerdere antwoorden mogelijk.
3) Genoemd bij de open antwoordcategorie.
Bron: CBS; pilot onderzoek naar Digitale Veiligheid & Criminaliteit, 2018.

11. Kennis internetveiligheid, 2018[1)]

	Weet (ongeveer) wat ermee wordt bedoeld			Van gehoord, weet niet wat ermee bedoeld wordt			Nooit van gehoord		
	Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens	Schatting	Ondergrens	Bovengrens
	% internetgebruikers								
Back-ups maken	89,5	89,1	89,8	6,6	6,4	6,9	3,9	3,6	4,1
Een antivirusprogramma	92,9	92,6	93,2	4,5	4,2	4,7	2,6	2,4	2,8
Firewall	73,8	73,4	74,3	16,9	16,5	17,3	9,3	8,9	9,6
Spam	90,1	89,7	90,5	6,1	5,9	6,4	3,8	3,5	4,0
DDos aanval	55,6	55,1	56,2	22,9	22,5	23,4	21,5	21,0	21,9
Hacken	89,2	88,9	89,6	7,4	7,2	7,7	3,3	3,1	3,6
Phishing	71,7	71,2	72,2	12,3	12,0	12,7	15,9	15,5	16,4
Pharming	15,6	15,2	16,0	29,3	28,8	29,8	55,1	54,6	55,7
Ransomware	38,1	37,5	38,6	27,2	26,7	27,7	34,8	34,2	35,3
Spyware	53,2	52,6	53,7	24,1	23,6	24,6	22,7	22,3	23,2
Cryptoware	26,8	26,4	27,3	33,1	32,6	33,7	40,0	39,5	40,6
Malware	42,1	41,6	42,7	27,0	26,5	27,5	30,9	30,3	31,4
Belfraude of wangiri	34,1	33,6	34,6	22,5	22,1	23,0	43,4	42,8	43,9
Microsoft helpdeskfraude	45,3	44,7	45,8	22,8	22,3	23,2	32,0	31,5	32,5

[1)] Personen van 12 jaar of ouder met internetgebruik.
Bron: CBS; pilot onderzoek naar Digitale Veiligheid & Criminaliteit, 2018.

12. Geneigdheid doorgeven persoonlijke informatie via internet, 2018[1)]

In hoeverre bent u geneigd de volgende persoonlijke informatie door te geven via internet?	Schatting	Ondergrens	Bovengrens
	% internetgebruikers		
Uw naam			
Ik heb hier geen problemen mee	44,1	43,6	44,7
Ik doe dit alleen als ik de ander vertrouw	24,2	23,8	24,7
Ik deel dit alleen als het moet	24,2	23,8	24,7
Ik deel dit niet via internet	7,4	7,1	7,7
Uw geboortedatum			
Ik heb hier geen problemen mee	32,9	32,4	33,5
Ik doe dit alleen als ik de ander vertrouw	23,4	23,0	23,9
Ik deel dit alleen als het moet	33,6	33,1	34,1
Ik deel dit niet via internet	10,0	9,7	10,4
Uw adresgegevens			
Ik heb hier geen problemen mee	13,0	12,6	13,4
Ik doe dit alleen als ik de ander vertrouw	26,9	26,4	27,4
Ik deel dit alleen als het moet	44,0	43,4	44,5
Ik deel dit niet via internet	16,1	15,7	16,5
Uw Burgerservicenummer			
Ik heb hier geen problemen mee	1,6	1,5	1,8
Ik doe dit alleen als ik de ander vertrouw	8,0	7,7	8,3
Ik deel dit alleen als het moet	36,7	36,2	37,3
Ik deel dit niet via internet	53,7	53,1	54,2
Contactgegevens zoals telefoonnummer of e-mailadres			
Ik heb hier geen problemen mee	13,7	13,3	14,1
Ik doe dit alleen als ik de ander vertrouw	30,9	30,4	31,4
Ik deel dit alleen als het moet	44,8	44,3	45,4
Ik deel dit niet via internet	10,6	10,2	10,9
Betalingsgegevens zoals banknummer of creditcardnummer			
Ik heb hier geen problemen mee	1,4	1,3	1,5
Ik doe dit alleen als ik de ander vertrouw	11,9	11,6	12,3
Ik deel dit alleen als het moet	43,2	42,7	43,8
Ik deel dit niet via internet	43,5	42,9	44,0
Informatie over uw gezondheid			
Ik heb hier geen problemen mee	6,6	6,3	6,9
Ik doe dit alleen als ik de ander vertrouw	13,0	12,6	13,4
Ik deel dit alleen als het moet	29,4	28,9	29,9
Ik deel dit niet via internet	51,0	50,5	51,6
Informatie over uw werk			
Ik heb hier geen problemen mee	9,3	8,9	9,6
Ik doe dit alleen als ik de ander vertrouw	15,4	15,0	15,8
Ik deel dit alleen als het moet	28,1	27,6	28,6
Ik deel dit niet via internet	47,2	46,7	47,8
Een foto van uzelf			
Ik heb hier geen problemen mee	18,4	18,0	18,8
Ik doe dit alleen als ik de ander vertrouw	27,4	26,9	27,8
Ik deel dit alleen als het moet	23,3	22,8	23,7
Ik deel dit niet via internet	31,0	30,5	31,5
Een foto van iemand anders, zonder toestemming van diegene			
Ik heb hier geen problemen mee	2,6	2,4	2,8
Ik doe dit alleen als ik de ander vertrouw	11,4	11,0	11,8
Ik deel dit alleen als het moet	7,8	7,5	8,1
Ik deel dit niet via internet	78,2	77,8	78,7

[1)] Personen van 12 jaar of ouder met internetgebruik.
Bron: CBS; pilot onderzoek naar Digitale Veiligheid & Criminaliteit, 2018.

13. Bezorgdheid over internetveiligheid, 2018[1)]

	Schatting	Ondergrens	Bovengrens
In hoeverre bent u bezorgd dat de volgende zaken u kunnen overkomen?	% internetgebruikers		
Computervirus of -infectie			
Zeer bezorgd	24,4	24,0	24,9
Een beetje bezorgd	47,3	46,7	47,8
Bijna niet bezorgd	21,6	21,1	22,0
Helemaal niet bezorgd	6,7	6,5	7,0
Ongewenste e-mail, ook wel spam genoemd			
Zeer bezorgd	18,6	18,2	19,0
Een beetje bezorgd	37,6	37,1	38,2
Bijna niet bezorgd	28,3	27,8	28,8
Helemaal niet bezorgd	15,5	15,0	15,9
Het hacken van een apparaat (bv. computer/ tablet/telefoon), social media of e-mailaccount			
Zeer bezorgd	30,2	29,7	30,8
Een beetje bezorgd	42,3	41,7	42,8
Bijna niet bezorgd	20,8	20,4	21,3
Helemaal niet bezorgd	6,7	6,4	7,0
Software die de computer blokkeert of bestanden versleutelt (ransomware)			
Zeer bezorgd	30,3	29,8	30,8
Een beetje bezorgd	38,7	38,2	39,2
Bijna niet bezorgd	22,0	21,5	22,4
Helemaal niet bezorgd	9,0	8,7	9,3
Misleidende e-mails of vervalste websites waarmee geprobeerd wordt persoonlijke informatie te verkrijgen (phishing/pharming)			
Zeer bezorgd	30,7	30,2	31,2
Een beetje bezorgd	37,6	37,1	38,1
Bijna niet bezorgd	20,7	20,3	21,2
Helemaal niet bezorgd	11,0	10,6	11,4
Misbruik van uw bank- of persoonsgegevens			
Zeer bezorgd	42,2	41,7	42,8
Een beetje bezorgd	34,1	33,6	34,6
Bijna niet bezorgd	16,8	16,4	17,2
Helemaal niet bezorgd	6,9	6,6	7,2

[1)] Personen van 12 jaar of ouder met internetgebruik.
Bron: CBS; pilot onderzoek naar Digitale Veiligheid & Criminaliteit, 2018.

14. Activiteiten ter bescherming van persoonlijke gegevens, 2018[1)]

	Schatting	Ondergrens	Bovengrens
Hoe vaak voert u onderstaande activiteiten uit?			
	% internetgebruikers		
Lezen of raadplegen van privacyregels vóór het invullen van persoonlijke informatie			
Altijd	8,0	7,7	8,3
Vaak	10,8	10,5	11,2
Soms	26,7	26,2	27,2
Zelden	29,6	29,1	30,1
Nooit	21,0	20,5	21,4
Het invullen van verzonnen persoonsgegevens			
Altijd	0,9	0,8	1,1
Vaak	4,5	4,3	4,8
Soms	16,1	15,7	16,5
Zelden	14,0	13,6	14,4
Nooit	56,5	56,0	57,0
Toegang weigeren tot uw geografische locatie, foto's of contacten op uw mobiele internet apparatuur			
Altijd	12,3	11,9	12,6
Vaak	30,7	30,2	31,2
Soms	25,6	25,1	26,1
Zelden	8,9	8,6	9,2
Nooit	14,1	13,8	14,5
Beperkte toegang geven tot uw persoonlijke gegevens en informatie op sociale netwerksites zoals Facebook en Twitter			
Altijd	17,4	17,0	17,9
Vaak	19,4	18,9	19,8
Soms	16,4	16,0	16,8
Zelden	7,9	7,6	8,2
Nooit	21,3	20,9	21,8
Toestaan dat persoonlijke informatie wordt gebruikt voor commerciële doeleinden (denk aan cookies)			
Altijd	7,9	7,6	8,2
Vaak	26,5	26,0	27,0
Soms	27,4	26,9	27,9
Zelden	14,6	14,2	15,0
Nooit	19,4	19,0	19,8
Cookies verwijderen			
Altijd	11,2	10,8	11,5
Vaak	22,0	21,6	22,5
Soms	27,7	27,2	28,1
Zelden	16,1	15,7	16,6
Nooit	18,4	17,9	18,8
Controleren of de website waarop u persoonlijke informatie moet verstrekken veilig is, bijvoorbeeld door te letten op https-beveiliging			
Altijd	27,8	27,3	28,3
Vaak	24,2	23,7	24,7
Soms	18,0	17,6	18,4
Zelden	11,9	11,6	12,3
Nooit	14,1	13,7	14,5
Nagaan welke persoonlijke informatie van u beschikbaar is op websites of via zoekmachines als Google met het doel deze aan te vullen of te verwijderen			
Altijd	4,5	4,3	4,8
Vaak	8,9	8,6	9,3
Soms	28,6	28,1	29,1
Zelden	20,6	20,2	21,1
Nooit	31,2	30,7	31,7

[1)] Personen van 12 jaar of ouder met internetgebruik.
Bron: CBS; pilot onderzoek naar Digitale Veiligheid & Criminaliteit, 2018.

15. Bescherming van internetapparatuur en/of persoonlijke informatie op het internet, 2018[1)]

	Schatting	Ondergrens	Bovengrens
Kunt u aangeven hoe vaak u of iemand anders voor u onderstaande dingen doet?			
	% internetgebruikers		
Maken van back-ups op een andere computer of op een externe harde schijf			
Vaak	21,4	21,0	21,9
Soms	34,3	33,8	34,8
Zelden	17,9	17,5	18,3
Nooit	22,1	21,7	22,6
Opslaan van gegevens in de cloud			
Vaak	24,3	23,8	24,7
Soms	23,6	23,1	24,0
Zelden	14,8	14,4	15,2
Nooit	32,4	31,9	32,9
Up-to-date houden of vernieuwen van computerprogramma's (bv. besturingssysteem, virusscanner of internetbrowser)			
Vaak	45,2	44,7	45,8
Soms	29,0	28,5	29,5
Zelden	12,2	11,8	12,6
Nooit	10,2	9,8	10,5
Tussentijds zelf controleren op virussen zonder dat de scanner hierom vraagt			
Vaak	16,6	16,2	17,0
Soms	30,1	29,6	30,6
Zelden	20,8	20,4	21,3
Nooit	28,6	28,1	29,1
Onderhouden van een firewall			
Vaak	18,1	17,7	18,5
Soms	20,8	20,4	21,3
Zelden	18,5	18,1	19,0
Nooit	33,5	33,0	34,0
Onderhouden van een spamfilter			
Vaak	17,9	17,5	18,4
Soms	21,5	21,1	22,0
Zelden	19,7	19,2	20,1
Nooit	32,9	32,4	33,4
Toegang tot uw apparaten beschermen met een toegangscode, wachtwoord, vingerafdruk etc.			
Vaak	63,6	63,0	64,1
Soms	16,7	16,3	17,1
Zelden	6,2	6,0	6,5
Nooit	10,2	9,9	10,5
Aanpassen van de veiligheidsinstelling op uw internetbrowser			
Vaak	15,6	15,2	16,0
Soms	27,7	27,2	28,1
Zelden	23,3	22,9	23,8
Nooit	28,8	28,3	29,3
Zelf regelmatig wachtwoorden veranderen			
Vaak	14,6	14,2	15,0
Soms	36,8	36,2	37,3
Zelden	28,5	28,1	29,0
Nooit	17,8	17,3	18,2

15. Bescherming van internetapparatuur en persoonlijke informatie op het internet, 2018[1] (slot)

	Schatting	Ondergrens	Bovengrens
	% internetgebruikers		
Sterke wachtwoorden gebruiken (voldoende en verschillende letters/tekens)			
Vaak	59,9	59,4	60,4
Soms	24,8	24,3	25,3
Zelden	7,6	7,3	7,9
Nooit	5,3	5,0	5,5
Gebruik maken van een wachtwoordmanager			
Vaak	8,6	8,3	8,9
Soms	7,7	7,4	8,0
Zelden	9,0	8,7	9,4
Nooit	66,9	66,3	67,4
Verschillende wachtwoorden gebruiken			
Vaak	40,6	40,1	41,2
Soms	33,7	33,1	34,2
Zelden	14,0	13,7	14,4
Nooit	8,7	8,4	9,0
Het instellen of wijzigen van het wachtwoord van uw Wi-Fi netwerk			
Vaak	8,6	8,3	8,9
Soms	17,4	17,0	17,8
Zelden	21,1	20,6	21,5
Nooit	47,2	46,6	47,7

[1] Personen van 12 jaar of ouder met internetgebruik.
Bron: CBS; pilot onderzoek naar Digitale Veiligheid & Criminaliteit, 2018.

16. Andere vormen van internetveiligheid, 2018[1)]

	Schatting	Ondergrens	Bovengrens
Kunt u aangeven hoe vaak u doorgaans onderstaande zaken doet?	**% internetgebruikers**		
Online bankzaken of betalingen doen via een Wi-Fi netwerk op openbare plekken			
Altijd	4,8	4,5	5,0
Vaak	11,3	11,0	11,7
Soms	17,2	16,8	17,7
Nooit	63,0	62,5	63,6
E-mails openen van onbekende afzenders			
Altijd	2,4	2,3	2,6
Vaak	13,0	12,6	13,3
Soms	34,4	33,8	34,9
Nooit	47,9	47,4	48,5
Bestanden of documenten openen van onbekende afzenders			
Altijd	1,0	0,9	1,2
Vaak	5,7	5,4	5,9
Soms	19,5	19,1	20,0
Nooit	71,2	70,7	71,7

1) Personen van 12 jaar of ouder met internetgebruik.
Bron: CBS; pilot onderzoek naar Digitale Veiligheid & Criminaliteit, 2018.

Onderzoeks-verantwoording

Design en weging

Maatschappelijk gezien is er veel behoefte aan informatie rondom slachtofferschap van de verschillende digitale delictsvormen zoals hacken, ransomware, cyberpesten, identiteitsfraude, koop- en verkoopfraude, en daarnaast ook de impact ervan op slachtoffers in zowel financiële als emotionele zin. Ook is er behoefte aan meer gegevens rondom cybersecurity; wat doen mensen zelf om te voorkomen dat zij slachtoffer worden van digitale criminaliteit?

Niet alle digitale incidenten worden gezien als delicten (strafbare feiten). Daarnaast valt er binnen de delicten vooral onderscheid te maken tussen hacken en oplichting/fraude. Het belangrijkste doel van het pilotonderzoek 'Digitale Veiligheid & Criminaliteit' was dan ook meer inzicht te krijgen in de verschillende vormen van digitale criminaliteit in Nederland. Hiertoe is geprobeerd de vraagstellingen zoals deze in de Veiligheidsmonitor worden gehanteerd te verbeteren, en ook vraagstellingen te ontwikkelen voor nieuwe digitale delictsvormen zoals die via het internet tot stand komen.
In deze bijlage worden de opzet en de uitvoering van het pilotonderzoek Digitale Veiligheid & Criminaliteit beknopt besproken. Achtereenvolgens komen aan de orde:

1. Vragenlijst
2. Onderzoeksdesign en veldwerk
3. Steekproef
4. Dataverwerking
5. Weging
6. Betrouwbaarheid.

Ad 1) Vragenlijst

De vragenlijst die voor dit pilotonderzoek is ontwikkeld gaat enerzijds in op het internetgebruik en de ervaren internetveiligheid van personen en anderzijds op slachtofferschap van digitale criminaliteit. Voor het deel over het internetgebruik en de ervaren internetveiligheid heeft het onderzoek ICT-gebruik huishoudens en personen als basis gediend, en voor het deel over slachtofferschap was de Veiligheidsmonitor vertrekpunt. Beide onderzoeken worden al langere tijd door het CBS uitgevoerd. In deze tijd is kennis opgedaan over welke vragen goed en minder goed werken, en ook over welke informatie ontbreekt. Om de informatiebehoefte zo breed mogelijk af te dekken, is ook gekeken naar bestaande onderzoeken, zowel nationaal als internationaal, en rapporten en relevante publicaties op dit terrein. Uit deze veelheid aan informatie is door het CBS een conceptvragenlijst samengesteld en als eerste stap intern collegiaal besproken. Hierna is contact gezocht met andere partijen om de conceptvragenlijst inhoudelijk te verbeteren. De vragenlijst is besproken met experts van de politie, diverse afdelingen van het ministerie van Justitie en Veiligheid en het WODC. Daarnaast is deze ter beoordeling ook voorgelegd aan specialisten op het gebied van cybercrime zoals Rutger Leukfeldt die onder andere als lector verbonden is aan de Haagse Hooge School en Marianne Junger, werkzaam aan de Universiteit Twente.

De hieruit voortvloeiende vragenlijst is door het Vragenlab van het CBS aan een aantal vrijwilligers voorgelegd en getest op zaken als taalgebruik, begrijpelijkheid, volgorde van vragen, routing, enzovoort. Op basis van de bevindingen zijn de afzonderlijke vragen verder aangepast. De eindvragenlijst is vervolgens geprogrammeerd in Blaise 5 (door

het CBS ontwikkelde software voor elektronische vragenlijsten) en getest om fouten in vraagstellingen en routing te achterhalen.

De vragen over internetgebruik en internetveiligheid zijn in principe aan iedere respondent gesteld. Bij de vragen over slachtofferschap wordt bij iedere delictsvorm telkens eerst gevraagd of de respondent hiervan slachtoffer is geweest. Indien dit het geval is, worden enkele vervolgvragen gesteld over bijvoorbeeld de impact ervan en of er melding en aangifte is gedaan. Dit principe wordt ook bij de Veiligheidsmonitor gebruikt. Daarbij wordt geregeld gebruik gemaakt van open vragen, zodat respondenten eigen antwoorden konden formuleren en zaken konden aandragen. Deze informatie kan eventueel worden gebruikt voor het maken van de beoogde output. De vragenlijst bestaat uit de volgende vraagblokken:

Digitale veiligheid
- Internetgebruik en -activiteiten
- Privacy en beveiliging persoonsgegevens
- Internetveiligheid

Ervaren digitale criminaiteit
- Fraude in het betalingsverkeer
- Aan- en verkoopfraude
- Andere vormen van fraude
- Computercriminaliteit
- Online psychisch geweld
- Andere online incidenten

Slotvragen (vragen aan niet-gebruikers van het internet); de reden waarom zij hier geen gebruik van maken en of zij in de afgelopen vijf jaar dan wel in de afgelopen twaalf maanden te maken hebben gehad met fraude of oplichting)

Achtergrondkenmerken (vragen over maatschappelijke positie, onderwijsniveau, enzovoort)

Een tekstversie van de vragenlijst is online te raadplegen (CBS, 2019c).

Ad 2) Onderzoeksdesign en veldwerk

De onderzoekspopulatie betreft personen van 12 jaar of ouder in particuliere huishoudens in Nederland. Deze populatie komt overeen met die in het onderzoek 'ICT-gebruik huishoudens en personen'. Het is belangrijk om jongeren mee te nemen in dit onderzoek omdat zij naar verhouding veel gebruik maken van het internet en daardoor een grotere kans lopen om in aanraking te komen met allerlei vormen van digitale criminaliteit.

Voor het verzamelen van de onderzoeksgegevens is gekozen voor alleen Cawi (Computer-assisted web interviewing), dat wil zeggen dat steekproefpersonen uitsluitend via het internet een vragenlijst konden invullen. Middels een aanschrijfbrief en een bijgevoegde folder zijn alle getrokken steekproefpersonen benaderd met het verzoek tot deelname. Daarnaast is het onderzoek ook aangekondigd via de website van het CBS en via enkele vormen van sociale media. Hieronder volgt een opsomming van een aantal randvoorwaarden die bij het veldwerk zijn aangehouden:

1. De doelpopulatie bestaat uit personen van 12 jaar of ouder in particuliere huishoudens in Nederland.
2. Steekproefpersonen ontvangen een aanschrijfbrief en een folder met het verzoek om

de vragenlijst via internet (Cawi) in te vullen. In de brief zijn een inlogcode en een gebruikersnummer opgenomen. Daarnaast wordt in de brief ingegaan op het doel van het onderzoek. De folder is toegespitst op het onderwerp digitale criminaliteit. Twee weken na de verzending van de aanschrijfbrief wordt een rappelbrief verstuurd naar degenen die op dat moment nog niet hebben gerespondeerd. Weer twee weken later wordt nogmaals een rappelbrief verzonden.

3. Er wordt gebruik gemaakt van conditionele kansincentives. Respondenten hebben door deel te nemen kans op het winnen van een Ipad, en kunnen meteen aan het einde van het invullen van de vragenlijst zien of ze deze gewonnen hebben.
4. Het aantal uit te zetten (bruto) steekproefeenheden omvat 100 000 personen.
5. Het veldwerk wordt uitgezet in vijf porties in de periode oktober tot en met december 2018.
6. De verwachte respons bedraagt 30 procent. De responskansen voor de verse steekproef zijn gebaseerd op realisatiecijfers van eerdere CBS-onderzoeken.
7. De steekproefpersonen worden per aanschrijfbrief benaderd voor deelname via internet (Cawi).
8. De vragenlijst wordt uitsluiten aangeboden in de Nederlandse taal.
9. De vragenlijst is gebouwd in een lay-out die geschikt is voor het invullen met een smartphone.
10. De aanschrijfbrief en rappelbrieven worden samengesteld op basis van een standaard opmaak. Daarnaast hanteert het CBS het beleid dat voor personen van 12 tot en met 15 jaar toestemming wordt gevraagd aan de ouders of verzorgers om deel te mogen nemen aan het onderzoek. Vanaf 16 jaar wordt dit niet meer gedaan. Er worden dus afzonderlijke brieven gehanteerd voor beide leeftijdscategorieën.
11. De medewerkers van het CBS-Contact Center Inbound krijgen een korte instructie over het onderzoek, zodat zij vragen van respondenten kunnen beantwoorden en hen op weg kunnen helpen waar nodig. Ook is op de CBS-website informatie geplaatst voor respondenten over dit onderzoek.

Ad 3) Steekproef

De beoogde doelpopulatie wordt verkregen door personen in beschouwing te nemen die als ingezetene zijn geregistreerd in de Basisregistratie Personen (BRP), die deel uitmaken van particuliere huishoudens en die minimaal 12 jaar zijn op 1 oktober 2018 (begindatum van het veldwerk). De institutionele bevolking, dat zijn bewoners van inrichtingen, instellingen en tehuizen, wordt niet benaderd.

Er wordt één personensteekproef getrokken. Gezien de omvang van de te trekken steekproef (100 000 personen) kan de steekproef niet uit één steekproefkader worden getrokken. Het 'evenredig' deel van de steekproef wordt getrokken uit het kader dat standaard door het CBS wordt gebruikt voor personensteekproeven waarvoor de waarneming in 2018 start (het reguliere kader), terwijl het 'aanvullend' deel wordt getrokken uit een reservekader. Er is geen overlap tussen de kaders.

De te trekken steekproef is een gestratificeerde tweetrapssteekproef. In de eerste trap worden per coropgebied deelgemeenten geselecteerd via een systematisch steekproefontwerp met kansen evenredig aan de inwoneraantallen. De benodigde steekproef voor het DVC-onderzoek is zo groot dat alle deelgemeenten zelfselecterend zijn. De tweede trap is een enkelvoudig aselecte steekproef van personen in de geselecteerde deelgemeenten, met omvangen per deelgemeente zoals vastgesteld in de eerste trap. Op deze manier ontstaat een zelfwegende steekproef, dat wil zeggen dat elke persoon die tot de doelpopulatie behoort, dezelfde kans heeft om in de getrokken steekproef te komen.

Verder is besloten om met een aselecte steekproef te werken zonder stratificatie, dus er is geen oververtegenwoordiging van bepaalde groepen. De uit te zetten steekproef wordt verdeeld over vijf porties van 20 000 personen.

Respons

In 2018 werden 100 000 personen voor deelname aan het pliotonderzoek, Digitale Veiligheid en Criminaliteit, benaderd. In totaal hebben 38 148 personen meegedaan, een responspercentage van 38,1 procent.

Tabel 1 toont de verdeling van de achtergrondkenmerken voor de Nederlandse populatie van 12 jaar en ouder voor wat betreft de uitgezette steekproef en de respons. Dit geeft een beeld van de representativiteit van de responderende groep. De kolom met verschillen laat zien welke bevolkingsgroepen over- of ondervertegenwoordigd zijn.

1. Verdelingen uitgezette steekproefpopulatie en respons naar achtergrondkenmerken, 2018

	Uitzet steekproef (%)	Totaal respons (%)	Verschil in %-punten tussen uitzet en respons
Geslacht			
Man	49,5	50,6	1,1
Vrouw	50,5	49,4	–1,1
Leeftijd			
12 tot 18 jaar	7,8	9,9	2,1
18 tot 25 jaar	9,5	7,2	–2,3
25 tot 35 jaar	14,7	11,1	–3,6
35 tot 45 jaar	13,8	12,2	–1,6
45 tot 55 jaar	16,6	15,9	–0,7
55 tot 65 jaar	15,6	18,5	2,9
65 tot 75 jaar	13,0	17,3	4,3
75 jaar of ouder	9,1	7,9	–1,2
Herkomst			
Nederlandse achtergrond	77,7	84,3	6,6
Migratie-achtergrond, westers	10,2	8,8	–1,4
Migratie-achtergrond, niet-westers	12,1	6,9	–5,2
Type huishouden			
Eenpersoonshuishouden	20,6	16,1	–4,5
Ongehuwd stel zonder kinderen	7,9	7,7	–0,2
Gehuwd stel zonder kinderen	22,9	30,1	7,2
Ongehuwd stel met kinderen	7,5	6,8	–0,7
Gehuwd stel met kinderen	32,4	33,0	0,6
Eenouder huishouden	7,7	5,7	–2,0
Overig of onbekend huishouden	0,7	0,4	–0,3
Inkomenskwintiel van huishouden			
Eerste kwintiel (laagste inkomens)	11,6	7,6	–4,0
Tweede kwintiel	15,2	12,3	–2,9
Derde kwintiel	19,2	19,7	0,5
Vierde kwintiel	24,3	26,5	2,2
Vijfde kwintiel (hoogste inkomens)	29,7	33,9	4,2
Provincie			
Groningen	3,4	3,5	0,1
Friesland	3,8	3,8	0,0
Drenthe	2,8	2,9	0,1
Overijssel	6,7	7,2	0,5
Flevoland	2,4	2,2	–0,2
Gelderland	12,0	12,8	0,8
Utrecht	7,5	7,8	0,3
Noord-Holland	16,5	15,1	–1,4
Zuid-Holland	21,4	20,1	–1,3
Zeeland	2,2	2,4	0,2
Noord-Brabant	14,7	15,4	0,7
Limburg	6,5	7,0	0,3

In vrijwel elk surveyonderzoek is er sprake van selectiviteit in de respons. Dit is ook het geval bij het pilotonderzoek Digitale Veiligheid & Criminaliteit. Mannen responderen in dit onderzoek beter dan vrouwen en zijn daardoor iets oververtegenwoordigd. Bij leeftijd is de jongste leeftijdsgroep van 12 tot 18 jaar oververtegenwoordigd is, net als de 55- tot 75-jarigen. De overige leeftijdsgroepen zijn ondervertegenwoordigd. Andere groepen die zijn ondervertegenwoordigd zijn personen met een (niet-westerse) migratieachtergrond, eenpersoonshuishoudens, eenoudergezinnen en huisoudens in de laagste twee inkomenskwartielen. Personen met een Nederlandse achtergrond, personen die deel uitmaken van een gehuwd stel zonder kinderen, en huishouden in het hoogste inkomenskwartiel zijn iets oververtegenwoordigd. In regionaal opzicht zijn er minder grote verschillen zichtbaar, hoewel personen in Noord-Holland en Zuid-Holland iets minder goed vertegenwoordigd zijn dan personen in de overige provincies. Om de respons representatief te maken voor de doelpopulatie is gebruik gemaakt van een weegmodel.

Ad 4) Dataverwerking

Het dataproces omvat alle stappen die nodig zijn om van de ruwe onderzoeksgegevens (dat wil zeggen de antwoorden die respondenten gegeven hebben op de vragen in de vragenlijst) een onderzoeksbestand te maken waaraan plausibele statistische informatie te ontlenen is. De verwerking van de data is zoveel mogelijk geautomatiseerd. Het dataproces voor het pilotonderzoek Digitale veiligheid & Criminaliteit bestaat uit een aantal functioneel van elkaar te onderscheiden processtappen. Het gaat daarbij om:

- *Ordenen en controleren van de onderzoeksgegevens*
  Nadat het veldwerk is beëindigd zijn alle onderzoeksgegevens van de personen die gerespondeerd hebben geordend aan de hand van het datamodel dat voor de vragenlijst is ontwikkeld. Vervolgens zijn de onderzoeksgegevens bewerkt tot bruikbare microdata voor verdere statistische bewerkingen, bijvoorbeeld in het geval van vragen met meerkeuze-antwoorden, en worden alle variabelen voorzien van labels. Daarna zijn alle onderzoeksgegevens samengevoegd tot één SPSS-microdatabestand, waarna er consistentie- en volledigheidscontroles op de data zijn uitgevoerd.
- *Koppeling onderzoeksgegevens met administratieve registers*
  Tijdens deze processtap zijn alle verzamelde en gecontroleerde onderzoeksgegevens gekoppeld met de gegevens uit de Basisregistratie Personen (BRP) en het Sociaal Statistisch Bestand (SSB). Het resultaat is een bestand dat geschikt is voor onderzoeksdoeleinden.
- *Afleiden van publicatievariabelen*
  Vervolgens zijn er publicatievariabelen afgeleid op basis van de informatie in het onderzoeksbestand. Dit betreft de slachtofferschapsvariabelen in het bijzonder. Hierbij is ook gebruik gemaakt van de informatie verkregen middels de open vragen Deze variabelen vormen de grondslag voor deze publicatie.
- *Weging*
  Door uitval en non-respons is er sprake van selectiviteit bij de verkregen onderzoeksgegevens. Op basis van de beschikbare steekproefgegevens en registerkenmerken is hiervoor gecorrigeerd door de onderzoeksgegevens te herwegen naar populatiekenmerken. Hierna volgt een korte beschrijving van de weging van het pilotonderzoek Digitale Veiligheid & Criminaliteit (DVC).

Ad 5) Weging

Startgewichten en weegmethode

De steekproef voor het DVC-onderzoek was bij benadering zelfwegend, dat wil zeggen dat iedere persoon in de doorsnede van het steekproefkader en doelpopulatie ongeveer

dezelfde kans had om in de steekproef getrokken te worden. De startgewichten voor een weging worden doorgaans evenredig gekozen met de reciproke van de trekkingskansen. Bij de weging van het DVC-onderzoek had daarom ieder te wegen record in de respons een startgewicht gelijk aan het quotiënt van populatieomvang (14 866 576) en responsomvang (38 148), i.e. startgewicht ≈ 389,71. De weging zelf is uitgevoerd met het R-package weeg, een uitbreiding op survey; hierbij is gebruikgemaakt van de weeg-implementatie van de lineaire regressieschatter.

Weegmodel

Vanwege de overeenkomst in thema heeft het weegmodel van het onderzoek ICT-gebruik huishoudens en personen als inspiratie gediend voor de weegfactor van het DVC-onderzoek. Verschillende termen in dat model zijn specifiek voor het ICT-onderzoek en daarom weggelaten. Verder staat de grotere responsomvang van het DVC-onderzoek een meer gedetailleerde uitsplitsing van leeftijd toe.

In het weegmodel voor de Veiligheidsmonitor worden verschillende termen uitgekruist met politiedistrict, te weten *geslacht x leeftijd, huishoudgrootte, stedelijkheid, herkomst, en gestandaardiseerd besteedbaar huishoudensinkomen*.

Het uiteindelijk gekozen weegmodel bestaat uit de basis, aangevuld met uitkruisingen van geslacht en leeftijd in drie categorieën met politiedistrict, en met uitkruisingen van regionale kenmerken met herkomstindikkingen:
geslacht(2) x { *leeftijd*(18) + *leeftijd*(4) x *burgerlijke staat*(2) + *herkomst*(7) } + *burgerlijke staat*(4) +
regionale eenheid(10) x { *herkomst*(3) + *inkomen*(5) + *huishoudgrootte*(5) + *stedelijkheid*(5) + *geslacht*(2) x *leeftijd*(7) } + *politiedistrict*(43) x { *geslacht*(2) + *leeftijd*(3) } +
provincie(16) x *herkomst*(2) + *grote steden*(5) x *herkomst*(3) + *grote steden*(2) x *herkomst*(7)

Weegvariabelen

Hier volgt een opsomming van de in de hiervoor beschreven weegmodellen gebruikte variabelen:

- *geslacht:* man (1) of vrouw (2).
- *leeftijd* wordt op meerdere manieren ingedikt en meegenomen in het weegmodel. Indikkingen zijn als volgt:
  - *leeftijd*(3): 12 tot 35 jaar, 35 tot 55 jaar, 55 jaar of ouder
  - *leeftijd*(4): 12 tot 35 jaar, 35 tot 55 jaar, 55 tot 75 jaar, 75 jaar of ouder
  - *leeftijd*(7): 12 tot 25 jaar, 25 tot 35 jaar, ..., 65 tot 75 jaar, 75 jaar of ouder
  - *leeftijd*(18): 12 tot 14 jaar, 14 tot 16 jaar, 16 tot 18 jaar, 18 tot 20 jaar, 20 tot 25 jaar, ..., 80 tot 85 jaar, 85 jaar of ouder
- *burgerlijke staat* (2/4): gehuwd (1) vs. ongehuwd (2), of in vieren als gehuwd (incl. partnerschap) (1), gescheiden (2), verweduwd (3), of nooit gehuwd (4).
- *herkomst:* onbekende herkomst is ingedeeld bij personen met een Nederlandse achtergrond. Indikkingen zijn als volgt:
  - *herkomst*(2): Nederlandse, of een niet-Nederlandse migratieachtergrond;
  - *herkomst*(3): persoon van Nederlandse of met westerse, of niet-westerse migratieachtergrond;
  - *herkomst*(7): persoon van Nederlandse, westerse, Marokkaanse, Turkse, Surinaamse, Antilliaanse, of anderszins met een niet-westerse migratie-achtergrond;

- *inkomen:* indikking in kwintielen van gestandaardiseerd besteedbaar huishoudinkomen (in percentielen) uit het voorlopig inkomensbestand 2017, met onbekende inkomens in laagste kwintiel;
- *huishoudgrootte:* aantal personen in huishouden, tot vijf of meer, met onbekende omvang bij 'vijf of meer'.
- *stedelijkheid van de gemeente:* zeer sterk, sterk, matig, weinig, of niet stedelijk;
- *provincie:* standaard regionale indeling 'provincieplus' in zestienen (provincie, of gemeente indien één van de vier grootste gemeenten);
- *landsdeel:* standaard regionale indeling in Noord-, Oost-, West-, en Zuid-Nederland;
- *grote steden*(2/5). In vijven als Amsterdam (1), Rotterdam (2), Den Haag (3), Utrecht (4), of elders in Nederland (0), en in tweeën als indicatorvariabele voor grootste vier gemeenten.

Een meer gedetailleerde nota over de uitgevoerde weging van het onderzoek Digitale Veiligheid & Criminaliteit is eventueel op aanvraag beschikbaar.

Ad 6) Betrouwbaarheidsmarges

Het onderzoek Digitale veiligheid en criminaliteit is uitgevoerd bij een steekproef. Dit betekent dat de weergegeven percentages schattingen betreffen. Om een indicatie te geven van de precisie van deze schattingen worden in de bijlagetabellen ook de 95%-betrouwbaarheidsintervallen in de vorm van een boven- en ondergrens weergegeven. Deze intervallen bevatten met 95% zekerheid de werkelijke (onbekende) waarde. De betrouwbaarheidsintervallen zijn berekend met Complex Samples (in SPSS).
Indien een schatting 0 procent is, heeft geen enkele respondent in het onderzoek dit antwoord gegeven. Dit betekent niet dat dit helemaal niet voorkomt in de populatie.

Methodologische toelichting slachto erschap digitale criminaliteit

Met dit onderzoek is het thema slachtofferschap van digitale criminaliteit onder burgers voor het eerst in Nederland gedetailleerd, breed en op zeer grote schaal onderzocht. Er is in overleg met diverse experts een nieuwe vragenlijst ontwikkeld en met de daarmee verzamelde data is de informatie zoals beschreven in dit rapport samengesteld. In deze bijlage wordt uitvoerig beschreven hoe en waarom welke beslissingen zijn genomen. Het thema 'slachtofferschap van digitale criminaliteit' en het meten daarvan is erg complex. Bij het analyseren van de gegevens bleek dan ook dat de in het onderzoek gebruikte vraagstellingen niet altijd perfect waren. Daardoor moesten soms keuzes worden gemaakt. Deze worden ook in deze bijlage beschreven. Allereerst wordt in deze bijlage ingegaan op de indeling van slachtofferschap van digitale criminaliteit en onderliggende delicten (paragraaf 1). Daarna volgen enkele algemene punten die bij het lezen van dit rapport van belang zijn (paragraaf 2). Vervolgens wordt per delict een beschrijving gegeven van eventueel ondervonden problemen (paragraaf 3). Afgesloten wordt met een verantwoording van niet in dit rapport opgenomen informatie waar in de enquête wel vragen over gesteld zijn (paragraaf 4).

De in het onderzoek gehanteerde vraagstellingen, waar ook in deze bijlage naar verwezen wordt, staan in de vragenlijst Digitale Veiligheid en Criminaliteit 2018. (CBS, 2019c).

1. Indeling en operationalisatie van slachto erschap van digitale criminaliteit

Slachtofferschap van digitale criminaliteit is in dit onderzoek ingedeeld in vijf hoofdgroepen. Deze zijn: hacken, vermogensdelicten, interpersoonlijke niet-seksuele incidenten, interpersoonlijke seksuele incidenten en identiteitsfraude zonder financiële schade. De hoofdgroepen corresponderen grotendeels met de vragenblokken D tot en met F in de vragenlijst. Daarnaast wordt een inschatting gegeven van de omvang van het ontvangen van phishing.

Hacken (hoofdstuk 3)
In de vragenlijst is specifiek alleen naar hacks gevraagd waarbij gegevens van de respondent zijn verstoord, geblokkeerd of gestolen. Spontane antwoorden elders in de open antwoordmogelijkheden van de vragenlijst dat er sprake was van 'hacken' (van social media, e-mail, device, maar zonder verdere informatie) zijn niet in het cijfer meegenomen omdat we niet weten wat de gevolgen waren. Indien bij een andere hoofdgroep van delicten is aangegeven dat er een vorm van hacken aan vooraf is gegaan, is het hackdelict ondergebracht bij de subcategorie 'hacken als modus operandi'. De detailinformatie van deze hackdelicten is beschreven in het hoofdstuk van het betreffende delict.

Vermogensdelicten (hoofdstuk 4)
Hiertoe behoren alle delicten die zijn gepleegd met een financieel motief, en waarbij de daders ook succes hadden en dus geld hebben verdiend. Hierbij zijn alle respondenten

gerekend die in een van de 'fraude'-blokken (blokken D) van de vragenlijst aangaven dat ze financiële schade hadden, inclusief degenen bij wie de schade (deels) is vergoed. Tevens zijn de delicten ransomware en cryptoware (blok E) en de slachtoffers van chantage of bedreiging zonder geweld (blok F) hiertoe gerekend, indien de slachtoffers aangaven dat ze financiële schade hadden. De antwoorden 'weet niet' zijn gerekend als 'geen financiële schade'. In blok D3 (andere vormen van fraude) is de vraag naar financiële schade iets anders gesteld. Respondenten konden daar aangeven of ze 'er geld mee kwijt zijn geraakt'. Degenen die antwoordden dat ze er geen geld mee kwijt zijn geraakt, hebben wellicht de schade volledig vergoed gekregen en zijn er dus uiteindelijk geen geld mee kwijt geraakt. Zij zijn in feite wel slachtoffer van een vermogensdelict, maar zijn hiertoe niet meegerekend. Het slachtofferschap van deze delicten kan hierdoor wat onderschat zijn.

Interpersoonlijke incidenten (hoofdstukken 5 en 6)
Dit zijn incidenten die behoren tot laster, stalken en bedreiging met geweld (blok F). We gebruiken hier de term 'incidenten' omdat het vaak om lichte vormen van slachtofferschap gaat. Aan de hand van de vraag 'Was er de laatste keer sprake van een seksuele (bij-) bedoeling?' is slachtofferschap opgesplitst in de twee hoofdcategorieën 'seksueel' en 'niet-seksueel'. Deze informatie is alleen beschikbaar voor het laatste incident. Slachtoffers die zowel seksuele als niet-seksuele incidenten ondervonden (dit kan op basis van de vraagstelling niet worden vastgesteld) zijn tot de seksuele incidenten gerekend.

Identiteitsfraude zonder nancieel verlies (hoofdstuk 7)
Dit zijn delicten waarbij de dader geen geld heeft verdiend (geoperationaliseerd als: het slachtoffer had geen financiële schade), maar wél persoons-, of bankgegevens van het slachtoffer heeft misbruikt door zich voor te doen als het slachtoffer.

Phishing (hoofdstuk 8)
Het slechts ontvangen van phishing wordt niet gezien als slachtofferschap, omdat mensen er niet zijn ingetrapt en nog geen gevolgen ondervinden. Er is ook niet expliciet naar het hele scala aan phishingactiviteiten gevraagd omdat dat niet het doel van het onderzoek was. Toch is het mogelijk een inschatting te geven van de omvang en daarmee de slaagkans van deze criminele activiteiten. Voor phishing als totaal kan echter alleen een schatting van de minimale omvang van het 'slechts ontvangen' worden gegeven en dus alleen een maximale slaagkans. Deze totale (minimale) omvang van phishing is berekend door alle vormen van phishing die door de hele vragenlijst heen door respondenten zijn opgegeven bij elkaar te tellen. In hoofdstuk 8 is iets dieper ingegaan op enkele vormen van phishing.

2. Enkele algemene punten

Verborgen slachto erschap
Verborgen slachtofferschap is niet gemeten en kan ook niet gemeten worden. Hierbij gaat het bijvoorbeeld om hacks waarvan het slachtoffer de gevolgen (nog) niet heeft gemerkt, nepboetes die niet als dusdanig herkend zijn en gewoon betaald zijn en persoonlijke incidenten (roddels, pesterijen) waarvan mensen geen last hebben gehad.

Zeer recente delicten
De enquête vraagt naar slachtofferschap in de afgelopen 12 maanden. Enkele respondenten zullen op het moment van enquêtering zeer recent slachtoffer zijn geweest.

Bij de vragen over vergoeding, melding en aangifte ontbrak een antwoordoptie van de strekking 'weet ik nog niet' of 'ben ik nog van plan'. Deze cijfers zullen daarom iets onderschat zijn.

Extra informatie uit open vragen

Omdat deze vragenlijst nieuw is en over een relatief onontgonnen en complex thema gaat, zijn er door de hele vragenlijst veel open antwoordmogelijkheden aangeboden. Dit maakte de analyse tijdrovender, maar geeft wel een beter beeld van wat er werkelijk gebeurd is. Indien uit een opmerking van de respondent blijkt dat hij of zij de vraag niet goed begrepen heeft is hiervoor gecorrigeerd in de analyses. Het kwam bijvoorbeeld vaak voor dat het slachtoffer bij de vragen over fraude in het betalingsverkeer (blok D1) aangaf dat het slechts om het ontvangen van phishing ging. In die gevallen zijn deze voorvallen overgeheveld naar 'phishing'.

Daarnaast zijn aan de hand van antwoorden op de open vragen enkele extra categorieën samengesteld bij de detailinformatie over de delicten. In iedere tabel is weergegeven welke categorieën het betreft. Het is evident dat de cijfers bij deze niet vooraf aangeboden categorieën een onderschatting zullen opleveren, omdat niet iedere respondent die het betreft eraan denkt dit bij de open vraag aan te geven.

'Nieuw' ontdekte delicten

In blok G is gevraagd naar andere online incidenten die nog niet eerder in de vragenlijst zijn behandeld. Hierin werden, naast hacken en phishing, veel incidenten opgegeven die al eerder aan bod zijn gekomen. Enkele respondenten hebben gemeld dat hen verzocht is katvanger te zijn. Katvangers zijn mensen wiens naam, adres of bankrekening wordt gebruikt door oplichters om fraude mee te plegen. Dit komt zo sporadisch voor dat het niet als apart delict is opgenomen. Het enige in de open antwoordmogelijkheid gemelde delict waar in de vragenlijst niet expliciet naar gevraagd is en dat als apart vermogensdelict is opgenomen, is whaling, oftewel het 'verzoek om geld door een zogenaamde bekende, bijvoorbeeld via whatsapp'. 15 Respondenten meldden dat ze dit verzoek hebben ontvangen; één van hen werd slachtoffer. We verwachten dat de respondenten die dit is overkomen dit zeker zouden melden in de vragenlijst omdat het zo'n aangrijpend voorval is. Ondanks het feit dat we hier niet expliciet naar hebben gevraagd, verwachten we dus dat dit delict in 2018 inderdaad nog erg weinig voorkwam.

3. Opmerkingen per hoofdstuk

Paragraaf 4.1 en hoofdstuk 7: fraude via het betalingsverkeer

Dit betreft vormen van identiteitsfraude waarbij de dader er financieel op vooruit is gegaan door gebruik te maken van iemands persoons- of bankgegevens. We hebben dit delict verdeeld in twee hoofdgroepen aan de hand van de vraag naar wat er precies is gebeurd (D1_6). Bij de eerste had de dader toegang tot de rekening van het slachtoffer en heeft hij of zij er geld van opgenomen, overgeschreven of er betalingen mee gedaan. Bij de tweede heeft de dader een lening, abonnement, goederen of diensten verkregen op naam van het slachtoffer. Het bestellen van goederen of diensten werd vaak opgegeven bij de open vraag. Slachtoffers die opgeven dat ze financiële schade hebben geleden zijn gerekend tot de vermogensslachtoffers (paragraaf 4.1), slachtoffers die geen financiële schade hebben geleden tot de slachtoffers van identiteitsfraude zonder financiële schade (hoofdstuk 7). Bij hen bleef het dus bij een poging.

Een deel van deze fraude zal via phishing zijn gegaan. Daar is in de enquête (bij vraag D1_5) niet expliciet naar gevraagd en antwoordcategorie 7 beslaat niet alle vormen van phishing. Het totaal dat door phishing is gebeurd is benaderd door het totaal van de antwoordcategorieën 1 en 2 uit vraag D1_5 waarbij de respondent bij de vervolgvragen tevens aangaf dat de dader geen bekende in real life was, plus de antwoordcategorieën 7 en 8 en de antwoorden 'phishing' op de open vraag.
Het totaal waar een hack aan vooraf ging betreft de antwoordcategorieën 9, 10, 11 en 12 uit vraag D1_5, plus de antwoorden 'gehackt' op de open vraag.

Vraag D1_5 Hoe is men (vermoedelijk) de laatste keer aan de persoonlijke gegevens gekomen?

- ☐ 1. Ik had mijn bankpas in goed vertrouwen ter beschikking gesteld
- ☐ 2. Ik had mijn persoonlijke gegevens in goed vertrouwen aan een bekende ter beschikking gesteld
- ☐ 3. Overnemen van mijn identiteit door diefstal van paspoort of ID kaart
- ☐ 4. Diefstal van bankpas/creditcard
- ☐ 5. Skimmen van bankpas/creditcard
- ☐ 6. Scannen van mijn mobiele telefoon, bijvoorbeeld door contactloos betalen (ook wel shimming genoemd)
- ☐ 7. Via een e-mail en vervolgens doorgeleid naar een website die nep of onbetrouwbaar bleek te zijn (phishing/pharming)
- ☐ 8. Ik had mijn gegevens doorgegeven op een webshop of via de telefoon
- ☐ 9. Kopiëren van mijn persoonlijke gegevens via het internet door in te breken op mijn apparaat (bv. computer/tablet/telefoon), social media of e-mailaccount
- ☐ 10. Via malware (bv. een computervirus of trojan horse)
- ☐ 11. Via het registreren van mijn toetsaanslagen (key logging)
- ☐ 12. Door computerinbraak bij een bedrijf of bank waar mijn persoonlijke gegevens bekend zijn
- ☐ 13. Op een andere wijze, namelijk: ...
- ☐ 14. Weet niet

Paragraaf 4.2: fraude bij online handel

De vraag naar slachtofferschap van fraude online handel blijkt bij sommige respondenten verkeerd geïnterpreteerd te zijn. Uit de open antwoordopties blijkt dat enkele personen die iets besteld hebben en niet ontvangen, maar daarbij wél het geld terugkregen door de verkoper, deze vraag hebben bevestigd. Dit blijkt ook uit de vraag over financiële schade (D2_9) in combinatie met de manier van betalen (D2_8). Daarom zijn een aantal 'slachtoffers' niet meegeteld in het slachtofferpercentage. Dit betreft degenen die aangaven dat de schade helemaal vergoed is terwijl het product niét via PayPall of creditcard was betaald. Hierbij zijn een onbekend aantal slachtoffers die via gelijk oversteken hebben betaald onterecht niet meegenomen, maar ook een onbekend aantal personen die het geld teruggestort kregen door de verkoper omdat het product niet geleverd kon worden wél.

Daarnaast zijn respondenten die aangaven dat ze géén financiële schade hadden en degenen die zeggen dit (nog) niet te weten niet als slachtoffer gerekend. Mogelijk wachtten laatstgenoemden nog op het bestelde product of op teruggave van hun geld door de verkoper. Ook zijn degenen die aangeven dat ze de financiële schade gedeeltelijk terug hebben gekregen niet als slachtoffer meegerekend, aangezien oplichters dit waarschijnlijk niet doen.

Paragraaf 4.3: hoofdstuk 7 en 8, overige vermogensdelicten

In blok D3 is gevraagd naar acht 'overige' vormen van fraude. Deze betreffen vrijwel allemaal fraudevormen waarbij de dader een financieel motief had en de meeste behoren ook tot een vorm van phishing. Bij alle acht delictvormen is de respondent als slachtoffer van een vermogensdelict gerekend indien hij of zij bij de vraag 'is dit u ook in de afgelopen 12 maanden weleens overkomen?' aangeeft 'ja, en daar ben ik geld mee kwijtgeraakt'. Dit geeft waarschijnlijk een lichte onderschatting (zie eerdere opmerkingen in deze onderzoeksverantwoording).

Enkele vraagstellingen dekten niet helemaal de lading en/of waren wellicht iets te karig met de voorbeelden (zie verderop). We verwachten echter niet dat dit een grote onderschatting van de percentages slachtofferschap geeft, omdat uit onderzoek blijkt dat slachtoffers de vraagstellingen eerder juist wat ruimer interpreteren.

Bij blok D3 is voor mensen die slachtoffer zijn geworden en daarnaast herhaaldelijk benaderd zijn, onbekend of de detailvragen (vragen D3_4 tot en met D3_13) zijn beantwoord over het voorval waar geld mee is verloren of over een andere poging. In deze gevallen is er vanuit gegaan dat de detailvragen zijn ingevuld voor het schade-incident. Alleen bij het antwoord 'ben bang dat het vaker mis gaat' is de kans groot dat hierbij gedacht is aan de herhaalde pogingen. De meeste slachtoffers zullen er waarschijnlijk niet nóg eens intrappen. Dit item is daarom niet weergegeven bij degenen die schade hebben geleden (hoofdstuk 4), wel bij degenen die alleen phishing hebben ontvangen (hoofdstuk 8).

Hieronder worden de 'overige' vermogensdelicten afzonderlijk besproken.

Nepboete/nepfactuur of nepactie

Als eerste werd gevraagd of de respondent per e-mail een nepboete of nepfactuur heeft ontvangen (D3_1_1). Als tweede is gevraagd of de respondent aan een nepactie heeft meegedaan (D3_1_2). Let wel, bij de tweede vraag gaat het niet om blootstelling aan, maar om daadwerkelijke participatie. Uit de vervolgvragen bleek dat slachtoffers al direct bij de eerste vraag ook aan nepacties en andere nepmails zoals mails van 'banken' dachten. Dit komt waarschijnlijk doordat het de eerste vraag over nepmails was. Deze twee categorieën zijn daarom samengevoegd tot 'nepboete/nepfactuur of nepactie'. Slachtoffers van de traditionele mails van nepbanken behoren tot slachtoffers van fraude in het betalingsverkeer.Omdat er waarschijnlijk veel bankphishingmails zijn opgegeven zonder financiële schade kan echter geen schatting gegeven worden van het aantal personen dat een nepboete/nepfactuur of nepactie heeft ontvangen en er niet zijn ingetrapt. In hoofdstuk 8 zijn alle personen die bij deze vragen hebben opgegeven dat ze er geen geld mee kwijt zijn geraakt samengevoegd met alle andere niet bevraagde vormen van phishing die in de enquête zijn opgegeven en onder de categorie 'overige vormen van phishing' geschaard. Hierover kan dus geen detailinformatie worden geven.

Overige identiteitsfraude

Hier gaat het allereerst om identiteitsfraude voor het aanvragen van zorgvergoeding (D3_1_3). Niet gevraagd is naar de identiteitsfraude die wordt gepleegd bij medische hulp. Ook is gevraagd naar identiteitsfraude bij het plegen van misdrijven (D3_1_4). Bedoeld wordt hier eigenlijk misdrijven als verkeersovertredingen of zwart rijden. Maar uit de vervolgvragen blijkt dat sommige respondenten identiteitsfraude *an sich* al als het 'misdrijf' beschouwen. Bij deze twee vragen is het dus niet duidelijk hoe zijn geïnterpreteerd. Daarom is besloten om beiden samen te nemen als 'overige identiteitsfraude'. Daarbij dient te worden opgemerkt dat er mogelijk nog andere vormen van identiteitsfraude zijn die niet direct betrekking hebben op het betalingsverkeer. Respondenten die aangaven financiële schade te hebben gehad als gevolg van de overige identiteitsfraude, worden gerekend tot de slachtoffers van overige vermogensdelicten. Respondenten zonder financiële schade zijn toegekend aan de categorie 'overige identiteitsfraude zonder financiële schade' (hoofdstuk 7).

Voorschotfraude

Door te vragen of respondenten in de afgelopen 5 jaar weleens per e-mail benaderd zijn met het verzoek een klein bedrag te betalen voor iets dat zij graag zouden willen hebben, zoals een hoofdprijs of een geliefde, om vervolgens om steeds meer geld gevraagd te worden, is het slachtofferschap van voorschotfraude vastgesteld (D31_5). Een tekortkoming bij deze vraag is dat deze vorm van phishing niet altijd via e-mail hoeft te gaan, en dat het niet altijd gaat om iets wat mensen graag zelf zouden willen hebben. Het is de vraag in hoeverre respondenten bijvoorbeeld Nigeriaanse fraude, datingfraude en erfenisfraude meenemen bij deze vorm van phishing.

Microsoftscam

Mensen geven op verschillende plekken in de vragenlijst aan dat ze last hebben gehad van de Microsoftbellers, maar in D3_1_7 wordt er pas echt naar gevraagd. De vraag luidt: 'Is het u in de afgelopen 5 jaar weleens overkomen dat een zogenaamde medewerker van Microsoft belde met de vraag om bepaalde software te installeren op uw computer'. Ondanks het feit dat de fraudeurs niet beginnen met de vraag of ze software mogen installeren op de computer meet deze vraag waarschijnlijk wel alle Microsoftscam.
Er zijn echter ook andere, veel minder voorkomende, maar vergelijkbare vormen van helpdeskfraude, bijvoorbeeld van de 'Belastingdienst' of 'Ziggo'. Deze werden sporadisch genoemd in het blok fraude via het betalingsverkeer en zijn niet gerekend bij de Microsoftscam. Ook heeft de Microsoftscam soms een andere ingang, bijvoorbeeld een pop-up op het computerscherm. Dit wordt met deze vraagstelling niet gemeten.

Wangirifraude

Dit is gemeten met de vraag: `Is het u in de afgelopen 5 jaar weleens overkomen dat u een melding kreeg van een gemiste oproep van een onbekend buitenlands nummer en door terug te bellen kreeg u uiteindelijk te maken met een hoge telefoonrekening?' (D3_1_8). In deze vraag zit het erin trappen impliciet verborgen. In hoeverre mensen benaderd zijn door deze vorm van phishing is daardoor eigenlijk alleen gemeten bij degenen die in de afgelopen 5 jaren slachtoffer zijn geweest. Dat geeft een onderschatting. Aan de andere kant is de verwachting dat bij deze groep te veel phishing is gemeten, omdat personen niet zeker kunnen weten dat zij met Wangiri te maken hadden als zij niet terug hebben gebeld. Het is een vorm van phishing die lastig is te meten. Daarnaast speelt de tekortkoming van de vraag naar 'geld kwijtgeraakt' (zie eerdere opmerkingen hierover) hier waarschijnlijk een grote rol, omdat de telefoonprovider vaak de schade zal betalen.

Afpersingsmails

In blok F (F4) is gevraagd of mensen slachtoffer zijn geweest van chantage, afpersing of bedreiging zonder geweld. Uit de (open) antwoorden bij de vervolgvragen blijkt dat de meeste respondenten het onderscheid hiertussen niet zo goed weten. Bovendien blijkt uit de open vragen dat met name de in 2018 zeer populaire porno-phishingmail hier is opgegeven, en terecht want bij vraag F1 wordt ook gevraagd naar het ontvangen van seksueel getinte berichten. Het zal hier dus meestal niet om serieuze bedreiging of chantage zal gaan. Ook in blok G werd de porno-afpersingsmail vaak genoemd. Al deze categorieën zijn samengevoegd tot 'afpersing' en zijn tot de vermogensdelicten (bij financiële schade) of phishing (bij geen financiële schade) gerekend. Helaas verdwijnen daarbij wel de serieuze bedreigingen zonder geweld en chantages in deze groep.

4. Wel in het onderzoek gevraagd maar niet in dit rapport opgenomen

Slachto erschap in de afgelopen 5 jaar

Ieder vragenblok begint met de vraag of het incident in de afgelopen 5 jaar is gebeurd. Er worden geen cijfers over slachtofferschap in de afgelopen 5 jaar gegeven, omdat het geheugeneffect hierbij een te grote rol speelt. De 5-jaars vraag is alleen gesteld om het 'telescoping-effect' te minimaliseren: uit eerder onderzoek blijkt namelijk dat de respondent vaak geneigd is om delicten uit een verder verleden op te geven indien alleen naar de afgelopen 12 maanden wordt gevraagd. Door eerst naar de afgelopen 5 jaar te vragen kunnen respondenten toch alles opgeven wat ze hebben meegemaakt, en wordt de schatting van het slachtofferschap in de afgelopen 12 maanden nauwkeuriger.

Aantal delicten en herhaald slachto erschap

In onderzoek naar traditionele criminaliteit wordt vaak niet alleen een schatting gegeven van het percentage slachtoffers, maar ook van het aantal delicten dat deze slachtoffers ondervonden hebben. Indien iemands fiets bijvoorbeeld twee keer in hetzelfde jaar werd gestolen telt dit als twee fietsdiefstallen. Bij digitale criminaliteit is het voor de meeste delicten niet mogelijk om een schatting van het totale aantal delicten te geven. Eén delict zorgt namelijk vaak voor veel slachtoffers, en in de enquête meten we het aantal slachtoffers.

Ook is het op grond van de vraagstelling niet mogelijk een schatting te geven van het aantal keren dat iemand slachtoffer is geweest ('herhaald' slachtofferschap). Bij de vraag 'hoe vaak is dit in de afgelopen 12 maanden gebeurd' kan namelijk niet bepaald worden hoe vaak het in feite zelfde delict door het slachtoffer meegeteld wordt. Zo kan een stalker meerdere keren een bericht sturen, of dezelfde stalker stuurt een whatsapp-bericht én beledigt de persoon op social media. Of er is een aantal keer een bedrag van de rekening afgeschreven door dezelfde dader. Daarnaast laat de huidige vraagstelling het niet altijd toe onderscheid te maken tussen het aantal pogingen en het aantal successen.

In dit rapport wordt daarom voor de verschillende delictsoorten enkel het percentage slachtoffers gegeven. Voor de meeste delicten zal dat een goede schatting zijn van het totale slachtofferschap, dus inclusief herhaald slachtofferschap. De slachtofferincidentie is namelijk zo laag en het leereffect zo hoog, dat de kans zeer klein is dat men in hetzelfde jaar vaker dan eens slachtoffer wordt van hetzelfde delict. Alleen bij delicten als aankoopfraude of persoonlijke incidenten zoals laster kan het wel gebeuren dat men vaker slachtoffer wordt.

Manier van gegevensverkrijging door dader(s)
In de hoofdstukken over interpersoonlijke incidenten is niets opgenomen over hoe de daders 'de' gegevens hebben verkregen. Niet alle antwoordcategorieën pasten bij dit type incident. Bovendien zijn 'de gegevens' bij deze incidenten vaak verzonnen. Het gaat immers niet altijd om echte gegevens, maar om roddels, nepfoto's, enzovoort.

Duur van het incident
Dit is eveneens niet opgenomen in de hoofdstukken over interpersoonlijke incidenten omdat de vraagstelling (F17) lastig te interpreteren is: 'U gaf aan dat er in de afgelopen 12 maanden één of meerdere voorvallen waren. Hoe lang was er de laatste keer sprake van online psychisch geweld? (Eenmalig – minder dan 1 week – meer dan 1 week, langer dan 1 maand, enzovoort,'. De vraag is of 'de laatste keer' niet per definitie eenmalig is. Veel gestalkten vulden bijvoorbeeld 'eenmalig' in.

Bekendheid dader(s)
In ieder vragenblok is gevraagd of de dader bekend is bij het slachtoffer. Deze vraag veronderstelt dat het slachtoffer kan weten wie de dader is, bijvoorbeeld omdat hij gepakt is of omdat het sowieso al een bekende was. In de vervolgvraag kan de respondent kiezen uit een aantal 'bekenden'. Deze vragen zijn eigenlijk alleen van toepassing op interpersoonlijke incidenten, waarbij het slachtoffer de dader kan kennen. Bij veel vermogensdelicten, zoals fraude in het betalingsverkeer is deze kans klein. Daarom is alleen in de hoofdstukken over interpersoonlijke incidenten (hoofdstukken 5 en 6) informatie opgenomen over de bekendheid met de dader(s).

Contact met de dader voorafgaande aan het delict
Bij alle delicten (exclusief hacken en fraude bij online handel) is gevraagd hoe vaak er voorafgaande aan het voorval contact met de dader is geweest. Deze vraag is eigenlijk alleen relevant voor interpersoonlijke incidenten en wellicht voor aankoopfraude. Het is dan interessant om te weten om wat voor contact het ging. Maar de antwoordopties (dagelijks- minstens 1 keer per week maar niet dagelijks – minstens 1 keer per maand, maar niet wekelijks-minder dan 1 keer per maand – nooit) sluiten niet aan op de vraag. Ze geven een frequentie per tijdsinterval en dat zegt niets als er geen verdere informatie is over de doorlooptijd. Daarom wordt hierover niet gerapporteerd.

Manier waarop aangifte wordt gedaan bij politie
Cijfers over de manier waarop slachtoffers aangifte hebben gedaan bij de politie (bijvoorbeeld op het bureau, telefonisch, via internet) zijn niet opgenomen in dit rapport. De politie heeft deze informatie namelijk zelf op integraal niveau. In dit onderzoek is deze vraag vooral gesteld voor eventueel toekomstig methodologisch onderzoek zoals eerder uitgevoerd bij het CBS (Reep, 2017).

Ondertekening proces-verbaal bij aangifte
In de enquête is gevraagd of, indien er aangifte is gedaan bij de politie, het slachtoffer hierbij een 'proces-verbaal' heeft ondertekend. Daarbij is niet uitgelegd wat precies bedoeld wordt. Aangezien de term 'proces-verbaal' wordt gebruikt kunnen respondenten denken dat dit iets anders is dan de aangifte. Ook wordt niet expliciet gevraagd naar een schriftelijke handtekening en kunnen respondenten ondertekening met DigiD ook hiertoe rekenen. De betekenis en daarmee de waarde van het percentage 'aangifte met ondertekening proces-verbaal' is dus voor meer uitleg vatbaar.

Verschillen onderzoeken Digitale Veiligheid en Criminaliteit, Veiligheidsmonitor en ICT-onderzoek

Het onderzoek naar Digitale Veiligheid & Criminaliteit (DVC) is een nieuw (pilot)onderzoek dat door het Centraal Bureau voor de Statistiek in samenwerking met de Nationale Politie is uitgevoerd in 2018. Het onderzoek heeft als hoofddoel om slachtofferschap van digitale criminaliteit onder burgers zo nauwkeurig mogelijk in kaart te brengen, en gaat daarnaast in op het bewustzijn van burgers ten aanzien van hun internetgebruik en eventuele risico's. Voor dit onderzoek is er een vragenlijst gehanteerd waarbij gebruik is gemaakt van verbeterde vraagstellingen uit twee bestaande CBS-onderzoeken: de Veiligheidsmonitor (VM) en het onderzoek ICT-gebruik huishoudens en personen (ICT-onderzoek). Dit is aangevuld met vraagstellingen uit andere externe onderzoeken op het terrein van internet-gebruik en internetveiligheid. Daarnaast zijn er ook nieuwe vraagstellingen ontwikkeld voor het zo gedetailleerd mogelijk meten van het slachtofferschap van nieuwe- of bestaande vormen van digitale criminaliteit, en aanverwante thema's zoals de gevolgen voor de slachtoffers, bekendheid met de dader(s), melding en aangifte, en redenen indien er geen melding of aangifte is gedaan.

Door de gekozen onderzoeksopzet en de gehanteerde uitgangspunten bij het ontwikkelen van de vraagstellingen kan de indruk ontstaan dat de uitkomsten van het onderzoek DVC vergeleken kunnen worden met die van de reguliere onderzoeken VM en ICT-onderzoek. Dit is echter niet het geval. Hiervoor zijn er te veel verschillen tussen de onderzoeken. Hierna wordt kort ingegaan op deze verschillen.

Verschillen met de Veiligheidsmonitor:
Vragen over digitale criminaliteit, zoals identiteitsfraude, online aan- en verkoopfraude, hacken en cyberpesten worden sinds 2012 ongewijzigd opgenomen in de grootschalige VM. De resultaten hiervan worden periodiek gepubliceerd. Ontwikkelingen op het gebied van digitale criminaliteit gaan echter zeer snel waardoor de in 2012 ontwikkelde vraagstellingen niet goed meer aansluiten op de actuele ontwikkelingen op dit gebied. Belangrijk doel van het pilot-onderzoek DVC is dan ook om de bestaande vraagstellingen uit de VM te verbeteren en nieuwe vragen te ontwikkelen om daarmee het meten van digitale criminaliteit in zijn totaliteit te verbeteren. Vanuit deze doelstelling is voor het pilotonderzoek DVC een veel bredere en gedetailleerdere set van vraagstellingen voor het meten van slachtofferschap van digitale criminaliteit ontwikkeld dan het deel dat in de VM hierop betrekking heeft.

Zo wordt – in tegenstelling tot bij de VM – aan respondenten eerst gevraagd of ze in de afgelopen 5 jaar slachtoffer zijn geweest van de onderscheiden online delicten, en daarna pas de vraag gesteld of dit ook in de afgelopen 12 maanden het geval was. Hiermee wordt de kans op telescoping door de respondent (het in de tijd ten onrechte naar voren halen van gebeurtenissen) kleiner. Daarnaast is er gedetailleerder ingegaan op verscheidene vormen van oplichting/fraude waar burgers via het internet slachtoffer van (kunnen) worden. Ook werd de vraagstelling over online aan- en verkoopfraude verbeterd. Over het

hacken van computerapparatuur of accounts – wat vaak vooraf gaat aan delicten als fraude of aan delicten in de persoonlijke sfeer – is meer gedetailleerde informatie verzameld. Hierdoor is een betere afbakening van slachtofferschap van deze delictsvorm mogelijk. Verder is dieper ingegaan op interpersoonlijke online incidenten zoals stalken, bedreigen etc. Waar nodig, is in de vragenlijst gebruik gemaakt van open vragen, zodat respondenten eigen antwoorden konden formuleren en zaken konden aandragen.

Naast inhoudelijke verschillen (in vraagstellingen) zijn er ook veel onderzoekstechnische en uitvoeringsverschillen tussen het DVC-onderzoek en de Veiligheidsmonitor. Denk hierbij aan zaken als de onderzoekspopulatie, onderzoeksperiode en wijze van veldwerk, context van de vragenlijst, en dataproces en weging. De verschillen tussen beide onderzoeken zijn opgenomen in het hiernavolgende schema in deze bijlage.

Verschillen met het onderzoek ICT-gebruik van huishoudens en personen

Behalve op het slachtofferschap van digitale criminaliteit wordt in het DVC-onderzoek ook uitgebreid ingegaan op het bewustzijn van burgers omtrent hun internetgebruik en eventuele gevaren. In hoeverre houden zijn zich bezig met internetveiligheid? Hierbij is in bepaalde gevallen gebruik gemaakt van vraagstellingen uit het ICT-onderzoek. Dit onderzoek wordt al sinds 2005 door het CBS uitgevoerd. Het betreft een onderzoek dat in EU- verband jaarlijks binnen alle lidstaten wordt uitgevoerd aan de hand van een geharmoniseerde vraagstelling. Ook voor internetgebruik en internetveiligheid beoogde de nieuw ontwikkelde DVC-vragenlijst bestaande vraagstellingen waar mogelijk te verbeteren en nieuwe vragen te ontwikkelen, vooral op het gebied van internetveiligheid.

Zo is in het nieuwe DVC-onderzoek meer informatie verzameld over het gebruik van WIFI en hierop aangesloten apparatuur, en het gebruik van internet via openbare plekken. Ook is er meer gevraagd over de frequentie van bepaalde internetactiviteiten en van online aankopen. Verder ging veel aandacht uit naar privacyaspecten, beveiliging van persoonsgegevens en kennis van de internetgebruiker over internetveiligheid.

Net als voor de VM geldt ook voor het ICT-onderzoek dat er behalve verschillen in vraagstellingen ook veel onderzoekstechnische en uitvoeringsverschillen bestaan met het DVC-onderzoek. Ook hier gaat het weer om zaken als de onderzoekspopulatie, onderzoeksperiode en wijze van veldwerk, context van de vragenlijst en dataproces en weging. Deze verschillen zijn opgenomen in het navolgende schema.

Conclusie

Door de verschillen tussen de onderzoeken kunnen de uitkomsten van de Veiligheidsmonitor (over digitale criminaliteit) en het onderzoek naar ICT-gebruik bij huishoudens en personen (over internetgebruik en internetveiligheid) niet zonder meer vergeleken worden met de uitkomsten uit het DVC-onderzoek op deze terreinen.

Belangrijkste onderzoeksverschillen tussen Digitale Veiligheid & Criminaliteit, Veiligheidsmonitor en ICT-gebruik van huishoudens en personen

	Digitale Veiligheid & Criminaliteit	Veiligheidsmonitor	ICT-onderzoek
Frequentie onderzoek	(Voorlopig) eenmalig.	Vanaf 2012 jaarlijks; Vanaf 2017 tweejaarlijks in de oneven jaren.	Jaarlijks.
Veldwerk en wijze van dataverzameling	Aanschrijfbrief met inloggegevens en verzoek om via invullen vragenlijst op internet deel te nemen (CAWI). Twee rappels per brief, telkens 2 weken na de aanschrijfbrief.	Aanschrijfbrief met inloggegevens met verzoek om via invullen vragenlijst op internet deel te nemen. 3 weken na verzending aanschrijfbrief volgt er een schriftelijk rappel, inclusief schriftelijke vragenlijst (PAPI). 3 weken na 1e rappel is er een 2e rappel, opnieuw met schriftelijke vragenlijst. 1,5 week na 2e rappel telefonische rappel met verzoek om alsnog via internet of papier in te vullen.	Aanschrijfbrief met inloggegevens met verzoek om via invullen vragenlijst op internet deel te nemen (CAWI). Na 2 rappels telkens na 3 weken worden non-respondenten telefonisch benaderd met vragenlijst (CATI). Personen zonder telefoonnummer krijgen een 3e rappelbrief.
Gebruikte modes	Uitsluitend CAWI.	Bij aanschrijving alleen CAWI, vanaf 1e rappel ook PAPI.	Bij aanschrijving alleen CAWI. Na 2 rappels ook CATI bij beschikbaarheid telefoonnummer.
Periode van waarneming	Oktober – medio december.	1e week augustus – 30 november.	April – medio juni.
Steekproef en doelpopulatie	100 000 steekproefpersonen van 12 jaar of ouder, 5 porties van elk 20 000 personen. Gestratificeerde tweetrapssteekproef. In de eerste trap worden per coropgebied deelgemeenten geselecteerd. Tweede trap is een enkelvoudig aselecte steekproef van personen in de geselecteerde deelgemeenten, met omvangen per deelgemeente zoals vastgesteld in de eerste trap.	Cijfers 2017: Ca. 380 000 steekproefpersonen van 15 jaar of ouder (landelijke steekproef + oversampling gemeenten). Doel is landelijk minimaal 65 000 respondenten met minimaal 750 respons voor elk politiedistrict en 300 respons voor elke 70 000+ gemeente of politie- basisteam. Uitzet in 3 porties, waarbij landelijke deel ongeveer de helft door CBS en ander helft door onderzoeksbureau I&O Research. Oversampling door I&O Research. Steekproef voor landelijk deel gestratificeerd naar Sub-Basisteam, voor lokaal deel naar primaire eenheid. Per stratum zelfwegend. Daarna screening en uitdunning.	Cijfers 2018: Ca 12 200 steekproefpersonen van 12 jaar of ouder. Doel is landelijk minimaal 4 300 respondenten in leeftijdsgroep 16–74 jaar (Eurostat). Gestratificeerde tweetrapssteekproef. In de eerste trap worden per coropgebied deelgemeenten geselecteerd. Tweede trap is een enkelvoudig aselecte steekproef van personen in de geselecteerde deelgemeenten, met omvangen per deelgemeente zoals vastgesteld in de eerste trap.
Respons	38 000 personen. Responspercentage 38,2 procent.	Cijfers 2017: Ca. 150 000 personen, waarvan 68 000 vast en > 80 000 lokale oversampling. Responspercentage 39,3 procent. Verhouding 56 procent CAWI en 44 procent PAPI.	Ca. 5 000 personen. Responspercentage 39,5 procent. Verhouding 73 procent CAWI en 27 procent CATI.
Weging	Weegmodel van ICT als inspiratie. Specifieke zaken voor ICT wel weggelaten. Ook overeenkomsten met de VM voor de regio's. Geslacht en leeftijd gekruist met politiedistrict, en uitkruisingen van regionale kenmerken met herkomstindikkingen. Gewogen naar Regionale eenheid, Politiedistrict, provincie, Grote steden.	Naar geografische, demografische en sociaaleconomische kenmerken. In weegmodel worden verschillende termen uitgekruist met politiedistrict, te weten geslacht x leeftijd, huishoudgrootte, stedelijkheid, herkomst, en inkomen. Ook gewogen naar Basisteam, G4, 70 000+ gem. en oversampling.	Naar geografische, demografische en sociaaleconomische kenmerken. In weegmodel worden verschillende termen uitgekruist op basis van geslacht, leeftijd, burgerlijke staat, huishoudgrootte, herkomst, inkomen, stedelijkheid, landsdelen en provincie+ (incl. grote steden).
Vragenlijst en context van het onderzoek	Richt zich behalve op het meten van digitale criminaliteit ook op hoe burgers gebruik maken van het internet, omgaan met privacy en beveiliging van persoonlijke gegevens en bekend zijn met internetveiligheid. Opbouw van de vragenlijst is als volgt: – Internetgebruik en -activiteiten waaronder online aankopen – Privacy en beveiliging persoonsgegevens – Internetveiligheid – Digitale fraude – Aan- en verkoopfraude – Andere vormen van fraude – Computervredebreuk – (hacken) – Online psychisch geweld – Andere online incidenten – Slotvragen en achtergrondkenmerken	Richt zich vooral op de subjectieve veiligheid van burgers en slachtofferschap van burgers van veel voorkomende (traditionele) criminaliteit en digitale criminaliteit. Opbouw van de vragenlijst is als volgt: – Leefbaarheid woonbuurt – Beleving overlast in de buurt – Veiligheidsbeleving – Slachtofferschap, traditioneel – Slachtofferschap, digitaal – Tevredenheid laatste politiecontact – Oordeel functioneren politie (algemeen en in buurt) – Oordeel functioneren gemeenten – Preventie – Onveilige plekken – Achtergrondkenmerken	Richt zich voornamelijk op internettoegang en het internetgebruik van burgers. Binnen het internetgebruik kunnen thematische onderwerpen wisselen conform harmonisatie- afspraken tussen de lidstaten. Opbouw van de vragenlijst is als volgt: – Internettoegang – Internetgebruik waaronder – Communicatie en activiteiten – Cloud computing – Digitale overheid – Online aankopen – Vaardigheden – Veiligheid en Privacy – Betaald werk, beroep, bedrijf – ICT-gebruik op het werk – Onderwijs, tijdsbesteding

Literatuur

CBS (2018a), *Cybersecuritymonitor 2018.* https://www.cbs.nl/nl-nl/publicatie/2018/38/cybersecuritymonitor-2018

CBS (2018b), *Veiligheidsmonitor 2017.* https://www.cbs.nl/nl-nl/publicatie/2018/09/veiligheidsmonitor-2017

CBS (2019a), *ICT-gebruik van huishoudens en personen (ICT).* https://www.cbs.nl/nl-nl/onze-diensten/methoden/onderzoeksomschrijvingen/korte-onderzoeksbeschrijvingen/ict-gebruik-van-huishoudens-en-personen--ict--

CBS (2019b), *Veiligheidsmonitor (vanaf 2012).* https://www.cbs.nl/nl-nl/onze-diensten/methoden/onderzoeksomschrijvingen/korte-onderzoeksbeschrijvingen/veiligheidsmonitor--vanaf-2012--

CBS (2019c), Vragenlijst Digitale Veiligheid & Criminaliteit, 2018. https://www.cbs.nl/nl-nl/publicatie/2019/29/digitale-veiligheid-en-criminaliteit-2018

Domenie, M.M.L., E.R. Leukfeldt, J.A. van Wilsem, J. Jansen, W.Ph. Stol (2013), *Slachtofferschap in een gedigitaliseerde samenleving Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit.* Boom Lemma uitgevers Den Haag 2013. Beschikbaar op http://cybersciencecenter.nl/media/1058/2013-slachtofferschap-in-een-gedigitaliseerde-samenleving.pdf

NOS (2018), WhatsApp-fraudeurs zeer actief: 'Feestdagen zijn cashdagen'. https://nos.nl/artikel/2260997-whatsapp-fraudeurs-zeer-actief-feestdagen-zijn-cashdagen.html

NRC (2019), Fraudehelpdesk: steeds meer oplichting via WhatsApp en sms. https://www.nrc.nl/nieuws/2019/05/25/fraudehelpdesk-steeds-meer-oplichting-via-whatsapp-en-sms-a3961563

Reep, C.M.M. (2017), *Fraude met online handel Antwoorden uit de Veiligheidsmonitor vergeleken met het politieregister.* Centraal Bureau voor de Statistiek, Heerlen. https://www.cbs.nl/-/media/_pdf/2017/12/fraude-met-oneline-handel.pdf

Reep, C.M.M. en M. Junger (2018), *Victims of cybercrime in Europe: a review of victim surveys.* Crime Science. 2018;7:5 https://rdcu.be/KFq9

Medewerkers

Math Akkermans
Willem Gielen
Rianne Kloosterman
Kim Knoops
Ger Linden
Elke Moons
Carin Reep