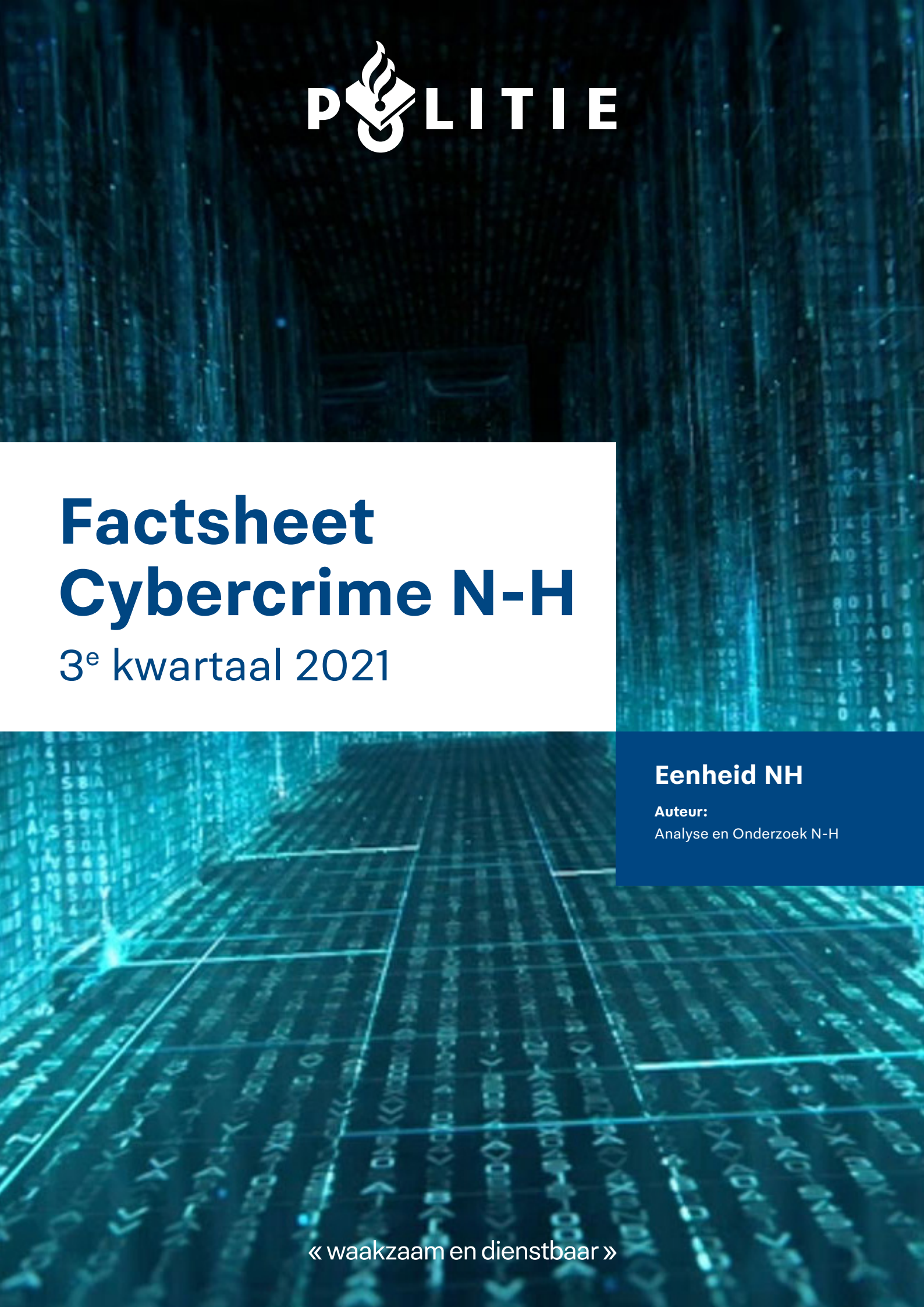


Factsheet Cybercrime N-H

3e kwartaal 2021

Eenheid NH

Auteur:
Analyse en Onderzoek N-H

« waakzaam en dienstbaar »

Cybercrime kwartaal 3

1. Waarom deze factsheet?

Om een beeld op het gebied van cybercrime te geven is de factsheet over het 3e kwartaal 2021 opgesteld. Deze factsheet is aangevuld met input vanuit het Cybercrime Team Noord-Holland, de digitale platformen en digitale wijkagenten. In deze factsheet wordt geen onderscheid gemaakt tussen gedigitaliseerde criminaliteit en cybercrime in enge zin. Beide zal worden aangeduid als 'cybercrime'.

2. Waar komen de cijfers vandaan?

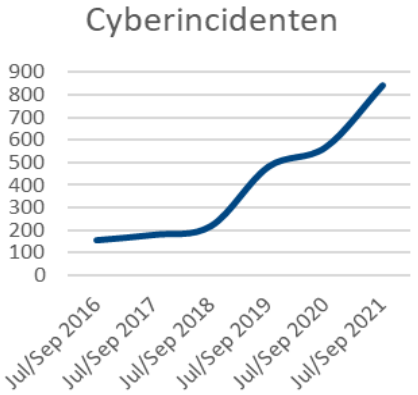
Alle cijfers die gebruikt zijn in deze factsheet zijn op basis van aangiften en meldingen bij de politie. De slachtoffers / melders van deze incidenten zijn woonachtig of gevestigd binnen het geografisch gebied van de eenheid Noord-Holland. Deze factsheet laat slechts het topje van de ijsberg zien van wat er daadwerkelijk gebeurt op het gebied van cybercrime. Ter illustratie, het slachtofferonderzoek van het CBS geeft aan dat het percentage slachtoffers van bijvoorbeeld hacken groter is dan het percentage slachtoffers van fietsendiefstal. De leeftijden op pag. 2 zijn ingedeeld op basis van computergeneraties (What's Happening Online?, 2018). Deze generaties geven aan in hoeverre iemand is opgegroeid met ICT en de computervaardigheden behorende bij deze generaties.

3. Aantal incidenten

Het totaal aantal meldingen en aangiften in de eenheid Noord-Holland in het derde kwartaal van 2021, is gestegen ten opzichte van dezelfde periode in 2020. Het gaat om een stijging van 48%. De stijging van het aantal aangiftes/meldingen is een trend die we al sinds 2016 zien.

4. Top 10 incidenten

In naastgelegen tabel zijn de meest voorkomende soorten cybercrime in Eenheid Noord-Holland weergegeven van het derde kwartaal. Enkele vormen krijgen extra aandacht in deze factsheet. Zo zijn vriend-in-nood fraude en Helpdeskfraude beide afgenomen vergeleken met dezelfde periode in 2020. Daarnaast is opvallend dat Fraude bankgegevens/ internetbankieren wederom enorm gestegen is in onze eenheid. Dit is onder andere te verklaren door de toename van het aantal Bankmedewerker fraude. Deze soort fraude komt voor in diverse varianten, maar de basis is dat het slachtoffer wordt gebeld door een 'nep bankmedewerker'. Vervolgens wordt hij of zij verleid om geld over te maken of om de inloggegevens van het internetbankieren door te spelen naar de oplichters. Soms wordt de bankpas van het slachtoffer opgehaald, soms wordt de computer van het slachtoffer overgenomen, kortom er zijn diverse varianten van deze soort fraude.



In de top 10 cybercrime van dit kwartaal is te zien dat Diefstal cryptomunten en Diefstal gegevens zijn toegenomen vergeleken met vorig jaar. Ransomware blijft de opvallende afwezige vorm van cybercrime in de top 10.
In de vorige factsheet hadden we het reeds over de ontwikkeling rondom de FluBot Malware. De aangiften omtrent de FluBot Malware gaan over de periode rond de 3e week van mei 2021. In de tussentijd zijn geen nieuwe aangiften in onze eenheid bekend van deze malware. Wel kwam vanuit de

Top 10 Cybercrime 3e kwartaal 2021

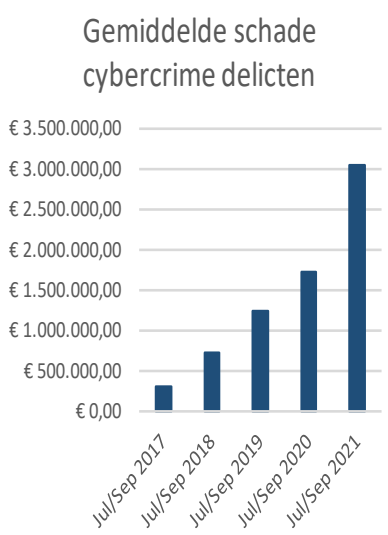
3e kwartaal 2021 afgezet tegen vergelijkbare periode 2020, 2019, 2018 en 2017

	2017	2018	2019	2020	2021	2021 t.o.v. 2020
Fraude bankgegevens / internetbankieren	12	25	222	302	**535**	▲233
Vriend-in-noodfraude	5	9	16	79	**67**	▼12
Misbruik accounts voor bestellingen	17	20	76	46	**62**	▲16
Helpdeskfraude	39	53	64	68	**56**	▼12
Telecomfraude	-	1	1	2	**18**	▲16
Sextortion	5	6	9	3	**14**	▲11
Diefstal Cryptomunten	-	2	3	-	**12**	▲12
Factuurfraude	19	5	18	19	**11**	▼8
Diestal gegevens	3	6	6	-	**10**	▲10
Smaad / laster / belediging	8	2	7	7	**10**	▲3
Overige cybercrime	71	89	58	39	**36**	▼3
Totaal	**179**	**218**	**480**	**566**	**840**	**▲274**

Landelijke Eenheid het bericht dat er een nieuwe variant van de FluBot is opgedoken. Deze variant verspreid zich d.m.v. een namaak beveiligings-update voor Android toestellen.

5. Schade in euro's

Het totaal bedrag dat met cybercrime in de eenheid Noord-Holland is buitgemaakt in het derde kwartaal van 2021 is €3.049.832,-. Dat is een kleine afname vergeleken met vorig kwartaal, maar een enorme toename vergeleken met voorgaande jaren. Dat is een toename van €1.325.538,91 vergeleken met het 3e kwartaal van 2020. De totale schade is dus bijna 56% gestegen ten opzichte van het vorige jaar.



Het is geen verrassing dat de meeste schade het afgelopen kwartaal gemaakt is door Fraude bankgegevens/ internetbankieren omdat dit delict 64% van het totale aantal incidenten betreft. Wat wel opvallend is, is dat Diefstal cryptomunten op nummer 2 staat van de meeste schade met een bedrag van €295.525,43. Terwijl dit delict maar 12 aangiftes betreft afgelopen kwartaal. Ook beleggingsfraude staat hoog wat betreft de hoeveelheid schade per aangifte. Met dit delict is namelijk €121.730,43 buitgemaakt in slechts 9 aangiftes.

6. Slachtoffers/ melders

Iets meer dan de helft van de slachtoffers/ melders is vrouw (53%) en iets minder dan de helft is een man (47%). Het is opmerkelijk dat dit percentage wel erg verschilt per delict. Zo is bij Vriend-in-Nood fraude en Misbruik accounts voor bestellingen merendeel van de slachtoffers vrouw. Terwijl bij de Diefstal cryptocurrency en Helpdeskfraude (Tech Support Scam) juist de meerderheid van de slachtoffers man is.

Top 3 per generatie

Voor het eerst sinds 2016 zij niet Generatie X, maar de Babyboomers de generatie die de meeste aangiftes/ meldingen hebben gemaakt (35%). 10% meer dan vorig kwartaal. Daarnaast is het opvallend dat Vriend-in-nood fraude alleen nog bij de twee oudste generaties in de top 3 staat, en dat Sextortion enkel bij de jongste generatie in de top 3 voorkomt.

Particulier vs Bedrijven

Net als het eerste half jaar van 2021 zijn de meeste slachtoffers/ melders particulier (98%). Deze groep leidt dan ook de meeste schade (€2.717.712,90). Bedrijven zijn in 1% van de gevallen aangever/ melder van cyberdelicten. Net als stichtingen, vereniging, scholen, banken of zorginstellingen.

98%
€2.717.712,90

1%
€196.094,07

1%
€36.816,49

Digitieners
(0-24)
7% (▼4%)

1. Fraude bankgegevens/internetbankieren (30)
2. Sextortion (8)
3. Telecomfraude (4)

Millennials
(25-39)
15% (▼5%)

1. Fraude bankgegevens/internetbankieren (68)
2. Misbruik accounts voor bestellingen (12)
3. Helpdeskfraude (Tech Support Scam) (6)

Generatie X
(40-59)
29% (▼6%)

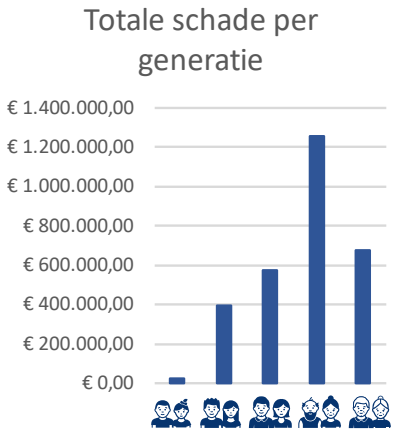
1. Fraude bankgegevens/internetbankieren (121)
2. Misbruik accounts voor bestellingen (29)
3. Helpdeskfraude (Tech Support Scam) (23)

Babyboomers
(60-75)
35%(▲10%)

1. Fraude bankgegevens/internetbankieren (188)
2. Vriend-in-Noodfraude (33)
3. Helpdeskfraude (Tech Support Scam) (19)

Vooroorlogse generatie (75+)
14% (▲5%)

1. Fraude bankgegevens/internetbankieren (94)
2. Vriend-in-Noordfraude (12)
3. Helpdeskfraude (Tech Support Scam) (2)



7. Digitale wijkagenten

Op YouTube was er een filmpje aangetroffen wat sterk leek op Doxing. Doxing is het publiceren van gevoelige persoonsgegevens van een individu of een organisatie/ bedrijf en is in strijd met de Wet bescherming persoonsgegevens (Wbp). De digitale wijkagent heeft de eigenaar van het filmpje opgespoord en een stopgesprek gevoerd. Ook is het materiaal van YouTube verwijderd.Daarnaast zijn digitale wijkagenten in onze eenheid betrokken bij het landelijke project “Gamen met de Politie”. Hierbij kunnen jongeren populaire online computerspellen samen met de politie spelen. Doel van deze pilot: op een laagdrempelige manier verbinden met jongeren die veelal online actief zijn. Zo kan de politie horen wat er speelt en kan effectiever het politiewerk in de wijk worden uitgevoerd.

8. Betaaldiensten/ waardedragers

Money mules (geldezels) blijven een veel gebruikte manier voor het cashen van illegaal verkregen geld. Daarnaast worden diverse cryptocurrencies nog steeds gebruikt om geld weg te sluizen. Dit zien we ook terug bij beleggingsfraude. Slachtoffers denken bijvoorbeeld te beleggen in crypto, maar eigenlijk maken ze hun online valuta over naar een oplichter.

9. Cybercrime Team N-H

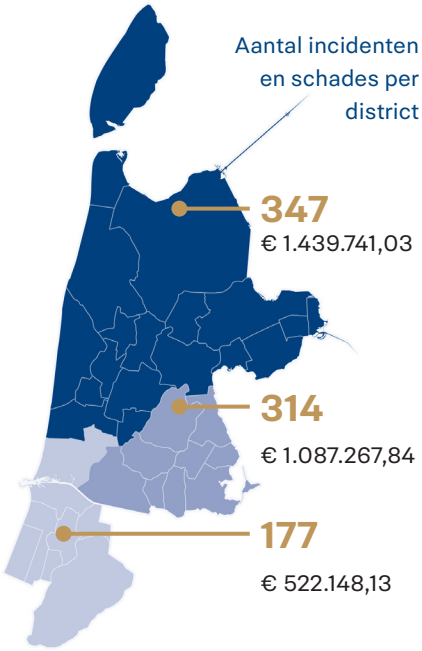
Dit kwartaal heeft het CCT N-H een actie uitgevoerd in het onderzoek naar een zorginstelling. Hierdoor is voorkomen dat medische gegevens op straat zijn gekomen. Daarnaast is het CCT bezig met het voorbereiden van Cease en Desist gesprekken. Naar aanleiding van het onderzoek naar de Remote Access Trojan “Imminent Monitor”, zijn de kopers van deze RAT benaderd. Zij worden uitgenodigd op een politiebureau om daar een stopgesprek te voeren met collega’s. Het CCT N-H is ook, in samenwerking met Noord-Holland Samen Veilig, bezig met project Het Slachtoffers Spreekt. Slachtoffers kunnen hun verhaal doen, waaardoor andere burgers steeds bewuster en weerbaarder worden tegen cybercriminelen. Ten slotte notificeert het CCT, in samenwerking met het Nationaal Cyber Security Centrum, slachtoffers. Het gaat specifiek om bedrijven/instanties waarbij accounts binnen hun infrastructuur zijn geinfecteerd met bepaalde malware.

10. Cyber platformen districten

In Noord-Holland Noord (N-H-N) loopt een uitgebreid onderzoek naar pinpasfraude. In dit onderzoek zijn 35 aangiftes te koppelen aan dezelfde dadergroep. Ook zijn al enkele pinners geïdentificeerd. Daarnaast is in N-H-N een pilot gestart om de aanpak van cybercrime te verbeteren. Er zijn vijf zij-instromers aangetrokken om de Werkgroep Cybercrime te versterken. Het doel: cybercrime effectiever bestrijden door een beter gecoördineerde aanpak. Cybercrime kent tenslotte geen gemeente- of provinciegrenzen.
In Zaanstreek-Waterland heeft het onderzoek Breakout gedraaid. In dit onderzoek is een verdachte aangehouden voor het wederrechtelijk toegang verkrijgen tot de server van een multinational. Met deze toegang heeft de verdachte derden in staat gesteld de online wachtrij voor populaire goederen over te slaan.
In Kennemerland is een onderzoek afgerond naar een persoon die dreigde met Doxing van gegevens van GGD medewerkers. Deze persoon bleek via Telegram deze gegevens aan te bieden. Dit onderzoek was een deelonderzoek van de Landelijke Eenheid. De verdachte is veroordeeld. Daarnaast loopt bij de DR Kennemerland een onderzoek naar pinpasfraude. De oudere slachtoffers werden gebeld door de `bank`. Waarna hun pinpas en pincode zijn opgehaald en zonder toestemming geld is afgeschreven.

11. Opvallende casus

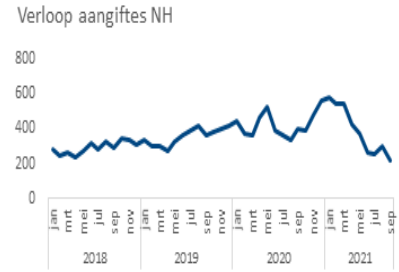
Opvallend aan de cyberdelicten van het afgelopen kwartaal is dat ze steeds complexer worden. Bijvoorbeeld ook de eerder beschreven variaties op de Bankmedewerker fraude. Er is een aangifte binnengekomen waarbij eerst via een phishing link de inloggegevens van de bankrekening afhandig werden gemaakt. Toen is er direct geld overgemaakt door de daders. Vervolgens werd het hoogbejaarde slachtoffer gebeld door een nep bankmedewerker

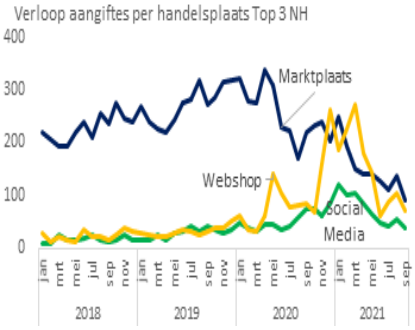


die haar vertelde over de ‘verdachte’ transactie. Het slachtoffer downloadde een programma waarmee de dader kon meekijken op de laptop. Ten slotte heeft het slachtoffer zelf via de laptop ingelogd op de bankrekening. Vanaf dat moment had het slachtoffer geen controle meer over de computer en is onder eigen ogen al het spaargeld naar onbekende rekeningen overgemaakt. Dit lijkt allemaal omslachtig, maar het is wel effectief. Er is ruim €20.000 buitgemaakt.

12. LMIO

Het LMIO registreert de meldingen van internetoplichting waarbij digitaal aangifte is gedaan via Politie.nl. Ongeveer 20% van deze aangiftes wordt vervolgens weer ingetrokken. In deze rapportage wordt uitgegaan van het netto aantal aangiftes. Vanaf deze alinea worden de LMIO cijfers behandeld. Deze cijfers gaan over de eerste 9 maanden van 2021.





12.1 Slachtofferbeeld

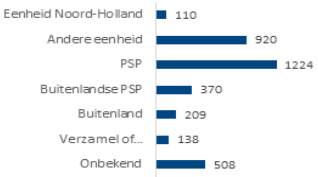
In de eerste 9 maanden van 2021 zijn er landelijk 37.703 netto aangiftes van internetoplichting gedaan. 9,35% (2704) van deze aangevers woont in de eenheid Noord-Holland. Het aantal aangiftes is voor het eerst lager dan vorig jaar (daling van 1,7%)[1]. Het aantal aangiftes van internetoplichting laat altijd een grillig verloop zien. Deze grilligheid is nog sterker sinds de corona-pandemie. Het lijkt er nu op dat het aantal aangiftes weer stabiliseert naar het niveau voor deze pandemie en mogelijk zelfs nog verder daalt. Tegelijkertijd blijft de verschuiving van Marktplaatsfraude[2] naar oplichting via webwinkels (en sociale media) ook sinds de versoepelingen van de coronamaatregelen zichtbaar. Een mogelijke verklaring is dat burgers nog steeds meer aankopen doen via webwinkels en daarmee ook malafide webwinkels, in plaats van via Marktplaats. Een andere verklaring is dat oplichters inzien dat het verdienmodel van oplichting via webwinkels (en sociale media) lucratiever is dan van Marktplaatsfraude.

12.2 Schade N-H jan t/m sep 2021

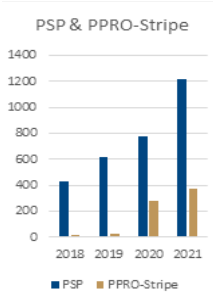
Totaal schade: €631.640,54
Gem. schade per aangifte: €179,49
Hoogste schadebedrag: €34.194,60

12.3 Waar gaat het geld naar toe

In onderstaande grafiek staat een overzicht van het soort rekeningen waar slachtoffers hun geld naar overmaken wanneer zij worden opgelicht.



De meerderheid gaat via Payment Services Providers. Het aantal aangiftes bij 'Eenheid Noord-Holland' en bij 'Andere eenheid' betreffen Nederlandse rekeningen, waarbij de oplichters woonachtig zijn in Eenheid Noord-Holland of dus een andere eenheid.



De belangrijkste verschuiving de afgelopen jaren is de groei van het gebruik van PSP's. Steeds vaker maken slachtoffers hun geld over via een iDealbetaling[3] die afgewikkeld wordt via een PSP, dan wel via een buitelandse PSP, zoals PPRO-Stripe.

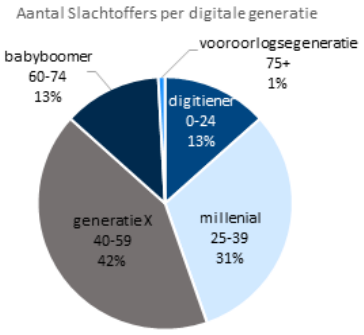
12.4 Verdachtenbeeld

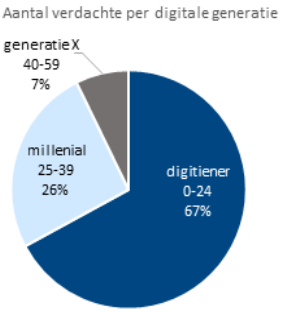
Katvangers/oplichters

In de eerste 9 maanden van 2021 waren er landelijk 6190 aangiftes van internetoplichting waarbij 3 of meer aangiftes tegen het betreffende rekeningnummer gekoppeld konden worden. Ook zijn alle rekeninghouders geïdentificeerd. Bij 9,6% (593) van deze aangiftes is de rekeninghouder woonachtig in Eenheid Noord-Holland. Al deze aangiftes zijn te koppelen aan 139 gebruikte bankrekeningen. Op dit moment is er onvoldoende zicht op het aantal opgepakte zaken van internetoplichting in Noord-Holland van 2021. Dit komt door de LMIO pilot, waarbij aangiftes worden gerouteerd naar de eenheid waar de verdachte woont. Deze pilot is binnenkort afgerond.

12.5.Leeftijd verdachte/ slachtoffer

In onderstaande grafieken is het aantal slachtoffers en verdachte rekeninghouders weergegeven per digitale generatie van jan t/m sep 2021 in Eenheid Noord-Holland.





[1] Vergeleken over de eerste 9 maanden van 2021.

[2] Aangiftes gerelateerd aan Marktplaats laten al langere tijd een daling zien. Dat is mede toe te schrijven aan preventieve maatregelen van Marktplaats. Mogelijk heeft de afname deels ook te maken met het feit dat er door de corona-pandemie geen festivals en evenementen hebben plaatsgevonden. Fraude met toegangskaarten vond voor corona op grote schaal namelijk plaats op Marktplaats.

[3] Past bij de ontwikkeling van toename van aangiftes tegen webwinkels. Bij webwinkels wordt veelal via iDeal betaald.