Uitvoeringsprogramma Vergroten digitale weerbaarheid

Utrechtse inwoners, ondernemers en organisaties weerbaar in een gedigitaliseerde wereld

Gemeente Utrecht

utrecht.nl/
digitaleveiligheid

Inhoudsopgave

Voorwoord

Onze samenleving digitaliseert steeds meer. Het digitale landschap verandert snel met de opkomst van nieuwe applicaties, diensten en technologieën en de doorontwikkeling van bijvoorbeeld kunstmatige intelligentie. Dit biedt grote voordelen: processen gaan efficiënter en makkelijker en digitalisering bespaart ons daarmee in veel gevallen tijd. Tegelijkertijd worden we afhankelijk van systemen en hun ontwikkelaars. Systemen raken ook steeds meer met elkaar verweven en zijn afhankelijk van elkaar, waardoor een kwetsbaarheid in een van de onderdelen effecten kan hebben op het hele systeem. Hierdoor kunnen de gevolgen van een cyberincident groot en ernstig zijn, met effecten voor meerdere organisaties en groepen in de samenleving. Ook kwaadwillenden zijn zich hier terdege van bewust en maken op grote schaal misbruik van kwetsbaarheden of voeren bewust digitale aanvallen uit op kwetsbare individuen, objecten of systemen. Digitale criminaliteit en online normoverschrijdend gedrag[1] veroorzaken veel schade, variërend van economische verliezen en emotionele schade tot verstoring van diensten, van de (lokale) openbare orde en bedreigingen voor de nationale veiligheid en onze democratie. Volgens het Centraal Bureau voor de Statistiek gaf 15% van de Nederlanders van 15 jaar of ouder in 2022 aan dat ze de laatste twaalf maanden slachtoffer zijn geweest van online criminaliteit. Dat gaat om 2,2 miljoen mensen! Het totale schadebedrag van online criminaliteit bedroeg in 2021 afgerond 680 miljoen euro. Digitale criminaliteit en ander schadelijk onlinegedrag heeft daarmee een zeer ondermijnend karakter en vormt wereldwijd een voortdurende uitdaging voor samenlevingen. Onze aanhoudende inspanningen zijn nodig om digitale criminaliteit en online aangejaagde ordeverstoringen te voorkomen en te bestrijden.

Ook Utrecht zet zich al enkele jaren in om digitale criminaliteit en online normoverschrijdend/schadelijk gedrag te voorkomen en te bestrijden en bewoners en ondernemers weerbaar en veerkrachtig te maken tegen de effecten hiervan. De raad heeft de Visie Digitale stad vastgesteld, waarin digitale weerbaarheid van de eigen organisatie, de stad, bewoners en ondernemers een van de pijlers is. In de Veiligheidsagenda ’23-’26 is de prioriteit ‘Vergroten digitale veiligheid en online weerbaarheid’ opgenomen. In de Regionale Veiligheidsstrategie 2023–2026, tot slot, is Digitale veiligheid en cybercriminaliteit één van drie gezamenlijke regionale prioriteiten.

In dit uitvoeringsprogramma staat hoe we in de periode 2023–2026 aan digitale weerbaarheid willen werken. Hiermee werken we de pijler ‘digitale weerbaarheid van bewoners en ondernemers’ uit de Visie digitale stad én de bovengenoemde prioriteit uit de Veiligheidsagenda ’23-’26 uit. Soms doen we dit heel concreet en soms wat abstracter, omdat het landschap van de digitale criminaliteit zeer snel verandert en we daarin flexibel willen blijven. We willen namelijk met onze activiteiten en interventies op de (middel)lange termijn ook kunnen inspelen op toekomstige ontwikkelingen. We gaan door met effectieve interventies en ontwikkelen nieuwe. De raad heeft in het coalitieakkoord budget beschikbaar gesteld voor deze investeringen. Daarmee kunnen we verder bouwen aan het fundament om Utrechtse inwoners en ondernemers bewust, weerbaar en veerkrachtig te maken in een gedigitaliseerde wereld.

Sharon A.M. Dijksma
Burgemeester

1 Online gedrag dat niet strafbaar is, maar wel schadelijk, zoals cyberpesten, sexting, het verspreiden van desinformatie of het delen van boodschappen die leiden tot schadelijke polarisatie of maatschappelijke onrust.

Een urgent probleem

Landelijk beeld

Het Cybersecuritybeeld 2023 van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) waarschuwt dat digitale dreigingen in Nederland een ernstige zorg blijven. Er zijn diverse redenen voor deze zorg. Ten eerste is er een complexe wisselwerking tussen digitale en niet-digitale dreigingen en ontwikkelingen. Cyberaanvallen kunnen zowel de oorzaak als het gevolg zijn van storingen in bijvoorbeeld de energievoorziening, verkeerslichteninstallaties of bij zorginstellingen. Ten tweede zijn digitale processen, systemen en netwerken erg complex en met elkaar verweven binnen ketens. Een kwetsbaarheid in een van deze processen kan bij een aanval of verstoring impact hebben op de hele keten. Bovendien zijn sommige systemen verouderd en kwetsbaar voor aanvallen van cybercriminelen, die hiervan maar al te graag misbruik maken. Ook is er een concentratie van informatie en digitale processen, vooral bij bedrijven die clouddiensten aanbieden. Dit maakt ze aantrekkelijke doelwitten voor misbruik. Met alle gevolgen van dien: bij een aanval op een clouddienst kunnen in een keer veel organisaties tegelijk worden getroffen. Ook wereldwijde spanningen, zoals de oorlog in Oekraïne, leiden tot cyberaanvallen door statelijke actoren die bijvoorbeeld uit zijn op destabilisatie, wat weer kan leiden tot openbare orde incidenten. Ook desinformatie of het selectief verspreiden van nieuws spelen daarbij een rol.

Georganiseerde misdaad

Criminelen stappen steeds vaker in de digitale criminaliteit. Het criminele verdienmodel ligt meer en meer in digitale criminaliteit en de pakkans is klein. Volgens het Wetenschappelijk Onderzoek- en Documentatiecentrum en het Openbaar Ministerie wordt het merendeel van digitale criminaliteit veroorzaakt door ondermijnende, georganiseerde misdaad. Digitale criminaliteit is een belangrijk werkterrein van traditionele criminele organisaties geworden, die digitaal afpersen of gestolen informatie verkopen en misbruiken. Er zijn nieuwe netwerken van online daders bijgekomen die een technische specialisatie hebben. Deze specialisatie verkopen ze, waardoor voor andere criminelen slechts een basis technische kennis voldoende is. Onderling kopen en verkopen ze cybercrimediensten en -toolkits via illegale marktplaatsen op het darkweb (het zogenaamde Cybercrime-as-a-service (CaaS)[2]. Ook delen criminelen bijvoorbeeld op fora en Telegramkanalen werkzame aanpakken. Daarnaast zien we dat drugsgerelateerde criminaliteit en digitale criminaliteit meer en meer

2 Het aanbieden van cybercrimediensten en -toolkits via illegale marktplaatsen op het darkweb, zoals bijvoorbeeld voor het uitvoeren van een DDoS aanval of scripts voor phishing.

met elkaar verweven zijn geraakt. Criminelen plegen cyberdelicten, vaak in combinatie met drugsdelicten en/of wapenbezit.

Een verontrustende ontwikkeling in cybercrime[3] is social engineering, waarbij aanvallers psychologische manipulatie gebruiken om informatie te verkrijgen van hun potentiële slachtoffers. Ze kunnen zich voordoen als legitieme partijen, zoals banken of bekende websites of als collega's of familieleden, om gebruikers te verleiden gevoelige informatie te verstrekken of geld over te maken.

Technologische ontwikkelingen

De technologische ontwikkelingen op het gebied van ICT volgen elkaar in rap tempo op. Toch doorzien niet alle gebruikers de effecten goed. Kunstmatige intelligentie (AI) is een tweesnijdend zwaard in cybercrime. Enerzijds kunnen criminelen AI gebruiken om aanvallen te automatiseren en te verfijnen, waardoor ze efficiënter en gevaarlijker worden. Ook kan AI via stem- en beeld imitatie (deep fake) bedoeld of onbedoeld worden gebruikt om slachtoffers te maken, omdat echt en nep bijna niet meer te onderscheiden zijn. Anderzijds kan kunstmatige intelligentie de veiligheid verbeteren door snellere detectie van dreigingen, zoals cyberaanvallen en verdachte activiteiten. AI kan ook helpen bij het voorspellen van openbare orde incidenten en het analyseren van grote hoeveelheden gegevens. Zo kunnen overheden, binnen de bevoegdheden van het lokaal bevoegd gezag, proactief handelen en mensen beter beschermen.

3 Misdrijven die gepleegd worden met een ICT-middel (bijvoorbeeld een computer, smartphone of internetbrowser) die gericht zijn op ICT, zoals hacking, mal- of ransomware en virussen

In een wereld die steeds meer afhankelijk is van digitale technologieën, is het cruciaal om deze en nieuwe technologieën en de bedreigingen die zij kunnen vormen, serieus te nemen. Een goed en actueel beeld van (statelijke) actoren, plegers én de (potentiële) slachtoffers is daarbij cruciaal. Net als het voortdurend investeren in cyberbeveiliging en de bijbehorende handelingsperspectieven om slachtofferschap en maatschappelijke effecten tot een minimum te beperken.

Digitale criminaliteit en de weerbaarheid

Digitale criminaliteit raakt inwoners, ondernemers en organisaties, met grote financiële, economische en emotionele gevolgen én effecten op de openbare orde. We maken verschil tussen cybercrime en gedigitaliseerde criminaliteit[4]. Cybercrime bestaat uit misdrijven die gepleegd worden met een ICT-middel (bijvoorbeeld een computer, smartphone of internetbrowser) die gericht zijn op ICT, zoals hacking, DDoS-aanvallen[5], mal- of ransomware[6] en virussen. Gedigitaliseerde criminaliteit betreft misdrijven waarbij ICT als middel wordt ingezet om traditionele vormen van criminaliteit te plegen, zoals fraude met betaalproducten[7], ID-fraude en online handel (samen: digitale fraude), maar ook digitaal kinderlokken, sextortion[8], sexting en chantage via e-mail of social media.

Het verspreiden van nepnieuws of oproepen die kunnen leiden tot openbare ordeverstoringen worden, zeker als het niet strafbaar is, niet geregistreerd als (digitale) criminaliteit.

De kans dat plegers worden opgepakt of uitgeleverd voor hun daden is klein. Ze verschuilen zich achter anonieme accounts, versleutelde internetverbindingen en bevinden zich vaak buiten de geografische grenzen van het lokaal bevoegd gezag.

Inwoners, ondernemers en organisaties zijn nog onvoldoende weerbaar tegen digitale criminaliteit en online normoverschrijdend gedrag. Niet iedereen past de basismaatregelen toe, zoals het gebruik van unieke wachtwoorden en multifactorauthenticatie[9] (twee of meer methodes gebruiken om toegang te krijgen tot een onlineapplicatie). Daarnaast is kennis over desinformatie essentieel om de weerbaarheid te vergroten. Dit is nodig om onze democratische rechtsorde te beschermen en openbare orde incidenten te voorkomen.

4 Traditionele misdrijven waarbij ICT als middel wordt ingezet, maar niet het doel is. Voorbeelden zijn helpdeskfraude, fraude met online handel en sextortion
5 Criminelen versturen enorm veel dataverkeer naar een server, website of app. Omdat er zoveel verzoeken tegelijk verwerkt moeten worden, wordt het verkeer van en naar de website geblokkeerd en kan zelfs de server van de dienst crashen. Gevolg is dat de dienst slecht of helemaal niet bereikbaar is voor bezoekers.
6 Malware die je systeem, netwerk of data op slot zet. Criminelen eisen betaling om weer toegang te krijgen tot systemen.
7 Simmen of skimming: het onrechtmatig kopiëren van betaalkaartgegevens.
8 Dreigen met het doorsturen van (pikant getinte) beelden als chantagemiddel.
9 Een extra veiligheidslaag in de toegangsvereisten van een systeem of applicatie. Factoren worden ingedeeld in drie categorieën: iets weten (bijvoorbeeld een wachtwoord), iets hebben (bijvoorbeeld een token) of iets zijn (bijvoorbeeld een vingerafdruk). Bij minimaal twee factoren, spreken we van multifactor authenticatie.

Wat weten we?

Er is geen goed inzicht in het Utrechtse slachtofferschap, daderschap en schadebedragen van de verschillende vormen van digitale criminaliteit. Van veel delicten zijn geen gegevens beschikbaar, waardoor we een onvolledig cijfermatig beeld hebben.

In tabel 1[10] worden de politiecijfers van de gemeente Utrecht over respectievelijk cybercrime en digitale fraude (de drie meest voorkomende vormen van digitale fraude[11]) voor de jaren 2019 t/m 2023 weergegeven. Deze cijfers[12] vertellen echter niet het hele verhaal. Belangrijk te vermelden is het feit dat de aangifte- en meldingsbereidheid van digitale criminaliteit laag is, gemiddeld tussen de 15 en 20%: de werkelijke aantallen liggen waarschijnlijk veel hoger. Er zijn meerdere redenen voor de lage aangifte- en meldingsbereidheid. Dit heeft te maken met onder andere de anonimiteit en complexiteit van digitale delicten, een gebrek aan vertrouwen in de wetshandhaving, schaamte, onwetendheid over aangifteprocedures, tijdsintensieve aangifteprocessen en de neiging van slachtoffers om zelf oplossingen te zoeken voor hun problemen.

In tabel 2 staat hoeveel procent van de slachtoffers volgens een landelijke enquête van het CBS in 2022 melding of aangifte deed van online criminaliteit bij politie.

Tabel 1. Politiecijfers over aangiftes cybercrime en digitale fraude in de gemeente Utrecht

Onderwerp	2019	2020	2021	2022
Cybercrime	87	168	299	269
Digitale fraude	1427	1618	1278	1136

Tabel 2. CBS-data over aangifte en meldingen van online criminaliteit bij politie

Melding/aangifte	Online criminaliteit totaal	Online oplichting en fraude	Hacken	Online bedreiging en intimidatie	Overige online delicten
Melding bij politie	20,5%	27,2%	12,2%	16,5%	33,7%
Aangifte bij politie	18,6%	25,9%	11,2%	13,3%	26,8%

10 Het betreft het aantal misdrijven (strafbare feiten). Dit komt nagenoeg overeen met aangiftes, maar kan iets hoger zijn. De misdrijven kunnen betrekking hebben op particulieren of bedrijven.
11 Fraude met betaalproducten, ID-fraude en fraude met online handel.
12 Bron: Veiligheidscoalitie/politie - 2023

Tabel 3. CBS-data over emotionele of psychische gevolgen online criminaliteit, 2022

Gevolgen	Online criminaliteit totaal	Online oplichting en fraude	Hacken	Online bedreiging en intimidatie	Overige online delicten
Minder vertrouwen in mensen	36,6%	41,7%	21,9%	42,2%	41,7%
Minder veilig voelen	30,3%	22,0%	37,4%	37,1%	28,7%
Slaapproblemen	7,5%	4,9%	4,8%	15,5%	6,9%
Depressieve klachten	7,2%	4,5%	2,8%	16,8%	9,4%
Angstklachten	6,8%	3,0%	3,7%	17,0%	6,1%
Voorval telkens opnieuw beleven	6,6%	5,7%	2,8%	10,9%	10,2%

Digitale criminaliteit heeft grote gevolgen voor slachtoffers. Uit een landelijke enquête van het CBS blijkt dat de totale financiële schade onder particuliere slachtoffers in 2021 wordt geschat op 680 miljoen euro. Daarnaast ervaren veel slachtoffers emotionele en psychische klachten, zoals depressieve klachten en onveiligheidsgevoelens (zie tabel 3). Het meest voorkomende gevolg is het hebben van minder vertrouwen in mensen (gemiddeld zo'n 37%). Online bedreigen en intimidatie (bestaand uit online bedreiging met geweld, online pesten, online stalken en shamesexting[13]) veroorzaakt het meest frequent (28%) emotionele en psychische gevolgen. Het is dan ook niet verrassend dat slachtoffers van online criminaliteit dezelfde behoefte hebben aan informatie, emotionele, financiële en praktische ondersteuning als slachtoffers van traditionele criminaliteit.

13 Sexting is het versturen van seksueel getinte berichten of pikante foto's en video's. Dit is in essentie onschuldig. Wanneer de seksueel getinte beelden in de verkeerde handen terechtkomen en ongewild verspreid worden, is sprake van 'shame sexting'. De beelden worden doorgestuurd uit bijvoorbeeld wraak of na een ruzie.

Onze ambitie

Het college werkt aan een veilige en leefbare stad voor onze inwoners, ondernemers en bezoekers. Het vergroten van de digitale veiligheid en online weerbaarheid in de stad is een prioriteit in de Veiligheidsagenda 2023–2026. Onze ambitie is dan ook:

Utrechtse inwoners, ondernemers en organisaties zijn weerbaar in een gedigitaliseerde wereld

De groei van digitale criminaliteit vraagt van de gemeente en haar partners om de aanpak van criminaliteit te optimaliseren en de strafrechtelijke en bestuursrechtelijke aanpak goed op elkaar te laten aansluiten. Wat we al doen om offline criminaliteit aan te pakken en te voorkomen, moeten we ook doen voor gedigitaliseerde criminaliteit.

Er zijn veel partijen actief op het thema digitale veiligheid, bijvoorbeeld om slachtofferschap te voorkomen. De verantwoordelijkheid voor de opsporing en vervolging van strafbare feiten ligt bij het OM. De burgemeester heeft de wettelijke taak regie te voeren over het veiligheidsbeleid.

We werken samen met maatschappelijke partners en andere instanties. In die netwerken speelt de gemeente een coördinerende, verbindende en faciliterende rol, soms ook financieel. Samen maken we bewoners, ondernemers en organisaties bewust van online risico's, bieden we ondersteuning om digitaal weerbaarder te worden en blijven we plannen ontwikkelen om de digitale veiligheid in de Utrechtse wijken en buurten verder te versterken. We maken daarbij gebruik van bestaande, bewezen effectieve interventies of ontwikkelen deze.

In dit uitvoeringsprogramma werken we onze ambitie voor de jaren 2023 tot en met 2026 uit.

Dit gaan we doen:

- (potentiële) slachtoffers bewust en weerbaar maken tegen vormen van digitale criminaliteit en online normoverschrijdend gedrag;
- (potentiële) plegers bewust maken van de risico's en gevolgen van hun online gedrag voor zichzelf en de maatschappelijke impact die dat online gedrag kan hebben;
- aan de weerbaarheid van de stad werken samen met de stedelijke community voor cyberweerbaarheid;
- ons voorbereiden op mogelijke cybercrises.

De doelgroepen waar we ons op richten zijn enerzijds de slachtoffers, waarbij we specifiek aandacht hebben voor kinderen, jongeren en hun ouders/verzorgers, senioren en Utrechtse ondernemers, in het bijzonder mkb'ers en zzp'ers.

Anderzijds richten we ons op plegers van digitale criminaliteit. We maken het criminelen lastiger hun werk voort te zetten. Net als in de aanpak van traditionele criminaliteit betekent dat dat deze vorm van criminaliteit minder lucratief moet worden. Dit doen we bijvoorbeeld door barrièremodellen te ontwikkelen en (potentiële) daders weerbaar te maken tegen de aantrekkingskracht van digitale criminaliteit. Ook vergroten we hun moreel kompas en empathisch vermogen ten opzichte van slachtoffers.

Uitgangspunten

1. Business as usual

We gaan door met de effectieve interventies en activiteiten van de afgelopen jaren. Daarnaast is en blijft digitale weerbaarheid een onderdeel van de andere veiligheidsthema's van de gemeente, zoals Utrecht zijn we samen, Grenzen stellen perspectief bieden, crisisbeheersing, Agenda tegen uitbuiting, openbare orde en maatschappelijke onrust en de Visie digitale stad. Vanzelfsprekend zorgen we dat ook de gemeentelijke organisatie zelf digitaal weerbaar is. We hebben de basis op orde voor de eigen digitale systemen (hardware en software) en digitale informatievoorziening.

2. Samen met partners

We werken samen met (publieke en private) partners in de stad en erbuiten[14]. Partners in het sociaal domein, zoals DOCK en JoU, spelen enerzijds een rol bij het in kaart brengen van de vraag. Anderzijds leggen zij de verbinding tussen het aanbod en de doelgroep. Digitale veiligheid is een relatief nieuw focusgebied: daardoor ontwikkelen veel partijen nieuwe initiatieven om de aanpak te verbeteren. Denk daarbij aan gemeentes, (regionale) samenwerkingsverbanden, ministeries en maatschappelijke organisaties. We zoeken aansluiting bij deze partijen en initiatieven en werken regionaal samen. Ook onze eigen initiatieven ontwikkelen we in nauwe samenwerking met deze partijen. Zo leren we van elkaar én voorkomen we dat we dubbel werk doen. Met de andere G4 gemeenten Amsterdam, Rotterdam en Den Haag wisselen we interventies uit en leren we van elkaar.

3. In wijken en buurten

We zoeken zoveel mogelijk de bestaande netwerken van bewoners en ondernemers in buurten en wijken op en sluiten aan op de signalen, wensen en behoeftes van bewoners en ondernemers daar. We maken hierbij gebruik van de partners in het sociaal domein. In verschillende wijken zijn Stadsmakers Digitale Veiligheid[15] actief. Deze Stadsmakers wonen in Utrecht en willen graag hun steentje bijdragen aan de digitale veiligheid van hun wijk. Dit doen zij op verschillende manieren: de een geeft weerbaarheidstrainingen aan senioren, de ander geeft gastlessen op school. Deze activiteiten kunnen voortkomen uit vragen van partners uit de stad of kunnen de Stadsmakers zelf initiëren; aansluitend op ieders expertise.

14 Politie, OM, sociale partners zoals welzijnsorganisaties als JoU, DOCK, Bibliotheek Utrecht, onderwijsinstellingen, Veiligheidsregio Utrecht, Veiligheidscoalitie Midden Nederland. Daarnaast werken we samen met Platform Veilig Ondernemen, KvK, VNO-NCW, U-tech community en andere (lokale) private partners, zoals banken, cybersecuritybedrijven, etc. Verder wordt er samengewerkt met de G4, de VNG, het Centrum voor Criminaliteitspreventie en Veiligheid en het Rijk. We werken samen met onderzoeksinstellingen op het gebied van digitale criminaliteit, zoals van de Hogeschool Utrecht, de Haagse Hogeschool en Saxion Hogeschool. Tot slot werken we samen met Stadsmakers Digitale Veiligheid, bewoners van Utrecht die buren en wijk helpen zich te beschermen tegen digitale criminaliteit.

15 Stadsmakers digitale veiligheid wonen in Utrecht en willen graag hun steentje bijdragen aan de digitale veiligheid van de stad en haar inwoners. Dit doen zij op verschillende manieren: de een geeft weerbaarheidstrainingen aan senioren, de ander geeft gastlessen op school. Deze activiteiten kunnen voortkomen uit vragen van partners uit de stad, of kunnen de Stadsmakers zelf initiëren; aansluitend op ieders expertise.

"Trek je collega's mee in deze beweging, want we kunnen niet langer bevangen door koudwatervrees weifelend langs de rand van het digitale zwembad staan toekijken… JUMP!"

Remco Spithoven, lectoraat Maatschappelijke Veiligheid (Saxion)

4. Inclusief

Als we willen dat iedereen in onze stad meedoet, moeten we digitale veiligheid te koppelen aan digitale inclusie. Alleen zo kunnen we een veerkrachtige en rechtvaardige samenleving bevorderen. Digitale inclusie betekent dat Utrechters toegang hebben tot, gebruik kunnen maken van, en weerbaar zijn voor digitale technologie en zo onderdeel (willen) uitmaken van de digitale samenleving. Met speciale aandacht voor groepen in een kwetsbare positie zoals laaggeletterde Utrechters, senioren die niet zelfstandig overweg kunnen op het internet, Utrechters met een beperking en mensen met beperkte financiële middelen. Door ook deze doelgroepen te betrekken bij digitale veiligheidsinitiatieven, vergroten we niet alleen hun digitale vaardigheden, maar beschermen we hen ook tegen online bedreigingen en misbruik. Bovendien versterkt dit de sociale cohesie en economische kansen.

5. Groot helpt klein

We zien dat het voorkomen van een digitale inbraak of aanval voor veel kleinere organisaties niet zo vanzelfsprekend is als het voorkomen van fysieke inbraak, door bijvoorbeeld een goed slot te kopen. Kleinere organisaties voelen de noodzaak minder of hebben de kennis en de middelen niet. In de community voor cyberweerbaarheid ontwikkelen we samen met grote organisaties manieren om digitale weerbaarheid te vergroten bij bedrijven die hier nog niet zo mee bezig zijn. Dit doen we omdat er veel verwevenheid en dus ketenafhankelijkheid kan zijn in processen. Denk hierbij aan toeleveranciers van producten of goederen en afnemers. Dat zijn mogelijk kleinere organisaties, zoals mkb of zzp'ers. Door deze kleinere ondernemers aan te spreken op de mede verantwoordelijkheid in de opgave om Utrecht als stad weerbaar te maken, worden maatschappelijke gevolgen beperkt.

Het uitgangspunt 'groot helpt klein' geldt ook voor de wijze waarop we samenwerken in de regio. We initiëren en/of participeren in trajecten waarmee we werken aan regionale digitale weerbaarheid. Het maakt ons samen verantwoordelijk voor een weerbare stad en regio.

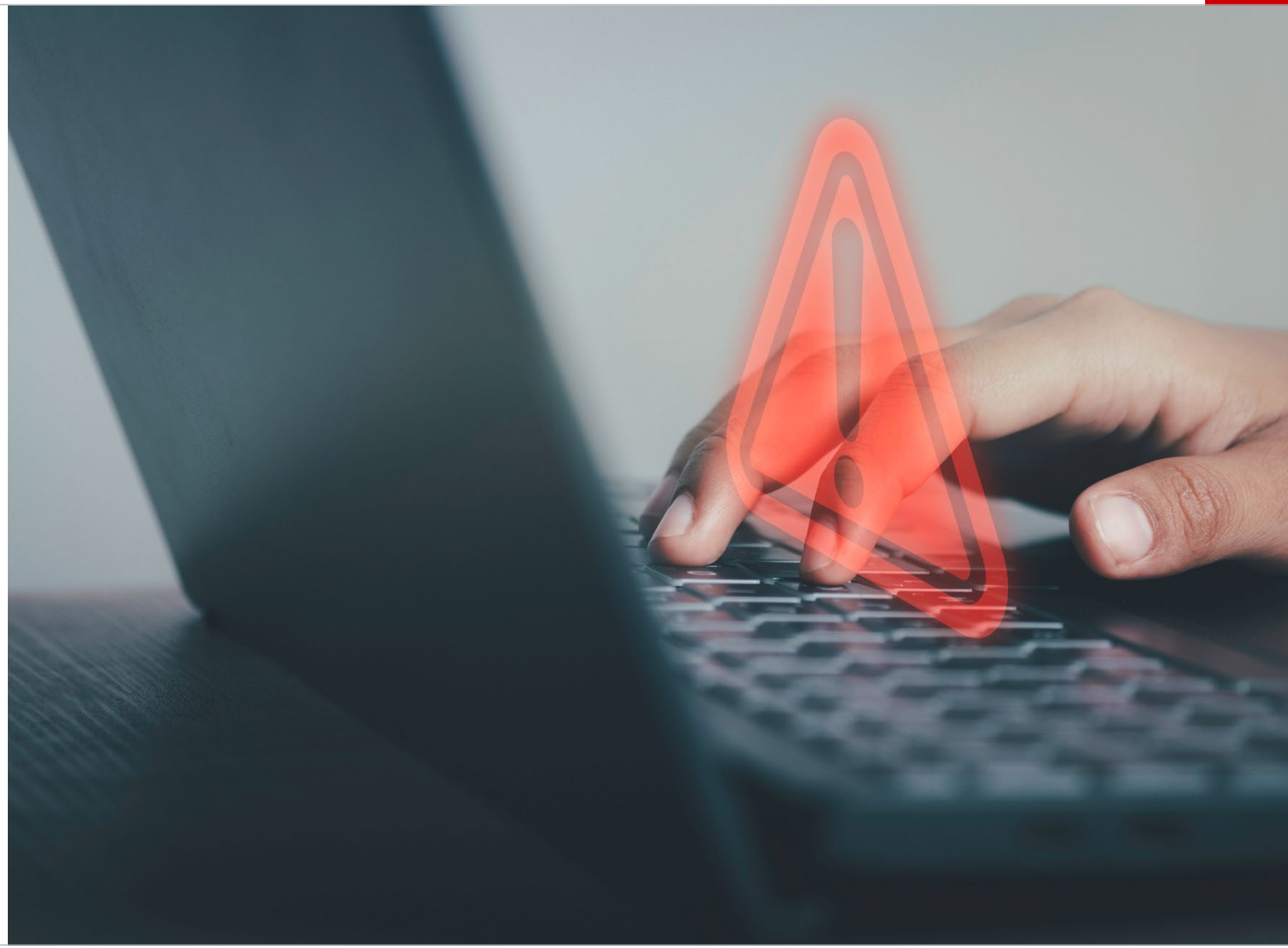
6. Informatiegestuurd

Weten waarover we het hebben is natuurlijk de basis. Dus willen we een actueel en betrouwbaar beeld van digitale criminaliteit, dreigingen, kwetsbaarheden en incidenten, in een zich snel ontwikkelend technologisch landschap. Een goede online informatie positie is ook belangrijk om zicht te hebben op online gedragingen die oproepen of leiden tot verstoring(en) van de openbare orde. Alleen daarmee kunnen wij en onze partners proactief reageren, handelingsperspectief formuleren, passende beveiligingsmaatregelen nemen, maar ook educatieve initiatieven ontwikkelen.

Momenteel hebben we nog geen goed cijfermatig beeld. Ook een duiding ontbreekt. Daarnaast weten we dat er niet altijd aangifte wordt gedaan van digitale criminaliteit. Om onze informatiepositie te verbeteren, sluiten we daarom onder andere aan bij een landelijk initiatief om de 'Zicht op ondermijning' methodiek in te zetten voor digitale criminaliteit.

De aangiftebereidheid ligt gemiddeld tussen de 15 en 20%. We zetten daarom in op het verhogen van de meldings- en aangiftebereidheid bij politie, maar ook bij partners (zoals bij banken en de Fraudehelpdesk), met wie we samenwerken aan digitale weerbaarheid. Tot slot is het belangrijk de technologische ontwikkelingen en de effecten daarvan op de samenleving goed in beeld te hebben, zodat we tijdig kunnen inspelen op eventuele nieuwe dreigingen.

Tegelijkertijd weten we dat cijfers niet alles zeggen. Ons uitgangspunt is dus niet enkel datagedreven werken, maar cijfers interpreteren in de context, samen met betrokken partners in de aanpak en in gesprek met doelgroepen en slachtoffers. Op basis van deze combinatie leren we en sturen we bij.



Doelgroepen

De doelgroepen waar we ons specifiek op richten met onze aanpak zijn onder te verdelen in (potentiële) slachtoffers en plegers. We splitsen daarbij de slachtoffers uit in drie subgroepen: 1. kinderen, jongeren en hun ouders/verzorgers, 2. senioren en 3. mkb'ers en zzp'ers. Deze groepen zijn namelijk extra kwetsbaar op het gebied van digitale criminaliteit. Bij onze aanpak op plegers houden we rekening met het feit dat sommigen onbewust/onbedoeld dader worden of slachtoffer en pleger tegelijkertijd zijn.

Slachtoffers

Kinderen, jongeren en ouders/verzorgers

Wat zien we?

De jeugd is actief op online platforms, sociale media en interactieve apparaten. In deze digitale wereld lijken soms andere omgangsnormen te gelden dan in de fysieke wereld. Kinderen en jongeren zijn zich niet altijd bewust van de keuzes die zij online maken en wat de gevolgen zijn van dit online gedrag. Deze gevolgen spelen zich niet alleen online af, maar hebben ook impact in de fysieke wereld. Hoe je digitaal of op sociale media op elkaar reageert, zou hetzelfde moeten zijn als op het schoolplein. Door het gebrek aan digitale geletterdheid, vervagen online omgangsnormen. Ook kan het ontbreken van digitale geletterdheid hen kwetsbaar maken voor een breed scala aan digitale dreigingen, nepnieuws of desinformatie.

Daarnaast maakt het ontbreken van digitale geletterdheid kinderen in de basisschoolleeftijd doelwit voor cyberpesten, oplichting en misbruik (zoals shame sexting en grooming[16]). Digitale platforms kunnen een broedplaats zijn voor oplichters en criminelen die zich specifiek richten op jonge kinderen. Het is daarom van belang kinderen mediawijs en digitaal weerbaar te maken.

Ook bij jongeren in de leeftijd van 12 tot 21 jaar zien we een gebrek aan digitale geletterdheid en bewustzijn van de mogelijke risico's van online gedrag. Jongeren kunnen slachtoffer worden van cybercriminaliteit door bijvoorbeeld te klikken op kwaadaardige links of persoonlijke informatie te delen met onbekenden. Daarnaast zijn jongeren zich niet altijd bewust van de gevolgen of strafbaarheid van hun gedragingen op het internet en sociale media. Het feit dat persoonsgegevens of inloggegevens online te vinden zijn, betekent bijvoorbeeld niet dat je ze zomaar mag gebruiken. Wat in de fysieke wereld niet mag, mag ook niet in de online wereld.

Digitalisering en digitale criminaliteit zorgen ook voor nieuwe uitdagingen in de opvoeding van kinderen en jongeren. Ouders en verzorgers (hierna: ouders) maken zich zorgen over de veiligheid, het welzijn en gedrag van hun kinderen in een steeds meer gedigitaliseerde wereld en worstelen met hoe ze hen hierin kunnen opvoeden, vooral als ze zelf niet volledig vertrouwd zijn met digitale technologieën. Daarnaast zijn ouders niet altijd goed op de hoogte van het leven van hun kind in de digitale wereld.

Wat willen we bereiken?

Kinderen en jongeren kennen en herkennen de kansen, uitdagingen en risico's van de snel veranderende digitale tijd. Ze zijn zich bewust van hun online gedrag en de gevolgen die dit heeft in de online én fysieke wereld. Ook ouders kennen de risico's van de online wereld. Zij helpen hun kinderen zich veilig en verantwoord online te begeven en gebruik te maken van digitale middelen, zodat zij digitaal weerbaar zijn en zichzelf kunnen beschermen.

16 Er is sprake van grooming als een volwassene via ICT contact legt met een kind, met de intentie om dat kind te ontmoeten met het doel om seksueel misbruik te plegen of kinderpornografische afbeeldingen te produceren.

Dit doen we al en ontwikkelen we verder:

Wat	Samen met	Termijn
Samen werken aan online jongerenwerk en online welzijns-werk jongeren, waarmee jongeren leren een bewuste en kritische houding in te nemen.	JoU en DOCK	2023-2026
Scholen, Bibliotheek Utrecht en het Mediateam[17] werken samen om passende interventies aan te bieden.	Scholen, Bibliotheek Utrecht, het Mediateam	2023-2026
Ondersteunen van scholen met het lesaanbod veilig en weerbaar. In dit lesaanbod is het aanbod van mediawijsheid opgenomen, met o.a. lesmateriaal voor online sociaal gedrag en het aangeven van online grenzen.	Diverse partners	2023-2026
In gesprek met kinderen, jongeren en hun ouders over de informatie-behoefte; het samenbrengen van vraag en aanbod.	Diverse partners	2023-2026

Wat	Samen met	Termijn
Inzetten van het Mobiel Media Lab op scholen en in buurten.	Scholen, wijk-partners en politie	2023-2026
Aanbieden HackShield[18] en HackShield in de Klas. Meedenken met HackShield over nieuwe initiatieven of doorontwikkeling van bestaand aanbod.	Scholen, bibliotheken en individuen	2023-2026
Via tienerwerk op 15 basisscholen inspelen op vragen die er leven over de online leefwereld van kinderen en daarmee laag-drempelig bespreekbaar maken in de klas en op het schoolplein.	JoU, Tienerwerk	2023-2026

Wat	Samen met	Termijn
Uitvoeren Agenda tegen uitbuiting, met het oog op het voorkomen van jonge slachtoffers van online misbruik. Bijvoorbeeld door een campagne om te voorkomen dat jongeren als geldezels worden ingezet.	Samenwerkings-partners, zoals politie	2023-2026
Uitvoeren interventies speerpunt “versterken van de online aanpak” uit Utrecht zijn we Samen 2.0, Uitvoeringsprogramma tegen schadelijke polarisatie, radicalise-ring en extremisme.	Diverse partners	2023-2026
Inzetten op meldings- en aangif-tebereidheid.	Samenwerkings-partners	2023-2026

17 Mediateam ontwikkelt lesmateriaal voor primair en voortgezet onderwijs op het gebied van mediawijsheid, informatievaardigheden, ICT basisvaardigheden en computational thinking.
18 HackShield is een game die kinderen tussen de 8 en 12 jaar oud weerbaar maakt tegen cybercriminaliteit

Dit zijn onze nieuwe acties:

Wat	Samen met	Termijn
Meetbaar maken van de effectiviteit van het bestaande aanbod en peilen van de behoeftes van de doelgroep.	Onderzoeks-instellingen	2024-2025
Ontwikkelen en aanbieden voorlichting voor ouders van kinderen in de basisschoolleeftijd over de online wereld waarin hun kinderen zich begeven.	DOCK, Capgemini, Bibliotheek en wijken	2024
Meewerken aan de transitie van HackShield Academy naar Point of You (inclusief eigen platform en campagne) als passend middel voor bewustwording online gedrag en grenzen van jongeren.	O.a. Flavour en Saxion Hogeschool	2024

Senioren

Wat zien we?

We richten ons op de doelgroep 65+, rekening houdend met het feit dat er onderlinge verschillen zijn in digitale geletterdheid. Senioren zijn een kwetsbare groep als het gaat om digitale veiligheid. Een deel van hen heeft beperkte kennis van moderne technologieën, zijn minder vertrouwd met de online wereld en kunnen daardoor gemakkelijker slachtoffer worden van cybercriminaliteit. Verschillende (welzijns)organisaties en bibliotheken zetten zich in voor digitale inclusie, om de digitale kloof te dichten. Wanneer senioren digitaal (blijven) meedoen, is het belangrijk dat zij dit verantwoord kunnen doen en beter bewapend zijn tegen online misbruik en criminaliteit.

> “Ik heb weleens gehoord van phishing, maar ik weet niet wat het is”.
>
> **Deelnemer weerbaarheidstraining**

Een van de grootste zorgen is het toenemend aantal cyberdelicten dat gericht is op senioren. Het gemiddelde schadebedrag van een cyberdelict bij senioren is met €2700 hoger dan bij jongere mensen. Criminelen gebruiken diverse technieken zoals vriend-in-nood-fraude[19], bankhelpdeskfraude[20] en phishing[21] om persoonlijke gegevens te stelen of (financiële) fraude en identiteitsdiefstal te plegen. Bovendien kan het gebrek aan digitale vaardigheden en vertrouwen in de online wereld bij senioren hen belemmeren om ten volle te profiteren van de digitale wereld. Ze kunnen zich buitengesloten voelen van sociale interactie, essentiële diensten en informatiebronnen die online beschikbaar zijn.

Wat willen we bereiken?

Verschillende partijen in de stad die zich bezighouden met senioren en (digitale) weerbaarheid zijn met elkaar verbonden en brengen succesvolle initiatieven samen. Waar leemtes zijn, breiden we het bestaande aanbod uit met nieuwe initiatieven. Daarnaast spelen we snel en adequaat in op trends en ontwikkelingen, passen onze interventies hierop aan en nemen de doelgroep hierin actief mee.

19 Bij vriend-in-noodfraude krijgt het slachtoffer via WhatsApp zogenaamd een dringend verzoek van een vriend(in), familielid of bekende om snel geld over te maken. In werkelijkheid komt het appje van een cybercrimineel die zich voordoet als een bekende en geld wil aftroggelen.
20 Helpdeskfraude is een vorm van telefonische oplichting, waarbij fraudeurs doen alsof ze helpdeskmedewerkers van grote, bekende bedrijven zijn. Tegen betaling kunnen ze je helpen met niet-bestaande virussen, of proberen toegang tot je computer te verkrijgen. Ook bankhelpdeskfraude komt veel voor, dan bellen zogenaamd medewerkers van een bekende bank.
21 Via e-mail, sms of Whatsapp proberen informatie (zoals wachtwoorden) te verkrijgen.

Dit doen we al en ontwikkelen we verder:

Wat	Samen met	Termijn
Training Veilig Online voor senioren om hun online weerbaarheid te vergroten.	Stadsmakers digitale veiligheid, partners als Capgemini, DOCK	2023-2026
Organiseren van Digicafés.	Stadsmakers digitale veiligheid, Bibliotheek Utrecht (Informatiepunt Digitale Overheid)	2023-2026
Innovatieve interventies zoals het bordspel 'Weerbaar op het web'. actief verspreiden onder de doelgroep.	Wijken, DOCK	2023-2026
Inzetten op meldings- en aangiftebereidheid.	Samenwerkingspartners	2023-2026

Dit zijn onze nieuwe acties:

Wat	Samen met	Termijn
Interactieve film 'Echt of nep?' actief uitzetten bij de samenwerkingspartners.	DOCK, Buurtteams, wijken	2023-2024
Doorontwikkelen weerbaarheidstraining en uitbreiding aantal trainingen.	Capgemini, DOCK, wijken	2024
Verkennen van nieuwe locaties waar senioren samenkomen om initiatieven uit te zetten.	DOCK, Bibliotheek, wijken	2024
De mogelijkheid om aan te sluiten bij bestaande netwerken met betrekking tot senioren en veiligheid onderzoeken. Met als doel kennis en informatie-uitwisseling, handelingsperspectieven delen en samen inspelen op trends en ontwikkelingen.	Netwerkpartners senioren en (digitale) veiligheid	2024-2025

Foto gemaakt tijdens Cyber Boost Sessie voor ondernemers in november 2023.

Mkb en zzp

Wat zien we?

Het midden- en kleinbedrijf (mkb) en zelfstandigen (zzp) zijn steeds vaker slachtoffer van cybercriminaliteit. Cybercriminelen vallen ondernemers op verschillende manieren aan, zoals via phishing, ransomware of een DDoS aanval (zie begrippenlijst). Het doel is vaak toegang tot inloggegevens of andere gevoelige informatie om door te verkopen, af te persen, zakelijke identiteitsfraude[22] te plegen of om geld van zakelijke rekeningen te halen. Kleinere ondernemers zijn zich beperkt bewust van de gevaren van cybercriminaliteit. Zij denken dat er bij hen niets te halen valt en wanen zich veilig. Basismaatregelen zoals het maken en testen van back-ups of multifactorauthenticatie worden niet altijd voldoende doorgevoerd.

De gevolgen zijn groot: de kosten van een beveiligingsincident voor Nederlandse mkb'ers worden geschat op gemiddeld €270.000. Van de mkb'ers die gehackt worden, is 60% binnen zes maanden failliet door verloren productietijd. Daarnaast heeft een cyberaanval grote impact op de mentale gezondheid van een ondernemer. Zij ervaren bijvoorbeeld slapeloosheid, schuldgevoel en (in mindere mate) symptomen van trauma. Niet alleen tijdens de aanval, maar ook een week, maand of zelfs een jaar na het incident.

Er zijn verschillende publieke en commerciële organisaties die ondernemers op digitale risico's wijzen, zoals het Digital Trust Center (DTC), Platform Veilig Ondernemen Midden-Nederland (PVO), de politie, financiële dienstverleners, verzekeraars en cybersecurity-professionals. In het najaar van 2024 kan voor sommige bedrijven het beveiligingsniveau van netwerken en systemen worden afgedwongen. Vanaf oktober 2024 gaat namelijk de Europese richtlijn NIS2 gelden als Nederlandse wetgeving.

Wat willen we bereiken?

We willen bereiken dat zo min mogelijk Utrechtse ondernemers slachtoffer zijn van digitale criminaliteit. De bewustwording onder ondernemers is vergroot doordat we, met betrokken partners, veel voorkomende vormen van digitale criminaliteit blijvend agenderen. Ondernemers houden in hun bedrijfsvoering rekening met digitale risico's en investeren in beveiligingsmaatregelen. Ondernemers zijn veerkrachtig, zodat zij hun werkzaamheden na een cyberaanval zo spoedig mogelijk kunnen voortzetten.

22 Bij identiteitsfraude maken criminelen misbruik van valse of gestolen identiteitsgegevens. Ze kopen bijvoorbeeld op naam van iemand anders spullen zonder te betalen.

Dit doen we al en ontwikkelen we verder:

Wat	Samen met	Termijn
Organiseren van bijeenkomsten om bewustwording en veerkracht te creëren rondom het thema cybercriminaliteit. Zo organiseerden we in maart 2023 een grootschalig cyberevent voor Utrechtse ondernemers en in november 2023 trainingen rondom cyber response. Daarnaast biedt PVO Midden-Nederland doorlopend cyber-weerbaarheidstrainingen aan voor ondernemersverenigingen.	Netwerkpartners als PVO, financiële dienstverleners, KVK, U-tech community.	2023-2026
Op de website van het Cybernetwerk Utrecht bundelen we lokale initiatieven rondom preventie en handelings-perspectief. Zo is er informatie te vinden over soorten cyber-criminaliteit bij ondernemers, tips, informatie over evenementen zoals cyberweerbaarheids-trainingen, gratis cyberweer-baarheidsscans en beschikbare subsidiemogelijkheden voor het verhogen van de cyberveiligheid van een onderneming.	Netwerkpartners als PVO, financiële dienstverleners, KVK, U-tech community.	2023-2026

Wat	Samen met	Termijn
Gebruik maken van bestaande netwerken en structuren om het thema cyberweerbaarheid te agenderen.	Bijvoorbeeld het netwerk rondom het Keurmerk Veilig Ondernemen (KVO) op bedrijven-terreinen en winkelgebieden, het netwerk van Ondernemer Centraal en het Ondernemersfonds	2023-2026
Zo goed mogelijk ondersteunen van ondernemers(verenigingen) die aan de slag willen met het verbeteren van hun cyberweer-baarheid. We geloven hierbij in de kracht en de collectiviteit van het lokale netwerk en stemmen ons aanbod en dat van onze partners af op de desbetreffende ondernemersvereniging, branche of de individuele ondernemer.	PVO	2023-2026

Wat	Samen met	Termijn
Via www.utrecht.nl/ondernemen delen we een aantal online scans die ondernemers kunnen doen om de online weerbaarheid van hun bedrijf in kaart te brengen.		2023-2026
Ondernemers stimuleren om een melding te maken of aangifte te doen en hen wijzen op het beschikbare aanbod.	Fraudehelpdesk, politie, Slachtofferhulp Nederland	2023-2026

Dit zijn onze nieuwe acties:

Wat	Samen met	Termijn
Beter zicht op de meest voorkomende vormen van digitale criminaliteit en schadebedragen bij verschillende typen ondernemingen. Hiermee differentiëren we de doelgroep in grootte, branche of sector.	Fraudehelpdesk, politie	2023-2024
Praktische manieren ontwikkelen om mkb'ers te ondersteunen, bijvoorbeeld via een loket of adviestraject. Als regiogemeente willen we dit nog te ontwikkelen instrumentarium bij succes ook inzetten voor de regio.	Ondernemer Centraal. In de toekomst: Bureau Regionale Veiligheidsstrategie Midden-Nederland, PVO Midden-Nederland en provincie Utrecht	2023-2024
Onderzoeken hoe de MKB werkplaats een rol kan spelen bij het digitaal weerbaar maken van Utrechtse ondernemers.	MKB Werkplaats	2023-2024
Een rondgang langs de bestaande KVO's en georganiseerde ondernemers om het onderwerp digitale veiligheid te agenderen.	Andere afdelingen van de gemeente, zoals Wijken en Economische Zaken	2023-2026
Het aanbod voor ondernemers van (lokale) partners inzichtelijk en overzichtelijk maken en dit aanbieden aan ondernemers op een manier die bij hen past. Tegelijkertijd onderzoeken we of we dit aanbod uit kunnen breiden.	Platform Veilig Ondernemen Midden-Nederland (PVO), Kamer van Koophandel, U-Tech Community, Digital Trust Center (DTC) en Ondernemer Centraal.	2023 - 2026
Inzetten op de veerkracht na een cyberincident, door aan te sturen op een stappenplan bij cyberincidenten. Dit implementeren en testen we tijdens een incident response training, gericht op hoe te handelen na een cyberaanval.	Gemeente in samenwerking met netwerkpartners	2025

Plegers

Wat zien we?

Ondermijnende, georganiseerde misdaad gaat schuil achter een groot deel van de cyberaanvallen. Drugsgerelateerde en digitale criminaliteit zijn meer en meer met elkaar verweven geraakt. Ook de omvang, normalisering, verwevenheid met de bovenwereld en het georganiseerde karakter wijzen op georganiseerde criminaliteit.
De politie treft regelmatig drugs en wapens aan op locaties die een verband hebben met digitale criminaliteit. Sociale media/platforms en internet spelen een grote rol bij het ontstaan van daderschap van digitale en andere vormen van criminaliteit. Zo wordt het handelen in en aanschaffen van drugs bijvoorbeeld sterk vergemakkelijkt door online platforms en het dark web. Zoals beschreven in Grenzen stellen, perspectief bieden, worden afspraken voor drugsdeals onder meer via WhatsApp, Snapchat en Telegram gemaakt. Social media kunnen hiernaast ondersteunend zijn aan het rekruteringsproces van jonge aanwas, omdat zij een platform bieden waar influencers te zien zijn met grote sommen geld.

De crimineel die zelf onvoldoende technische kennis heeft, kan gebruik maken van ‘cybercrime-as-a-service’. De crimineel koopt een cybercrimeproduct waarmee een cyberdelict gepleegd kan worden. Doordat de dader digitale criminaliteit op afstand kan plegen, zijn de risico’s erg laag, terwijl de opbrengst hoog is.

Terwijl jongeren steeds bedrevener raken in het gebruik van technologie en het navigeren op het internet, zien we ook een toename van hun betrokkenheid bij digitale misdrijven. In 2021 was landelijk in 47% van de zaken iemand van 21 jaar of jonger betrokken tegenover 33% in 2018. Ook in absolute zin neemt het aantal cybercrimezaken met jonge verdachten toe: van 278 in 2018 tot 1329 in 2021. Daar zijn meerdere redenen voor. Een belangrijke factor is de toegankelijkheid van technologie en internet.

> “Ik heb geen medelijden met mijn slachtoffers. Als ik het niet doe, doet iemand anders het. Ik moet toch ook eten”.
>
> **Pleger bankhelpdeskfraude**

Vrijwel iedere jongere heeft tegenwoordig eenvoudig toegang tot digitale middelen, waardoor ze altijd verbonden zijn met de digitale wereld. Dit geeft hen de mogelijkheid om schadelijke activiteiten uit te voeren, zonder direct toezicht van ouders of autoriteiten.
Een andere factor is het gebrek aan digitale geletterdheid, bewustzijn en moreel kompas. Jongeren plegen soms strafbare feiten of vertonen ander schadelijk en/of normoverschrijdend onlinegedrag, zonder dat zij dit doorhebben. Jongeren zoeken de grenzen van de onlinewereld op, waarbij ze niet of nauwelijks wroeging hebben; het slachtoffer is voor hen anoniem of ze zijn in de veronderstelling dat de bank het schadebedrag zal vergoeden.

Er zijn risicofactoren die de kans groter maken dat iemand een dader wordt, maar ook beschermende factoren die daderschap kunnen voorkomen. Deze factoren zijn voor digitale criminaliteit hetzelfde als voor ‘reguliere’ criminaliteit en drugscriminaliteit. Er is dan ook nadrukkelijk aandacht voor preventie en weerbaarheid, waarbij aansluiting wordt gezocht bij de gemeentelijke aanpak tegen drugsgerelateerde criminaliteit (Grenzen Stellen, Perspectief Bieden).

Internet is ook een plek waar desinformatie ontstaat, met in uitzonderlijke gevallen als doel het aanwakkeren van polarisatie en ondermijning van de democratische rechtsorde. Online oproepen via social media kunnen leiden tot geweld, rellen en ongeregeldheden. Denk bijvoorbeeld aan de avondklokrellen in verschillende gemeenten tijdens de Coronapandemie die socialemediagebruikers aanjaagden en organiseerden. Online en offline staan voortdurend met elkaar in verbinding en versterken elkaar. Online oproepen tot geweld hebben in potentie een enorm bereik met alle openbare orde risico’s van dien. Er is sprake van een snelle mobilisatie van grote groepen en online gedeelde filmpjes van rellen en verstoringen kunnen weer tot nieuwe spanningen leiden. Dit maakt dat we instrumenten nodig hebben om wanordelijkheden in de kiem te smoren. De huidige wet- en regelgeving biedt op dit moment onvoldoende handvatten om online gecreëerde of aangejaagde openbare ordeverstoringen tegen te gaan.

Wat willen we bereiken?

Jongeren zijn zich bewust van de risico’s en gevolgen van hun onlinegedrag en de maatschappelijke impact die dat gedrag kan hebben. Hierdoor zijn ze veerkrachtig en kunnen ze juist handelen wanneer zij (onbewust/onbedoeld) dader dreigen te worden van een onlinedelict of ander schadelijk onlinegedrag. Jongeren kunnen via uitbuiting verzeild raken in digitale criminaliteit zoals sextortion of geldezel[23] zijn, waardoor ze dader, maar tegelijkertijd ook slachtoffer zijn. Hiervoor is nadrukkelijk aandacht in de aanpak. Verdachten worden opgespoord en zo mogelijk vervolgd. Het (herhaald) daderschap is tot een minimum beperkt. Jongeren worden met de aanpak niet wijzer gemaakt dan ze al zijn; we houden rekening met de dunne lijn tussen voorlichten en verleiden of uitlokken.

Online aangedreven ordeverstoringen worden zoveel mogelijk tegen gegaan voordat het een fysiek effect heeft op straat. De burgemeester wil en moet optreden waar dit het meeste effect heeft, ook online. Bijvoorbeeld door het opleggen van een last onder dwangsom waarmee direct en preventief kan worden opgetreden, voordat ongeregeldheden zich voltrekken. Een bestuurlijke maatregel gericht op het beëindigen en voorkomen van herhaling, kan snel worden getroffen. Online gedragingen die kunnen leiden tot ordeverstoringen vallen onder de reikwijdte van bevoegdheden van burgemeesters wanneer de online gedraging een effect kan hebben in de desbetreffende gemeente.

Steeds meer jongeren belanden in de cybercriminaliteit. En vooral: online fraude. Daarover is op onder meer TikTok en Telegram een hele wereld te vinden die de F-game wordt genoemd. NOS sprak met plegers en slachtoffers en maakte hier een filmpje over.

23 Geldezelschap of geldezel is het verschijnsel waarbij criminelen gebruik maken van de bankrekening van een ander om geld wit te wassen of te verplaatsen. Vaak wordt daarvoor gebruik gemaakt van zogenaamde "katvangers", personen die hun bankrekening beschikbaar stellen in ruil voor een kleine vergoeding

Dit doen we al en ontwikkelen we verder:

Wat	Samen met	Termijn
Inzetten Hack_Right, om first offender jonge hackers op het rechte pad te krijgen én houden.	Politie	2023-2026
Digitale criminaliteit opnemen in het plan van aanpak Preventie en weerbaarheid, als onderdeel van Grenzen stellen, perspectief bieden.	-	2023-2026
Inzetten van social mediacampagnes om de doelgroep gericht te bereiken, bijvoorbeeld ter voorkoming van daderschap binnen geldezelschap.	-	2023-2026
Doorontwikkelen handreiking 'Online aangejaagde ordeverstoringen'.	CCV	2023-2026
Ontwikkelen van barrièremodellen.	CCV	2023-2026
Pleiten voor landelijke wetgeving en instrumentarium zodat de burgemeester kan optreden bij (vrees voor) ernstige orde verstoringen die online worden veroorzaakt en aangejaagd.	-	2023-2026
Beschikbaar stellen van het lesaanbod veilig en weerbaar om daderschap te voorkomen.	Scholen	2023-2026

Dit zijn nieuwe acties die we starten:

Wat	Samen met	Termijn
Verdiepend onderzoek naar de problematiek in Utrecht, zodat inzichtelijk wordt welke specifieke doelgroepen zich met welke vormen van digitale criminaliteit bezighouden.	Samenwerkingspartners, w.o. Politie, OM, RVS en RIEC	2024-2026
Op basis van de bevindingen uit bovenstaand onderzoek onderzoeken of en hoe het preventieve aanbod voor potentiële daders en een persoonsgerichte aanpak voor cyberdaders kan worden geoptimaliseerd.	Samenwerkingspartners	2024-2026
Vergroten vakbekwaamheid ten behoeve van persoonsgerichte aanpak, o.a. herkennen van signalen digitale criminaliteit en inzetten van passend aanbod.	Samenwerkingspartners	2024- 2026
Onderzoeken of en hoe re_B00TCMP in Utrecht kan worden georganiseerd, waarbij de ervaringen, aandachtspunten en adviezen van andere initiatieven uit het land worden meegenomen.	Politie, JoU, Utrechtse cybersecuritybedrijven	2024- 2025
Ontwikkelen van een integrale aanpak rondom geldezels.	Politie, Halt, Slachtofferhulp Nederland	2024-2025

Digitale weerbaarheid van de stad

Digitale aanvallen en/of calamiteiten kunnen een grote impact hebben op de maatschappij en de openbare orde in de stad. In Utrecht hebben we daarom een community voor cyber-weerbaarheid opgericht, waarmee we werken aan de digitale weerbaarheid van de stad als geheel. Daarnaast bereiden we ons voor op crises met een digitale component samen met de traditionele crisispartners en de partners uit de community.

Community voor cyberweerbaarheid

Wat zien we?
Bedrijven zijn met elkaar verbonden. Organisaties nemen producten of diensten af van andere partijen, zoals software (bijvoorbeeld voor salarisadministratie, klantregistratie of bevoorrading), dataopslag of clouddiensten. Weinig organisaties kunnen zonder toeleverancier of afnemer opereren. Werken aan de digitale weerbaarheid van de eigen organisatie is dus niet genoeg. Er is sprake van keten-afhankelijkheid. Door de digitale vervlechting ben je afhankelijk van de digitale weerbaarheid van je toeleveranciers en afnemers.

Bij een digitale storing of incident overstijgen de effecten vaak individuele organisaties en kunnen hun weerslag hebben op de hele Utrechtse samenleving. Om die reden is in 2019 een community voor cyberweerbaarheid (hierna: community) opgericht. Hierin werken we samen aan de digitale weerbaarheid van Utrecht als stad. Dit doen we onder andere door informatie- en kennisuitwisseling en het samen ontwikkelen van concrete initiatieven. Bij de community zijn organisaties aangesloten die een bijdrage leveren aan producten en diensten van de Utrechtse samenleving, zoals onderwijsinstellingen, ziekenhuizen, cybersecuritybedrijven, de provincie, vervoersmaat-schappijen, politie en de Veiligheidsregio Utrecht.

Wat willen we bereiken?
Het belang van samenwerken in de community is een vanzelf-sprekendheid. De ketenafhankelijkheid wordt door alle betrokkenen ingezien. Betrokken organisaties leren van elkaar en zijn zo gezamenlijk minder kwetsbaar voor cybercriminaliteit. Meer partijen zien het belang in van de community en sluiten zich er bij aan; vrijwillig, maar niet vrijblijvend. Door samen te werken hebben we korte lijntjes bij incidenten, delen we kennis en verminderen we de kwetsbaarheid.

Dit doen we al en ontwikkelen we verder:

Wat	Samen met	Termijn
Organiseren van community-bijeenkomsten om kennis- en informatie-uitwisseling te stimuleren. Thema's : digitaal veilig werken, cybercrises, ketenafhankelijkheid en weerbaar-heid van digitale infrastructuur.	Input van community-partners	2023-2026
Samen oefenen voor cybercrises (zie ook volgend hoofdstuk 'Crisisbeheersing').	Community	2023-2026
Structureel in gesprek met onze communitypartners om te blijven peilen waar de behoeftes liggen.	Community	2023-2026
Uitwisselen van ideeën en ervaringen uit rondom een community, ecosysteem of andere vergelijkbare initiatieven.	Met Amsterdam, Rotterdam en Den Haag	2023-2026

Wat	Samen met	Termijn
Inzetten op meldings- en aangiftebereidheid	Samenwerkings-partners	2023-2026

Dit zijn onze nieuwe acties:

Wat	Samen met	Termijn
Leren van elkaars best practices rondom veilig digitaal werken (bijvoorbeeld medewerkers-bewustzijn)	Community onder leiding van community-manager gemeente Utrecht	2023-2026
Digitale weerbaarheid agenderen bij mkb'ers en zzp'ers in de stad en regio	Community onder leiding van community-manager gemeente Utrecht	2023-2026
Verkennen van behoefte voor een CISO-netwerk voor CISO's van overheidsorganisaties uit Midden-Nederland (gemeenten, provincies, waterschappen)	Bureau Regionale Veiligheidsstrategie Midden-Nederland (RVS)	2024
Samen kansrijke trajecten verkennen voor de aanpak van digitale risico's in de keten, zoals bijvoorbeeld het stellen van voorwaarden aan toeleveranciers.	Community onder leiding van community-manager gemeente Utrecht	2023-2026
De geleerde lessen uit de community delen met organisaties die (nog) niet betrokken zijn.	Community onder leiding van community-manager gemeente Utrecht	2023-2026

Crisisbeheersing

Wat zien we?
Net zoals we voorbereid zijn op rampen als branden of overstromingen, moeten we rekening houden met de gevolgen van een digitale crisis. Denk aan een cybercrisis, waarin een aanvaller systemen van de gemeente platlegt. Of een digitaal incident waardoor maatschappelijke voorzieningen uitvallen, zoals het openbaar vervoer of ziekenhuizen. Het kan ook gaan om een online dreiging waardoor scholen niet open kunnen. Ook een aanval bij een ketenpartner waardoor het uitvoerend proces bij een andere (Utrechtse) organisatie uitvalt, behoort tot de mogelijkheden. We moeten ons daarom als stad voorbereiden op de mogelijke gevolgen van een crisis en de kans erop zo klein mogelijk maken.

De gemeentelijke organisatie bereidt zichzelf voor door de eigen systemen te beschermen tegen aanvallen en te oefenen met digitale incidenten en crises. Ook maatschappelijke instellingen in de stad moeten zich voorbereiden op digitale dreigingen en incidenten. Veel organisaties in bijvoorbeeld de zorg of de verkeersinfrastructuur zijn hier al actief mee bezig. Uit een eerdere cybercrisisoefening zien we de behoefte om de rollen en verantwoordelijkheden van partners uit de community voor cyberweerbaarheid in relatie tot crisisbeheersing te verduidelijken.

Wat willen we bereiken?
De bestaande crisisstructuren zijn goed ingericht en voorbereid op digitale crises. Binnen deze structuren wordt blijvend de dialoog gevoerd met maatschappelijke instellingen, organisaties en samenwerkingsverbanden, waar de risico's van een digitale crisis regelmatig worden geagendeerd. Door voortschrijdend inzicht worden de crisisstructuren geoptimaliseerd.

Dit doen we al en ontwikkelen we verder:

Wat	Samen met	Termijn
Digitale crisis is onderdeel van opleiden, trainen en oefenen van de crisisfunctionarissen	-	2023-2026
Voorbereiden met stedelijke partners op digitale crises en op mogelijk langer durende ontwrichtende maatschappelijke effecten van een langdurige crisis.	Crisispartners	2023-2026

Dit zijn onze nieuwe acties:

Wat	Samen met	Termijn
In het Stedelijk Veiligheidsnetwerk de voorbereiding op digitale crisis als aandachtspunt agenderen.	Netwerkpartners	
Informeren en trainen van maatschappelijke partners over de werkwijze bij crises	VRU	2024-2026
Versterken van opleiden, trainen en oefenen met digitale crisis van de crisisorganisatie	Crisisorganisatie	2024-2026
Deelnemen aan landelijke ISIDOOR oefening.	-	2025

Communicatie

Communicatie kan een grote rol hebben bij de ambitie om de bewustwording en de weerbaarheid van inwoners, bedrijven en organisaties te vergroten.

Daarbij nemen we de volgende uitgangspunten mee:

- Digitale criminaliteit is een grensoverschrijdend probleem. Daarom proberen we zoveel mogelijk vanuit communicatie aan te haken op campagnes, acties en middelen die landelijk of door (landelijke) partners worden ontwikkeld.
- We werken samen met (publieke en private) partners in de stad en erbuiten.
- We zoeken zoveel mogelijk de bestaande netwerken van bewoners en ondernemers in de stad en in wijken op en sluiten aan op de signalen, wensen en behoeftes van bewoners en ondernemers daar.
- Omdat het landschap van digitale criminaliteit zeer snel verandert, willen we ook qua communicatie inzet flexibel blijven, zodat we kunnen inspelen op toekomstige ontwikkelingen.
- We meten en toetsen zoveel mogelijk onze communicatie inzet en gaan door met effectieve interventies en ontwikkelen.

Financiën

Er is structureel budget van €30.000 euro per jaar beschikbaar voor de aanpak van digitale weerbaarheid. In het coalitieakkoord zijn aanvullend gelden beschikbaar gekomen voor digitale weerbaarheid. We investeren daarmee in zowel de stad (bewoners en organisaties) als onze eigen organisatie (assets) om deze digitaal weerbaarder te maken. Om die reden zijn de middelen voor de uitvoering 50/50 verdeeld over de programma's Veilige Stad en Aantrekkelijke Groene Leefomgeving en Erfgoed. Daarmee vergroten we enerzijds de weerbaarheid van inwoners, ondernemers en organisaties en brengen we onze crisisbeheersing verder op orde. Anderzijds vergroten we de weerbaarheid van onze assets in de buitenruimte (zoals de openbare verlichting en verkeersregelinstallaties). De interventies uit dit Uitvoeringsprogramma zijn gericht op de weerbaarheid van inwoners, ondernemers en organisaties en de crisisbeheersing. Naast de inzet van personeel (1,9 fte) vanuit de reguliere structurele begroting Veilige stad zijn er vanuit het coalitieakkoord voor de periode tot en met 2026 middelen ter beschikking gesteld. Vanuit deze middelen wordt een extra formatieplek van 1 fte gedekt, het resterende budget wordt besteed aan de diverse activiteiten zoals verwoord in dit uitvoeringsprogramma. Het betreft onder andere campagnes en campagnematerialen, trainingen en evenementen, kosten voor ondersteunende digitale platforms, onderzoek en inhoudelijke advisering t.b.v. kennis en expertise.

Financiën uitvoeringsprogramma Digitale Veiligheid (x €1.000)	2023	2024	2025	2026
Personele inzet (1fte)	92	92	92	92
Activiteitenbudget	63	188	188	188
Totaal benodigd budget	155	280	280	280

Reeds gedekt in de begroting (x €1.000)	2023	2024	2025	2026
Structureel budget voor digitale veiligheid	30	30	30	30
Bijdrage coalitieakkoord programma Veilige stad	125	250	250	250
Saldo niet gedekte kosten	**0**	**0**	**0**	**0**

Verantwoording

Voor het verbeteren van de digitale weerbaarheid zijn middelen beschikbaar gesteld vanuit het coalitieakkoord. We verantwoorden over de voortgang op dit uitvoeringsprogramma via de jaarlijkse rapportage van de Veiligheidsagenda 23-26. Voor deze verantwoording wordt het Utrechts sturingsmodel, Rijker Verantwoorden, gehanteerd, waarbij we naast cijfers ook verhalen en ervaringen gebruiken om te laten zien wat we hebben gedaan en wat het effect is.

Begrippen en afkortingen

Begrippenlijst

In deze begrippenlijst vind u eerst algemene begrippen en vervolgens meer specifieke vormen van cybercriminaliteit.

Algemene begrippen

Begrip	Toelichting
Cybercrime	Misdrijven die gepleegd worden met een ICT-middel (bijvoorbeeld een computer, smartphone of internetbrowser) die gericht zijn op ICT, zoals hacking, mal- of ransomware en virussen.
Digitale inclusie	Digitale inclusie betekent dat Utrechters toegang hebben tot, gebruik kunnen maken van en weerbaar zijn voor digitale technologie en zo onderdeel (willen) uitmaken van de digitale samenleving. Met speciale aandacht voor groepen in een kwetsbare positie zoals laaggeletterde Utrechters, senioren die niet zelfstandig overweg kunnen op het internet, Utrechters met een beperking en mensen met beperkte financiële middelen.
Gedigitaliseerde criminaliteit	Traditionele misdrijven waarbij ICT als middel wordt ingezet, maar niet het doel is. Voorbeelden zijn helpdeskfraude, fraude met online handel en sextortion.
Geldezelschap	Geldezelschap of geldezel is het verschijnsel waarbij criminelen gebruik maken van de bankrekening van een ander om geld wit te wassen of te verplaatsen. Vaak wordt daarvoor gebruik gemaakt van zogenaamde "katvangers", personen die hun bankrekening beschikbaar stellen in ruil voor een vergoeding.
HackShield	HackShield is een game die kinderen tussen de 8 en 12 jaar oud weerbaar maakt tegen cybercriminaliteit.
Mediateam	Ontwikkelt lesmateriaal voor primair en voortgezet onderwijs op het gebied van mediawijsheid, informatievaardigheden, ICT basisvaardigheden en computational thinking.
Online normoverschrijdend gedrag	Online gedrag dat niet strafbaar is, maar wel schadelijk, zoals cyberpesten, shame sexting, het verspreiden van desinformatie of het delen van boodschappen die leiden tot schadelijke polarisatie of maatschappelijke onrust.
Stadsmakers digitale veiligheid	Stadsmakers digitale veiligheid wonen in Utrecht en willen graag hun steentje bijdragen aan de digitale veiligheid van de stad en haar inwoners. Dit doen zij op verschillende manieren: de een geeft weerbaarheidstrainingen aan senioren, de ander geeft gastlessen op school. Deze activiteiten kunnen voortkomen uit vragen van partners uit de stad, of kunnen de Stadsmakers zelf initiëren; aansluitend op ieders expertise.

Vormen van cybercriminaliteit

Vorm	Toelichting
CEO-fraude	Vorm van fraude waarbij een medewerker een e-mail krijgt waarbij de afzender de CEO of directeur lijkt. De afzender vraagt om een geldbedrag over te maken. Vaak is er volgens de afzender haast geboden bij de betaling. De medewerker maakt nietsvermoedend het geldbedrag over en later, wanneer de medewerker contact heeft gehad met de echte directeur, blijkt sprake te zijn van oplichting.
Cybercrime-as-a-service (CaaS)	Het aanbieden van cybercrimediensten en -toolkits via illegale marktplaatsen op het darkweb, zoals bijvoorbeeld voor het uitvoeren van een DDoS aanval of scripts voor phishing.
Distributed Denial-of-Service-aanval (DDoS aanval)	Criminelen versturen enorm veel dataverkeer naar een server, website of app. Omdat er zoveel verzoeken tegelijk verwerkt moeten worden, wordt het verkeer van en naar de website geblokkeerd en kan zelfs de server van de dienst crashen. Gevolg is dat de dienst slecht of helemaal niet bereikbaar is voor bezoekers.
Fraude met betaalproducten	Simmen of skimming: het onrechtmatig kopiëren van betaalkaartgegevens.
Fraude met online handel (internetoplichting)	Internetoplichting komt voor bij het (ver)kopen van spullen online, bijvoorbeeld via sociale media of een online marktplaats. Er is sprake van internet-oplichting als iemand een product betaalt, maar vervolgens niks ontvangt. Of een product wordt opgestuurd door de verkoper, maar ontvangt geen betaling.
Grooming: digitaal kinderlokken	Er is sprake van grooming als een volwassene via ICT contact legt met een kind, met de intentie om dat kind te ontmoeten met het doel om seksueel misbruik te plegen of kinderpornografische afbeeldingen te produceren.
Helpdeskfraude	Helpdeskfraude is een vorm van telefonische oplichting, waarbij fraudeurs bellen en doen alsof ze helpdeskmedewerkers van grote, bekende bedrijven zijn. Tegen betaling kunnen ze je helpen met niet-bestaande virussen, of proberen toegang tot je computer te verkrijgen. Ook bankhelpdeskfraude komt veel voor, dan bellen zogenaamd medewerkers van een bekende bank.
Identiteitsfraude	Bij identiteitsfraude maken criminelen misbruik van valse of gestolen identiteitsgegevens. Ze kopen bijvoorbeeld op naam van iemand anders spullen zonder te betalen.
Multifactorauthenticatie	Een extra veiligheidslaag in de toegangsvereisten van een systeem of applicatie. Factoren worden ingedeeld in drie categorieën: iets weten (bijvoor-beeld een wachtwoord), iets hebben (bijvoorbeeld een token) of iets zijn (bijvoorbeeld een vingerafdruk). Bij minimaal twee factoren, spreken we van multifactorauthenticatie.
Phishing	Via e-mail, sms of Whatsapp proberen informatie (zoals wachtwoorden) te verkrijgen.

Vorm	Toelichting
Ransomware	Malware die je systeem, netwerk of data op slot zet. Criminelen eisen betaling om weer toegang te krijgen tot systemen.
Sexting en shame sexting	Sexting is het versturen van seksueel getinte berichten, foto's of video's. Dit is in essentie onschuldig. Wanneer de seksueel getinte beelden in de verkeerde handen terechtkomen en ongewild verspreid worden, is sprake van ‘shame sexting’. De beelden worden doorgestuurd uit bijvoorbeeld wraak of na een ruzie.
Sextortion	Dreigen met het doorsturen van (pikant getinte) beelden als chantagemiddel.
Vriend-in-nood fraude	Bij vriend-in-noodfraude krijgt het slachtoffer via WhatsApp zogenaamd een dringend verzoek van een vriend(in), familielid of bekende om snel geld over te maken. In werkelijkheid komt het appje van een cybercrimineel die zich voordoet als een bekende en geld wil aftroggelen.

Afkortingenlijst

Afkorting	Toelichting
AI	Kunstmatige intelligentie
Caas	Cybercrime-as-a-service (zie begrippenlijst)
CBS	Centraal Bureau voor Statistiek
CISO	Chief Information Security Officer: houdt in een organisatie toezicht op de informatie-, cyber- en technologiebeveiliging.
DDoS	Distributed Denial-of-Service-aanval (type cyberaanval, zie begrippenlijst)
DOCK	Welzijnswerk Utrecht
DTC	Digital Trust Center: platform vanuit het ministerie van Economische zaken en Klimaat om (kleinere) ondernemers
G4	De vier grote steden: Amsterdam, Rotterdam, Den Haag, Utrecht
ISIDOOR	Een grootschalige cyberoefening georganiseerd door het NCSC in samenwerking met de NCTV.
JoU	Jongerenwerk Utrecht
KVO	Keurmerk Veilig Ondernemen
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NSCS	Nationaal Cyber Security Centrum
OM	Openbaar Ministerie
PVO en PVO M-NL	Platform Veilig Ondernemen. Regionaal is onze partner Platform Veilig Ondernemen Midden-Nederland (PVO M-NL)
RIEC	Regionale Informatie- en Expertise Centra: richten zich op ondermijnende criminaliteit
RVS	Bureau Regionale Veiligheidsstrategie Midden-Nederland
VRU	Veiligheidsregio Utrecht: samenwerkingsverband van en voor alle 26 Utrechtse gemeenten in de provincie Utrecht

Bronnen

CCV, Sociale media als hulpmiddel in de strijd tegen cybercriminaliteit
https://ccv-secondant.nl/platform/article/sociale-media-als-hulpmiddel-in-de-strijd-tegen-cybercriminaliteit-1

NSCR, Negatief en positief cybergedrag gaat vaak samen bij jongeren die ICT-onderwijs volgen
https://nscr.nl/negatief-en-positief-cybergedrag-gaat-vaak-samen-bij-jongeren-die-ict-onderwijs-volgen/

Universiteit van Twente, Probleemverkenning 'Cybercrime en Jeugd' - Een kwalitatief onderzoek naar de verschillende vormen van cybercriminaliteit gepleegd door jongeren tot 18 jaar, en hun achtergrondkenmerken, motieven en criminele carrières
https://essay.utwente.nl/63512/

Wetenschappelijk Onderzoek- en Documentatiecentrum, Jeugdige daders van cybercrime in Nederland
https://repository.wodc.nl/handle/20.500.12832/1975

Wetenschappelijk Onderzoek- en Documentatiecentrum, Meer kennis over cyber- en gedigitaliseerde criminaliteit nodig
https://www.wodc.nl/actueel/nieuws/2020/09/11/meer-kennis-over-cyber--en-gedigitaliseerde-criminaliteit-nodig

Wetenschappelijk Onderzoek- en Documentatiecentrum, Cyberdaders: uniek profiel, unieke aanpak
https://www.wodc.nl/actueel/nieuws/2020/01/28/cyberdaders-uniek-profiel-unieke-aanpak

Colofon

Januari 2024

Gemeente Utrecht
Openbare orde en veiligheid

Fotografie
Pagina 3: Femke van den Heuvel
Pagina 17: GRATE agency
Beeld op de cover en backcover zijn door AI gegenereerd

Ontwerp en Illustraties
Enof creatieve communicatie

Contactgegevens
Postbus 16200
3500 CE Utrecht
Telefoon: 14 300 (verkort nummer)