Gezocht: niet te hacken wachtwoord

Digitaal huiselijk geweld van ex-partners, via online accounts, is een groeiend probleem. Slachtoffers worden vaak niet serieus genomen. ‘Ze vroegen of ik overspannen was.’

tekst Alice Boothby, foto Alexandra España

Jaarlijks worden honderdduizenden mensen in Nederland slachtoffer van huiselijk geweld. Een steeds groter groeiende groep slachtoffers krijgt ook te maken met digitaal huiselijk geweld, waarbij online middelen worden ingezet om een (ex-)partner het leven zuur te maken. Door mee te lezen met e-mails, foto’s te verspreiden of een telefoon, laptop of smartwatch te tracken, probeert de ander op afstand invloed uit te oefenen. De consequenties kunnen groot zijn: wat als een kwaadwillende ex zich toegang weet te verschaffen tot de DigiD van de ander?

Paula van den Boom, directeur van SafetyNed, een online expert voor huiselijk geweld, kent de verhalen uit de praktijk als geen ander. SafetyNed is opgericht door vier grote opvangorganisaties (Arosa, Blijf Groep, Moviera en Perspektief) en ondersteunt, naast slachtoffers, ook hulpverleners, politie en justitie, door kennis te verzamelen en te delen. “Het geweld bouwt langzaam op,” zegt Van den Boom. “Na escalatie is vluchten vaak niet genoeg, het huiselijk geweld gaat online gewoon door.” Het digitaal geweld gaat vaak veel verder dan inbreken in een mailbox of socialmedia-account. Zo kwamen bij SafetyNed meldingen binnen van een zender met microfoon en gps-tracker die in de teddybeer van een kind werd gevonden, en slachtoffers die letterlijk in de kou werden gezet door een ex die de ‘slimme’ thermostaat op afstand bediende.

Gevoel van onmacht

Cijfers van het precieze aantal slachtoffers zijn er niet. Want net als bij fysiek geweld, voelt de stap om naar de politie te gaan vaak groot. Sophie* (42) deed uiteindelijk aangifte van computervredebreuk. Ze had al een tijdlang het gevoel dat ze gehackt was, maar kon de vinger niet precies op de wond leggen. “Ik had het gevoel dat mijn expartner meelas met mijn e-mails. Dat vermoeden werd bevestigd toen er foto’s van me verschenen op Facebook en Twitter. Op een gegeven moment ontving ik via Whatsapp wel honderden audioberichten per dag met vreselijke verwensingen. De angst sloeg toen echt toe.”

Toen Sophie aangifte deed, had ze het gevoel dat ze nergens terechtkon met specifieke vragen over haar digitale veiligheid. Ze meldde zich bij een lotgenotengroep van Blijf Groep Amsterdam, bij Slachtofferhulp en bij de politie. “Niemand kon me vertellen hoe ik mezelf online kon beveiligen, wat ik moest installeren. Ik heb het allemaal zelf opgezocht.” Uiteindelijk wist Sophie zo veel bewijsmateriaal te verzamelen dat haar ex kon worden veroordeeld. Maar zodra hij vrijkwam, verschenen er weer belastende foto’s van Sophie op Twitter. “Ik belde de politie en lichtte hen in over het bewuste twitteraccount. Ze wisten niet goed wat ze ermee aan moesten. Toen zakte de moed me pas echt in de schoenen.”

Dat gevoel van onmacht herkent Sarah* (41), eveneens slachtoffer van digitaal huiselijk geweld. Ze is op het moment van schrijven verwikkeld in een rechtszaak met haar ex, die haar Googleaccount tien maanden lang heeft gehackt en zich daarmee toegang verschafte tot haar foto’s en e-mails. Of eigenlijk: hij heeft haar laten hacken, ‘want zo technisch onderlegd was hij ook weer niet.’

Andere prioriteiten

De mishandelingen bij Sarah begonnen psychisch, al dreigde haar ex ook met fysiek geweld. Later sloeg de terreur digitaal toe. Sarah had het gevoel dat ze werd afgeluisterd. Ze hoorde een echo tijdens telefoongesprekken, en haar telefoon werd soms heel warm. De inhoud van gesprekken die ze in privésfeer voerde, werden later tegen haar gebruikt in de rechtszaal. Sarah stapte naar de politie, maar kreeg niet het gevoel dat ze serieus werd genomen.

Sarah: “Tijdens de aangifte was er geen digitaal rechercheur aanwezig en er werd me gevraagd of ik ‘niet een beetje overspannen was.’” Een uitspraak die pijn deed. “De politie adviseerde me mijn e-mail niet meer te gebruiken en alle gesprekken buitenshuis te voeren. Maar hoe moet dat, met drie kinderen? Dat kan gewoon niet.” Ook kreeg ze het advies om de fraudehelpdesk te bellen en dat ze de feiten zelf maar moest achterhalen. “Feiten als een IP-adres, dat alleen de politie mag opvragen.”

Toen Sarah zelf een computeranalist inschakelde, zag deze bijna meteen dat er een vreemde telefoon aan haar Googleaccount was gekoppeld. Sarah: “Ik stond maandenlang met 0-1 achter. Terwijl ik met mijn gezin midden in een proces zat met Veilig Thuis en een advocaat, las mijn ex alles mee. Heel beangstigend.” De politie kon het afgelopen jaar weinig voor Sarah betekenen. De zaak werd niet vervolgd vanwege andere landelijke prioriteiten.

Inmiddels heeft Sarah noodgedwongen al haar accounts moeten verwijderen, is de camera van haar laptop afgeplakt, gebruikt ze een beveiligingssleutel om in te kunnen loggen in haar belangrijkste accounts, en heeft ze een duur telefoonabonnement met een onbeperkte 4G-internetbundel, omdat het gebruik van wifi in huis op dit moment te risicovol is. Sarah: “Ik blijf waakzaam. En die waakzaamheid zal nooit meer weggaan.”

Stap in de goede richting

Volgens Paula van den Boom van SafetyNed staat Sarahs verhaal niet op zichzelf. In het werkveld lopen hulpverleners tegen een kennisachterstand aan. SafetyNed maakt al een behoorlijke slag door hen trainingen aan te bieden. “Maar,” stelt Van den Boom. “Met een jaarlijkse training ben je er niet. Het probleem groeit zo hard, daar moeten ze in meegroeien.” Als stap in de goede richting lanceerde SafetyNed onlangs de app Serious Game. Deze helpt hulpverleners bij het maken van een risicoinschatting en legt ze verschillende casussen voor. Van den Boom hoopt hiermee ‘de hele keten te raken’. “Denk aan politie, wijkteams, Veilig Thuis, Centrum voor Seksueel Geweld. Iedereen die in contact komt met slachtoffers van digitale dreiging.”

SafetyNed wil ook binnenkort naar de Tweede Kamer om daar de verhalen te vertellen van slachtoffers, omdat digitaal huiselijk geweld vaak onterecht als abstract wordt afgedaan. “Wraakporno, daar kunnen mensen zich een voorstelling van maken. Dat iemands smartwatch afgaat zodra hij of zij een paar meter van huis is, omdat een ex dat heeft ingesteld om te zieken, is moeilijker om je voor te stellen. Digitaal huiselijk geweld is een breed maatschappelijk probleem. Daar wil ik graag voor lobbyen.”

***De namen van zowel Sophie als Sarah zijn om veiligheidsredenen gefingeerd.**

‘Terwijl ik met mijn gezin in een proces zat met Veilig Thuis en een advocaat, las mijn ex alles mee’

Politie Amsterdam

Rik Langedijk (54), teamleider van Cybercrime Amsterdam, herkent het beeld dat een computervredebreukzaak vaak lastig is om op te lossen. “Maar dat we sinds 2015 een team Cybercrime hebben, geeft aan hoe belangrijk wij het vinden.” Team Cybercrime werkt met ondersteuning van Team Digitale Opsporing en zorgt voor de preventie en opsporing van cybercrime in Amsterdam.
Door middel van cursussen en presentaties probeert het team collega’s bewust te maken van de impact van computervredebreuk. Langedijk kan niet precies zeggen hoeveel aangiftes van computervredebreuk in de relationele sfeer er spelen in de stad. De aangiftebereidheid is volgens hem namelijk vrij laag. “Er zijn de afgelopen jaren zaken geweest waarbij verdachten tot drie jaar kregen voor computervredebreuk, maar dan heb je het echt over grootschalige onderzoeken waarbij meerdere accounts werden gehackt.”

Computervredebreuk

Computervredebreuk is strafbaar gesteld in artikel 138ab van het Wetboek van Strafrecht. Er staat een gevangenisstraf van maximaal 4 jaar op, afhankelijk van het type zaak. Vaak wordt onterecht gedacht dat het alleen om ‘hacken’ gaat. Ook wanneer je zonder instemming binnen een relationele sfeer inlogt met de gegevens van een ander, pleeg je computervredebreuk.

Digitaal scheiden

Ga je uit elkaar? Scheid dan ook digitaal. Reset wachtwoorden en verbreek eventueel gedeelde e-mailadressen en cloud-accounts. Stel, indien mogelijk, een tweestapsverificatie in. Dit maakt de kans op gehackt worden kleiner. Kijk voor meer tips op laatjeniethackmaken.nl.

Dossier

Wanneer je slachtoffer van digitaal huiselijk geweldbent geworden, is het belangrijk dat je een dossier opbouwt. Maak screenshots en verzamel zo veel mogelijk bewijs. Belangrijk om te weten is dat onder andere Google, Twitter en Facebook inzicht geven in wanneer er vanaf welk apparaat is ingelogd. Als je vervolgens aangifte doet, kun je dit dossier gebruiken. Neem eventueel ook contact op met SafetyNed, zij kunnen je adviseren over eventuele vervolgstappen.