Cybercriminaliteit en digitalisering

Arnor Maertens

Klikken kent gevolgen

Bachelorproject

Academiejaar: 2025-2026

Lesgever: Coudenys Siegfried

HO GENT

Inleiding

Het blauwe licht van de smartphone snijdt door het donker. Een melding licht het startscherm op: een verkeersboete die dringend betaald hoort te worden. Hartslag versnelt. Zonder na te denken wordt al snel de mail geopend. Op de website vullen de vingers haastig persoonlijke gegevens in. Naam, wachtwoord, bankgegevens en rijkregisternummer worden ingevuld. Een zucht van opluchting volgt, de schuld is namelijk ingelost. Maar de werkelijkheid is genadeloos. Realiteit barst los, grote sommen geld verdwijnen van de bankrekening. Weggesluisd naar onzichtbare rekeningen, terwijl het slachtoffer nog nietsvermoedend opgelucht de telefoon weglegt en verdergaat met het dagdagelijks leven. Dit is geen fictie en ook geen scène uit een true-crime serie, maar het is de realiteit voor velen. Enkel en alleen via phishingpogingen werd er in 2023 ongeveer 40 miljoen euro buitgemaakt (*Cijfers 2023: "Phishing en Andere Kapers op de Kust"* | *Febelfin*, 2024). In veel van deze gevallen, zelfs voordat de fout werd opgemerkt, is de buit al lang verdwenen en ontraceerbaar geworden alsof het geld nooit had bestaan.

Dit is maar één voorbeeld van een casus die zich afgelopen maanden dikwijls voordeed tijdens mijn stageperiode bij Digibank Gent en Digibank Plus. Deze casussen trokken steeds mijn aandacht. 'Hoe kan dit steeds voorkomen?' klonk het in mijn hoofd. Thema's van cybercriminaliteit[1] nemen steeds toe en treden vaak op in de media, maar ook in de omgeving van veel personen. Vandaag de dag is het niet meer te ontwijken. Denk maar aan de tal van phishingpogingen via mail of de talloze telefoontjes die geld willen aftroggelen. Cybercriminaliteit, blijft toenemen net als het aantal slachtoffers.

Dit artikel heeft de bedoeling om het bewustzijn rond cybercriminaliteit te vergroten. Cybercriminaliteit is gekoppeld aan digitale inclusie, en daarom heeft de maatschappij een gedeelde verantwoordelijkheid rond dit thema. Met dit artikel wil ik niet alleen de gevaren aantonen, maar vooral de rol van sociaal werk onderstrepen. Digitale veiligheid is een basisrecht. Vaak zijn het kwetsbare groepen (niet alleen kwetsbare groepen) die slachtoffer worden. Dat vraagt niet enkel politionele en juridische begeleiding, maar er is ook nood aan een empathisch en luisterend oor. Het is van groot belang dat kwetsbare groepen zich veilig kunnen voelen en ergens terecht kunnen. Door cybercriminaliteit bespreekbaar te maken en alertheid te bevorderen bij sociaal werkers, kunnen we sleutelen aan een samenleving waarbij taboe een verhaal van verleden tijd wordt.

In dit artikel wordt aangegeven wat cybercriminaliteit precies is en wat het inhoudt. Bovendien wordt er gekeken naar wie kwetsbaar is voor dit fenomeen en welke effecten dit heeft (niet enkel financieel). Hiernaast worden er ook verschillende perspectieven bekeken waar het precies fout loopt. En tot slot wordt het belang van sociaal werk op dit thema besproken en welke rol precies een sociaal werker kan en hoort in te nemen.

Dit artikel werd geconstrueerd uit een literatuurstudie waarbij informatie gehaald is uit documentaires, websites, artikels, etc. Hiernaast heb ik ook informatie gehaald uit een open interview, waarbij ik een slachtoffer van cybercriminaliteit bevraag om zo dit werkstuk meer karakter te geven. Maar ook vanuit mijn stageperiode bij Digibank Gent en Digibank Plus heb ik ervaring verwerkt die ik gedurende mijn stageperiode heb opgedaan.

[1] Cybercriminaliteit omvat diverse activiteiten zoals phishing en fraude.

Het digitale tijdperk is aangebroken

Het internet en de computer bestaan inmiddels al een tijdje. Maar de computer en het internet die wij kennen, kunnen we niet vergelijken met wat het was jaren geleden. Technologie evolueert razendsnel. We zitten op een hogesnelheidstrein die steeds nieuwe technologie introduceert. Toen de Vlaamse overheid in september 1996 haar eerste website online zette (*Geschiedenis van de Vlaamse Overheid*, z.d.), kon niemand vermoeden wat er zou volgen. Inmiddels komen we meer in contact met onze overheid online dan offline. Vandaag doen we onze belastingen online, betalen we onze boetes door enkele muisklikken en solliciteren we op vacatures die we online terugvinden. Het internet is geen extraatje meer, het is eerder een must-have. Men zou kunnen zeggen dat we nu zijn aangekomen in een tijdperk waar digitale toepassingen en snufjes onmisbaar zijn geworden.

> 'Al die overheidswebsites, het begint op een doolhof te lijken.'
> - Client van Digibank Plus

Tijdens de COVID-19-pandemie is het belang van technologie en goede en veilige verbindingen extra zichtbaar geworden. De pandemie legde onze digitale afhankelijkheid van technologie bloot. Plots moesten we thuiswerken, online lesgeven, cliënten online ontvangen. Wie geen stabiele verbinding had of de technologie niet beheerste, viel uit de boot. In 2019 had de EU al een digitale strategie gelanceerd om mensen en bedrijven een nieuwe generatie technologieën aan te reiken (*De Europese Digitale Strategie in België*, z.d.).

De Vlaamse regering reageerde met het ambitieuze investeringsplan 'Vlaamse Veerkracht'. Het investeringsplan moest de Vlaamse welvaart en het welzijn van haar inwoners helpen versterken na de akelige coronaperiode. Het investeringsplan rust op zeven uitdagingen, waarbij Vlaanderen digitaal transformeren op een vlotte, veilige en privacy bestendige manier er één van is. Het was de bedoeling dat België vooropliep in de digitale revolutie en dus mee was met zijn tijd. Zo klonk het: 'We moeten opklimmen tot de wereldtop van naties die technologieën als artificiële intelligentie, robotica en internet-of-things[2] inzetten om de samenleving beter te maken.' (*Relanceplan Vlaamse Regering – Vlaamse Veerkracht*, z.d.)

De technologiegezinde houding van onze samenleving (en overheid) zorgt ervoor dat veranderingen mogelijk zijn. Dat betekent aanpassen of 'survival of the fittest'. En daar schuilt net het gevaar. Terwijl de overheid volop inzet op digitalisering, is er een grote groep van burgers die dreigt achter te vallen.

De digitale kloof

Er ontstaat een onderscheid tussen mensen die mee kunnen met de digitale wereld en de mensen die achterblijven of moeite hebben met volgen. Dit noemen we de digitale kloof. Simpelweg mensen toegang geven tot de digitale wereld voldoet niet. De digitale kloof verwijst naar een samenspel van toegang, vaardigheden, attitudes en efficiëntie. Dit wil dus zeggen dat mensen ook moeten beschikken over bepaalde vaardigheden en attitudes, maar ook dat deze digitale wereld efficiënt hoort te zijn. Denk maar aan de onoverzichtelijke of verouderde webpagina's die alles bemoeilijken.

[2] Internet-of-things verwijst naar apparaten die via internetverbinding met elkaar verbonden zijn en met elkaar kunnen communiceren.

Hoewel inmiddels bijna alle Vlamingen (99%) minstens één toestel hebben dat kan connecteren met het internet, zien we dat bepaalde groepen het moeilijker hebben. Zo heeft een kwart van de Vlamingen met een laag inkomensniveau nog nood aan een extra toestel. Voor ongeveer een derde van de Vlamingen met een laag inkomensniveau is betere connectie te duur (zowel internet als mobiel internet). Dit bemoeilijkt het voor hen om mee te zijn met de digitale wereld. (*Imec.Digimeter 2024 | Imec Vlaanderen*, z.d.)

Digibank Gent en Digibank Gent gaven cliënten gratis toestellen en konden goedkoper internet aanbieden (mist men voldoet aan de voorwaarden).

Vlamingen ervaren spanning en druk. Omdat de maatschappij (en hun omgeving) hen dwingt om mee te zijn met digitale technologieën. Het is geen keuze, maar het wordt nu eenmaal opgedrongen. Ondanks dit stagneert de digitale geletterdheid[3]. Volgens de Imec Digimeter (2024) is er geen progressie in het aantal Vlamingen voor wie het omgaan met digitale technologieën als 'makkelijk' wordt ervaren. Sterker nog, voor meer dan de helft (56%) van de Vlamingen gaan deze veranderingen en ontwikkelingen veel te snel om te volgen. Verwarrende lay-outs, moeilijk taalgebruik en gebruiksonvriendelijke webpagina's maken het er niet beter op.

'Graag had ik mijn loonbriefjes nog steeds fysiek maar ik moet nu eenmaal mee met de tijd.'

- Medewerker sociale economie (client van Digibank Gent)

De Barometer Digitale Inclusie (2024), een ander onderzoeksrapport dat zich ook bezighoudt met het bestuderen van hoe mensen in Vlaanderen en België omgaan met technologie, legt de vinger op de wonde dat inkomensniveau, gezinssamenstelling en leeftijd alle drie discriminerende factoren zijn. Zo hebben de inkomensarme huishoudens verhoudingsgewijs tien keer meer de kans om geen internetaansluiting te hebben dan gezinnen met een hoog inkomen (die inmiddels wel bijna allemaal aangesloten zijn).

De Barometer stelt dat in 2023, vier op de tien Belgen tussen 16 en 74 jaar digitaal kwetsbaar[4] zijn, ofwel omdat ze geen gebruik maken van het internet, ofwel omdat ze zwakke algemene digitale vaardigheden hebben. (*Barometer Digitale Inclusie 2024*, z.d.)

Dit wil zeggen dat veel mensen zichzelf niet beschouwen als bekwaam om bepaalde basisactiviteiten online uit te voeren, zoals online solliciteren, uitvoeren van banktransacties, aanvragen van diensten, etc. Hierbij wordt ook aangetoond dat leeftijd, inkomen en opleidingsniveau cruciale factoren zijn. Het percentage personen met zwakke digitale vaardigheden is afgelopen twee jaar bij alle lagen van de bevolking over het algemeen gedaald, maar toch zien we enkele groepen die achterblijven. Onderstaande grafiek toont die aanzienlijke verschillen naargelang leeftijd. Binnen de oudste leeftijdsgroep is meer dan de helft digitaal kwetsbaar. Dit is zeer ontrustend nieuws, omdat deze mensen ook nog beroepmoeten doen op de digitale wereld. (*Barometer Digitale Inclusie 2024*, z.d.)

[3] Digitale geletterdheid gaat over het kunnen omgaan met technologie en apparaten zoals computers, gsm's en internet.

[4] Digitale kwetsbaarheid verwijst naar de mensen die niet (volledig) kunnen deelnemen aan onze digitale samenleving. Dit wordt gedefinieerd door enerzijds 1° het deel niet-gebruikers van het internet samen met 2° het deel gebruikers dat over zwakke algemene digitale vaardigheden beschikt.

De lichte algemene daling in digitale kwetsbaarheid mag ons niet blind maken voor het feit dat er op dit gebied nog steeds opvallende verschillen bestaan tussen personen, met name naargelang het inkomensniveau. We zien in 2023 dat bijna zes op de tien mensen in een laaginkomen huishouden leven digitaal kwetsbaar zijn. Dit is meer dan twee keer zo hoog als het percentage van mensen die in een hoog inkomen huishouden wonen. (*Barometer Digitale Inclusie 2024*, z.d.)

Verder zien we ook een groot verschil tussen onderwijsniveau waarbij bijna zeven op de 10 personen met een diploma lager secundair onderwijs digitaal kwetsbaar zijn. Dit is dan weer drie keer hoger dan bij personen met een diploma hoger onderwijs. En laatste schokkende waarneming is dat eenoudergezinnen juist digitaal kwetsbaarder zijn geworden en dus geen vooruitgang boeken. (*Barometer Digitale Inclusie 2024*, z.d.)

Desondanks de verschillende initiatieven (zoals digipunten) om een e-inclusieve samenleving[5] te bereiken, zien we nog steeds veel digitale uitsluiting. We spreken van digitale uitsluiting wanneer iemand uitgesloten dreigt te worden door een tekort aan digitale toegang of vaardigheden. Iedereen is vatbaar voor digitale uitsluiting en we zien dit ook bij elke laag van onze samenleving. Maar toch merken we in de praktijk dat bepaalde sociaal kwetsbare groepen meer risico lopen op digitale uitsluiting omwille van hun toegang of vaardigheden.

Digibank Gent en Digibank Plus bestaat voor iedereen, toch zien we voornamelijk werkzoekenden, laag inkomen huishoudens, medewerkers uit de sociale economie, mensen met een beperking en ouderen.

Een ander gevaar dat digitalisering met zich meebrengt is cybercriminaliteit. Dit fenomeen heeft wel al tientallen jaren bestaan. Zo was de allereerste vorm van cybercriminaliteit te merken in 1934, toen twee dieven het Franse telegraafnetwerk infiltreerden om financiële informatie te stelen. (*Cybercrime: History, Global Impact & Protective Measures [2025]*, 2025).

Digitalisering creëert nieuwe kansen en mogelijkheden voor cybercriminelen. Ze hebben toegang tot steeds geavanceerdere technieken om toegang te krijgen tot systemen, gegevens te stelen, etc. Men zou zelfs kunnen stellen dat cybercriminaliteit een inherent gevolg is van digitalisering. Gepaard met mensen die niet goed mee kunnen met het digitale verhaal brengt dit gevaren met zich mee. In wat volgt leg ik cybercriminaliteit uit en wat de gevolgen ervan zijn voor het slachtoffer.

Een complexe definitie van cybercriminaliteit

Op de website van Mediawijs is de volgende definitie van cybercriminaliteit terug te vinden: Cybercriminaliteit is een overkoepelende term voor misdaden die gepleegd worden via media, met als doel schade te berokkenen aan andere media(gebruikers). Cybermisdaden kunnen zich richten op bedrijven of organisaties, maar ook op onschuldige mensen. (*Mediawijs*, 2024) Omdat we voor meer en meer zaken gebruikmaken van het internet, is er ook meer cybercriminaliteit. Zo is cybercriminaliteit in ons land de enige vorm van criminaliteit die toeneemt in plaats van daalt. Volgens cijfers van de federale politie daalt het aantal misdrijven in België, maar stijgt cybercriminaliteit. Over een periode van tien jaar zien we bijna een verdriedubbeling (281,5%). Deze stijging wijst op een structureel probleem dat maar steeds groter wordt (*"Aantal*

[5] Een e-inclusieve samenleving is een samenleving waarin iedereen kan deelnemen aan de digitale wereld ongeacht leeftijd, inkomen, opleiding of beperking.

Misdrijven Daalt in België, Maar Cybercriminaliteit Blijft Stijgen", 2025).

De definitie toont aan dat cybercriminaliteit niet één vaste vorm kent, maar het is eerder een fenomeen dat zich ontplooit op diverse manieren. Bovendien blijven online oplichters creatieve manieren vinden om mensen te misleiden; hierbij maken ze gebruik van nieuwe trends zoals AI. Denk maar aan de bewerkte video's van bekende personen.

De indicator voor 'digitale vaardigheden' die door Statbel en Eurostat wordt gebruikt, werd in 2021 uitgebreid met vaardigheden met betrekking tot online veiligheid. Sindsdien werd dit domein gebruikt (naast de andere domeinen) om algemene digitale vaardigheden te berekenen. Van alle vaardigheidsdomeinen lijken de vaardigheden die betrekking hebben op online veiligheid verreweg het minst beheerst te worden door alle gebruikers. (*Barometer Digitale Inclusie 2024*, z.d.)

Ongeacht geslacht, leeftijd en nationaliteit zien we dat bij elke laag een deel geen digitale vaardigheden heeft op het gebied van online veiligheid. Meer dan één op de vier gebruikers heeft namelijk geen digitale vaardigheden op dit gebied.

We zien echter wel dat er nog steeds grote ongelijkheden blijven tussen mensen, naargelang hun sociaaleconomische, culturele en professionele achtergrond. Werkzoekenden hebben vaker geen digitale vaardigheden rond online veiligheid dan werkende personen. Wat echt merkwaardig is, is dat meer dan zes op de tien internetgebruikers met een lage opleiding geen online veiligheid vaardigheden hebben. Terwijl dit bij hoger onderwijs veel lager ligt.

Bovendien zien we dat mensen met een lager inkomen ook vaker geen digitale vaardigheden hebben dan personen met een hoger inkomen. Dit zijn weer sociaal kwetsbare groepen die slechter scoren. Terwijl deze personen vaak worden blootgesteld, omdat ze bijvoorbeeld het internet nodig hebben bij het solliciteren of eventuele opleidingen te volgen. (*Barometer Digitale Inclusie 2024*, z.d.)

Zoals eerder aangegeven zijn het vaak sociaal kwetsbare groepen die geen toegang hebben of over bepaalde vaardigheden niet beschikken. Het zijn mensen die reeds kwetsbaar zijn en die ook op het internet dus een kwetsbare positie innemen. Online surfen en gebruikmaken van technologie is niet risicoloos. Wanneer men niet beschikt over de nodige digitale vaardigheden (zowel algemene als vaardigheden rond online veiligheid), heeft men een grotere kans om slachtoffer te worden van cybercriminaliteit.

Hierbij hoort sociaal werk een rol te spelen. Sociaal werk richt zich op het ondersteunen van individuen en groepen die moeilijk kunnen participeren in de samenleving. Omdat hun dagelijks leven zich steeds meer online afspeelt, is bescherming en waarschuwing tegen cybercriminaliteit een essentieel onderdeel geworden van de integrale ondersteuning die sociaal werkers bieden aan hun cliënten. Het verhogen van het welzijn van cliënten begint bij het versterken van hun zelfredzaamheid en weerbaarheid.

Meer dan geld alleen

In het begin van het artikel gaf ik aan dat er miljoenen euro's gestolen worden in België elk jaar, enkel en alleen door cybercriminaliteit. Bij nieuwsberichten en krantenkoppen lezen we verhalen van mensen die zelfs duizenden euro's verliezen. Natuurlijk kunnen we niet elk verhaal met elkaar vergelijken. Sommigen verliezen veel meer dan anderen. Cybercriminelen zijn meesters in manipulatie en durven zeker manipulatie te gebruiken om hun doel te bereiken. Zo kunnen ze de oplichting gedurende een langere periode in stand houden. Hierdoor loopt het financiële nadeel voor het slachtoffer enkel maar op (*Informaticacriminaliteit Augustus 2024*, 2024).

Dit komt bijvoorbeeld vaak voor bij investeringsfraude, waarbij de oplichters in het begin resultaten tonen van winst, zodat het slachtoffer geneigd is om meer te investeren.

Het is inmiddels wel duidelijk dat cybercriminaliteit veel schade kan veroorzaken bij het slachtoffer en/of hun omgeving. Maar naast de financiële schade die het slachtoffer oploopt, is er ook veel schade aan zijn/haar emoties. Vaak wordt deze psychische impact van cybercriminaliteit onderschat en krijgt het ook niet de aandacht die het verdient.

Volgens Maria Genova, journalist en expert op het gebied van cyberveiligheid, ervaren slachtoffers vaak intense gevoelens van angst, stress en hulpeloosheid. Veel slachtoffers krijgen langdurige psychologische gevolgen door het besef dat onbekenden toegang hebben tot persoonlijke en intieme informatie. Genova wijst erop dat veel slachtoffers de schuld bij zichzelf leggen en dat deze gevoelens van falen het zoeken naar hulp bemoeilijken. Daarom kan je verhalen horen van slachtoffers die niet naar de politie stappen of dit maar zeer laat doen (*De Vries & De Vries*, 2025).

> Ik ben niet naar de politie gestapt, omdat een familielid van mij agent is. Ik had schrik dat hij hiervan iets zou te weten komen en dat zo ook naasten van mij het te weten zouden komen.
>
> - Geïnterviewd slachtoffer van cybercriminaliteit

Slachtoffers hebben zelfverwijt dat resulteert in diepe schaamte. Ze hebben het gevoel dat ze ‘dom’ zijn geweest. Het maatschappelijk oordeel klinkt vaak als volgt: ‘Hoe kon je daarvoor vallen?’. Er wordt vaak aan ‘victim blaming’[6] gedaan, zoals men dat ook bij armoede doet (denk maar aan het model Vranken). Maar dit zorgt er wel voor dat slachtoffers bang zijn voor het oordeel van hun omgeving. Er wordt een emotionele muur gecreëerd waarbij het slechte nieuws zelfs niet wordt gezegd tegen familie of geliefde. Bovendien verliezen slachtoffers ook hun basisvertrouwen in de medemens (en technologie).

Om een beter besef te krijgen van de emotionele schade die cybercriminaliteit teweegbrengt, ben ik in gesprek gegaan met een slachtoffer. Hij vertelde dat vooral schaamte en stress een grote rol speelden en hij had nooit gedacht dat hij hierin zou trappen. Uit het interview was ook duidelijk dat iedereen slachtoffer kan worden, ongeacht leeftijd, geslacht, etc. Hij vertelde mij ook dat de doorsnee burger niet veel wist over cybercriminaliteit en dat hij zelf toen informatie heeft moeten opzoeken. Het zou echter meer gestandaardiseerd moeten worden om hier kennis over te krijgen, hoe je hier precies mee omgaat of hoe je anderen kan helpen bij zulke situaties, klonk het.

> Ik had altijd gedacht dat ik hier nooit slachtoffer zou van worden.
>
> - Geïnterviewd slachtoffer van cybercriminaliteit

Who’s to blame?

We horen te stoppen met ‘victim blaming’ en de schuld volledig bij het slachtoffer te leggen. Want er zijn nog andere partijen die komen kijken bij dit verhaal van cybercriminaliteit. Een grote rol speelt de politie. Digitale misdrijven kan men niet vergelijken met traditionele fysieke misdrijven. Overal hangen camera’s die helpen misdrijven te traceren. Voor cybercriminaliteit is dit een stuk moeilijker. Het geld dat gestolen wordt, verdwijnt in meerdere rekeningen over de hele wereld of wordt omgezet in niet-traceerbare munten of cadeaukaarten. Het is

[6] De schuld bij het slachtoffer leggen. Het is de fout van het slachtoffer dat hij/zij is gevallen voor de oplichting.

simpelweg moeilijker geworden om een dader aan te duiden, omdat het geld moeilijk traceerbaar is en/of omdat het vaak ook gaat over internationale gevallen.

In de Pano-documentaire 'De scam machine' getuigden cybermagistraten van het parket Antwerpen dat ze in een absolute minderheid van alle dossiers verder kunnen. En dit betekent nog niet dat ze er een iemand voor kunnen laten opdraaien of dat ze het geld kunnen recupereren. (*VRT MAX*, z.d.)

Niet enkel in Antwerpen is dit het geval dat veel dossiers blijven liggen en niet opgelost geraken. Dit komen we overal in België tegen. Maar hierdoor verliezen slachtoffers wel de hoop om ooit hun geld terug te zien. En in veel situaties gaat het over geld dat broodnodig is. Bovendien speelt het al dan niet terugkrijgen van het gestolen geld een rol in de psychologische verwerking van het slachtoffer. Cybercriminaliteit groeit explosief en wij kunnen niet volgen. Dit omdat er ook vaak grote organisaties met vele medewerkers achter cybercriminaliteit zitten. [7]

'Als uit die telefoontjes een interessant target naar boven komt, wordt die persoon doorgespeeld aan iemand in sales'

- Anonieme getuige die bij een callcenter heeft gewerkt. *(Nws*, 2025c
-

Het gerecht heeft te weinig mensen in dienst om de grote hoeveelheid internetfraude- en phishingaangiftes te kunnen verwerken. Dit zorgt ervoor dat verschillende parketten in ons land een ondergrens hebben moeten invoeren. Het parket van Oost-Vlaanderen gaat geen zaken van internetfraude meer onderzoeken als het gaat over minder dan 1000 euro verlies. In West-Vlaanderen ligt deze grens op 2500 euro. (*Nws*, 2024)

De verantwoordelijkheid mag dus niet langer enkel bij de kwetsbare burger liggen, terwijl het systeem tekortschiet in het beschermen en vervolgen. Cybercriminaliteit krijgt 'vrij spel'. Hier hoort zeker op geïnvesteerd te worden.

Maar ook bedrijven spelen een cruciale rol in onze online veiligheid, maar in de realiteit zien we dat winstbejag de bescherming van gebruikers vaak in de weg staat. Vooral op sociale mediaplatformen zoals Facebook en X worden we voortdurend blootgesteld aan cybercriminaliteit in de vorm van phishing of investeringsfraude. Deze worden vaak vermomd in advertenties.

Hoewel platformen zoals Facebook officiële regels hanteren tegen valse advertenties en 'word-snel-rijk'-beloftes, blijven er toch zulke advertenties massaal verschijnen. Dit wijst erop dat de bedrijven achter deze platformen hun verantwoordelijkheid niet serieus genoeg nemen. Voor Meta (moederbedrijf van Facebook) lijkt het bestrijden van deze online criminaliteit eerder een kwestie van onwil dan van onmacht. Uit onderzoek van Pano blijkt dat het bedrijf naar schatting tien procent van zijn jaarlijkse omzet haalt uit deze advertenties. De winst gegenereerd door deze advertenties ligt vele malen hoger dan de maximale boetes die zij riskeren. Daarom maken ze de cynische afweging om dat risico te nemen (*Nw*s, 2025b). Dit zorgt er wel voor dat de gebruikers blootgesteld worden aan cybercriminaliteit en dus ook een grotere kans hebben om slachtoffer te worden. Bovendien is het schandalig dat dit werkelijkheid is.

'Alles wat de groei vertraagt, is een probleem, zelfs veiligheid.'

- Een insider bij Meta (*Nws*, 2025b)

[7] Een callcenter is een kantoor waar medewerkers telefonisch contact hebben met klanten. In dit geval om slachtoffers te maken.

Bedrijven leggen de schuld te vaak bij de gebruiker zelf om zo buiten schot te blijven. In de bankensector bijvoorbeeld zien we dat banken verplicht zijn om slachtoffers van phishing te vergoeden, behalve in gevallen van 'grove nalatigheid'. Deze term is echter niet duidelijk gedefinieerd in onze Belgische wet, waardoor banken vrij zijn om te interpreteren en zo dus terugbetalingen te weigeren. Jean Cattaruzza, de ombudsman voor financiële diensten, stelt dat banken vaker hun verantwoordelijkheid moeten nemen en meer slachtoffers horen terug te betalen, wat nu dus tot op heden niet gebeurt. (*Nws,* 2025a)

Uit internationaal onderzoek blijkt dat vier op de tien slachtoffers van onlinefraude geen geld terug krijgt. (*Ilegems*, 2024)

Deze houding beperkt zich echter ook niet alleen tot de financiële sector; ook platformen zoals verkoopwebsites of marketingplatforms wijzen bij gelijkaardige incidenten waarbij er valse advertenties zijn onmiddellijk naar de gebruiker. Hoewel deze bedrijven verdienen aan hun platformen, weigeren ze de bijhorende verantwoordelijkheid te dragen. Het is essentieel dat bedrijven inzien dat hun gebruikers beschermen hun fundamentele taak is (en niet zomaar bijzaak). Hogere winstcijfers mogen daarom ook niet primeren op veiligheid.

Maar ook over onze maatschappij kunnen we wat vertellen. Dat technologie vandaag onmisbaar geworden is, is duidelijk. Toch toont zowel mijn gesprek met een slachtoffer als recent onderzoek een verontrustende realiteit: een groot deel van onze bevolking weet weinig over cybercriminaliteit en de gevaren ervan. Het slachtoffer waarmee ik had gesproken, vertelde dat hij pas toen het al te laat was dingen moest opzoeken om met de gevaren aan de slag te gaan.

De digitale geletterdheid is ongelijk verdeeld. Veel mensen weten wel hoe ze bijvoorbeeld een app kunnen gebruiken, maar begrijpen niet welke gevaren op de loer liggen. Deze onwetendheid maakt burgers gemakkelijke doelwitten voor cybercriminelen. Zolang we de signalen niet herkennen, zoals de verdachte link, het foutieve mailadres, de te mooie aanbieding, etc., blijven we dweilen met de kraan open. Digitale veiligheid en de eraan gekoppelde gevaren zouden basiskennis moeten zijn. Eigenlijk zouden vaardigheden van digitale veiligheid in ieders achterhoofd moeten zijn gegrift, net zoals we links en rechts kijken voordat we oversteken.

Naast de onwetendheid speelt er ook nog een andere factor een grote rol. In onze samenleving rust er een taboe op het slachtofferschap van cybercriminaliteit. Slachtoffers worden door zichzelf en/of hun omgeving vaak neergezet als naïeve personen. Vaak hoor je: 'Hoe kon ik zo dom zijn?' of 'Hoe val je nu daarvoor?'. Dit taboe zorgt ervoor dat slachtoffers alleen de lasten gaan dragen in plaats van samen met een vertrouwenspersoon, zoals een familielid of partner, om hulp te zoeken. Het taboe zorgt ervoor dat het slachtoffer beschaamd is om het te vertellen. Dit taboe helpt niemand in het verwerken en het zetten van volgende stappen, integendeel zelfs. De strijd tegen cybercriminaliteit begint niet alleen met betere technologie en kennis, maar vooral ook met minder oordeel.

Wat betekent dit voor het sociaal werk?

Cliënten in de hulpverlening bevinden zich steeds meer online, zowel binnen als buiten hun hulpverleningstraject. Ze plannen hun afspraken digitaal, hebben contact met hun maatschappelijk assistent via WhatsApp en moeten inloggen op verschillende overheidswebsites. Deze digitalisering biedt kansen, maar vergroot ook de kwetsbaarheid.

Uit cijfers en onderzoek blijkt dat bepaalde sociaal kwetsbare groepen vaker weinig tot geen vaardigheden hebben op het vlak van online veiligheid, vergeleken met andere groepen. Hierdoor is de kans groter dat wanneer zij in contact komen met vormen van cybercriminaliteit, ze hier ook slachtoffer van worden. Dit is bijzonder problematisch: deze kwetsbare groepen hebben het financieel en sociaal vaak al niet breed, en een incident met cybercriminaliteit kan hun situatie verder verslechteren.

> Ik ben niet alleen al mijn spaargeld kwijt, ik leende nog eens bij, …
>
> - Slachtoffer cybercriminaliteit (*Nws*, 2023).

Cybercriminaliteit zorgt er ook voor dat dat heerst in onze samenleving. Bovendien kan men zo het incident verwerken en eventueel ook met behulp van de sociaal werker een persoonlijk netwerk verder uitbouwen.

Volgens de internationale definitie richt sociaal werk zich op sociale verandering, sociale cohesie, empowerment en bevrijding van mensen. Sociaal werkers werken aan het welzijn van cliënten en streven naar sociale rechtvaardigheid. Juist deze kwetsbare groepen vormen het doelpubliek van sociaal werkers.

In gevallen van cybercriminaliteit is het cruciaal om snel te handelen. Sociaal werkers zijn frontliniewerkers waarbij een vertrouwensband centraal staat. Zij horen die signalen van slachtoffers op te vangen en ermee aan de slag te gaan. Bescherming en waarschuwing tegen cybercriminaliteit hoort een essentieel onderdeel te zijn van de integrale ondersteuning.

Door de cliënt te informeren en te begeleiden rond de gevaren zal hij/zij ook meer zelfredzaam worden. Door digitale vaardigheden als het herkennen van een phishingmail aan te leren, nemen ze hun regie op en worden ze versterkt in het online bewegen. Maar sociaal werkers kunnen ook een psychosociale rol spelen wanneer het slachtofferschap tot negatieve gevolgen leidt, zoals sociaal isolement of zelfverwijt. Hierbij biedt de sociaal werker een luisterend oor en doorbreekt het taboe

Maar ook hoort sociaal werkers signalen op te vangen en deze door te spelen naar het beleid toe. Op welke manier worden onze cliënten benaderd? Waarom klikken ze op een bepaalde link? Signaleren is een krachtig element dat ervoor kan zorgen dat er bepaalde maatregelen worden genomen en dus veranderingen realiteit worden.

Maar dit is gemakkelijker gezegd dan gedaan. Op mijn stageplekken (Digibank Gent en Digibank Plus) vroeg ik aan collega-digicoaches of zij vinden dat andere sociaal werkers en collega's beschikken over genoeg vaardigheden om cybercriminaliteit te herkennen en ermee om te gaan. De respons was negatief: veel sociaal werkers zijn niet in staat om de gevaren van de digitale wereld te herkennen en hierop te reageren.

Digitaal wegwijs maken hoort deel te zijn van onze hulpverlening, dat bijdraagt aan het verhogen van welzijn. Dit betekent dat sociaal werkers hierrond moeten bijscholen. Maar hiervoor is wel tijd en ruimte nodig. Sociaal werkers zitten vaak al met overvolle agenda's en de hedendaagse besparingen maken het er niet beter op.

Desondanks is het, gezien de groeiende cybercriminaliteit die steeds meer slachtoffers maakt, noodzakelijk dat sociaal werkers mee zijn in dit verhaal en hun cliënten kunnen beschermen tegen de gevaren. De sociale dimensie van cybercriminaliteit vraagt om een mensgerichte benadering die verder kijkt dan alleen technische of juridische aspecten – precies waar sociaal werk zijn kracht ligt.

Conclusie

De digitale wereld biedt ongekende kansen, maar brengt ook aanzienlijke gevaren met zich mee. Niet enkel kwetsbare groepen, maar iedereen kan slachtoffer worden. Cybercriminaliteit is geen kleinschalig fenomeen meer, maar een structureel probleem dat ons miljoenen euro's kost en bovendien veel psychologische wonden teweegbrengt. Met 'victim blaming' komen we er niet. Cybercriminaliteit is een verhaal met veel partijen, waarbij de verantwoordelijkheid niet bij één partij mag en kan liggen. Zo kampt de politie met tekorten en hoge drempels, bedrijven laten eerder winstbejag primeren dan hun gebruikers beschermen, en de maatschappij zit met een taboe dat het slachtofferschap verslechtert. Dit vraagt om een aanpak waarbij preventie, bescherming en begeleiding samengaan.

Sociaal werkers staan aan de frontlinie bij kwetsbare groepen die vaker het meeste risico lopen, en kunnen hun vertrouwensband inzetten om het verschil te maken. Het versterken van digitale vaardigheden, het bieden van psychosociale ondersteuning en het bestrijden van het taboe zijn allemaal onderdelen geworden van het integrale ondersteuning die sociaal werkers kunnen bieden rond cybercriminaliteit. Echter, hiervoor moet ook tijd en ruimte zijn.

Wanneer alle partijen samenwerken op een gecoördineerde manier en elk hun steentje bijdragen, kunnen we pas sleutelen aan een samenleving waarin digitale veiligheid een basisrecht is en waarbij 'victim blaming' en haar taboe verleden tijd zijn.

Bronnenlijst

Aantal misdrijven daalt in België, maar cybercriminaliteit blijft stijgen. (2025, 30 oktober). Nieuwsblad. https://www.nieuwsblad.be/binnenland/aantal-misdrijven-daalt-in-belgie-maar-cybercriminaliteit-blijft-stijgen/101189182.html

Barometer digitale inclusie 2024. (z.d.). Koning Boudewijnstichting. https://kbs-frb.be/nl/barometer-digitale-inclusie-2024

Cijfers 2023: “Phishing en andere kapers op de kust” | Febelfin. (2024, 20 juli). Febelfin. https://febelfin.be/nl/themas/fraude-veiligheid/cijfers-en-trends/cijfers-2023-phishing-en-andere-kapers-op-de-kust

Cybercrime: History, Global Impact & Protective Measures [2025]. (2025). BlueVoyant. https://www.bluevoyant.com/knowledge-center/cybercrime-history-global-impact-protective-measures-2022

Cybercriminaliteit in België. (z.d.). FOD Economie. https://economie.fgov.be/nl/themas/online/digitale-economie-cijfers/beveiligde-internetservers/cybercriminaliteit-belgie

De Europese digitale strategie in België. (z.d.). Vertegenwoordiging in België. https://belgium.representation.ec.europa.eu/strategie-et-priorites/politiques-europeennes-cles-pour-la-belgique/la-strategie-numerique-europeenne-en-belgique_nl

De Marez, L., Georges, A., Sevenhant, R., Devos, E., & imec. (2025). imec.digimeter 2024. In Imec.Digimeter. Imec. https://www.imec.be/sites/default/files/2025-03/imec.digimeter-2024-rapport.pdf

Digital Shadows: Unseen Victims of Cyber Warfare. (2023). Weird Press Photo. https://weirdpressphoto.org/2023/digital-shadows

Geschiedenis van de Vlaamse overheid. (z.d.). Vlaanderen.be. https://www.vlaanderen.be/geschiedenis-van-de-vlaamse-overheid

Hoe u nepadvertenties op Facebook kunt herkennen. (2024). Keepersecurity. https://www.keepersecurity.com/blog/nl/2024/10/07/how-to-spot-fake-ads-on-facebook/

Ilegems, M. (2024). 4 op 10 slachtoffers van financiële cybercriminaliteit krijgt geen geld terug. Trends DataNews. https://datanews.knack.be/nieuws/4-op-10-slachtoffers-van-financiele-cybercriminaliteit-krijgt-geen-geld-terug/

imec.digimeter 2024 | imec Vlaanderen. (z.d.). Imec. https://www.imec.be/nl/kennisuitwisseling/techmeters/digimeter/imecdigimeter-2024

Informaticacriminaliteit augustus 2024. (2024). Lokale Politie Regio Puyenbroeck. https://www.politie.be/5416/nieuws/informaticacriminaliteit-augustus-2024

Mediawijs. (2024, 22 mei). Wat is cybercriminaliteit? https://www.mediawijs.be/nl/artikels/wat-cybercriminaliteit

Nws, V. (2023, 7 maart). Niko werd slachtoffer van investeringsfraude: “Ik raakte mijn spaargeld (400.000 euro) kwijt en leende bij” | VRT NWS: nieuws. VRTNWS. https://www.vrt.be/vrtnws/nl/2023/03/07/slachtoffer-van-investeringsfraude/

Nws, V. (2024, 8 juli). Parket Oost-Vlaanderen onderzoekt geen internetoplichting meer voor bedrag onder 1.000 euro | VRT NWS: nieuws. VRTNWS.

https://www.vrt.be/vrtnws/nl/2024/07/08/via-internet-opgelicht-voor-bedrag-dat-onder-1-000-euro-ligt-da/

Nws, V. (2025a, november 18). “Banken volgen wet te weinig en moeten slachtoffers van phishing vaker terugbetalen”, zegt ombudsman financiën | VRT NWS: nieuws. VRTNWS. https://www.vrt.be/vrtnws/nl/2025/11/18/phishing-banken-wetgeving/

Nws, V. (2025b, november 26). “Het is van niet willen”: Meta kan veel meer doen tegen nepadvertenties, maar kiest voor miljardenwinst | VRT NWS: nieuws. VRTNWS. https://www.vrt.be/vrtnws/nl/2025/11/24/pano-facebook-scam-machine-rol-van-meta/

Nws, V. (2025c, november 27). 240 telefoons per dag en feestjes met cocaïne: Pano spreekt met online oplichter die Belgen belt vanuit Belgrado | VRT NWS: nieuws. VRTNWS. https://www.vrt.be/vrtnws/nl/2025/11/24/pano-facebook-scam-machine-wie-zijn-de-oplichters/

Oplichters gebruiken deepfake van premier De Wever en journaliste Goedele Devroy voor valse advertentie. (2025). Vrt Nws. https://www.vrt.be/vrtnws/nl/2025/09/25/factcheck-bart-de-wever-vals-beleggingsplatform/

Relanceplan Vlaamse Regering – Vlaamse veerkracht. (z.d.). Vlaanderen.be. https://www.vlaanderen.be/publicaties/relanceplan-vlaamse-regering-vlaamse-veerkracht

VRT MAX. (z.d.). https://www.vrt.be/vrtmax/a-z/pano/2025-nj-/pano-s2025-nj-a6/