# CYBERCRIMINALITEIT is OVERAL

## Je zet je fiets toch ook op slot?

Bescherm jij jezelf voldoende tegen cybercriminaliteit of ga je er net als veel anderen van uit dat het jou niet overkomt? Misschien heb je niet altijd zin om ermee bezig te zijn, maar 1 op de 5 jongeren wordt slachtoffer van cybercriminaliteit. Met heftige gevolgen.

***Lees in deze folder wat je zelf kan doen om te voorkomen dat je slachtoffer wordt van cybercriminaliteit.***

## Cybercriminaliteit?

Cybercriminaliteit is een veelkoppig monster. Sommige misdrijven zijn vooral een bedreiging voor bedrijven. Je kunt bijvoorbeeld denken aan een website die onbereikbaar wordt of allerlei vormen van malware zoals virussen en gijzelsoftware. Andere misdrijven kunnen ook jou als persoon treffen. Een online bestelling wordt niet geleverd, je persoonsgegevens worden verspreid op internet of je wordt met een sexueel getint materiaal of een deepfake gechanteerd. Online shaming, oplichting, dating fraude, sextortion... Je kent al deze vormen van online criminaliteit waarschijnlijk wel van naam. Maar wat kan je doen om je ertegen te beschermen? Dat lees je verderop.

## Dit overkomt mij niet!

Veel jongeren denken “Dat overkomt mij niet!” Maar niets is minder waar. Iedereen kan slachtoffer worden van de slimme trucs van cybercriminelen.
Als je denkt dat je geen interessant doelwit bent voor cybercriminelen, dan zit je ernaast. Dat ben je wel! Jongeren zijn juist vaak doelwit. Ze zijn minder risicomijdend, beter van vertrouwen en vaak wat impulsiever dan ouderen. Dat maakt jou een aantrekkelijk slachtoffer. Vaak zijn criminelen uit op je geld.. Lees verder en leer hoe je je kan beschermen.

## Hoe bescherm ik mijzelf?

Eigenlijk is de belangrijkste tip: gebruik je gezond verstand. Als iets te mooi is om waar te zijn, dan is dat vaak ook zo. Verder kan je op twee terreinen maatregelen nemen: wees je bewust van je eigen gedrag en regel een aantal technische zaken. Eerst een paar tips over je eigen gedrag:

### 1. Gebruik je gezond verstand

Vertrouwen in mensen is prachtig, maar helaas is niet iedereen te vertrouwen. Zeker online is dat zo. Denk dus goed na over eventuele gevolgen als je bijvoorbeeld een seksueel getinte foto stuurt.

Lees ook je mails kritisch voordat je op een link klikt, informatie invoert op een website of even snel betaalt. Zo voorkom je dat je slachtoffer wordt. Zoek altijd op reviews voordat je bij een nieuwe online shop iets koopt. Zo kom je er snel achter of de shop trouwbaar is en onder welke voorwaarden je je aankopen doet.

### 2. Reageer nooit onder tijdsdruk

Een bekende en helaas goed werkende truc van criminelen is om je onder druk te zetten. In de haast of stress denk je niet helder meer na. Je wil snel van dat vervelende gevoel af en doet dus wat ze aangeven dat je moet doen. Dat is precies hun bedoeling! Trap er niet in. Als je dus wordt benaderd door iemand die bijvoorbeeld zegy bij je bank te werken en  aangeeft dat er iets mis is of dat ze iets van je nodig hebben en dat er haast bij is, haal dan je gezonde wantrouwen uit de kast. En ga door naar tip 3 hieronder.

### 3. Vraag hulp en praat erover

Vraag je vrienden of ouders of ze even meekijken en -denken. Zie je een leuke actie op TikTok? Of twijfel je over een bericht van bijvoorbeeld een winkel. Is die wel echt? Kijk er dan eerst met iemand anders naar voordat je verdere stappen zet.

Maar ook als er nog geen directe aanleiding is, kan het geen kwaad om met vrienden zo nu en dan over cybercriminaliteit te praten. Samen houdt je elkaar op de hoogte: Hoe gaan criminelen online te werk? Zo help je elkaar om alert te zijn en niet te snel te vertrouwen op wat mensen je doen geloven.

## Het kan ook jou overkomen:

***1 op de 5 jongeren was in 2021 slachtoffer van online criminaliteit.***

**4. Deel niet zomaar persoonlijke informatie**

Met persoonsinformatie kan iemand identiteitsfraude plegen. Geef daarom nooit zomaar belangrijke informatie zoals BSN-nummer of foto's van belangrijke documenten (diploma, ID-kaart of paspoort). Met deze informatie kan een crimineel in jouw naam een lening aanvragen of zich voordoen als jou om bijvoorbeeld je opa en oma te misleiden.

**5. Social media accounts op privé**

Zet je social media accounts standaard op 'privé' zodat alleen je eigen vrienden je berichten kunnen zien. Connect ook alleen met mensen die je persoonlijk kent of op een andere manier vertrouwt. Want hoe meer je prijsgeeft online, hoe makkelijker je slachtoffer wordt van cybercriminelen.

Naast deze tips over je eigen gedrag, is het ook belangrijk een paar technische dingen te regelen. Niet het leukste klusje, maar het hoort er gewoon bij in de maatschappij om je waardevolle spullen op slot te zetten. Anders maak je het criminelen écht te makkelijk!

**1. Gebruik unieke en sterke wachtwoorden!**

Toegegeven: het is best lastig om ingewikkelde en unieke wachtwoorden te gebruiken. We weten allemaal dat het belangrijk is maar we doen het toch niet. Daar maken criminelen gebruik van om digitaal bij je in te breken. Gebruik dus wachtwoorden van minimaal 14 tekens en gebruik voor ieder account een ander wachtwoord. Gebruik hierbij eventueel de hulp van een digitale wachtwoord-kluis. Dat is makkelijk en veilig.

**2. Gebruik  tweestapsverificatie**

Bij veel apps kun je tweestapsverificatie gebruiken. Stel dat standaard in. Het is als een dubbel slot op je fiets. Kleine moeite en écht een goeie extra bescherming.

**3. Voer updates uit**

Bij elke softwareupdates op je telefoon of laptop worden zwakke plekken hersteld. Zorg er dus voor dat updates automatisch worden geïnstalleerd. Zo kost het je geen tijd en geven je (beveiligings)software en apparaten je voortaan de beste bescherming.

## Wat moet ik doen als ik toch slachtoffer word?

Mocht je toch slachtoffer worden van cybercriminaliteit, schaam je dan niet! Het kan écht iedereen overkomen.

**1. Praat erover**

Laat vooral aan anderen weten dat je slachtoffer bent geworden. Informeer bijvoorbeeld je

ouders of vrienden zodat ze je kunnen steunen en helpen. Het is niet niks wat je meemaakt. Ook kunnen jullie samen kijken welke stappen er gezet moeten worden. Praten over slachtofferschap van cybercrime helpt. Het helpt jou om te verwerken wat er is gebeurd en we worden ons met elkaar steeds bewuster van de methoden. Zo kunnen we nieuwe delicten voorkomen.

**2. Meld het misdrijf**

Afhankelijk van het misdrijf waarvan je slachtoffer bent geworden is het belangrijk om dit te melden bij de betrokken organisaties. Meld het bijvoorbeeld bij het social media platform waar je contact hebt gehad, bel je bank als er geld afhandig is gemaakt. Bij de meeste bedrijven hebben ze specialisten die zich met oplichting bezighouden. Zij kunnen je vaak verder helpen.

**3. Doe aangifte bij de politie**

Doe ook altijd aangifte bij de politie. Nu denkt je misschien dat dit toch geen nut heeft, maar dat heeft het wel. De kans is misschien klein dat jouw zaak meteen wordt opgelost, maar door zaken te bundelen wordt de kans groter dat criminelen worden gepakt. Ook helpt het de politie om inzicht te houden wat er precies speelt en op deze manier kunnen anderen gewaarschuwd worden.

**4. Verander je wachtwoorden**

Als een account is gehackt of je persoonlijke gegevens zijn gestolen, dan is het verstandig om je wachtwoorden te veranderen. Zo voorkom je dat criminelen bij andere accounts kunnen.

**5. Zoek jezelf online op**

Als je denkt dat jouw naam of jouw foto's illegaal worden gebruikt, zoek jezelf dan eens op het internet. Vaak kun je deze gegevens laten verwijderen. Als het je niet lukt, benader dan Helpwanted, zij kunnen je daarbij helpen.

**Meer info bij**

- Helpwanted.nl
- Fraudehelpdesk.nl
- Cybercrimeinfo.nl
- checkjelinkje.nl/appjelinkje

Deze flyer is ontwikkeld in eem samenwerking tussen het Veiligheidsnetwerk Oost-Nederland en het lectoraat Maatschappelijke Veiligheid van de Hogeschool Saxion, onder financiering van de Citydeal Lokale Weerbaarheid Cybercrime in samenwerking met het Centrum voor Criminaliteitspreventie en Veiligheid.