Waar kan je Cybercrime melden.

Weet wat je moet doen als je slachtoffer wordt. Als je denkt dat je het slachtoffer bent geworden van een cybermisdaad, moet je dit melden bij de **lokale politie** 0900-8844 en in sommige gevallen **de FBI** en de **Federal Trade Commission.** Dit is belangrijk, zelfs als de overtreding niet zo ernstig lijkt. Jouw melding kan de autoriteiten helpen bij hun onderzoek of voorkomen dat criminelen in de toekomst misbruik maken van anderen.
Als je denkt dat cybercriminelen je identiteit hebben gestolen. Dit zijn enkele stappen die je moet nemen.

1. Neem contact op met de **bedrijven en banken** waarvan je weet dat daar fraude heeft plaatsgevonden.
2. Plaats fraudewaarschuwingen en haal je kredietverslagen op. Een fraudewaarschuwing is een gratis melding die u aan uw kredietrapport kunt toevoegen en waarbij u uw identiteit moet verifiëren voordat u een lening onder uw naam kunt afsluiten. Fraudewaarschuwingen fungeren als een tweede vorm van authenticatie om ervoor te zorgen dat u de enige bent die leningen kan afsluiten of kredietaccounts onder uw naam kunt openen. De fraudewaarschuwing is voor maximaal één jaar geldig. Uitgebreide fraudewaarschuwing is zeven jaar geldig en is bedoeld voor slachtoffers van fraude.Er zijn drie belangrijke situaties waarin je een fraudewaarschuwing moet plaatsen: als je denkt dat je het slachtoffer bent geworden van fraude, als je het slachtoffer bent geworden van identiteitsdiefstal of als je jou identiteit wilt beschermen tegen diefstal.
3. Je kredietverslag is een overzicht van je financiële geschiedenis, inclusief leningen, kredietkaarten en betalingsgedrag. In Nederland kun je dit opvragen via Stichting BKR. Dit is gratis, maar een gewaarmerkt overzicht kost €16,45.
4. **Slachtofferhulp Nederland** (0900-0101) biedt ondersteuning aan slachtoffers van cybercrime, zoals online fraude, identiteitsdiefstal en hacking. Via hun website kan je gratis advies en tips krijgen. Ze helpen je met emotionele steun, juridisch advies en/of praktische hulp. Ze biedt gesprekken en begeleiding om je te helpen omgaan met de gevolgen. Ze geven informatie over je rechten en helpen bij het doen van aangifte. Ze geven advies over hoe je verdere schade kunt voorkomen en je digitale veiligheid kunt verbeteren.
5. **Fraudehelpdesk** (088-786 7372) helpt slachtoffers van cybercrime door waarschuwingen, advies en Meldpunt. Ze informeren over actuele fraudepraktijken, zoals phishing, identiteitsdiefstal en online oplichting. Ze geven tips over hoe je fraude kunt herkennen en voorkomen. Je kunt verdachte situaties melden, zodat ze anderen kunnen waarschuwen en eventueel doorverwijzen naar de juiste instanties.
6. **Centraal Meldpunt Identiteitsfraude (CMI)** (088-900 1000) helpt slachtoffers van identiteitsfraude en biedt ondersteuning bij cybercrime-gerelateerde identiteitsdiefstal. Ze kunnen je helpen bij het meldingen van identiteitsfraude bij andere instanties zoals de Belastingdienst en/of politie. Ze geven advies, ondersteuning en tips om identiteitsfraude te voorkomen en helpen slachtoffers bij het herstellen van de gevolgen. Zij raden bijvoorbeeld het gebruik van de KopieID-app aan. Voor bewustwording en preventie organiseren zij presentaties en workshops.
7. **Autoriteit Financiële Markten (AFM)** (0800-540 0540) speelt een belangrijke rol in het bestrijden van financiële cybercriminaliteit. Ze richten zich vooral op toezicht op financiële instellingen, waarschuwingen, regelgeving, Onderzoek en handhaving. Zij controleert of banken, beleggingsinstellingen en andere financiële partijen zich houden aan wetgeving tegen witwassen en fraude. Ze waarschuwen consumenten en bedrijven voor risico's zoals marktmanipulatie in de cryptosector, zoals 'pump and dump'-praktijken, die vanaf eind 2024 verboden worden. Ze legt boetes op aan bedrijven die zich niet aan de regels houden, zoals

bij overtredingen van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft).

8. **Autoriteit Consument en Markt (ACM)** (088-070 7070) speelt een rol in het bestrijden van digitale fraude en cybercrime, vooral binnen de digitale economie en online consumentenbescherming. Ze richten zich op toezicht op online platforms, bescherming tegen misleidende praktijken en concurrentie en marktwerking. Zij controleert of digitale diensten voldoen aan de regels van de Digital Services Act (DSA), die sinds 2024 in werking is getreden. Ze treden op tegen bedrijven die consumenten misleiden met valse aanbiedingen, verborgen kosten of oneerlijke handelspraktijken. Ze voorkomt dat bedrijven de markt manipuleren, bijvoorbeeld door kartelvorming of misbruik van een economische machtspositie.
9. De **ANWB Cyberhulp** kan je helpen online veiliger te maken. Hulp bij het instellen van FMA op je apparaten, hulp bij (mogelijke) incidenten en een verzekering voor als er toch iets gebeurt.
10. Daarnaast kan men gebruik maken van de **Consumentenbond en HCC**.

Alex Hol