Afspraken over de hulp van de Cyberwacht

cyberwacht

In het kort

Waar gaat dit over?

In dit reglement vindt u de voorwaarden die horen bij de Cyberwacht. De Cyberwacht is de hulplijn bij cybercriminaliteit. U kunt ons bellen als u bent gehackt, ook als u hierover twijfelt. Onze specialisten helpen u dan snel verder.

Wie en wat bedoelen we?

Bij deze voorwaarden hoort een moeilijke woordenlijst. Hierin staat precies wat we met alle termen in de voorwaarden bedoelen. Deze woorden zijn te herkennen als onderstreepte tekst. Hieronder vindt u alvast de belangrijkste begrippen op een rij:

- Als het in deze voorwaarden over ‘wij’, ‘we’ of ‘ons’ gaat, dan bedoelen we de Cyberwacht en Sparklab B.V. De Cyberwacht is een product dat is ontwikkeld door Sparklab B.V., een onderneming die hoort bij Nationale-Nederlanden. Het bezoekadres van de Cyberwacht is: Saturnusstraat 60 - unit 70, 2516 AH in Den Haag.
- Met ‘partners’ bedoelen we de bedrijven waarmee we samenwerken om de Cyberwacht aan te bieden. Zij voeren de dienstverlening uit die u met hen heeft afgesproken.
- De ‘klant’ is de persoon die de dienstverlening afneemt en dus contact opneemt met de Cyberwacht. Dit kan zowel een particuliere klant zijn als een persoon die belt namens een bedrijf. In het geval van een particuliere klant is dit ook degene die betaalt voor de dienstverlening. Deze persoon noemen we vanaf nu gewoon ‘u’ of ‘uw’.
- Onder 'cybercriminaliteit’ verstaan wij:
  - Malware op uw computersysteem of computernetwerk.
  - Inbraak in uw computersysteem of computernetwerk.
  - (D)DoS- aanval.
  - Gegevensinbreuk.
  - Cyberafpersing.

Een 'hack' is een voorval waarbij u te maken heeft met ‘cybercriminaliteit'.

Wat is de Cyberwacht?

De Cyberwacht is de telefonische hulplijn die u belt bij een hack. Stel, uw laptop start op met de melding: “Uw computer is vergrendeld, u moet losgeld betalen als u weer toegang wilt”. Of een hacker heeft ingebroken en gegevens verzameld. Dan belt u direct naar de Cyberwacht. Onze specialisten helpen u dan meteen. Ook als u twijfelt of u gehackt bent dan kunt u ons bellen.

De Cyberwacht werkt samen met partners om zo alle cyberspecialismen samen te brengen op één plek. De Cyberwacht organiseert de dienst zodat u niet zelf hoeft te zoeken naar verschillende bedrijven die gespecialiseerd zijn in het oplossen van een bepaald type hack. Wij nemen de zoektocht naar de juiste dienstverleners uit handen en bieden u één loket waar alle cyberspecialismen zijn vertegenwoordigd.

Wat is het nummer van de Cyberwacht?

U kunt ons bellen op 070 – 513 55 55.

Om de dienstverlening van de Cyberwacht te verbeteren voeren wij regelmatig experimenten uit. Dit betekent dat u de Cyberwacht tijdens een experiment op een ander nummer belt dan hierboven wordt genoemd. Wij gebruiken andere telefoonnummers om de herkomst van onze klanten te kunnen herkennen.

Wat zijn de openingstijden van de Cyberwacht?

Onze specialisten staan op werkdagen voor u klaar tussen 08:00 en 21:00 uur. Op zaterdag van 09:00 tot 15:00 uur. Wanneer wij niet bereikbaar zijn door drukte, bellen wij u binnen één uur terug.

Hoe helpt de Cyberwacht?

Dat is afhankelijk van de situatie. Als u contact opneemt dan stellen we altijd eerst samen met u het probleem vast. Daarna zijn er twee opties:

1. **Eenvoudige hacks en advies**
   Uw probleem vereist algemene kennis en kan met behulp van telefonisch advies verholpen worden. Het team van de Cyberwacht helpt u direct met uw probleem.
2. **Ernstige en complexe hacks**
   Uw probleem vereist specialistische kennis of kan niet via de telefoon verholpen worden. Hiervoor geeft de Cyberwacht u de optie om een partner in te schaken om u van dienst te zijn. U beslist zelf of u gebruik maakt van onze partners. Wanneer u beslist doorverbonden te worden, sturen wij tegelijkertijd uw persoonsgegevens door. Deze zijn nodig om de dienst uit te voeren, bijvoorbeeld om u terug te bellen bij drukte. U sluit dan zelf een contract met deze dienstverlener. Als Cyberwacht werken we samen met verschillende specialistische partners, zoals IT-securityspecialisten en juristen. Verderop kunt u lezen welke partners dit zijn. De mogelijkheid voor u om te beslissen of u gebruik wenst te maken van de hulp door deze partners is standaard onderdeel van onze dienstverlening.

Soms is een hack complexer dan op voorhand ingeschat. In deze situatie zullen wij u onze partners aanbevelen om u specialistische dienstverlening te bieden. Ook in deze situatie maakt u zelf de keuze of u doorverbonden wilt worden.

Wie zijn de partners?

Student aan Huis

Student aan Huis is een IT-dienstverlener die u helpt bij hacks waarbij telefonische hulp niet voldoende is. Student aan Huis kijkt, via speciale software, mee op uw computersysteem of neemt, indien gewenst, uw computersysteem over en voert handelingen voor u uit.

Northwave
Northwave is een cybersecurity dienstverlener die u helpt bij ernstige en complexe hacks. Northwave onderzoekt cyberrisico's en helpt u deze op te lossen.

Waarbij helpt de Cyberwacht?

Wanneer helpen wij u?

Wij helpen u in onderstaande gevallen:

- **Malware op uw computersystemen of computernetwerk**
  Dit is software of code die ontworpen is om toegang te krijgen tot uw computersysteem of om uw computersysteem te beschadigen of te verstoren. Hieronder valt ook uw website.
- **Inbraak in uw computersysteem of computernetwerk**
  Iemand anders die, zonder uw toestemming, inbreekt in uw computersysteem of computernetwerk. Met het doel om toegang te verkrijgen, gegevens te verkrijgen of schade te veroorzaken aan uw computersysteem of computernetwerk. Hieronder valt ook uw website.
- **(D)DoS- aanval**
  Hierbij (over)belast iemand uw computersysteem of computernetwerk waardoor deze niet goed meer werken. Hieronder valt ook uw website.
- **Gegevensinbreuk**
  Hieronder verstaan wij het verliezen van persoonlijke gegevens uit uw computersysteem. De persoonlijke gegevens zijn hierdoor, zonder dat u daarvoor toestemming heeft gegeven, weg, beschadigd, ontoegankelijk of openbaar. Dit zijn alle digitale data die niet in het RAM-geheugen staan. Ook diefstal valt hieronder. Hieronder valt ook uw website.
- **Cyberafpersing**
  Wanneer iemand een schade veroorzaakt op uw computersysteem of computernetwerk en geld vraagt om het probleem op te lossen. Of wanneer iemand dreigt schade te veroorzaken op uw computersysteem of computernetwerk en u geld vraagt dit te voorkomen. Onder geld verstaan we ook cryptogeld. Hieronder valt ook uw website.

Wat kunt u van ons verwachten?

Wij helpen u op de volgende manieren:

- Wij stellen samen met u het probleem (de vorm van cybercriminaliteit) vast;
- De specialist die door u is ingeschakeld onderzoekt de oorzaak van de hack;
- Deze specialist herstelt (waar mogelijk) de schade aan uw persoonlijke data en software. Zodat uw computersysteem of computernetwerk weer zo goed mogelijk werkt. Waarbij we de situatie zo dichtbij mogelijk zoals die was vlak voordat de hack plaatsvond terugbrengen;
- We geven u advies over preventie.

Soms is het nodig, dat door uzelf beslist wordt, om een specialistische partner in te schakelen. Als u dit niet wilt, kan het zijn dat wij niet in de bovenstaande verwachtingen kunnen voldoen. Onze hulp gaat nooit verder dan is toegestaan door wet- en regelgeving.

Wat verwachten wij van u?

Bij een mogelijke hack is het belangrijk dat u snel handelt en de juiste stappen neemt. Doet u dit niet, dan is het mogelijk dat wij u niet kunnen helpen.

1. Zet het computersysteem niet uit. Hierdoor verliest u mogelijk waardevolle informatie.
2. Verbreek de verbinding met het internet. Hierdoor hebben andere personen geen toegang meer tot uw computer.
3. Neem contact met ons op.
4. Geef ons alle mogelijke informatie die nodig is om de omvang en oorzaak van het probleem vast te stellen. Hierbij gaat het niet alleen over informatie over de hack, maar ook informatie over uw computersysteem en mogelijk aanwezige back-ups.

Waarbij helpt de Cyberwacht niet?

Wij garanderen niet u in alle situaties te kunnen helpen. Cybercriminaliteit is complex en ieder computersysteem en iedere hack is uniek. Wij doen altijd ons best om u zo goed mogelijk te helpen, maar zijn hierbij vaak afhankelijk van de informatie die u ons geeft. U kunt ons niet voor de door ons verrichte dienstverlening aansprakelijk stellen voor schade die ontstaat door het (onjuist) opvolgen van ons advies. Ook kunt u ons niet aansprakelijk stellen voor schade door de dienstverlening van de door u ingeschakelde partner. Ook is er geen aansprakelijkheid wanneer wij of één van de dienstverleners (ten behoeve van u) handelingen uitvoeren op uw computersysteem. Indien er toch sprake is van een schadevergoeding zal deze voor ons nooit hoger zijn dan het bedrag dat de dienstverlening door ons u heeft gekost.

Wanneer helpen wij u niet?

- Wij helpen u niet wanneer u software gebruikt die u illegaal verkregen heeft of wanneer u hiervoor geen licentie heeft.
- Wij betalen voor u geen geldbedrag (ook niet in cryptogeld) om de hack, veelal een digitale afpersing, op te lossen.
- Wij helpen u niet om het geld dat digitaal is gestolen terug te krijgen. Of het terugkrijgen van kosten die ontstaan zijn door de hack, zoals een hoge (telefoon)rekening door gebruik van uw data en bandbreedte.
- Wij vergoeden geen geldbedrag (ook geen cryptogeld) die u heeft betaald om de hack op te lossen.
- Wij helpen u niet wanneer u een bestelling heeft gedaan bij een nep-webshop en/of deze bestelling heeft betaald. Wij raden u aan om aangifte te doen bij de Politie.
- Wij helpen u niet bij online fraude met een gestolen identiteit. Wij raden u aan om aangifte te doen bij de Politie.

Wanneer u in deze situaties contact met ons opneemt brengen wij de kosten voor onze dienstverlening in rekening.

Overmacht?

Het kan gebeuren dat wij onze dienstverlening niet kunnen leveren door overmacht. Dit betekent dat wij telefonisch niet bereikbaar zijn, door bijvoorbeeld: storing bij de telefooncentrale of onderbezetting bij onze partners of een soortgelijke situatie. In deze gevallen proberen wij de problemen zo snel mogelijk te verhelpen en adviseren wij u om ons later nog eens te bellen. Wij zijn niet aansprakelijk voor eventuele schade die zich bij u voordoet, omdat de Cyberwacht niet bereikbaar is door overmacht.

Hoe lost de Cyberwacht klachten op?

Wij garanderen niet dat wij u in alle situaties kunnen helpen. Natuurlijk doen wij altijd ons best om u zo goed mogelijk van dienst te zijn. Daarom horen wij graag van u als u een klacht heeft over onze dienstverlening. Doe dit zo snel mogelijk, dan geeft u ons de kans om eventuele schade zo veel mogelijk te beperken. Zoals wettelijk voorgeschreven heeft u twee maanden na ontdekking van de klacht de tijd om deze bij de Cyberwacht kenbaar te maken. U kunt uw klacht telefonisch aan ons doorgeven, via 070 513 55 55. Wij zullen uw klacht uiterlijk binnen 14 dagen beantwoorden. Als wij meer tijd nodig hebben om uw klacht op te lossen, dan laten wij u binnen 14 dagen weten wanneer u antwoord van ons kan verwachten.

Ieder computersysteem en iedere hack is uniek. Daarom bekijken wij per klacht hoe wij deze samen het best kunnen oplossen.

Hoe betaalt u de Cyberwacht?

U betaalt het bedrag dat u telefonisch met de Cyberwacht overeen bent gekomen. U ontvangt een factuur per e-mail van de Cyberwacht voor de verrichte dienstverlening van ons en die van onze partners. U betaalt € 1,49 per minuut voor de Cyberwacht, tenzij u gebruik maakt van een actie, promotie of de Cyberwacht afneemt via één van onze partners. U betaalt de factuur in één keer en na afname van de dienstverlening. Iedere keer dat u belt naar de Cyberwacht, en dus opnieuw gebruik maakt van de dienstverlening, ontvangt u een nieuwe factuur. Alle tarieven van de Cyberwacht zijn inclusief btw.

Neemt u extra diensten af van onze partners dan gaat u een overeenkomst aan met hen en betaalt u de partner voor deze afgenomen dienst.

Wanneer betaalt u de Cyberwacht?

U dient een factuur binnen 21 dagen te betalen. Het is niet mogelijk om opnieuw gebruik te maken van de diensten van de Cyberwacht voordat uw eerdere factuur is betaald.

Wat gebeurt er als u niet betaald?

Is het betaaltermijn van 21 dagen verstreken, dan start namens Sparklab B.V. Nationale-Nederlanden een debiteurenprocedure waarin het factuurbedrag alsnog wordt geïncasseerd met buitengerechtelijke kosten en wettelijke rente.

Moeilijkewoorden-lijst

Computersysteem
Met een ‘computersysteem’ bedoelen wij hardware, software, elektronische media, infrastructuur en telefoonsysteem.

Elektronische media
Met elektronische media bedoelen we bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd’s.

Infrastructuur
Dit zijn de apparaten die ervoor zorgen dat uw computersysteem blijft werken, zoals uw modem, router en wifi toegangspunt.

Telefoonsysteem
Dit is uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Malware
Dit is software of code die ontworpen is om toegang te krijgen tot uw computersysteem of om uw computersysteem te beschadigen of te verstoren.

Inbraak
Iemand anders die, zonder uw toestemming, toegang heeft tot uw computersysteem of computernetwerk. Met het doel om toegang te verkrijgen, gegevens te verkrijgen of schade te veroorzaken aan uw computersysteem of computernetwerk.

(D)DoS- aanval
Hierbij (over)belast iemand uw computersysteem of computernetwerk waardoor deze niet goed meer werken.

Gegevensinbreuk
Hieronder verstaan wij het verliezen van persoonlijke gegevens uit uw computersysteem. De persoonlijke gegevens zijn hierdoor, zonder dat u daarvoor toestemming heeft gegeven, weg, beschadigd, ontoegankelijk of openbaar. Dit zijn alle digitale data die niet in het RAM-geheugen staan. Ook diefstal valt hieronder.

Cyberafpersing
Wanneer iemand een schade veroorzaakt op uw computersysteem of computernetwerk en geld vraagt om het probleem op te lossen. Of wanneer iemand hiermee dreigt, tenzij u geld betaalt. Onder geld verstaan we ook cryptogeld.

Cybercriminaliteit
Gevallen van:
- Malware op uw computersystemen of computernetwerk.
- Inbraak in uw computersysteem of computernetwerk.
- (D)Dos- aanval.
- Gegevensinbreuk.
- Cyberafpersing.

Hack
Een voorval waarbij u te maken heeft met cybercriminaliteit.