



## ANWB Woonverzekering

# Cyberdekking

### Inhoud

Wat is CyberHelpdesk en Cyberdekking in het kort? .....	11
Hoe voorkom jij cyberincidenten? .....	11
Wat doet CyberHelpdesk? .....	11

### Cyberdekking

#### Algemeen

Wie is verzekerd? .....	11
Waar ben jij verzekerd? .....	11
Wat krijg jij maximaal vergoed? .....	11
Wat is jouw eigen risico per schadegebeurtenis? .....	11
Wat is indexering? .....	11

#### Online identiteitsdiefstal

Wat is verzekerd? .....	11
Wat vergoeden wij? .....	11
Wat zijn jouw verplichtingen? .....	11
Wat is niet verzekerd? .....	11

#### Data en systemen

Wat is verzekerd? .....	11
Wat vergoeden wij? .....	11
Wat zijn onze verplichtingen? .....	11
Wat zijn jouw verplichtingen? .....	11
Wat is niet verzekerd? .....	11

Zoeken in het document:

## Begrippenlijst

In deze voorwaarden lees je meer over jouw verzekering

Je leest onder andere

- wat verzekerd is
- voor welke schade jij bent verzekerd
- voor welke schade jij niet bent verzekerd
- hoeveel jij vergoed krijgt
- wat wij van jou verwachten

De Cyberdekking is een aanvulling op jouw inboedelverzekering. Bij deze verzekering horen ook algemene voorwaarden. Deze staan op [anwb.nl/polisvoorwaarden](https://anwb.nl/polisvoorwaarden).

### Wij hebben de voorwaarden zo makkelijk mogelijk voor jou gemaakt

- We beginnen met een vraag en daaronder lees je het antwoord.
- Je kunt direct in de voorwaarden zoeken. Dat doe je via de zoekfunctie naast de inhoudsopgave.
- De onderstreepte woorden zijn begrippen. Als je erop klikt, ga je naar de uitleg. Deze staat dan bovenaan op het scherm.
- Je scrolt makkelijk door de voorwaarden met behulp van de knoppen <Vorige | Volgende>. Deze staan onderaan de pagina aan de linkerkant.
- Wil je snel terug naar de inhoudsopgave? Klik dan op Inhoudsopgave, rechts onderaan de pagina.

## Wat is CyberHelpdesk en Cyberdekking in het kort?

De CyberHelpdesk is een telefonische hulpdienst die je kunt bellen als er sprake is van een cyberincident, dreiging van een cyberincident of als er hulp nodig is om een cyberincident te voorkomen. Je kunt van de CyberHelpdesk gebruik maken als je een inboedelverzekering hebt.

Heb je ook Cyberdekking afgesloten? Dan ben je onder voorwaarden voor bepaalde kosten verzekerd waarmee je te maken kan krijgen als jouw online identiteit is gestolen of als door een cyberincident herstel van data of software op jouw apparaat nodig is.

### CyberHelpdesk

De CyberHelpdesk wordt uitgevoerd door onze partner Cyberwacht. De experts van Cyberwacht kennen de bedreigingen die rondgaan op het internet en weten hoe te handelen. Ze zijn gespecialiseerd in ransomware, gelockte (e-mail) accounts, phishing-mails, geïnfecteerde harde schijven en virussen. Zij kijken als dat nodig is zelfs op afstand met je mee. En, als dat kan, helpt Cyberwacht je bij dit soort cyberincidenten ook om verloren data terug te zetten en om systemen te herstellen.

Het kan zijn dat Cyberwacht het probleem niet kan verhelpen maar ook dan kunnen zij je verder helpen.

Als je de Cyberdekking hebt afgesloten, kan Cyberwacht je naar ons doorverwijzen. Wij beoordelen dan of je recht hebt op specialistische hulp of een schadevergoeding.

Heb je geen Cyberdekking afgesloten? Dan kan Cyberwacht je helpen met het vinden van een geschikte specialist.

De kosten van deze specialist moet je wel zelf betalen.

### Cyberdekking

Je hebt recht op vergoeding van kosten als er sprake is van online identiteitsdiefstal of als herstel van data en/of systemen nodig is. Voordat je een beroep doet op deze dekking moet je eerst contact opnemen met de CyberHelpdesk.

Pas als zij er niet in slagen het cyberincident op te lossen, kan je een beroep op de dekking doen.

## Hoe voorkom jij cyberincidenten?

Het is belangrijk dat je voorkomt dat jouw online identiteit wordt gestolen zodat iemand anders online op jouw apparaat kan. Gebeurt dat toch? Dan kun je de CyberHelpdesk altijd bellen.

### Hoe kan je cyberincidenten voorkomen?

- Gebruik voor het vergrendelen van de toegang tot jouw apparaat veilige wachtwoorden\*
- Gebruik verschillende wachtwoorden voor jouw accounts
- Gebruik voor het beschermen van jouw online identiteit en voor de toegang tot data en software aanwezig op jouw apparaat veilige wachtwoorden

- Gebruik voor het beschermen van online opgeslagen data veilige wachtwoorden
- Deel jouw wachtwoorden niet met anderen
- Gebruik een digitale kluis waarin jij jouw veilige wachtwoorden bewaart
- Update steeds de software van het systeem en de applicaties die je op jouw apparatuur gebruikt binnen 14 dagen nadat deze beschikbaar is geworden
- Installeer steeds en onmiddellijk de beveiligingsupdates die door de fabrikant van jouw apparatuur wordt verstrekt
- Gebruik een actueel programma of app die jouw apparatuur beschermt tegen de meest voorkomende online bedreigingen zoals virussen, hacks en andere inbreuken
- Laat jouw apparatuur niet onbeheerd en onbeschermd achter op een locatie zodanig dat derden toegang tot jouw apparatuur krijgen.

\*Veilige wachtwoorden: Wachtwoorden waarbij gebruik is gemaakt van opeenvolgende tekens waardoor het wachtwoord moeilijk te kraken is. Je wijzigt het wachtwoord regelmatig.

### **Wat kan je nog meer doen?**

Het is verstandig dat je regelmatig een back-up van jouw bestanden maakt. Je kan jouw back-up op een externe schijf plaatsen, op een USB-stick of in de Cloud opslaan. Voer je niet regelmatig een back-up uit? Dan kan de CyberHelpdesk je misschien niet verder helpen.

## **Wat doet CyberHelpdesk?**

### **Wanneer helpt CyberHelpdesk jou?**

De CyberHelpdesk helpt jou in onderstaande gevallen:

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

### **Hoe helpt CyberHelpdesk jou?**

- Zij stellen samen met jou het probleem (de vorm van cybercriminaliteit) vast;
- De expert van Cyberwacht onderzoekt de oorzaak van het cyberincident;
- De expert van Cyberwacht herstelt (waar mogelijk) de schade aan jouw persoonlijke data en software. Het doel is om de data en software te herstellen naar het punt vlak voordat het cyberincident plaatsvond;
- Je krijgt advies over preventie.

### **Wanneer helpt CyberHelpdesk je niet?**

Je hebt geen recht op hulp van de CyberHelpdesk als je jouw apparatuur geheel of gedeeltelijk voor zakelijke of bedrijfsmatige doeleinden gebruikt.

# Cyberdekking

## Algemeen



### Wie is verzekerd?

Jij als verzekeringnemer en jouw gezin.



### Waar ben je verzekerd?

Je bent overal ter wereld verzekerd.



### Wat krijg je maximaal vergoed?

Wij vergoeden maximaal €2.000,- per schadegebeurtenis



### Wat is jouw eigen risico per schadegebeurtenis?

Je hebt geen eigen risico



### Wat is indexering?

Wij kunnen jaarlijks de premie aanpassen. Dit noemen wij indexering.

## Online identiteitsdiefstal



### Wat is verzekerd?

Jouw persoonlijke gegevens waarmee je je online identificeert zijn op een onrechtmatige wijze online door derden verkregen met als doel deze persoonlijke gegevens te gebruiken of daarmee te dreigen.



### Wat vergoeden wij?

De redelijke en noodzakelijke kosten die worden gemaakt door een notaris of andere bevoegde instantie die in Nederland gevestigd is, om jouw identiteit met zekerheid vast te kunnen stellen. Dit is nodig omdat een financiële dienstverlener of overheidsinstantie, op haar uitdrukkelijk verzoek, jouw identiteit met zekerheid moet vaststellen.

De extra kosten die je verschuldigd bent omdat je alsnog de beoogde financiële dienst wenst af te nemen nadat deze eerder door dezelfde financiële dienstverlener was gestaakt of beëindigd in verband met de identiteitsdiefstal.

Creditcard- of andere bankkosten die door jouw financiële instelling(en) in rekening worden gebracht om kaarten en/of bankrekeningen te annuleren en/of opnieuw uit te geven.

Een bedrag van € 100,- per werkdag die je als een vrije dag moest opnemen met een maximum van 5 werkdagen. Je hebt een verklaring van jouw werkgever nodig.



## Wat zijn jouw verplichtingen?

- Je meldt het cyberincident eerst bij de CyberHelpdesk. Zij geven advies om de online identiteitsdiefstal ongedaan te maken.
- Je meldt de online identiteitsdiefstal zo snel mogelijk bij ons.
- Je doet aangifte bij de politie van de identiteitsdiefstal.



## Wat is niet verzekerd?

- Kosten die worden gemaakt ten behoeve van de uitvoering van een dienst door een financiële dienstverlener die niet in Nederland gevestigd is.
- Kosten in verband met belangenbehartiging.
- Schade als de identiteitsdiefstal door een verzekerde is uitgevoerd dan wel dat deze bij de online identiteitsdiefstal betrokken was.
- Andere vermogensschade die je lijdt als gevolg van die identiteitsdiefstal. Zoals het betalen van losgeld, koersverlies, waardedalingen als gevolg van fraude.
- Schade als gevolg van diefstal van jouw online identiteit waarmee je jezelf (ook) zakelijk of ten behoeve van zakelijke of bedrijfsmatige activiteiten identificeert.

## Data en systemen



## Wat is verzekerd?

Als de CyberHelpdesk je niet meer kan helpen en de schade aan data en systemen als gevolg van een cyberincident waardoor data en/of software op jouw apparatuur is beschadigd, ontoegankelijk is geworden of verloren is gegaan..



## Wat vergoeden wij?

- Wij kunnen namens jou een specialist inschakelen. Wij vergoeden de kosten voor:
  - Het herstellen van de data naar het moment vóór het cyberincident
  - Overzetten van de herstelde data naar jouw apparatuur
  - Het herstellen van de getroffen software en/of van het getroffen besturingssysteem.
- Wij vergoeden deze kosten ook als je zelf een specialist inschakelt. Je moet dan wel eerst toestemming van ons krijgen.
- Wij vergoeden de redelijke en noodzakelijke kosten om vast te kunnen stellen of herstel van data en/of systemen nog mogelijk is.
- Wij vergoeden niet meer dan de redelijke en noodzakelijke kosten om data en/of systemen te herstellen.
- Alle verzendkosten in verband met het herstel van jouw apparatuur.



## Wat zijn onze verplichtingen?

De door ons ingeschakelde expert zal alle redelijke inspanningen leveren om data en/of besturingssystemen te herstellen. Herstel kan niet worden gegarandeerd.



## Wat zijn jouw verplichtingen?

- Je meldt het cyberincident eerst bij de CyberHelpdesk. Zij gaan proberen de schade aan data en systemen te verhelpen.
- Je meldt het cyberincident zo snel mogelijk na ontdekking bij ons.



## Wat is niet verzekerd?

- Schade aan data en systemen op apparatuur die geheel of gedeeltelijk voor zakelijke of bedrijfsmatige doeleinden wordt gebruikt.
- Kosten van herstel of vervanging van hardware.
- Kosten van herstel of vervanging van software of van het besturingssysteem die geen verband houdt met het cyberincident dat schade aan data en/of systeem heeft veroorzaakt.
- Een cyberincident dat ertoe heeft geleid dat data die opgeslagen is buiten jouw apparatuur, beschadigd is geraakt, verloren is gegaan of ontoegankelijk is geworden zoals data in de cloud.
- Kosten voor de terugkoop van softwarelicenties, bijvoorbeeld: licenties voor verwijderde software, games, muziek of films.
- Andere vermogensschade die je lijdt als gevolg van het cyberincident. Zoals het betalen van losgeld, koersverlies, waardedalingen als gevolg van fraude.
- Herstel van data die opgeslagen is in de cloud of op een gameconsole.
- Herstel van data die illegaal in jouw bezit is.

# Begrippenlijst

## Begrip

## Wat wij hieronder verstaan

### Cyberincident in het algemeen

Er is sprake van een cyberincident als een derde vanaf een ander apparaat met kwade bedoelingen een handeling verricht dat tot doel heeft om:

- jouw apparatuur niet of niet meer goed te laten functioneren,
- de toegang tot jouw data te verhinderen,
- jouw online identiteit te bemachtigen.

Je kunt daardoor niet meer vertrouwen op de juistheid van de opgeslagen informatie, je kunt de opgeslagen informatie niet meer benaderen of de systemen werken niet meer optimaal. Je kunt een cyberincident onder andere herkennen doordat de snelheid van jouw apparatuur verminderd is, bepaalde informatie op jouw apparatuur niet meer toegankelijk is, jouw apparatuur toont vreemde berichten, je ontvangt e-mails waaruit volgt dat je gehackt bent of je bent online slecht bereikbaar. De meest bekende vormen van cyberincidenten zijn ransomware (losgeld), phishing en de DDoS-aanval.

### Cyberincident als het om deze dekking gaat

Een cyberincident is een gebeurtenis die het gevolg is van handelingen die via een internet/onlineverbinding plaatsvinden en tot doel hebben online identiteitsdiefstal te plegen of data en software van jouw apparatuur te beschadigen.

### Gezin

Personen die in het Nederlandse bevolkingsregister op hetzelfde adres staan ingeschreven. Zij wonen in gezinsverband samen.

### Indexering

Elk jaar stijgen de kosten voor reparatie of vergoeding van schade. Voorbeelden hiervan zijn: stijgende lonen, stijgende materiaalkosten, betere maar ook duurdere reparatiemethoden of hogere vergoedingen op basis van rechtspraak. Het aanpassen van de premie om deze kostenstijgingen op te vangen heet indexering. Ieder jaar kunnen we deze indexering doorvoeren op de hoofdpremievervaldag. Deze datum staat op jouw polisblad.

### Jouw apparatuur

Al jouw apparatuur die je alleen particulier gebruikt en waarmee je online digitale gegevens (data) kan uitwisselen en verwerken. Deze data is op jouw apparatuur opgeslagen.

Jouw apparatuur bestaat uit een laptop of desktop personal computer, tablet of smartphone maar ook de Wi-Fi-router of een internettoegangspunt dat erop is aangesloten. Apparaten die deel uitmaken van Internet of Things, zoals smart-home devices, vallen hier niet onder ongeacht of deze apparaten verbonden kunnen worden met jouw apparatuur.

### Premie

Het bedrag dat je voor jouw verzekering betaalt.

### Online identiteitsdiefstal

Het zonder jouw toestemming, op onrechtmatige wijze online verkrijgen door derden van jouw persoonlijke gegevens waarmee je jezelf online identificeert met als doel deze persoonlijke gegevens te gebruiken of daarmee te dreigen.

### Schade aan data en systemen

Data en software op jouw apparatuur zijn door een cyberincident beschadigd geraakt, ontoegankelijk geworden of verloren gegaan.

# Begrippenlijst

Begrip

Wat wij hieronder verstaan

---

**Schadegebeurtenis**

Een voorval of een reeks van voorvallen die met elkaar verband houden, met één oorzaak en die schade tot gevolg heeft.

**Vergoeding**

Het bedrag dat wij betalen naar aanleiding van een schadegebeurtenis.

**Verzekerde**

Jij als verzekeringnemer en jouw gezin.

**Verzekeringnemer**

De persoon die de verzekering heeft afgesloten.