

Voorwaarden



> Cyberdekking

Inhoud

Wat is CyberHelpdesk en Cyberdekking in het kort?	2
Hoe voorkomt u cyberincidenten?	2
Wat doet CyberHelpdesk?	3

Cyberdekking

Algemeen

• Wie is verzekerd?	4
• Waar bent u verzekerd?	4
• Wat krijgt u maximaal vergoed?	4
• Wat is uw eigen risico per schadegebeurtenis?	4
• Wat is indexering?	4

Online identiteitsdiefstal

• Wat is verzekerd?	4
• Wat vergoeden wij?	4

• Wat zijn uw verplichtingen	4
• Wat is niet verzekerd?	5

Data en systemen

• Wat is verzekerd?	5
• Wat vergoeden wij?	5
• Wat zijn onze verplichtingen?	5
• Wat zijn uw verplichtingen?	5
• Wat is niet verzekerd?	6

Begrippenlijst	7
----------------------	---

Zoeken in het document:

In deze voorwaarden leest u meer over uw verzekering

U leest onder andere:

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

De Cyberdekking is een aanvulling op uw inboedelverzekering. Bij deze verzekering horen ook algemene voorwaarden. Deze staan op unigarant.nl/polisvoorwaarden.

Wij hebben de voorwaarden zo makkelijk mogelijk voor u gemaakt

- We beginnen met een vraag en daaronder leest u het antwoord.
- U kunt direct in de voorwaarden zoeken. Dat doet u via de zoekfunctie naast de inhoudsopgave.
- De onderstreepte woorden zijn begrippen. Als u erop klikt, gaat u naar de uitleg. Deze staat dan bovenaan op het scherm.
- U scrolt makkelijk door de voorwaarden met behulp van de knoppen <Vorige | Volgende>. Deze staan onderaan de pagina aan de linkerkant.
- Wilt u 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 u kunt bellen als er sprake is van een cyberincident, dreiging van een cyberincident of als er hulp nodig is om een cyberincident te voorkomen. U kunt van de CyberHelpdesk gebruik maken als u een inboedelverzekering heeft.

Heeft u ook de Cyberdekking afgesloten? Dan bent u onder voorwaarden voor bepaalde kosten verzekerd. Kosten waarmee u te maken kunt krijgen als uw online identiteit is gestolen of als door een cyberincident herstel van data of software op uw apparatuur 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 u mee. En, als dat kan, helpt Cyberwacht u 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 u verder helpen.

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

Heeft u geen Cyberdekking afgesloten? Ook dan kan Cyberwacht u helpen met het vinden van een geschikte specialist. De kosten van deze specialist moet u wel zelf betalen.

Cyberdekking

U heeft recht op vergoeding van kosten als er sprake is van online identiteitsdiefstal of als herstel van data en/of systemen nodig is. Voordat u een beroep doet op deze dekking moet u eerst contact opnemen met de CyberHelpdesk. Pas als zij er niet in slagen het cyberincident op te lossen, kunt u een beroep op de dekking doen.

Hoe voorkomt u cyberincidenten?

Het is belangrijk dat u voorkomt dat uw online identiteit wordt gestolen zodat iemand anders online op uw apparatuur kan. Gebeurt dat toch? Dan kunt u altijd de CyberHelpdesk bellen.

Hoe kunt u cyberincidenten voorkomen?

- Gebruik voor het vergrendelen van de toegang tot uw apparatuur veilige wachtwoorden*
- Gebruik verschillende wachtwoorden voor uw accounts
- Gebruik voor het beschermen van uw online identiteit en voor de toegang tot data en software aanwezig op uw apparatuur veilige wachtwoorden
- Gebruik voor het beschermen van online opgeslagen data veilige wachtwoorden
- Deel uw wachtwoorden niet met anderen
- Gebruik een digitale kluis waarin u uw veilige wachtwoorden bewaart

- Update steeds de software van het systeem en de applicaties die u op uw apparatuur gebruikt binnen 14 dagen nadat deze beschikbaar is geworden
- Installeer steeds en onmiddellijk de beveiligingsupdates die door de fabrikant van uw apparatuur wordt verstrekt
- Gebruik een actueel programma of app die uw apparatuur beschermt tegen de meest voorkomende online bedreigingen zoals virussen, hacks en andere inbreuken
- Laat uw apparatuur niet onbeheerd en onbeschermd achter op een locatie zodanig dat derden toegang tot uw apparatuur krijgen.

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

Wat kunt u nog meer doen?

Het is verstandig dat u regelmatig een back-up van uw bestanden maakt. U kunt uw back-up op een externe schijf plaatsen, op een USB-stick of in de Cloud opslaan. Voert u niet regelmatig een back-up uit? Dan kan de CyberHelpdesk u misschien niet verder helpen.

Wat doet CyberHelpdesk?

Wanneer helpt CyberHelpdesk u?

De CyberHelpdesk helpt 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 online identiteitsdiefstal valt hieronder, net als 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.

Hoe helpt CyberHelpdesk u?

- Zij stellen samen met u 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 uw persoonlijke data en software. Het doel is om de data en software te herstellen naar het punt vlak voordat het cyberincident plaatsvond;
- U krijgt advies over preventie.

Wanneer helpt CyberHelpdesk u niet?

U heeft geen recht op hulp van de CyberHelpdesk als u uw apparatuur geheel of gedeeltelijk voor zakelijke of bedrijfsmatige doeleinden gebruikt.

Cyberdekking

Algemeen



Wie is verzekerd?

U als verzekeringnemer en uw gezin.



Waar bent u verzekerd?

U bent overal ter wereld verzekerd.



Wat krijgt u maximaal vergoed?

Wij vergoeden maximaal € 2.000,- per schadegebeurtenis.



Wat is uw eigen risico per schadegebeurtenis?

U heeft geen eigen risico.



Wat is indexering?

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

Online identiteitsdiefstal



Wat is verzekerd?

Uw persoonlijke gegevens waarmee u zich 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 uw identiteit met zekerheid vast te kunnen stellen. Dit is nodig omdat een financiële dienstverlener of overheidsinstantie, op haar uitdrukkelijk verzoek, uw identiteit met zekerheid moet vaststellen.

De extra kosten die u verschuldigd bent omdat u 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 uw 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 u als een vrije dag moest opnemen met een maximum van 5 werkdagen. U heeft een verklaring van uw werkgever nodig.



Wat zijn uw verplichtingen?

- U meldt het cyberincident eerst bij de CyberHelpdesk. Zij geven advies om de online identiteitsdiefstal ongedaan te maken.
- U meldt de online identiteitsdiefstal zo snel mogelijk bij ons.
- U 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 de verzekerde is uitgevoerd dan wel dat deze bij de online identiteitsdiefstal betrokken was.
- Andere vermogensschade, die u lijdt als gevolg van de identiteitsdiefstal. Zoals het betalen van losgeld, koersverlies of waardedalingen als gevolg van fraude
- Schade als gevolg van diefstal van uw online identiteit waarmee u zich (ook) zakelijk of ten behoeve van zakelijke of bedrijfsmatige activiteiten identificeert.

Data en systemen



Wat is verzekerd?

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



Wat vergoeden wij?

- Wij kunnen namens u 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 uw apparatuur.
 - Het herstellen van de getroffen software en/of van het getroffen besturingssysteem.
- Wij vergoeden deze kosten ook als u een zelf een specialist inschakelt. U 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 uw apparatuur.



Wat zijn onze verplichtingen?

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



Wat zijn uw verplichtingen?

- U meldt het cyberincident eerst bij de CyberHelpdesk. Zij gaan proberen de schade aan data en systemen te verhelpen.
- U 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 dat 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 uw 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 u lijdt als gevolg van het cyberincident. Zoals het betalen van losgeld, koersverlies of waardedalingen als gevolg van fraude,
- Herstel van data die opgeslagen is in de cloud of op een gameconsole.
- Herstel van data die illegaal in uw bezit is.

Begrippenlijst

Begrip

Wat wij hieronder verstaan

Cyberincident in het algemeen	<p>Er is sprake van een cyberincident als een derde vanaf een ander apparaat met kwade bedoelingen een handeling verricht die tot doel heeft om:</p> <ul style="list-style-type: none">• uw apparatuur niet of niet meer goed te laten functioneren,• de toegang tot uw data te verhinderen,• uw online identiteit te bemachtigen. <p>U kunt daardoor niet meer vertrouwen op de juistheid van de opgeslagen informatie, u kunt de opgeslagen informatie niet meer benaderen of de systemen werken niet meer optimaal. U kunt een cyberincident onder andere herkennen doordat de snelheid van uw apparatuur verminderd is, bepaalde informatie op uw apparatuur niet meer toegankelijk is, uw apparatuur toont vreemde berichten, u ontvangt e-mails waaruit volgt dat u gehackt bent of u bent online slecht bereikbaar. De meest bekende vormen van cyberincidenten zijn ransomware (losgeld), phishing en de DDoS-aanval.</p>
Cyberincident als het om deze dekking gaat	<p>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 uw apparatuur te beschadigen.</p>
Gezin	<p>Personen die in het Nederlandse bevolkingsregister op hetzelfde adres staan ingeschreven. Zij wonen in gezinsverband samen.</p>
Indexering	<p>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 uw polisblad.</p>
Premie	<p>Het bedrag dat u voor uw verzekering betaalt.</p>
Online identiteitsdiefstal	<p>Het zonder uw toestemming, op onrechtmatige wijze online verkrijgen door derden van uw persoonlijke gegevens waarmee u zich online identificeert met als doel deze persoonlijke gegevens te gebruiken of daarmee te dreigen.</p>
Schade aan data en systemen	<p>Data en software op uw apparatuur zijn door een cyberincident beschadigd geraakt, ontoegankelijk geworden of verloren gegaan.</p>
Schadegebeurtenis	<p>Een voorval of een reeks van voorvallen die met elkaar verband houden, met één oorzaak en die schade tot gevolg heeft.</p>
Uw apparatuur	<p>Al uw apparatuur die u alleen particulier gebruikt en waarmee u online digitale gegevens (data) kan uitwisselen en verwerken. Deze data is op uw apparatuur opgeslagen. Uw 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 uw apparatuur.</p>
Vergoeding	<p>Het bedrag dat wij betalen naar aanleiding van een schadegebeurtenis.</p>
Verzekerde	<p>U als verzekeringnemer en uw gezin.</p>
Verzekeringnemer	<p>De persoon die de verzekering heeft afgesloten.</p>