

Informatie over de Cyberservice

**Als onderdeel van uw
inboedelverzekering in het
ZekerheidsPakket Particulieren**

Inhoud

| | |
|--|--------------------|
| Leeswijzer, Uw verzekering in het kort | pagina 3 |
| Polisvoorwaarden Cyberservice | 6 |

Leeswijzer

Uw verzekering in het kort

- **Waarvoor is deze verzekering?**
- **Waar bent u wel en niet voor verzekerd?**
- **Wat mag u van ons verwachten?**
- **Wat te doen bij schade?**

U kunt gebruik maken van onze Cyberservice. De Cyberservice is een dekking van de Inboedelverzekering die u heeft gesloten als onderdeel van het ZekerheidsPakket Particulieren. Bij deze dekking horen polisvoorwaarden. Wij zetten hier de belangrijkste punten uit de polisvoorwaarden op een rijtje. U leest onder andere wat de dekking inhoudt, wat u van ons mag verwachten en wat u moet doen bij schade.

Wij hebben ons best gedaan alles duidelijk voor u te maken. Als u na het lezen nog vragen heeft, dan kunt u contact opnemen met uw verzekeringsadviseur.

Heeft u schade? Belt u dan met de Cyberwacht. U kunt de Cyberwacht ook bellen als u vragen heeft over de veiligheid van uw apparatuur.

Telefoonnummer: 070-513 5550
Maandag tot en met vrijdag van 09.00 tot 20.00 uur
Zaterdag van 09.00 tot 15.00 uur

Waarvoor is de Cyberservice?

Uw computer kan gehackt worden. U kunt dan bijvoorbeeld niet meer bij uw documenten en foto's, of u kunt de computer helemaal niet meer gebruiken. Ook kan hierbij geld van uw bankrekening worden gestolen, of er kan misbruik worden gemaakt van uw identiteit. Met de Cyberservice bent u verzekerd voor deze situaties. De verzekering dekt niet alleen schade, maar we bieden ook hulp bij cyberincidenten. De dekking geldt niet alleen voor uw desktop computers, maar bijvoorbeeld ook voor uw laptops, tablets en smartphones.

Waar geldt de dekking?

Het maakt voor de Cyberservice niet uit waar de schade is ontstaan. De dekking geldt dus ook voor schade die ontstaat terwijl u uw apparatuur buitenshuis gebruikt.

Waar bent u bijvoorbeeld voor verzekerd?

- U kunt gebruik maken van de diensten van de Cyberwacht. Heeft u op een link in een mail geklikt en denkt u dat het misschien een phishing mail was? Of weet u zeker dat uw computer gehackt is? Dan kunt u de Cyberwacht bellen. De Cyberwacht gaat samen met u uitzoeken wat er aan de hand is. U kunt de Cyberwacht ook bellen als u advies wilt over het beveiligen van uw verzekerde apparatuur, of hulp bij het installeren van beveiligingssoftware. Het telefoonnummer van de Cyberwacht is 070-513 5550.
- U bent verzekerd voor diefstal van geld van uw (bank)rekening. Als er geld wordt gestolen van uw bankrekening door phishing of e-mailspoofing of doordat iemand onbevoegd toegang heeft tot uw rekening, vergoedt de bank in veel gevallen uw schade. De dekking van de Cyberservice is een soort vangnet voor als de bank de schade niet vergoedt. We kunnen u ook helpen om de schade te melden bij uw bank.
- U bent verzekerd voor identiteitsdiefstal. Maakt iemand misbruik van uw persoonsgegevens? Dan dekt deze verzekering de directe financiële schade die u lijdt. En we proberen samen met u te voorkomen dat er nog meer schade ontstaat.
- U bent verzekerd voor dataherstel en verwijderen

van malware/vervanging van hardware. Bij een cyberincident helpen we u om uw data te herstellen en de kwaadaardige software te verwijderen van uw verzekerde apparatuur. Dit is niet altijd mogelijk. We kunnen er ook voor kiezen de kosten voor het vervangen van de apparatuur te vergoeden.

- U bent verzekerd voor hulp bij cyberafpersing. Is uw computer gehackt en eist iemand losgeld van u om de schade ongedaan te maken? Dan is er sprake van cyberafpersing. Wij vergoeden geen losgeld. Maar we gaan wel samen met u kijken wat er aan de hand is, we proberen uw data veilig te stellen en te zorgen dat u uw computer weer veilig kunt gebruiken.

Waar bent u bijvoorbeeld niet voor verzekerd?

U bent bijvoorbeeld niet verzekerd voor:

- het verlies van bitcoins of andere cryptocurrencies;
- schade die verband houdt met gokken;
- schade die verband houdt met professionele of bedrijfsmatige activiteiten;
- schade die bestaat uit letsel, psychische schade, trauma, ziekte of overlijden.

Wat bepaalt de hoogte van de premie?

De premie is een vast bedrag dat niet afhangt van bijvoorbeeld uw leeftijd of uw gezinssamenstelling.

Wat krijgt u vergoed?

Bij een gedekte schade bestaat de schadevergoeding uit:

- hulp door de Cyberwacht en/of
- hulp door andere specialisten en/of
- schadevergoeding in geld (alleen bij de dekkingen Diefstal van geld van uw (bank)rekening, Identiteitsdiefstal en Vervanging van hardware).
- In de polisvoorwaarden leest u wat de maximale vergoeding per dekking is. Per jaar vergoeden wij voor alle dekkingen samen maximaal 5.000 euro. De hulp van de Cyberwacht telt niet mee voor dit maximum.

Voorbeeld:

U belt de Cyberwacht omdat uw computer gehackt is. Na onderzoek blijkt dat het niet mogelijk is de malware te verwijderen van uw computer. We

Aan deze informatie kunt u geen rechten ontleen. Uw rechten op dekking en dienstverlening staan in uw polis(voorwaarden).

vergoeden daarom de kosten van een vervangende computer. De Cyberwacht controleert of uw back-up veilig is en helpt u de gegevens van uw back-up op de vervangende computer te zetten. Ook krijgt u advies over de beveiliging van uw computer. Wij hebben in totaal 1.400 euro vergoed.

Een paar maanden later is uw computer opnieuw gehackt. Daarbij is een kopie van uw paspoort gestolen en er is 3.000 euro gestolen van uw bankrekening. Het totale schadebedrag van deze tweede schade is 4.000 euro (verlies van geld op bankrekening, verwijderen van malware en monitoring in verband met identiteitsdiefstal). Maar omdat de schade in hetzelfde verzekeringsjaar valt als de eerste schade vergoeden wij voor deze tweede schade maximaal 3.600 euro (5.000 euro min de 1.400 euro van de eerste schade). We overleggen met u wat u wilt. U kunt een gedeelte van de diefstalsschade voor eigen rekening nemen, maar u kunt er ook voor kiezen de monitoring achterwege te laten.

Kunnen wij de premie en voorwaarden wijzigen?

Ja, wij kunnen de premie en voorwaarden wijzigen. Als we wijzigingen doorvoeren, dan doen we dit altijd op de verlengingsdatum van uw inboedelverzekering. U hoort dit van tevoren van ons. Bent u het niet eens met de wijziging? Dan kunt u de verzekering opzeggen.

Wanneer eindigt de Cyberservice?

De Cyberservice eindigt op hetzelfde moment waarop uw inboedelverzekering eindigt.

Wat mag u van ons verwachten?

- De Cyberwacht helpt u bij schade en vragen over de beveiliging van uw apparatuur.
- We helpen u altijd zo snel mogelijk.
- We informeren u over veranderingen. Denk aan wijzigingen in de premie en voorwaarden of veranderingen in de dekking.

Wat zijn uw verplichtingen?

- Gebruik en onderhoud de verzekerde apparatuur volgens de aanbevelingen van de producent en de leverancier.

- Installeer updates van het besturingssysteem en andere beveiligingsupdates zo snel mogelijk en in elk geval binnen 14 dagen nadat deze beschikbaar komen.
- Zorg dat u passende beveiligingsmaatregelen installeert, zoals anti-virus software.
- Gebruik wachtwoorden die niet gemakkelijk te raden zijn, en verander uw wachtwoorden regelmatig.
- Laat de verzekerde apparatuur en uw gegevens nooit onbeheerd achter op een plaats waar ze toegankelijk zijn voor onbevoegden.
- Maak minimaal eenmaal per 14 dagen een back-up van uw data. Doet u dit niet? Dan kunt u geen aanspraak maken op de dekking voor dataherstel.
- Geef ons altijd de juiste informatie.
- Geef veranderingen in uw gegevens altijd zo snel mogelijk aan ons door. Denk aan wijzigingen in de contactgegevens of rekeningnummer.
- Betaal op tijd de premie.

Wat moet u altijd doen bij schade?

- Bel zo snel mogelijk de Cyberwacht via 070 513 5550.
- Doe direct aangifte bij de politie als er sprake is van een strafbaar feit.
- Doe er alles aan om verdere schade te voorkomen.
- Help mee aan alles wat wij doen om de schade af te handelen.

Waarom zijn sommige woorden in de polisvoorwaarden oranje?

Is een woord in de polisvoorwaarden oranje gekleurd? Dan hebben we voor dat woord in hoofdstuk 7 een begripsomschrijving opgenomen. In die begripsomschrijving leggen we uit wat we precies bedoelen met het woord. Als een dergelijk woord meerdere keren voorkomt op een pagina, kleuren we het alleen de eerste keer oranje.

Aan deze informatie kunt u geen rechten ontleen. Uw rechten op dekking en dienstverlening staan in uw polis(voorwaarden).



nationale
nederlanden

Polisvoorwaarden

Cyberservice

Deze polisvoorwaarden vormen één geheel met de polisvoorwaarden ZekerheidsPakket Particulieren (ZPP). Als er verschillen zijn, gelden de polisvoorwaarden van dit product.

Versie VM 2810-01

Inhoud

| | pagina |
|---|---|
| 1 | Wie is verzekerd? 8 |
| 2 | Welke apparatuur is verzekerd? 9 |
| 3 | Omschrijving van dekking: wat is verzekerd? 10 |
| 4 | Wat kunnen wij bij schade van elkaar verwachten? 12 |
| 5 | Wat krijgt u vergoed? 13 |
| 6 | Uitsluitingen: wat is niet verzekerd? 15 |
| 7 | Begrippenlijst 16 |

Heeft u schade? Belt u dan met de Cyberwacht. U kunt de Cyberwacht ook bellen als u vragen heeft over de veiligheid van uw apparatuur.

Telefoonnummer: 070-513 5550
Maandag tot en met vrijdag van
09.00 tot 20.00 uur
Zaterdag van 09.00 tot 15.00 uur

1 Wie is verzekerd?

De volgende personen kunnen gebruikmaken van deze verzekering:

- a. De verzekeringnemer. Dit is de persoon die deze verzekering heeft afgesloten en die ervoor zorgt dat de premie wordt betaald.
- b. Alle personen met wie de verzekeringnemer in gezinsverband samenwoont.

Als we in deze voorwaarden 'u' gebruiken, bedoelen we alle verzekerden.

2 Welke apparatuur is verzekerd?

Verzekerd zijn:

- computerapparatuur en bijbehorende randapparatuur; en
- smartphones, tablets, laptops; en
- andere wearable devices. Dit zijn op het lichaam draagbare armbanden, horloges, brillen en kleding die tot doel hebben de gebruiker te voorzien van persoonlijke **data** en/of omgevingsdata.

De apparatuur is alleen verzekerd als deze:

- onder uw directe controle staat en
- bedoeld is voor privégebruik en
- uw eigendom is of door u geleased is en
- dient voor het creëren, benaderen, verwerken, monitoren, opslaan, ophalen, weergeven, verzenden of ontvangen van privé data.

Als wij in deze polisvoorwaarden 'verzekerde apparatuur' of 'verzekerd apparaat' gebruiken, bedoelen we de apparatuur zoals in dit artikel omschreven.

Let op: smart home devices vallen hier niet onder. Smart home devices zijn apparaten of IoT componenten die verbonden zijn met en/of worden aangestuurd via het internet. Bijvoorbeeld camera's, airconditioning, verlichting of alarmsystemen.

3 Omschrijving van dekking: wat is verzekerd?

Met deze verzekering bent u verzekerd voor:

Als bij het ontstaan van de schade aan de volgende voorwaarden is voldaan:

1. Hulp en advies door de Cyberwacht

Is er sprake van diefstal van geld van uw rekening, **identiteitsdiefstal**, een **cyberincident** of **cyberafpersing**? Of vermoedt u dat hier sprake van zou kunnen zijn? Dan moet u zo snel mogelijk de Cyberwacht (070 513 5550) bellen. U kunt de Cyberwacht ook bellen als u vragen heeft over het voorkomen van cyberincidenten.

De Cyberwacht beantwoordt uw vragen en biedt hulp en advies bij schade. De Cyberwacht kan ook besluiten een gespecialiseerd bedrijf in te schakelen dat u verder helpt.

2. Diefstal van geld van uw (bank)rekening

Wij vergoeden het verlies van geld van uw (bank)rekening:

- a. als gevolg van een ongeautoriseerde elektronische overboeking door een onbevoegde **derde partij** die toegang heeft tot uw bankrekening, uw creditcard of debitcard, of een zogenoemde **mobile wallet**, en/of
- b. doordat u slachtoffer bent geworden van **phishing** of **email spoofing**.

U bent alleen verzekerd voor deze schade als:

- u binnen 72 uur nadat u de diefstal ontdekt heeft, de schade meldt bij de bank of het mobile wallet bedrijf, en
- u kunt aantonen dat de bank of het mobile wallet bedrijf de schade niet vergoedt, en
- u binnen 72 uur nadat u de diefstal ontdekt heeft, aangifte doet bij de politie.

Onder geld op een (bank)rekening verstaan we tegoeden in een officiële nationale munteenheid, die uw eigendom zijn en die een financiële instelling voor u beheert. Hier onder vallen niet digitale of virtuele munteenheden.

3. Identiteitsdiefstal

U bent verzekerd voor geldelijke verliezen die het directe gevolg zijn van identiteitsdiefstal, met uitzondering van verlies van inkomsten. Bijvoorbeeld: iemand heeft goederen besteld op uw naam en u moet de rekening betalen. Dit valt onder de dekking. Maar als u een dag niet kunt werken omdat u dingen moet regelen in verband met de identiteitsdiefstal, vergoeden we niet het verlies van inkomsten.

Wij vergoeden de schade alleen als u binnen 72 uur na het ontdekken van de identiteitsdiefstal:

- de identiteitsdiefstal bij ons meldt en
- bij de politie aangifte doet van de identiteitsdiefstal.

We vergoeden ook de redelijke en noodzakelijke kosten voor **krediet- en identiteitmonitoring**.

- a. De schade is veroorzaakt door een **gedekte gebeurtenis**. Gedekte gebeurtenissen zijn:

- diefstal van geld van een (bank)rekening, en
- identiteitsdiefstal, en
- een cyberincident dat invloed heeft op de **verzekerde apparatuur**, en
- cyberafpersing.

- b. Op de dekking Hulp en advies door de Cyberwacht, kunt u ook een beroep doen als u alleen vermoedt dat er een gedekte gebeurtenis heeft plaatsgevonden of als u advies wilt over het voorkomen van schade.

- c. U heeft tijdens de looptijd van de verzekering ontdekt dat deze gedekte gebeurtenis heeft plaatsgevonden. U heeft de gedekte gebeurtenis tijdens de looptijd van de verzekering bij de Cyberwacht gemeld. Vindt de gedekte gebeurtenis plaats kort voor het einde van de looptijd? Dan heeft u ook dekking als u de gebeurtenis bij de Cyberwacht meldt binnen 72 uur na het moment waarop de polis eindigt.

Let op: wij vragen u een gedekte gebeurtenis altijd zo snel mogelijk te melden. Voor sommige dekkingen geldt dat u de gebeurtenis altijd binnen 72 uur moet melden bij de Cyberwacht en eventueel ook bij andere instanties, zoals beschreven bij de verschillende dekkingen.

- d. Toen u deze verzekering afsloot was niet zeker dat de gedekte gebeurtenis zou plaatsvinden. U wist of vermoedde ook niet dat de gebeurtenis al had plaatsgevonden.
- e. De schade is niet ontstaan door een van de oorzaken genoemd in hoofdstuk 6.
- f. U heeft de volgende beveiligingsmaatregelen genomen:
 - U gebruikt en onderhoudt de **verzekerde apparatuur** volgens de aanbevelingen van de producent en de leverancier;
 - U kunt aantonen dat u updates van het besturingssysteem en andere

Met deze verzekering bent u verzekerd voor:**Als bij het ontstaan van de schade aan de volgende voorwaarden is voldaan:****4. Dataherstel en verwijderen van malware**

U bent verzekerd voor hulp van de Cyberwacht bij dataherstel en het verwijderen van malware na een gedekt **cyberincident**. De Cyberwacht zal de redelijke en noodzakelijk stappen zetten om:

- uw **data** terug te zetten en/of
- malware te verwijderen van het getroffen verzekerde apparaat.

Deze activiteiten zijn er op gericht om de situatie zoals die was onmiddellijk voor het optreden van het cyberincident, zo dicht mogelijk te benaderen. Als de Cyberwacht het probleem niet kan oplossen, kunnen we er ook voor kiezen om hiervoor een andere IT specialist in te schakelen.

Let op: u moet minimaal eenmaal per 14 dagen een **back-up** maken van uw gegevens. Als de meest recente back-up op het moment van de schade ouder is dan 14 dagen, kunt u geen aanspraak maken op onze hulp om uw data te herstellen.

5. Vervanging van hardware

Na een gedekt cyberincident vergoeden wij de redelijke kosten voor het vervangen van uw getroffen verzekerde apparaat als de Cyberwacht of de IT specialist die door ons is ingeschakeld, oordeelt:

- dat het niet mogelijk is om de malware te verwijderen van het getroffen verzekerde apparaat of
- dat de kosten van het herstellen van de data en/of het verwijderen van de malware niet in een redelijke verhouding staan tot de kosten van het vervangen van (delen van) het getroffen verzekerde apparaat.

Het vervangende apparaat is een apparaat met dezelfde kwaliteit en technische specificaties als het apparaat dat vervangen wordt.

6. Hulp bij cyberafpersing

U bent verzekerd voor hulp van de Cyberwacht bij cyberafpersing. Ontvangt u een bericht waarin gedreigd wordt schade toe te brengen aan een verzekerd apparaat of aan de data op een verzekerd apparaat? En waarin gezegd wordt dat u dit kunt voorkomen door **losgeld** te betalen? Dan is er sprake van cyberafpersing. In geval van cyberafpersing zal de Cyberwacht of een andere door ons ingeschakelde specialist de redelijke en noodzakelijke stappen zetten om u te helpen de cyberafpersing te beëindigen. Wij vergoeden geen losgeld. Als wij dit vragen, moet u de cyberafpersing melden bij de politie of andere instanties.

beveiligingsupdates zo snel mogelijk en in elk geval binnen 14 dagen nadat deze beschikbaar komen, installeert.

- U kunt aantonen dat u passende beveiligingsmaatregelen heeft geïnstalleerd, zoals anti-virus **software**.
- U gebruikt wachtwoorden die niet gemakkelijk te raden zijn, en verandert uw wachtwoorden regelmatig.
- Laat de verzekerde apparatuur en uw gegevens nooit onbeheerd achter op een plaats waar onbevoegden mogelijk toegang kunnen verkrijgen tot uw apparatuur en/of gegevens.
- U maakt minimaal eenmaal per 14 dagen een back-up van uw data. Doet u dit niet? Dan kunt u geen aanspraak maken op onze hulp om uw data te herstellen.

4 Wat kunnen wij bij schade van elkaar verwachten?

Is er sprake van een gedekte schade of vermoedt u dat hier sprake van is? Dan moet u zo snel mogelijk de Cyberwacht bellen. Deze verplichting geldt in aanvulling op de verplichtingen bij schade die beschreven zijn in de polisvoorwaarden ZekerheidsPakket Particulieren.

Als de schade gedekt is, dan zetten wij – in overleg met u – de volgende stappen:

| Herstel | Herstel en vergoeding | Vergoeding |
|--|---|---|
| De Cyberwacht beoordeelt of er sprake is van een cyberincident of een andere gedekte gebeurtenis , en of de schade verzekerd is. In veel gevallen kan de Cyberwacht het probleem zelf oplossen, bijvoorbeeld door de data te herstellen of de malware te verwijderen van uw computer. Ook kunnen ze u adviseren wat u moet doen als er geld is gestolen van uw bankrekening of als er sprake is van identiteitsdiefstal . | In sommige gevallen schakelen wij andere specialisten in om u te helpen. Bijvoorbeeld een bedrijf dat gespecialiseerd is in krediet- en identiteitmonitoring . Wij betalen deze kosten tot een maximum. Hoe hoog het maximum is leest u in het volgende hoofdstuk. Als de specialist het probleem niet kan oplossen voor dit bedrag, bespreken we met u hoe we verder gaan. | Voor de dekkingen Diefstal van geld op (bank)rekening, Identiteitsdiefstal en Vervanging van hardware ontvangt u een vergoeding. Hoe hoog die vergoeding is, leest u in hoofdstuk 5. |

5 Wat krijgt u vergoed?

Op welke dekking doet u een beroep?

Wat krijgt u vergoed?

Hoe hoog is de maximale vergoeding?

Alle dekkingen samen

Totaal verzekerd bedrag

Voor alle dekkingen samen vergoeden wij maximaal € 5.000,- per gebeurtenis. € 5.000,- is ook het maximum dat wij vergoeden per verzekeringsjaar. De datum waarop een **gedekte gebeurtenis** (of de eerste gedekte gebeurtenis van een reeks gedekte gebeurtenissen) plaatsvond, bepaalt in welk verzekeringsjaar de gebeurtenis valt.

In de leeswijzer onder 'Wat krijgt u vergoed?' staat met een voorbeeld beschreven hoe dit in de praktijk werkt.

a. Cyberwacht

De dienstverlening door de Cyberwacht

De Cyberwacht helpt u bij een **cyberincident** of als u denkt dat er sprake is van een cyberincident. De Cyberwacht geeft ook advies over het voorkomen van cyberincidenten. Bijvoorbeeld hulp bij het installeren van een virusscanner en tips om **phishing** mails te herkennen.

De dienstverlening van de Cyberwacht is zonder maximum meeverzekerd. Deze dienstverlening telt dus niet mee in de maximale vergoeding van € 5.000,- per jaar en de maximale vergoeding voor de verschillende dekkingen.

b. Diefstal van geld van uw (bank)rekening

Het geld dat van uw rekening gestolen is.

Wij vergoeden het geld dat van uw rekening gestolen is en dat niet vergoed wordt door uw bank of **mobile wallet** bedrijf, voor zover dit verzekerd is volgens de dekkingsomschrijving in hoofdstuk 3.

Wij vergoeden per gebeurtenis maximaal € 5.000,-.

c. Identiteitsdiefstal

Geldelijk verlies en kosten van specialisten

Wij vergoeden de directe financiële schade die u lijdt en we betalen de kosten van de gespecialiseerde bedrijven die we kunnen inschakelen om u te helpen, voor zover dit verzekerd is volgens de dekkingsomschrijving in hoofdstuk 3

Wij vergoeden per gebeurtenis maximaal € 5.000,-.

| Op welke dekking doet u een beroep? | Wat krijgt u vergoed? | Hoe hoog is de maximale vergoeding? |
|--|---|---|
| d. Dataherstel en verwijderen van malware | De kosten van IT specialisten Bij een gedekte schade betalen wij de kosten van de gespecialiseerde bedrijven die we kunnen inschakelen om uw data te herstellen en de malware te verwijderen van uw apparaten. | Wij vergoeden per gebeurtenis maximaal € 2.000,- |
| e. Vervanging van hardware | De kosten voor het aanschaffen van een ander apparaat Bij een gedekte schade ontvangt u het bedrag dat nodig is om een apparaat te kunnen kopen dat gelijkwaardig is aan het apparaat dat onbruikbaar is geworden door het cyberincident . Daarbij gaat het om een exemplaar van dezelfde soort en met dezelfde kwaliteit en technische specificaties. | Wij vergoeden per gebeurtenis maximaal € 2.000,-. |
| f. Hulp bij cyberafpersing | De kosten van IT specialisten Bij een gedekte schade betalen wij de kosten van de gespecialiseerde bedrijven die we kunnen inschakelen om u te helpen. Bijvoorbeeld de kosten van onderzoek. | Wij vergoeden per gebeurtenis maximaal € 2.000,-. |
| Eigen risico Voor de Cyberservice geldt geen eigen risico. | | |

6 Uitsluitingen: wat is niet verzekerd?

In de volgende gevallen bent u niet verzekerd. Dit betekent dat u bij schade of diefstal geen vergoeding ontvangt en dat wij uw schade niet herstellen.

U bent niet verzekerd voor schade:

- a. als de **gedekte gebeurtenis** of de omstandigheden die hebben geleid tot de gedekte gebeurtenis bij u bekend waren of redelijkerwijs bij u bekend hadden kunnen zijn voor de ingangsdatum van de verzekering;
- b. die u met opzet of door roekeloosheid heeft veroorzaakt of verergerd;
- c. die verband houdt met:
 - een handelen of nalaten van u als werknemer of zelfstandig ondernemer en/of
 - professionele of bedrijfsmatige activiteiten;
- d. die verband houdt met atoomkernreacties of molest. Wat dat precies inhoudt, leest u in het hoofdstuk Uitsluitingen van de polisvoorwaarden ZPP;
- e. die bestaat uit verlies of diefstal van spullen of schade aan spullen of schade die hiervan het gevolg is. Bijvoorbeeld: uw laptop is gestolen en hierdoor raakt u belangrijke **data** kwijt;
- f. die bestaat uit verliezen in verband met beleggingen of handelstransacties. Bijvoorbeeld schade die ontstaat doordat u geen aandelen kunt kopen of verkopen;
- g. die bestaat uit letsel, psychische schade, trauma, ziekte of overlijden;
- h. die verband houdt met gokken.

We vergoeden niet:

- i. extra kosten voor verbetering van (de beveiliging van) smartphones, tablets, laptops en andere verzekerde apparaten. Er is sprake van verbetering als het apparaat in een betere staat verkeert dan op het moment direct voorafgaand aan de schade;
- j. het verlies van cryptocurrencies en andere virtuele valuta zoals bijvoorbeeld bitcoins, of enige andere schade die verband houdt met cryptocurrencies;
- k. schade die verband houdt met non-fungible tokens (NFT's).

7 Begrippenlijst

| | |
|---|---|
| Back-up | Een kopie van uw data die is opgeslagen buiten uw verzekerde apparaat. Bijvoorbeeld op een externe harde schijf of in de cloud. De gegevens zijn op zo'n manier opgeslagen dat de back-up gebruikt kan worden om uw data te herstellen na een gedekte gebeurtenis. |
| Cyberincident | Iedere kwaadaardige handeling of malware die zich voordoet op uw verzekerde apparatuur. |
| Data | Digitale informatie, op welke manier deze ook wordt gebruikt, opgeslagen of getoond. Bijvoorbeeld: teksten, cijfers, afbeeldingen, video's, opnamen of software. |
| Derde partij | Een persoon of rechtspersoon anders dan de in deze polisvoorwaarden genoemde verzekerden. |
| E-mail spoofing | Een vervalsing of een onrechtmatige manipulatie van een e-mail, waardoor de ontvanger ervan ten onrechte gelooft dat de e-mail echt is en de afzender vertrouwt. |
| Gedekte gebeurtenis | Gedekte gebeurtenissen zijn: <ul style="list-style-type: none"> • diefstal van geld van een (bank)rekening, en • identiteitsdiefstal, en • een cyberincident dat invloed heeft op de verzekerde apparatuur, en • cyberafpersing. Gedekte gebeurtenissen met dezelfde oorzaak gelden als één gebeurtenis. De datum waarop de eerste gedekte gebeurtenis plaatsvond bepaalt in welk verzekeringsjaar de gebeurtenis valt. Dit is van belang voor het vaststellen van de schadevergoeding, omdat we maximaal 5.000 euro per gebeurtenis en per verzekeringsjaar vergoeden. |
| Hardware | De fysieke componenten van verzekerde apparatuur die gebruikt wordt voor het opslaan, opnemen, verzenden, ontvangen, verwerken, lezen, aanpassen of monitoren van data. |
| Identiteitsdiefstal | De diefstal van persoonsgegevens via internet die leidt tot, of zou kunnen leiden tot, onrechtmatig gebruik van deze persoonsgegevens. |
| Krediet- en identiteitmonitoring | Het monitoren van financiële transacties en/of krediet status (bijvoorbeeld het Bureau Kredietregistratie) en/of ongebruikelijke activiteiten met uw persoonlijke gegevens in openbare informatie en op websites. |
| Kwaadaardige handeling | Een ongeautoriseerde of illegale handeling van een derde partij, bedoeld om via een computersysteem of computernetwerk (waaronder internet) <ul style="list-style-type: none"> • toegang te krijgen tot data op uw verzekerde apparatuur en/of • schade te veroorzaken aan data op uw verzekerde apparatuur en/of • data afkomstig van uw verzekerde apparatuur te openbaren. |

| | |
|--------------------------------|---|
| Losgeld | Geld, bitcoins of andere digitale valuta die door een derde partij geëist worden in het kader van cyberafpersing. |
| Malware | Ongeautoriseerde of illegale software die is ontworpen voor het toebrengen van schade aan, het toegang verkrijgen tot of het verstoren van verzekerde apparatuur of computernetwerken. Voorbeelden van malware zijn virussen, spyware, computer worms, trojan horses, rootkits, ransomware, keyloggers, dialers en rogue security software. |
| Mobile wallet | Een online account waarin u geld kunt opslaan of ontvangen in een specifieke munteenheid. Het gaat hierbij om geld dat in online of offline winkels uitgegeven kan worden. |
| Persoonsgegevens | Alle data die ervoor zorgt dat een persoon direct of indirect kan worden geïdentificeerd. Bijvoorbeeld een naam, adres, geboortedatum, nummer van een identiteitsbewijs, burgerservicenummer, locatiegegevens of online identificatiegegevens. |
| Phishing | Een poging om gevoelige informatie te verkrijgen door zich in elektronische communicatie voor te doen als een betrouwbare partij. Gevoelige informatie is bijvoorbeeld een gebruikersnaam, een wachtwoord of creditcardgegevens. |
| Software | Een standaard, gemodificeerd of speciaal ontwikkeld programma, of een applicatie die draait op de verzekerde apparatuur. |
| Totaal verzekerd bedrag | Het totaal verzekerd bedrag is het maximale bedrag dat wij vergoeden per schadegebeurtenis en per jaar voor alle dekkingen tezamen. Dit bedrag is het totaal van de bedragen die wij aan u betalen, en de bedragen die wij betalen aan specialisten die wij inschakelen om u te helpen. De kosten van de Cyberwacht vallen hier niet onder. |
| Verzekerde apparatuur | <p>Apparaten, uitsluitend voor privé gebruik, die dienen voor het creëren, benaderen, verwerken, monitoren, opslaan, ophalen, weergeven, verzenden of ontvangen van privé data. Deze apparaten zijn uw eigendom of door u geleased en staan onder uw directe controle.</p> <p>Onder verzekerde apparatuur verstaan we alleen:</p> <ul style="list-style-type: none"> • computerapparatuur en bijbehorende randapparatuur; • smartphones, tablets, laptops; • andere wearable devices. Dit zijn op het lichaam draagbare armbanden, horloges, brillen en kleding die tot doel hebben de gebruiker te voorzien van persoonlijke data en/of omgevingsdata. <p>Let op: smart home devices vallen hier niet onder. Smart home devices zijn apparaten of IoT componenten die verbonden zijn met en/of worden aangestuurd via het internet. Bijvoorbeeld camera's, airconditioning, verlichting of alarmsystemen.</p> |

Meer weten?

 **Neem contact op met uw verzekeringsadviseur**