Information about CyberHelp

CyberHelp is part of your household contents insurance

Contents

Steps to take when you experience a cyber incident

You suspect that your computer has been hacked, your computer is flooded with ransomware, your personal data has fallen into the wrong hands or your identity is used to take out a loan. It is important that you act fast when these kinds of cyber incidents occur, so that you can mitigate any problems.

The Cyber Hotline
You may not directly notice a cyber incident has taken place. But even if you have the slightest suspicion a cyber incident has occurred, you must directly call the Cyber Hotline. **You will not be charged for this.**

Call the Cyber Hotline 0800 0233 088.

An employee of the Cyber Hotline will help to determine what is wrong and help you to mitigate the consequences of a cyber incident.

Engaging a specialist
If the cyber incident is not solved after talking to an employee of the Cyber Hotline, you can engage a technical, legal or fraud specialist to solve the cyber incident.

Your insurance will cover this service. You will pay € 100 yourself. This is called the policy excess. Any costs above €100 will be reimbursed up to a maximum of € 5,000. The only exception to this is if you experience a ransomware event, in which case the costs of a specialist will be reimbursed up to a maximum of € 2,500. We will consult with you about engaging a specialist first, and the specialist will only be engaged if you agree to it. If the costs exceed the reimbursement you will get based on your insurance, the specialist will still be available to you. If this is the case, you will in due time receive an estimate of the expected costs that are above the reimbursement amount. If you choose to go ahead with the work that costs more than the reimbursement that you are entitled to under the policy you will have to pay these costs to the specialist yourself.

CyberHelp Knowledge Portal
You can make use of the CyberHelp Knowledge Portal at any time. Our knowledge portal contains tips and information about cyber crime and identity fraud. We will explain what cyber crime is and how you can protect yourself from it. You can visit the CyberHelp Knowledge Portal on aon.mycybercentre.com

Reader's guide

You have a household contents insurance with us. CyberHelp is included in your household contents insurance policy and it has its some of its own policy conditions. We will set out the most important sections of these conditions here.

This insurance may contain words in the field of cyber that are foreign to you. That is why all words in blue are explained in the glossary. This glossary can be found at the end of this document.

CyberHelp in brief

What is the function of CyberHelp?
This cover provides help if you experience a cyber incident and it and protects you from the financial implications of cyber incidents.

Your computer may have frozen because a hacker blocked it, or someone may be stealing your identity and is using it to buy items, or someone may be holding you accountable because their personal data was leaked because of you.

These situations are referred to as cyber incidents. With CyberHelp, assistance is available to you for four different types of cyber incidents: security incidents, breach of privacy, identity fraud and ransomware. An employee of the Cyber Hotline will investigate the incident and will help fix the incident as soon as possible.

Aside from offering help, CyberHelp will also reimburse the damage and the costs of the specialists that are used to help fix the problem. For every kind of cyber incident the conditions of the policy that are set out below carefully state which damage and costs that relate to specialists can be reimbursed.

A cyber incident will generally occur via your computer. An unauthorised party will hack into your computer system to implement malware or to steal data. A privacy breach or identity fraud can also occur without a computer. The data may be on paper or on another device like a USB stick. CyberHelp also covers these cyber incidents.

A computer system includes many more devices than you may think. Aside from your PC, laptop or tablet, your smartphone, smartwatch and games consoles are also

considered to be computer systems. Computer systems basically include all devices that can be connected to the internet.

Business activities are not covered, and neither is the data that is being used for business activities. Therefore, if you use your computer system in both private and business settings, you cannot make use of CyberHelp. You *can* make use of CyberHelp if you use your device for activities for local organisations that you are a part of or if you process data for a local organisation that you belong to.

What steps to take when incurring damage

- Call the Cyber Hotline immediately.
- Do everything within your power to prevent any further damage.
- Cooperate with everything that we do to settle the damage.

What does your insurance cover?

- You have access to the Cyber Hotline and the CyberHelp portal.
- The cost of the investigation into the possible cyber incident.
- The cost of engaging a specialist.
- The cost of recovering your computer system after a cyber incident.
- The damage to third parties you must pay as a result of a privacy breach.
- The cost to mitigate the consequences of identity fraud.

What does your insurance <u>not</u> cover?

- Damage arising from complying with a fraudster's request to transfer an amount of money into his bank account.
- Damage to the computer system itself.
- Fines.
- Bodily injury or mental anguish, illness or death of a person.
- Damage and costs that arise from not using the safety measures mentioned in the conditions.
- Damage and costs that arise from the malfunctioning of a different system than your own, like internet companies, telecom companies or utility companies.
- Damage and costs that arise from using the computer system for business or putting corporate data on your device.

What is reimbursed?
You will receive free help from a Cyber Hotline employee whenever you suspect a cyber incident has occurred. If an employee cannot solve the cyber incident, a specialist can be used. In that case, the compensation of the damage and costs varies per incident as mentioned in the policy conditions.

What do you have to pay?
If you only use the Cyber Hotline, you will not be charged at all. In all other cases you must pay € 100.00. This is called the policy excess.

Who is insured?
The insured persons are mentioned in the policy conditions of your household contents insurance. Usually this includes yourself and any other family members living with you.

You cannot derive any rights from this Reader's Guide. In the CyberHelp Terms and Conditions you can find exactly what your insurance covers, which services you can expect and what your rights and duties are. Read these CyberHelp Terms and Conditions carefully.

CyberHelp Terms and Conditions

2020-01

In case of doubt or discussion, the stipulations in the Dutch version shall apply.

The CyberHelp Terms and Conditions form one whole with the terms and conditions of the household contents insurance. If any disputes arise, the CyberHelp policy conditions apply.

Read the CyberHelp terms and conditions carefully. They set out what your rights and obligations are and what is insured and what is not insured.

Table of contents

1. Overview of cover

CyberHelp provides cover up to a maximum of the insured amounts which are listed in this overview of cover. The insurer does not reimburse more than the maximum insured amount of EUR 5,000.00 a year, for all joint damage and costs as mentioned in article 2.

1. Excess

You have an excess of	€ 100,-

2. The maximum insured amount per year is **€ 5.000,-**

Within the maximum insured amount

- lost wages (see 2.1.3) are maximised to	20 days and € 250 per day and €2,500.00 per year
- ransomware (see 2.1.4) is maximised to	€ 2,500 per year

3. The period of insurance

The validity of the CyberHelp conditions is equal to and inextricably linked to the validity of your household contents insurance.

4. Area of cover

The whole world, except claims from the USA and Canada.

Do you think you have a cyber incident?

Call the Cyber Hotline 0800 0233 088.

2. What is insured?

You are insured for the damage and costs as mentioned in this article. The cyber incident and the damage and costs arising from it must have taken place and must be reported to the cyber hotline during the period of insurance. Are you experiencing a cyber incident? Report this as soon as possible via the Cyber Hotline.

2.1.1 Damage due to a privacy breach.

A privacy breach is unauthorised access by someone who is not insured under this policy, the theft of loss of personal data that you privately process, possess or manage. This personal data can be on your computer system or on paper. The data subject of whom these personal data were leaked, can suffer harm because their personal data is now public. The data subjects may try to recover this damage from you.

> Imagine you are having a party, and you have written down the names and addresses of all guests. You then accidentally leave this list of guests on the train, which causes these data to fall into the hands of unauthorised parties.
>
> Even though your guests have not suffered any harm, you want to know what you can do to mitigate the consequences of this privacy breach. Should you inform your guests, and what is the best way to go about this? Do you have a legal duty to report this? A specialist will then give you advice on the best course of action.

The personal data must: (a) be in your direct care, custody or under your control, or (b) in the care, custody or under the control of a third party provider with which you have a written agreement, in which that party undertakes to pay for all damage and costs arising from a privacy breach.

The following is reimbursed:

- Costs of a computer specialist to investigate which personal data have been seen by an unauthorised person.
- Costs for a lawyer, who will advice you on the best course of action in case of a privacy breach;
- The lawyer's fees for the investigation and defence in the court cases that have been filed against you by the data subjects;
- Damage incurred by data subjects.

2.1.2 Damage caused by a security incident.

A security incident is understood to mean:

- The failure of existing technical or physical security measures on your computer system which has allowed unauthorised persons to gain access to your computer system;
- A Denial of Service attack (DoS attack);
- Physical theft or loss of your computer system, which enables unauthorised parties to gain unauthorised access to data;
- Transfer of malicious code from your computer system to the computer system of a third party, which may cause damage to that third party.

This must involve a security incident on your own computer system, which you do not use for business purposes.

Imagine that your computer was hacked, and your photos were stolen and are being used on websites you do not want them to be on. You want to make the computer inaccessible to the hacker as soon as possible. The insurer will engage an IT specialist that can help you with this.

Imagine that your computer is hacked and infected with malware, which causes your contacts to receive requests for the transfer of money in your name. You want to clear your computer of this malware as soon as possible, and you must warn your contacts. The IT specialist engaged by the insurer will help you with this. You will also be advised on the best course of action to warn your contacts.

Imagine that your phone is stolen from your bag, and despite having a strong password, an unauthorised party gains access to your data. A specialist engaged by the insurer can investigate to what data the thief has gained access and will inform you of the best course of action.

The following is reimbursed:

- Claims of third parties that you are obligated to pay
- Costs for the help of a specialist. In this case this entails an IT specialist that will help you determine whether a security incident has occurred.

If this is the case, the specialist will help you to recover the computer system to its original state, as far as possible;

- The lawyer's fees for the investigation and the defence in the court cases, that have been filed against you by third parties that have been harmed by the security incident;

Note: When the computer system is stolen, the damage to or the value of the stolen computer system is not reimbursed.

2.1.3 Damage arising from identity fraud

Identity fraud is understood to mean: an incident in which unauthorised parties abuse your personal data or identifying data. These identifying data may come from your computer system, paper, or other carriers.

Imagine that your son is happy that he finally got his driver's licence, and he took a photo and put that on social media. Criminals then use his identity to sign up for a telephone contract, but your son gets the bills. A fraud specialist will help you void these contracts and prove that your son did not sign up for them.

Imagine that you receive an invoice for items that you supposedly purchased on the internet. These items were not bought by you, but by someone that unlawfully used your identity. You must immediately call the Cyber Hotline, but the creditor is not very patient and sends you a summons. You will have to prove that you did not order anything, or else you will have to pay the bill. You will be assisted by a specialist with this. The costs of the proceedings will also be paid. It will also have to be investigated whether your identity has been used for other things. An IT specialist will investigate your computer systems and reinstall security measures. A specialist will take care of all official statements and messages to supervising authorities and financial institutions.

Imagine you want to board a flight, but customs stops you from flying because you supposedly have not yet paid several traffic fines. These violations were committed by someone who stole your identity and rented cars in your name. You and a specialist will need days to gather evidence that you did not commit these violations. Your employer will therefore grant you unpaid leave. The costs of the specialist and the lost wages will be included in the insured amount reimbursed by insurance.

The following is reimbursed:

A. The costs of documents
The necessary costs for notary declarations or similar documents to prove to supervising authorities, financial institutions, credit providing institutions or credit agencies that identity fraud has been committed.

B. Lawyer's fees
The lawyer's fees for:

- Investigating and defending in court cases that have been filed against you by persons or organisations that have issued a loan to a third party that fraudulently used your identity;

- Disputing the court rulings which unjustly allow a claim against you as a consequence of the fact that an unauthorised party fraudulently uses or has used you identity.

- Verifying the correctness or completeness of your BKR (Dutch Credit Registration Office) data as a result of the fraudulent use of your identity.

C. Lost wages
Lost wages up to a maximum of 20 days at a maximum of € 250 per day
and a maximum of € 2,500 per year.

D. Loan application costs
The costs involved in you reapplying for a loan when the original application was rejected by the credit provider on the basis of incorrect information as a result of the identity fraud.

E. Telephone expenses
The telephone expenses involved in reporting and discussing an identity fraud with companies, law enforcement agencies, financial institutions, credit providers, or credit reporting agencies;

F. Identity restoration costs
The costs incurred by a fraud specialist assisting you in restoring your identity. The fraud specialist will help you to restore the information registered with financial institutions, credit providers, credit registration organisations, collection agencies or government institutions to what it was shortly before the identity fraud, where possible.

It is your choice if you want help to restore your identity. If you do want help, you must

1. explain to the insurer that you were the victim of fraud, and
2. report the identity fraud to the police.

The reimbursements referred to at A through F are available for a maximum of 12 months after the date on which the identity fraud first occurred.

2.1.4 Ransomware support costs

Ransomware is understood to mean: Malicious coding which prevents you from using all or part of your computer system. You may not use your computer system for business purposes.

Your computer has been infected with ransomware which is preventing you from opening your documents. For example, you can no longer access your holiday photos, or you can no longer access your computer at all. You call the Cyber Hotline. An employee of the Cyber Hotline helps you to remove the ransomware from your computer so that you regain access to all of your data. If this is not possible the specialist will help you restore your data from the latest available back up.

The following is reimbursed:

When you are faced with ransomware on your computer system, you will receive support from a computer specialist who will try to remove the ransomware from your computer system and restore system functionality, so that you can regain access to your computer system. The support may be offered by telephone. If it is not possible to remove the ransomware and you have a back-up, the computer specialist can try to restore your computer system using the back-up. They will do so only with your permission.

2.2 Interconnected cyber incidents

If multiple incidents are interconnected, they will be treated as one cyber incident. One incident may be the result of another, or the incidents may have the same cause. For example, an identity fraud could occur because of a security incident. The date of the first cyber incident determines the cover.

3. What is not insured?

In some cases, you are not insured for the loss and costs incurred for specialists. These are referred to as exclusions.

Exclusions

3.1.1 Loss, theft or damage of your computer system.

3.1.2 Ransom.

3.1.3. Statutory or contractual fines, penalties or compensatory measures or payments.

3.1.4 Taxes.

3.1.5 Loss incurred by the following persons or legal entities:

a. Loss incurred by a legal entity of which you are (partial) owner or in which you have a participating interest;

b. Loss incurred by a legal entity where you work or for which you perform activities;

c. Claims between insured persons.

3.1.6 Damage or costs related to:

a) Non-compliance with the security measures referred to in article 5.2

b) Bodily injury or mental anguish, illness or death of a person;

c) Your bankruptcy or suspension of payments

d) Any contractual liability or obligation;

e) Infringement of any copyright, trademark, patent or other intellectual property right, or infringement, publication or misuse of any trade secret;

f) Trade losses, trade obligations or changes in the value of accounts, any loss, transfer or theft of cash and cash equivalents or movable property of others which have been entrusted to your care, custody or control;

g) Theft, loss, damage or depreciation of cash and cash equivalents including e-currency (such as bitcoins), securities or investments;

h) A fraudulent instruction to a financial institution to transfer cash and cash equivalents from your account (money transfer fraud);

i) Social engineering fraud;

j) Intent, fraud, gross negligence or deliberate recklessness by you or a co-insured person, either or not as part of a group.

p) The laws applicable in the USA/Canada.

3.1.7 Damage or costs incurred as a result of an actual or perceived failure, interruption or disconnection of:

- mains services;
- telecommunication;

- other infrastructure supported by the internet. For example, services of your internet provider that manage your website or internet access.

3.1.8 Damage or costs relating to:

a. Fire, smoke, explosions, electromagnetic fields, lightning, wind, flooding, surface water, earthquakes, volcanic eruptions, tidal waves, landslides, hail, other natural disasters or any other physical incident, howsoever caused;
b. Overvoltage or induction;
c. the use of location-based services or location-based data, such as GPS and location-based applications or media;
d. Damage or costs relating to Conflict Situations;
e. Terrorism.

3.1.9 Damage or costs that are covered under another insurance, or would be covered if this insurance did not exist.

3.2.1 Damage and costs incurred as a result of a cyber incident that was already known or reasonably foreseeable on commencement of the insurance.

3.2.2 Business use of your computer system or business data stored on your computer system.

4. Who pays what?

If you believe that a cyber incident has occurred and you call the Cyber Hotline, the costs for the employee who provides support will be fully reimbursed by the insurer. There is no excess and the costs incurred for this service will not be included in the calculation of the total reimbursements per year. The maximum insured amount is irrelevant in this case; you may call as often as you want.

If the Cyber Hotline employee cannot resolve your cyber incident, they may engage a specialist. Before engaging a specialist, the insurer will inform you of the activities and the costs. The activities will be performed only if you permit them.

In the case where a specialist is used, there is an excess. You will be charged for the activities by the specialist. The insurer will then pay the costs exceeding the excess to the specialist up to the maximum insured amount and periods referred to in the CyberHelp overview of cover.

If the costs are expected to exceed the insured amount, the insurer will point this out in due time. You will also be told how high these costs are expected to be. You may then choose whether you would still like to make use of the specialist if the insurer no longer covers the costs. Should you wish to continue making use of the specialist, you will have to make your own arrangements with the specialist and pay them directly.

5. What are your obligations?

5.1
In the event of a cyber incident, you must:

- Report it as soon as possible to the Cyber Hotline;
- Provide all information about what happened and all information that may be necessary to assess your cyber incident ;
- Cooperate fully with the handling of the claim and the recovery of the loss from the person responsible, and refrain from any actions that may harm the interests of the insurer;
- Not acknowledge any liability, make any payments, take on any obligations, incur any costs or come to a settlement without the insurer's consent.

5.2

You must comply with the following security measures:

- Change the computer system supplier's standard, pre-set or supplied password immediately;
- Use a strong password or another strong security protocol, such as a fingerprint, to secure access to any device that can be connected to the internet. This obligation applies only in so far as the device allows you to set a strong password or another security protocol;
- Do not share your passwords with others and do not store them near your computer;
- Use reasonable security solutions: Install antivirus and antispyware software and firewalls on PCs and laptops, and update these as soon as an update becomes available, store and send data securely;
- Do not use a computer system with a jailbreak. The installation of a jailbreak bypasses the system security of the computer system built in by the manufacturer;
- Never leave your computer system unattended in a public space;
- Do not use your computer system for the peer-to-peer sharing of files;
- If you use a smartphone or tablet computer for banking affairs, you must use the mobile banking application of your bank or financial institution. Do not use the web interface of your bank, for example.

5.3

You agree to the use of a computer specialist who has been engaged by the insurer. You may also hire your own computer specialist, but only with the insurer's written permission.

5.4

You agree that the insurer will engage an attorney on your behalf to conduct the defence in any legal actions brought against you, if the costs do not exceed the cover and the insured amount.

5.5

You agree that the insurer may directly settle claims with third parties and pay them to those third parties on your behalf, if the claim does not exceed the cover and the insured amount.

5.6

If you fail to comply with any of the obligations referred to above (5.1 through 5.5), the insurer may refuse or reduce a payment.

6. List of definitions

Below you will find an explanation of the terms used in this document.

Cash and cash equivalents
Cash or securities.

Computer specialist
A computer expert who helps determine whether there has been a security incident and helps to restore the computer system as much as possible to its state before the incident.

Computer system
Any device that you own as a private individual, including the data stored thereon, used exclusively for private purposes, that can be connected to the internet and that you control.

Computer systems include: computers, smartphones, tablets, software or firmware, laptops, storage media such as external hard drives and USB drives, Internet of Things (IoT) devices, smartwatches, private cars, game consoles and multimedia devices.

Computer systems do not include devices that have been implanted or injected into a person.

Conflict situations
Armed or cyber conflict: when states or organized parties fight each other (or one, the other) with weapons, cyber assets, or military assets. This includes the armed action of a United Nations Peace Force;
• Civil war: a violent struggle between several inhabitants of the same state;
• Revolt: organized violent resistance within a state, directed against the public authorities;
• Domestic disturbances: organized violent acts in various places within a state;
• Riot: an organized local violent movement against public authorities;
• Mutiny: an organized violent movement of members of an armed force against public authorities.

Control
You control a computer system if you are the only person with access to it and unauthorised parties can only access it by illegal means.

Credit registration details
Your credit details, such as personal loans, repayment schemes and payment arrears as recorded by the Dutch credit registration office Stichting Bureau Krediet Registratie.

Cyber incident
A cyber incident may refer to a privacy breach, security incident or identity fraud.

Damage
Pure financial loss from third parties

Data subjects
Individuals whose personal data have fallen into the hands of an unauthorised individual.

Denial of Service attack (DoS attack)
Denial-of-service attacks (DoS-attack) and distributed-denial-of-service attacks (DDoS-attack) are deliberate and malicious attempts to block or hamper access to a computer system.

It is possible that unauthorised parties use such attacks in order to block access to your computer system. Or it could be a deliberate and malicious attack using your computer system in order to block access to another person's computer system.

Fraudulent instruction
An instruction given by an unauthorised party in your name, but which you did not consent or instruct;

Or a written instruction of yours that was forged or changed by an unauthorised party without your knowledge or consent.

Fraud specialist
A specialist who helps to recover information about you, as registered just before your personal data was misused, from agencies such as credit reporting agencies, lenders, debt collection agencies, and government agencies.

Identity fraud
The use of your identity by an unauthorised party, without your consent or without being allowed by law or on the basis of a court ruling.

Interconnected incidents
Incidents with the same cause or where an incident is the result of a previous incident.

Insurer
The insurer(s) of your household contents insurance policy.

Jailbreak
Performing a jailbreak bypasses the manufacturer's built-in security safeguards of the equipment, which, for example, also allows software to be installed on phones outside app stores. A computer system on which a jailbreak was performed is vulnerable for cyber incidents.

Lawsuit
A civil lawsuit as a consequence of a cyber incident.

Loss
Pure financial loss of third parties

Lost wages
Wages from employment which you missed out on in connection with identity fraud, because you had to take unpaid leave in order to deal with the identity fraud. For example in order to consult with your lawyer, law enforcement agencies, credit reporting agencies, or in order to make statements about the identity fraud.

Malicious code
Malicious code is a software programme, code or script intended to infect, damage or steal a computer system or data. Examples include: A virus, a Trojan horse and a computer worm.

Money
Coins and bank notes that are in circulation and that have a face value, money orders, bank cheques, personal cheques and traveller's cheques, e-currency such as bitcoins.

Peer to Peer
In a peer-to-peer network computer systems are directly linked and referred to as peers. Between these peers, files can be shared directly without the need for a central server, for example via Bluetooth.

Period of insurance
The period as indicated on the CyberHelp Overview of Cover, as included in clause 1.

Personal Data
All data relating to a natural person, such as residential address, e-mail, passport number and medical information.

Privacy breach
Privacy breach is the unauthorised access of personal data or the theft or loss of personal data by a person who is not insured under this policy, which you process, own or manage as a private individual.

Privacy legislation
All laws and regulations relating to the control, use or protection of personal data.

Private car
A passenger car you own or that you lease for private use.

Ransomware
Any type of malicious encryption that is used to lock down a computer system or network in order to restrict or fully block access, after which in many cases a ransom is demanded, promising to lift the lock-down after payment of the ransom.

Securities
Marketable or non-marketable securities.

Security incident
- The failure of existing technical or physical security measures on your computer system which has allowed unauthorised persons to gain access to your computer system;
- A Denial of Service attack (DoS attack);
- Physical theft or loss of your computer system, which has allowed unauthorised parties to gain unauthorised access to data;
- Transfer of malicious code from your computer system to the computer system of a third party, which may cause damage.

Social engineering fraud
In social engineering, criminals abuse human characteristics, such as curiousness, trust, greed, fear and ignorance in order to mislead people, often by first collecting personal information via the internet. This is done with the purpose of fraudulently convincing somebody by e-mail, SMS, instant messaging or telephone to transfer money or bring about the transfer of money.

Specialist
Technical, legal or fraud expert , who assists you in solving the cyber incident.

Strong password
A password of at least 8 characters, containing at least one capital letter, one lower-case letter, one figure and one other symbol.

Third party or third parties

- Legal entity
- Person not insured by this policy

Third Party Provider

A legal entity that you have a written contract with for them to provide you with IT services including cloud providers, hosting and data storage services

Unauthorised Party

Anyone who you do not want to access your computer system or personal data that is under your direct care, custody or under your control, or (b) in the care, custody or under the control of a third party provider

You, your or insured person
The words 'you', 'your' or 'insured person' mean the insured person/persons as mentioned on your household contents insurance policy.