Cyberassurance

Informations sur le produit et guide de prévention

Informations sur le produit

Description

Internet et les médias électroniques sont devenus nos compagnons quotidiens. Les risques que comporte la numérisation sont par conséquent importants. Qu'il s'agisse de l'utilisation abusive d'une carte de crédit ou de données, de l'infection d'un appareil électronique par un maliciel, de la perte de données ou de cybermobbing, la cyberassurance vous offre une couverture moderne et optimale. La couverture d'assurance prend effet à la date indiquée dans le contrat d'assurance, au plus tôt toutefois lors du paiement de la prime, et prend fin sans résiliation à la date mentionnée dans le contrat d'assurance.

Avantages

- → **Aide rapide et professionnelle**
  Vous pouvez déclarer très simplement un sinistre par téléphone et 24h/24 en ligne. La Bâloise veille immédiatement au traitement du sinistre en faisant appel à des spécialistes.
- → **Contrat transparent**
  La cyberassurance a une durée fixe et ne se prolonge pas automatiquement. Cela vous permet de fixer vous-même la durée du contrat.
- → **Protection complète et sur mesure**
  Qu'il s'agisse de l'utilisation abusive d'une carte de crédit ou de données, de maliciels ou de cyberharcèlement, l'étendue des prestations de la cyberassurance va bien au-delà des couvertures traditionnelles grâce aux deux modules «Safe Pay» et «Safe Surf».
- → **Conclusion simple**
  Vous pouvez vous assurer à tout moment et en quelques clics seulement. Il vous suffit de choisir entre une assurance individuelle ou familiale, de nous indiquer la durée et le module que vous souhaitez et de mentionner vos coordonnées. Le paiement se fait par carte de crédit ou PayPal.

Étendue des prestations

Safe Pay

Événements assurés	Couverture
Utilisation abusive de cartes	✔
Utilisation abusive de données	✔
Erreurs de livraison suite à des commandes en ligne	✔

Safe Surf

Événements assurés	Couverture
Infection par un maliciel	✔
Pertes de données	✔
Atteinte à la personnalité	✔

Exemples de sinistres et de prestations

Utilisation abusive de cartes: votre carte de crédit est volée et l'auteur du vol retire de l'argent à un distributeur.
Prestations: frais découlant de l'exercice des droits contre les auteurs et indemnisation du dommage économique résultant de l'utilisation abusive de la carte.

Utilisation abusive de données: vous êtes victime de phishing. Une personne réussit à accéder à votre compte bancaire en ligne et transfère de l'argent sur son compte.
Prestations: indemnisation du dommage économique lié à l'utilisation abusive de données.

Erreurs de livraison suite à des commandes en ligne: dans une boutique en ligne, vous commandez un nouveau smartphone et recevez un téléphone endommagé.
Prestations: frais de réparation du produit ou, en cas de dommage total, frais d'une nouvelle acquisition.

Infection par un maliciel: votre ordinateur portable est infecté par un cheval de Troie.
Prestations: frais de suppression du maliciel et, si nécessaire, frais relatifs à la restauration du système d'exploitation.

Perte de données: votre smartphone tombe par terre et vous ne pouvez plus accéder à vos photos.
Prestations: frais de récupération des données.

Atteinte à la personnalité: un groupe d'écoliers met des photos de votre fille sur Internet.
Prestations: frais découlant de l'exercice des droits de suppression des photos et, si besoin, frais d'un soutien psychologique ou d'un déménagement dans un autre lieu de domicile en Suisse.

Franchise

En cas de sinistre, une franchise de 50 CHF est prélevée.

Notification en cas de sinistre

La Bâloise doit être immédiatement informée en appelant le +41 58 285 97 89.

Guide de prévention

Si vous tenez compte des dix recommandations de sécurité suivantes, vous pouvez renforcer sensiblement votre sécurité lors de l'utilisation de votre ordinateur ou smartphone.

Recommandation n° 1: antivirus

Utilisez un outil de recherche de maliciels et mettez-le à jour régulièrement. Également appelés logiciels malveillants, les maliciels sont des programmes conçus pour nuire aux utilisateurs. On distingue de nombreuses catégories de maliciels: p. ex. virus, chevaux de Troie, rootkits, rançongiciels ou logiciels espions. Ces programmes malveillants partagent un même objectif: vous nuire.

Informations complémentaires:
Réalisez régulièrement une analyse complète pour rechercher la présence éventuelle de virus. Pour économiser les ressources du système, les antivirus vérifient uniquement les fichiers utilisés par l'ordinateur lors de l'analyse. En cas de vérification complète du système lancée manuellement, c'est tout le contenu de votre disque dur qui est analysé pour y détecter la présence éventuelle de maliciels.

Recommandation n° 2: pare-feu

Utilisez ou activez un pare-feu. Ce programme vous protège contre les attaques extérieures en surveillant le trafic des données et en autorisant uniquement des connexions connues ou permises. Les dernières versions de Windows comportent un pare-feu intégré.

Informations complémentaires:
De nombreux outils de recherche de maliciels proposent ce que l'on appelle des «suites», qui comprennent souvent des pare-feu. Il est essentiel qu'ils soient activés.

Recommandation n° 3: système d'exploitation

Installez rapidement les mises à jour d'exploitation et de sécurité régulières de votre système d'exploitation. Ces correctifs permettent de corriger des failles de sécurité connues dans le système d'exploitation, ce qui améliore la sécurité des paiements en ligne.

Informations complémentaires:
Les systèmes d'exploitation et programmes pour ordinateur et smartphone ne sont pas tous sans faille. Les concepteurs des maliciels tirent souvent parti des failles pour accéder à votre ordinateur ou smart-

phone. Ainsi, un fichier PDF en apparence anodin peut créer d'autres failles dans un système non mis à jour ou charger d'autres maliciels. Grâce aux mises à jour, ces risques sont réduits au minimum.

Recommandation n° 4: mot de passe
Le mot de passe est un élément de sécurité essentiel pour chaque service en ligne, par exemple lorsque vous faites des achats ou des opérations bancaires en ligne. N'écrivez jamais votre mot de passe. Utilisez si possible un mot de passe long (huit caractères minimum), ne figurant dans aucun dictionnaire et composé de caractères différents (majuscules, minuscules, caractères spéciaux et chiffres).

Informations complémentaires:
Un mot de passe fort étant difficile à mémoriser, vous pouvez utiliser l'astuce suivante: pensez à une phrase et utilisez l'initiale de chaque mot pour créer le mot de passe correspondant. Ainsi, la phrase «Ma maîtresse de 1re année s'appelait Mme Robin!» donne le mot de passe «Mmd1asaMR!». N'utilisez jamais le même mot de passe pour plusieurs services en ligne et changez régulièrement les mots de passe.

Recommandation n° 5: données d'accès
Conservez vos données d'accès en lieu sûr et ne les communiquez jamais à des tiers. Aucun prestataire en ligne sérieux (p. ex. boutique ou banque) ne vous demandera vos données d'accès complètes par téléphone ou e-mail.

Recommandation n° 6: accès WLAN
Si vous utilisez chez vous un réseau Wi-Fi (WLAN), vous devez dans tous les cas crypter la connexion à ce réseau. En cas d'accès non protégé, non seulement vous accroissez le risque de subir des attaques de pirates informatiques, mais vous offrez à toutes les personnes à proximité la possibilité de surfer gratuitement sur Internet. Vous devez donc activer le cryptage WPA2 au niveau de votre routeur WLAN. Utilisez un mot de passe aussi fort que possible pour ce cryptage.

Informations complémentaires:
Faites toujours preuve de prudence lorsque vous vous connectez à des réseaux WLAN gratuits. Les escrocs s'y connectent volontiers et les utilisent parfois uniquement pour espionner, naturellement sans y être autorisés, les données des appareils non protégés. N'effectuez jamais d'opérations bancaires sur des réseaux WLAN gratuits ou publics par le biais de connexions Internet non sécurisées. Il en va de même pour les cybercafés.

Recommandation n° 7: navigateur sécurisé
Vérifiez que votre navigateur est à jour. Vous pouvez également augmenter les paramètres de sécurité de votre navigateur. Vous devez ici désactiver ActiveX pendant les opérations d'e-banking. N'oubliez jamais de vous déconnecter dans les règles en cliquant sur le bouton correspondant («déconnexion» ou «log-out») lorsque vous quittez le service en ligne. Encore mieux: videz le cache de votre navigateur.

Informations complémentaires:
Il est plus simple d'utiliser des navigateurs sécurisés, p. ex. «NowProtected», pour effectuer des opérations sensibles (e-banking, achats en ligne). Ces services en ligne protègent toute la communication entre votre appareil et le serveur du service en ligne, depuis la connexion jusqu'à la déconnexion. Ils sont synonymes de sécurité, quel que soit l'appareil utilisé pour vous connecter au service concerné: ordinateur portable, smartphone, tablette, PC ou ordinateur public d'un hôtel.

Recommandation n° 8: navigation sécurisée
Dans la mesure du possible, assurez-vous que les liens que vous utilisez vous donnent réellement accès à la page Internet souhaitée. Soyez très prudent lorsque vous effectuez des opérations sensibles en ligne (p. ex. e-banking): n'affichez jamais ces pages Internet à l'aide d'un lien envoyé dans un e-mail. N'ouvrez aucune pièce jointe et ne cliquez pas aveuglément sur les liens se trouvant dans les e-mails de personnes que vous ne connaissez pas. Ces pièces jointes comportent souvent des maliciels, ou les liens peuvent vous faire afficher des pages Internet dangereuses cherchant à installer ces maliciels sur votre ordinateur.

Recommandation n° 9: backup
Une défaillance du matériel, une cyberattaque ou un vol d'ordinateur peut entraîner la perte d'archives numériques irremplaçables. Il est par conséquent important de sauvegarder régulièrement vos données ou des parties importantes de ces données, en les copiant sur un autre support, p. ex. un disque dur externe, une clé USB, etc. Prenez les mesures préventives à temps et sauvegardez régulièrement vos fichiers importants.

Recommandation n° 10: faites preuve de bon sens
Lorsque vous surfez et effectuez des opérations sensibles sur Internet, faites toujours preuve de bon sens.

Bâloise Assurance SA
Aeschengraben 21, case postale
CH-4002 Basel
Service clientèle 00800 24 800 800
serviceclientele@baloise.ch

www.baloise.ch

140.1286-1f 1.18 pdf