baloisedirect
Cyber-Versicherung

Produktinformation & Präventive Guidelines

Produktinformation

Beschreibung

Das Internet und elektronische Medien sind mittlerweile unsere täglichen Begleiter. Entsprechend gross sind die Risiken, welche die Digitalisierung bringt. Ob Kreditkarten- oder Datenmissbrauch, Infizierung eines elektronischen Gerätes mit Schadsoftware, Datenverlust oder Cyber-Mobbing - die Cyber-Versicherung der baloisedirect bietet Ihnen einen modernen und optimalen Schutz. Ihr Versicherungsschutz beginnt an dem im Versicherungsvertrag genannten Datum, frühestens jedoch mit Bezahlung der Prämie und endet ohne Kündigung an dem im Versicherungsvertrag aufgeführten Datum.

Vorteile

- Schnelle und professionelle Hilfe
  Schadenereignisse können Sie ganz einfach telefonisch und rund um die Uhr online melden. Die baloisedirect sorgt unverzüglich für eine Schadenregulierung durch Spezialisten.
- Transparenter Vertrag
  Die Cyber-Versicherung der baloisedirect hat eine feste Laufzeit und verlängert sich nicht automatisch. Auf diesem Wege können Sie die Vertragsdauer selber bestimmen.
- Kompletter und massgeschneiderter Schutz
  Egal ob Kreditkarten- oder Datenmissbrauch, Schadsoftware oder Cyber-Mobbing - durch die zwei Module «Safe Pay» und «Safe Surf» geht der Leistungsumfang der baloisedirect Cyber-Versicherung weit über traditionelle Deckungen hinaus.
- Einfacher Abschluss
  Sie können sich jederzeit und mit nur wenigen Klicks versichern. Sie müssen lediglich zwischen Familien- oder Einzelversicherung wählen, uns die gewünschte Laufzeit und Ihr gewünschtes Modul nennen sowie Ihre Kontaktinformationen angeben. Die Zahlung erfolgt via Kreditkarte oder Paypal.

Leistungsumfang

Safe Pay

Versicherte Ereignisse	Schutz
Kartenmissbrauch	✔
Datenmissbrauch	✔
Fehllieferungen bei Online-Bestellungen	✔

Safe Surf

Versicherte Ereignisse	Schutz
Infizierung mit Schadsoftware	✔
Datenverlust	✔
Persönlichkeitsverletzung	✔

Schaden- und Leistungsbeispiele

Kartenmissbrauch: Ihre Kreditkarte wird gestohlen und der Täter bezieht damit Geld am Automaten.
Leistungen: Kosten für die Durchsetzung von Ansprüchen gegen die Täter und Ersatz des Vermögensschadens aus dem Kartenmissbrauch.

Datenmissbrauch: Jemand verschafft sich via Phishing Zugang zu Ihrem e-Banking-Konto und überweist sich Geld auf sein Konto.
Leistungen: Ersatz der Vermögensschäden aus dem Datenmissbrauch.

Fehllieferung bei Online-Bestellungen: Sie bestellen in einem online Shop ein neues Smartphone und erhalten ein beschädigtes Telefon.
Leistungen: Kosten für die Reparatur der Ware oder im Totalschadenfall die Kosten einer Neubeschaffung.

Infizierung mit Schadsoftware: Ihr Laptop wird mit einem Trojaner infiziert.
Leistungen: Kosten für die Entfernung der Schadsoftware sowie, falls notwendig, die Wiederherstellung des Betriebssystem.

Datenverlust: Ihr Smartphone fällt zu Boden und Sie können nicht mehr auf Ihre Fotos zugreifen.
Leistungen: Kosten für die Datenrettung.

Persönlichkeitsverletzung: Eine Gruppe von Schülern verbreitet Fotos Ihrer Tochter im Netz.
Leistungen: Kosten der Durchsetzung von Ansprüchen auf Löschung der Fotos sowie bei Bedarf psychologische Betreuung oder Umzug an einen anderen Wohnort innerhalb der Schweiz.

Selbstbehalt
Im Schadenfall wird ein Selbstbehalt von CHF 50 erhoben.

Benachrichtigung im Schadenfall
Die baloisedirect ist sofort unter 0041 58 285 97 89 zu benachrichtigen.

Präventive Guidelines

Wenn Sie diese zehn Sicherheits-Empfehlungen berücksichtigen, dann können Sie die Sicherheit beim Gebrauch Ihres Computers oder Smartphones deutlich erhöhen.

Empfehlung Nr. 1: Antiviren-Software
Setzen Sie einen Schadsoftware-Scanner ein und halten Sie diesen immer aktuell.
Schadsoftware ist ein Sammelbegriff für Programme, die dazu entwickelt wurden, Benutzern Schaden zuzufügen. Es gibt zahlreiche Unterarten von Schadsoftware – z.B. Viren, Trojaner, Rootkits, Ransomware oder Spyware. Sie haben ein Ziel gemein: Ihnen zu schaden.

Zusatzinformationen:
Führen Sie regelmässig vollständige Virenscans durch. Um Systemressourcen zu sparen, prüfen Virenscanner jeweils nur Dateien, auf die gerade zugegriffen wird. Mit einer manuell gestarteten vollständigen Systemprüfung wird Ihre gesamte Festplatte nach Schädlingen durchsucht.

Empfehlung Nr. 2: Firewall
Aktivieren Sie oder setzen Sie eine Software-Firewall ein.
Ein Firewall-Programm schützt gegen Angriffe von aussen, indem es den Datenverkehr überwacht und nur bekannte oder erlaubte Verbindungen zulässt. Neuere Windows-Versionen haben eine integrierte Firewall.

Zusatzinformationen:
Viele Schadsoftware-Scanner bieten sogenannte «Suiten» an. Diese enthalten oft auch Software-Firewalls. Wichtig ist, dass diese aktiviert sind.

Empfehlung Nr. 3: Betriebssystem
Installieren Sie zeitnah die regelmässigen Service- und Sicherheitsupdates zu Ihrem Betriebssystem. Mit diesen «Patches» werden bekannte Fehler und Lücken im Betriebssystem geschlossen und somit die Sicherheit beim Online-Zahlungsverkehr erhöht.

Zusatzinformationen:
Nicht sämtliche Betriebssysteme und Programme für Computer oder Smartphones sind fehlerfrei. Die Autoren von Schadsoftware nutzen sehr oft diese Lücken, um in den Computer oder Smartphone einzudringen. Zum Beispiel kann ein unscheinbares PDF-Dokument weitere Lücken in ein nicht aktualisiertes System reissen oder weitere Schadsoftware nachladen. Mit Updates werden diese Risiken minimiert.

Empfehlung Nr. 4: Passwort
Das Passwort ist ein essentielles Sicherheitselemente bei jedem Online-Dienst, wie z.B. e-Shopping oder e-Banking. Schreiben Sie niemals Ihr Passwort auf und verwenden Sie ein möglichst langes Kennwort (mindestens 8 Zeichen) das sich in keinem Wörterbuch befindet und sich aus unterschiedlichen Zeichen (Gross-/Kleinschreibung, Sonderzeichen und Zahlen) zusammensetzt.

Zusatzinformationen:
Da ein starkes Passwort schwer zu merken ist, können Sie folgenden Ansatz verfolgen: Überlegen Sie sich einen Satz und verwenden Sie dann die Anfangsbuchstaben von jedem Wort für die Bildung eines Passworts: Aus «Meine Lehrerin in der 1. Klasse hiess Frau Peter!» wird dann «MLid1.KhFP!». Verwenden Sie nie das gleiche Passwort bei mehreren Online-Diensten und
ändern Sie die Passwörter regelmässig.

Empfehlung Nr. 5: Zugangsdaten
Bewahren Sie Ihre Zugangsdaten an einem sicheren Ort auf und geben Sie diese niemals weiter. Kein seriöser Online-Dienstleister (z.B. Shop oder Bank) wird Sie per e-Mail oder Telefon darum bitten, Ihre vollständigen Zugangsdaten mitzuteilen.

Empfehlung Nr. 6: WLAN-Zugang
Wenn Sie zuhause ein WLAN-Netzwerk verwenden, dann sollten Sie den Zugang zu diesem auf jeden Fall verschlüsseln. Bei einem ungeschützten WLAN-Zugang erhöhen Sie nicht nur das Risiko von Hacker-Angriffen, sondern bieten auch allen Personen in der näheren Umgebung die Möglichkeit, «gratis» im Internet zu surfen.
Aktivieren Sie deshalb bei Ihrem WLAN-Router die WPA2-Verschlüsselung und verwenden Sie hier ein möglichst starkes Verschlüsselungs-Passwort.

Empfehlung Nr. 7: Vorsicht bei Gratis-WLAN
Seien Sie immer vorsichtig beim Surfen in Gratis-WLAN-Netzwerken. Diese werden von Betrügern gerne «angezapft» und manchmal auch nur betrieben, um unerlaubt Daten der nicht geschützten Geräte abzuhorchen.
Online-Bankgeschäfte sollten nie mit einer ungesicherten Internetverbindung in offenen Netzen oder Gratis-WLAN-Netzen durchgeführt werden. Gleiches gilt für Internet-Cafés.

Empfehlung Nr. 8: Sicherer Browser
Stellen Sie sicher, dass Ihr Browser auf dem aktuellen Stand ist.
Zusätzlich können Sie die Sicherheitseinstellungen für Ihren Browser erhöhen. Dazu gehört die Ausschaltung von ActiveX während des e-Bankings.
Vergessen Sie nie, sich «abzumelden», also den «Logout»- oder «Abmelden»-Button zu drücken, wenn Sie Ihren Online-Dienst verlassen. Oder noch besser: Leeren Sie den Cache Ihres Browsers.

Zusatzinformationen:
Einfacher ist es, wenn Sie für heikle Internetgeschäfte (eBanking, eShopping etc.) sichere Browser wie z.B. «nowprotected» nutzen. Diese Online-Dienste schützen die komplette Kommunikation zwischen Ihrem Gerät und dem Server des Online-Dienstes von der Anmeldung bis zur Abmeldung. Sie garantieren zudem Sicherheit, unabhängig von welchem Gerät Sie sich mit dem entsprechenden Dienst verbinden: Laptop, Smart-Phone, Tablet, Festcomputer oder einem öffentlichen PC in einem Hotel.

Empfehlung Nr. 9: Sicheres Surfen
Wann immer möglich, überprüfen Sie, ob Ihnen zugestellte Links, auch tatsächlich auf die gewünschte Internetseite führen. Besondere Vorsicht ist bei sensiblen Internetgeschäften (z.B. e-Banking) geboten: Rufen Sie nie die jeweilige Zugangsseite via einem Ihnen per E-Mail zugestellten Link auf.
Öffnen Sie keine Anhänge und klicken Sie nicht unbedarft auf Links in E-Mails von Personen, die Sie nicht kennen. Oft verbirgt sich in diesen Anhängen Schadsoftware, oder Links könnten Sie auf gefährliche Internet-Seiten führen, die solche Schadsoftware auf Ihrem Computer zu installieren versuchen.

Empfehlung Nr. 10: Gesunder Menschenverstand
Lassen Sie beim Surfen und bei sensitiven Internetgeschäften immer den gesunden Menschenverstand walten.

Basler Versicherung AG
Aeschengraben 21, Postfach
CH-4002 Basel

Kundenservice 00800 24 800 800
baloisedirect@baloise.ch
www.baloisedirect.ch