# Assicurazione cyber

**Informazioni sul prodotto e linee guida preventive**

# Informazioni sul prodotto

## Descrizione

Oggigiorno non possiamo fare a meno di Internet e dei mezzi elettronici. Ma la digitalizzazione implica rischi notevoli. Che si tratti di uso illecito delle carte di credito o dei dati, l'infezione di dispositivi elettronici per mezzo di malware, la perdita di dati o il cybermobbing, l'assicurazione cyber offre una protezione moderna e ottimale. La copertura assicurativa decorre dalla data indicata nel contratto di assicurazione, tuttavia non prima del pagamento del premio, e termina senza necessità di disdetta alla data indicata nel contratto di assicurazione.

Il contraente può revocare la proposta di conclusione del contratto di assicurazione o la dichiarazione di accettazione dello stesso per iscritto o in un'altra forma che consenta la prova per testo. La revoca è valida e la copertura assicurativa si estingue se la revoca stessa perviene presso la Baloise entro 14 giorni dalla consegna del contratto. La data di ricevimento del contratto è determinante per l'inizio del termine di revoca.

La revoca rende inefficace sin dall'inizio il contratto di assicurazione. Il contraente è tuttavia tenuto a farsi carico delle eventuali spese esterne insorte in relazione alla stipula del contratto. Il premio già pagato viene rimborsato.

L'assicurazione è valida per i danni che si verificano (assicurazione di cose) o che sono causati (assicurazione responsabilità civile) nel corso della durata contrattuale. La validità geografica e le informazioni dettagliate sulla validità temporale sono indicate nelle condizioni contrattuali e nel contratto di assicurazione.

## Vantaggi

- **Aiuto rapido e professionale:** I sinistri possono essere notificati semplicemente per telefono oppure online 24 ore su 24. Gli specialisti della Baloise si occupano immediatamente della liquidazione del sinistro.
- **Contratto trasparente:** L'assicurazione cyber è un prodotto con durata fissa e non si proroga automaticamente. In questo modo, il contraente può decidere la durata che preferisce.
- **Copertura completa e personalizzata:** Uso illecito di carte di credito o di dati, malware o cybermobbing: grazie ai due moduli "Safe Pay" e "Safe Surf" le prestazioni dell'assicurazione cyber vanno ben oltre la copertura tradizionale.
- **Stipula semplice:** Il contratto di assicurazione può essere stipulato in qualsiasi momento con pochi clic. Basta scegliere tra assicurazione individuale o familiare, indicare la durata contrattuale desiderata, il modulo da includere e fornire le proprie informazioni di contatto. Il pagamento avviene tramite carta di credito o PayPal.

## Entità delle prestazioni

### Safe Pay

| Eventi assicurati | Copertura |
|---|---|
| Uso illecito di carte | ✓ |
| Uso illecito di dati | ✓ |
| Consegne errate di ordini online | ✓ |

### Safe Surf

| Eventi assicurati | Copertura |
|---|---|
| Infezione da malware | ✓ |
| Perdita di dati | ✓ |
| Lesione della personalità | ✓ |

## Esempi di danni e di prestazioni

**Uso illecito di carte:** qualcuno ruba la vostra carta di credito e la usa per prelevare denaro al bancomat.
Prestazioni: spese sostenute per far valere i propri diritti nei confronti dei malfattori e risarcimento del danno patrimoniale dovuto all'uso illecito della carta.

**Uso illecito di dati:** attraverso il phishing un malintenzionato ottiene l'accesso al conto di e-banking della persona assicurata e trasferisce denaro sul proprio conto.
Prestazioni: risarcimento dei danni patrimoniali derivanti dall'uso illecito dei dati.

**Consegna errata di ordini online:** avete ordinato un nuovo smartphone in uno shop online ma ricevete un telefono danneggiato.
Prestazioni: spese per la riparazione della merce o, in caso di danno totale, spese per il nuovo acquisto.

**Infezione da malware:** il laptop viene infettato da un trojan.
Prestazioni: spese per la rimozione del malware e, se necessario, per il ripristino del sistema operativo.

**Perdita di dati:** dopo una caduta dello smartphone non è più possibile accedere alle proprie foto.
Prestazioni: spese per il recupero dei dati.

**Lesione della personalità:** un gruppo di studenti diffonde le foto di vostra figlia in rete.
Prestazioni: spese per far valere i propri diritti di cancellazione delle foto e, se necessario, assistenza psicologica o trasferimento in un altro luogo di domicilio in Svizzera.

Tutte le coperture sono strutturate come assicurazione contro i danni.

**Franchigia:** In caso di sinistro è trattenuta una franchigia di CHF 50.

**Notifica in caso di sinistro:** Il sinistro deve essere notificato immediatamente alla Baloise chiamando il numero +41 58 285 97 89.

## Linee guida preventive

Questi dieci consigli sono utili per aumentare notevolmente la sicurezza nell'uso del computer e dello smartphone.

**Consiglio n. 1: software antivirus:** Installate un software per l'individuazione dei programmi di malware e tenetelo sempre aggiornato. Il malware è un termine generico per tutti quei programmi sviluppati per arrecare danno agli utenti. Esistono vari tipi di malware: es. virus, trojan, rootkit, ransomware o spyware. Tutti hanno un obiettivo comune: provocare danni.

Informazioni supplementari: Eseguite regolarmente la scansione completa per la ricerca dei virus. Per risparmiare le risorse del sistema, generalmente gli antivirus eseguono solo la scansione dei file in uso. Invece, avviando manualmente la scansione completa del sistema sarà esaminato l'intero disco rigido.

**Consiglio n. 2: firewall:** Attivate o utilizzate un programma di firewall. Il programma di firewall protegge il sistema contro gli accessi dall'esterno monitorando il traffico dei dati e consentendo soltanto le connessioni conosciute o autorizzate. Le versioni più recenti di Windows dispongono di un firewall integrato.

Informazioni supplementari: Molti programmi contro il malware offrono le cosiddette "Suite", che spesso contengono anche il firewall. L'importante è verificare che sia attivato.

**Consiglio n. 3: sistema operativo:** Eseguite tempestivamente gli aggiornamenti regolari di assistenza e sicurezza del proprio sistema operativo. Queste patch chiudono le falle e le lacune note del sistema operativo, aumentando così la sicurezza delle transazioni di pagamento online.

Informazioni supplementari: Non tutti i sistemi operativi e programmi per computer o smartphone sono privi di errori. Gli autori dei malware sfruttano queste falle per penetrare nel computer o nello smartphone. Ad esempio, un semplice documento PDF può generare altre falle in un sistema non aggiornato o installare altri malware. Con gli update questi rischi vengono ridotti al minimo.

**Consiglio n. 4: password:** La password è un elemento di sicurezza essenziale per ogni servizio online, come ad esempio l'e-shopping o l'e-banking. Non annotate mai la vostra password e scegliete una parola chiave quanto più lunga possibile (almeno 8 caratteri) che non si trovi in nessun dizionario e sia composta da caratteri diversi (maiuscole, minuscole, caratteri speciali e numeri).

Informazioni supplementari: Una password complessa è più sicura ma anche più difficile da memorizzare, questo pertanto il nostro suggerimento: pensate a una frase e usate le iniziali di ogni parola per creare la vostra password. Per esempio, da "La mia insegnante in 1a B si chiamava maestra Rossi!" diventa "Lmii1BscmR!". Non usate mai la stessa password per più servizi online e cambiate regolarmente le password.

**Consiglio n. 5: dati di accesso:** Conservate i vostri dati di accesso in un luogo sicuro e non inoltrateli in nessun caso. Nessun fornitore serio di servizi online (es. shop o banca) vi chiederà mai per e-mail o telefono di comunicare i vostri dati di accesso completi.

**Consiglio n. 6: accesso WLAN:** Se a casa utilizzate una rete WLAN, l'accesso ad essa deve assolutamente codificato. Se l'accesso alla rete WLAN non è protetto, non solo aumenta il rischio di attacchi da parte di hacker, ma anche tutte le persone nelle vicinanze possono navigare gratuitamente (a vostre spese!) in Internet. Per questo si raccomanda di attivare la codifica WPA2 per il router WLAN e di utilizzare una password di codifica particolarmente sicura.

Informazioni supplementari: Fate sempre particolarmente attenzione quando navigate su reti WLAN gratuite. Spesso sono "monitorate" da truffatori e a volte sono gestite al solo scopo di rubare i dati dei dispositivi non protetti. Le operazioni di e-banking non dovrebbero mai essere effettuate con una connessione Internet non protetta tramite le reti aperte o le reti WLAN gratuite. Lo stesso vale per gli Internet point.

**Consiglio n. 7: browser sicuro:** Accertatevi che il vostro browser sia aggiornato. Potete inoltre migliorare le impostazioni di sicurezza del browser, ad esempio disabilitando ActiveX durante le operazioni di e-banking. Non dimenticate di chiudere la sessione, ossia di premere il pulsante "Logout" o "Esci" prima di abbandonare il servizio online. O meglio ancora: cancellate la memoria cache del browser.

Informazioni supplementari: Per le operazioni in Internet con dati sensibili (e-banking, e-shopping ecc.), la cosa migliore è utilizzare browser sicuri, come ad esempio "nowprotected". Questi servizi online proteggono la comunicazione completa tra il vostro dispositivo e il server del servizio online dall'inizio alla fine della sessione. Inoltre garantiscono sicurezza su ogni tipo di dispositivo utilizzato per usufruire del servizio online, che si tratti di laptop, smartphone, tablet, computer o un PC pubblico in un hotel.

**Consiglio n. 8: navigazione sicura:** Verificate sempre ove possibile se i link che vi sono stati forniti conducono effettivamente alle pagine Internet desiderate. Per le operazioni in Internet con dati sensibili (es. e-banking) occorre prestare particolare attenzione: non aprite mai una pagina di accesso tramite un link che avete ricevuto per e-mail. Non aprite mai gli allegati e non cliccate sui link contenuti nelle e-mail inviate da persone sconosciute. Spesso in questi allegati si nascondono malware e i link potrebbero condurre su pagine Internet pericolose che tentano di installare questi malware sul vostro computer.

**Consiglio n. 9: backup:** Difetti dell'hardware, attacchi hacker o il furto del computer possono causare la perdita di archivi digitali insostituibili. È pertanto importante salvare regolarmente i propri dati o parti importanti di essi copiandoli su un supporto diverso come ad es. un disco rigido esterno, un disco USB, ecc. Prevenite tempestivamente il problema facendo regolarmente copie di sicurezza dei vostri dati.

**Consiglio n. 10: buon senso:** Quando navigate in Internet o eseguite delle operazioni con dati sensibili, affidatevi sempre al vostro buon senso!

**Baloise Assicurazione SA**
Aeschengraben 21
Casella postale
4002 Basel
Servizio clientela 00800 24 800 800
servizioclientela@baloise.ch
baloise.ch

140.1286-1i 12.21 pdf