

# CATTOLICA & CYBER RISK

PER METTERE IN SICUREZZA  
LA VITA DIGITALE DELL'IMPRESA



La soluzione che  
tutela la tua attività  
in caso di attacco  
informatico



Cattolica Assicurazioni ha una soluzione per tutto ciò che riguarda la tua vita. Perché la vita è fatta per essere vissuta.

PRONTI ALLA VITA. | [cattolica.it](http://cattolica.it) | scarica l'app   

**CATTOLICA**  
ASSICURAZIONI  
DAL 1896

# CATTOLICA & CYBER RISK

Gli ultimi anni hanno evidenziato un trend persistente di crescita degli attacchi informatici, della loro gravità e dei danni conseguenti.

Gli attaccanti non sono più "hackers", e nemmeno piccoli gruppi di "artigiani" del cybercrime ma sono veri e propri gruppi criminali organizzati che hanno, ad esempio, come bersaglio le aziende, i loro server, le reti e le piattaforme social.

La consapevolezza di questi rischi sta gradualmente crescendo grazie:

- allo **sviluppo stesso della tecnologia** presso le aziende. Questo ha comportato l'aumento:
  - dei dati generati e scambiati;
  - del numero di dispositivi connessi;
- a fattori comportamentali e normativi. Esempi sono la crescita del numero di attacchi in tutto il mondo, Italia compresa, la crescente attenzione dei media a questi fenomeni e l'entrata in vigore del regolamento GDPR.



## MA QUALI SONO I RISCHI CYBER PER LE AZIENDE E PER GLI STUDI PROFESSIONALI?

Il progressivo diffondersi degli strumenti tecnologici e digitali, così come la diffusione di internet e l'ingresso di nuove tecnologie, mette la tua attività di fronte alla necessità di difenderti dagli attacchi informatici e dalle estorsioni cyber.

### GLI ATTACCHI INFORMATICI

#### MALWARE

È un software o codice dannoso progettato per ottenere l'accesso illecito e/o interrompere il funzionamento del sistema informatico della tua attività. Il virus ne è un tipico esempio, ma ci sono anche altre tipologie. Ad esempio, il così detto ransomware che è in grado di limitare l'accesso ai file contenuti all'interno del dispositivo infettandolo e richiedendo, di conseguenza, un riscatto.

#### PHISHING/SOCIAL ENGINEERING

Si tratta di mail realizzate appositamente per spingere le persone a fornire informazioni personali come password o dati bancari o a consentire l'accesso ad un computer al fine di installare segretamente software dannosi.

#### ACCOUNT CRACKING

È la violazione dei sistemi informatici collegati ad internet o ad un'altra rete, allo scopo di danneggiarli, di rubare informazioni oppure di sfruttare i servizi telematici della tua attività (connessione ad Internet, traffico voce, sms, accesso a database, ecc.) senza la tua autorizzazione. Ad esempio, con il cracking di una password, si può accedere all'account di un utente, mentre con il cracking di una rete wi-fi non protetta è possibile intercettare tutto il traffico.

#### ERRORE UMANO

È un errore operativo o una negligenza, da parte di un dipendente, che comporta un danno, come, ad esempio, la scelta del software da utilizzare o un errore di impostazione dei parametri.

#### ATTACCO DDoS (Distributed Denial of Service)

Letteralmente "Interruzione Distributiva del Servizio", si intende un attacco dannoso mirato a sovraccaricare il sistema informatico avendo un traffico in entrata proveniente da una moltitudine di fonti che ingolfa le risorse del tuo sistema informatico.

#### 0-DAY

Si tratta di malware/attacco informatico precedentemente sconosciuti per il quale il nome stesso indica il tempo disponibile per rispondere a un nuovo problema di sicurezza.

Vi sono due tipi di attacchi "zero-day":

- una vulnerabilità zero-day rappresenta una falla nella protezione di un software presente su un browser o un'applicazione;
- un exploit zero-day, invece, rappresenta un attacco digitale che sfrutta le vulnerabilità zero-day al fine di installare software dannosi su un dispositivo.

## ESTORSIONE CYBER

L'estorsione cyber è una qualsiasi minaccia da parte di un terzo con l'intento di obbligarti a pagare "un riscatto" per evitare che le tue informazioni o i tuoi dati segreti vengano pubblicati in Rete o resi accessibili all'interno del tuo stesso computer.

Le conseguenze di uno di questi attacchi informatici possono essere anche molto gravi. Facciamo solo qualche esempio:

- la perdita totale dei dati di business, di quelli relativi al personale dipendente o di quelli sensibili relativi ai tuoi clienti o pazienti;
- l'accesso di un competitor ai dati aziendali;
- l'accesso dei dipendenti a documenti confidenziali;
- il blocco dei sistemi informativi;
- un danno d'immagine.

Gli impatti, quindi, possono essere anche molto rilevanti per la tua attività sotto diversi aspetti.

### AGGRAVIO DI COSTI, DOVUTO:

- all'impossibilità di proseguire con la tua attività, pur mantenendo attive le spese fisse;
- alle penali da sostenere per il mancato rispetto dei contratti dei servizi e infrastrutture;
- al danneggiamento dei componenti critici del sistema informativo, ricostruzione archivi e programmi;
- sostituzione degli assets.

### RIDUZIONE DELLE ENTRATE:

- per il blocco delle vendite o impossibilità di erogare servizi;
- per la perdita di contratti e opportunità di business.

### INVESTIGATIONS INTERNE:

da parte delle autorità giudiziarie e sugli azionisti.

# CATTOLICA & CYBER RISK

## LA SOLUZIONE PER I RISCHI INFORMATICI.

### A CHI È RIVOLTA

**Cattolica & CYBER RISK è la soluzione adatta a:**

**PICCOLE MEDIE IMPRESE**

**STUDI PROFESSIONALI**

che utilizzano strumenti tecnologici e che desiderano una **tutela** in caso di attacco informatico:

- dalle spese per la gestione della crisi;
- dalle perdite economiche e finanziarie;
- dai costi per far ripartire la tua attività;
- per i danni a terzi e per le richieste di risarcimento di terzi che ne derivano.

### POTRAI SCEGLIERE TRA DUE SOLUZIONI SULLA BASE DELLE TUE ESIGENZE

La **Formula Assistenza**: che prevede assistenza diretta a seguito di attacchi informatici tramite l'intervento in locale o in remoto di esperti. Saranno loro ad intervenire sui tuoi sistemi per riparare i danni dell'attacco. Non dovrai così pensare a nulla!

La **Formula Indennitaria**: per chi desidera appoggiarsi a propri consulenti ed esperti con il vantaggio di vedere risarcite le spese sostenute a riparazione dei danni provocati dagli attacchi informatici.

Con entrambe le formule avrai comunque una tutela economica in caso di danni a terzi per quanto tenuto a pagare, quale civilmente responsabile.

### PER LE SPESE PER LA GESTIONE DELLA CRISI

#### FORMULA ASSISTENZA

In caso di attacco informatico il nostro servizio di Assistenza:

- attiverà, su richiesta, un'attività di investigazione e ripristino del sistema;
- istruirà le pratiche per ottemperare alla legge o alla normativa vigente riguardante la protezione dei dati;
- organizzerà la difesa legale;
- predisporrà i servizi relativi alla gestione dell'emergenza mettendo in atto una serie di attività per limitare e gestire l'impatto provocato dall'attacco.

#### FORMULA INDENNITARIA

In caso di attacco informatico è previsto un risarcimento per:

- le spese sostenute per l'investigazione e il ripristino del sistema;
- istruire le pratiche per ottemperare alla legge o alla normativa vigente riguardante la protezione dei dati;
- organizzare la difesa legale;
- predisporre i servizi relativi alla gestione di emergenza mettendo in atto una serie di attività per limitare e gestire l'impatto provocato dall'attacco.

## PER LE PERDITE ECONOMICHE E FINANZIARIE DOVUTE AD UN ATTACCO INFORMATICO

Sia con la **Formula Assistenza** che con la **Formula Indennitaria**, se l'attacco informatico provoca un'interruzione totale o anche parziale dell'attività, avrai a disposizione una diaria giornaliera utile per far fronte alle perdite economiche e finanziarie.

## PER LA TUTELA DAI COSTI PER FAR RIPARTIRE L'ATTIVITÀ

### FORMULA ASSISTENZA

Con **Cattolica & Cyber Risk** mettiamo a tua disposizione un servizio di assistenza in caso di un attacco informatico o di estorsione cyber per:

- il ripristino dell'accesso al Sistema;
- il ripristino dei dati;
- rimuovere i malware;
- avere al tuo fianco esperti pronti a rispondere alle tue necessità.

Sarai così messo nella condizione identica a quella antecedente l'attacco informatico.

Non ti verrà addebitata alcuna spesa.

Se la tua azienda o studio tratta con carte di credito/prepagate dei tuoi clienti, ad esempio, per sistemi di pagamento on line (e-commerce, ecc.) e quindi ha ottenuto la certificazione per lo standard di sicurezza PCI DSS, ma a seguito di un attacco informatico questo è stato compromesso, avrai a disposizione un servizio di Assistenza che, tramite esperti del settore:

- indagherà sulla violazione;
- predisporrà l'istruttoria per riottenere la certificazione dello standard.

### FORMULA INDENNITARIA

Con **Cattolica & Cyber Risk** otterrai un risarcimento in caso di un attacco informatico o di estorsione cyber per le spese che hai sostenuto per:

- il ripristino dell'accesso al Sistema;
- il ripristino dei dati;
- rimuovere i malware;
- avere al tuo fianco esperti pronti a rispondere alle tue necessità.

Se la tua azienda o studio tratta con carte di credito/prepagate dei tuoi clienti, ad esempio, per sistemi di pagamento on line (e-commerce, ecc.) e quindi ha ottenuto la certificazione per lo standard di sicurezza PCI DSS, ma a seguito di un attacco informatico questo è stato compromesso, otterrai un indennizzo per le spese che hai sostenuto per l'attività di esperti del settore che:

- indagheranno sulla violazione;
- otterranno nuovamente la certificazione dello standard.

## PER UNA TUTELA DAI DANNI A TERZI E PER LE RICHIESTE DI RISARCIMENTO

Sia con la **Formula Assistenza** che con la **Formula Indennitaria** di **Cattolica&Cyber Risk** sarai tenuto indenne di quanto tenuto a pagare:

- a terzi, compresi i tuoi dipendenti, che ti abbiano chiesto un risarcimento per:
  - un danno o un furto;
  - un accesso non autorizzato;
  - la divulgazione a terzi dei loro dati sensibili o personali contenuti nel tuo sistema informatico;
- a terzi che, in seguito ad un attacco al tuo sistema informatico che non sei riuscito a contrastare, ti abbiano chiesto un risarcimento per aver subito:
  - un danno, un furto o un attacco sul loro sistema informatico;
  - un danno ai loro beni;
- a terzi qualora, tramite la tua pagina web, siano stati divulgati messaggi che abbiano causato un danno reputazionale, oppure dal contenuto diffamatorio o ancora che abbiano violato la proprietà intellettuale o la privacy.



**CATTOLICA & CYBER RISK**  
GESTISCE LA CRISI,  
FINANZIA LE PERDITE,  
TI SOLLEVA DAI COSTI.  
DA OGGI RIPARTIRE  
NON SARÀ PIÙ UN PROBLEMA.

**Cattolica Assicurazioni ha una soluzione per:**

**L'IMPRESA**, perché per la maggior parte degli imprenditori, l'azienda è la propria casa, un bene prezioso da proteggere e non mettere in pericolo.

**E per tutto il tuo mondo.**

**LA PERSONA**, perché che tu sia un libero professionista, un lavoratore autonomo o dipendente, è opportuno avere soluzioni che permettano a te e al tuo nucleo familiare di affrontare con serenità tutte le situazioni, anche le più gravi;

**LA CASA**, perché che tu sia proprietario o in affitto, è il rifugio dove vivi i tuoi affetti, le tue passioni;

**LA MOBILITÀ**, perché il bisogno di mobilità deve essere sempre soddisfatto con il massimo della protezione;

**IL FUTURO**, perché la vita è fatta di obiettivi più o meno importanti.

Risparmiare e investire anche piccole cifre, ti permette di raggiungerli.





**Società Cattolica di Assicurazione S.p.A.** - Sede Legale: Lungadige Cangrande, 16 - 37126 Verona - Italia - Pec: cattolica.assicurazioni@pec.gruppocattolica.it - Cap. Soc. Euro 685.043.940,00 i.v. - C.F. P.IVA Reg. Imp. Vr 00320160237 - Iscrizione Albi: Imprese IVASS n. 1.00012, Gruppi Assicurativi IVASS n. 019 - Partita IVA del Gruppo IVA Cattolica Assicurazioni 04596530230.

**Messaggio pubblicitario con finalità promozionali. Prima della sottoscrizione leggere attentamente il set informativo disponibile sul sito [www.cattolica.it](http://www.cattolica.it) e presso le Agenzie Cattolica Assicurazioni.**