Dai furti d'identità alle truffe online, crescono le soluzioni assicurative per proteggersi

# POLIZZE CYBER, SCUDO PER PRIVATI

## Colpiti 8,7 mln italiani: premi da 140 euro l'anno

Gli attacchi «cyber» alle scuole, e prima ancora alle compagnie aeree e ai supermercati, hanno riportato la cybersicurezza al centro del dibattito pubblico. Secondo una recente indagine commissionata da Facile.it a mUp Research, tra marzo 2025 e marzo 2026 circa 8,7 milioni di italiani hanno subito una violazione informatica. A finire più spesso nel mirino sono stati i profili social, gli account bancari e gli smartphone. L'indagine, diffusa ieri, è stata condotta a marzo su un campione di 1.001 persone, rappresentativo della popolazione italiana adulta tra i 18 e i 74 anni.

Se tra le imprese le polizze contro gli attacchi informatici sono più diffuse e possono arrivare a coprire i danni anche in situazioni come quella accaduta in alcuni supermercati italiani, meno conosciute sono le soluzioni assicurative rivolte ai privati. Facile.it ha analizzato l'offerta attualmente sul mercato, esaminando le coperture disponibili, le modalità di intervento e i relativi costi.

Il primo aspetto da considerare è la forma con cui vengono proposte queste tutele. Nella maggior parte dei casi, infatti, le coperture cyber per i consumatori non costituiscono polizze autonome, ma garanzie accessorie delle tradizionali assicurazioni casa. Per poterle attivare è quindi necessario sottoscrivere prima una polizza abitativa. Il modulo dedicato alla cybersicurezza può essere già compreso nell'assicurazione di base oppure richiedere il pagamento di un premio aggiuntivo.




Una parte delle soluzioni assicurative è dedicata alla prevenzione e all'assistenza tecnica. Molte polizze cyber mettono a disposizione degli assicurati software e strumenti online. I servizi possono comprendere il monitoraggio dei dati personali presenti in rete e programmi per identificare virus, malware, phishing e altri tentativi di attacco digitale. Quando si verifica un sinistro, alcune compagnie prevedono l'intervento di tecnici specializzati, che possono operare da remoto oppure in presenza. Il loro compito può essere, per esempio, rimuovere eventuali virus e ripristinare il corretto funzionamento dei dispositivi coinvolti.

Tra i bersagli degli attacchi ci sono anche conti correnti e carte elettroniche. Per questo alcune compagnie hanno introdotto garanzie che intervengono quando il furto di denaro avviene attraverso strumenti digitali. Le prestazioni possono andare dall'anticipo di denaro, nel caso in cui il furto si verifichi mentre l'assicurato si trova lontano da casa, fino al rimborso delle somme sottratte. Quest'ultimo è previsto entro i limiti del massimale stabilito dalla polizza.

Un capitolo distinto riguarda il furto d'identità e dei dati personali, un rischio spesso sottovalutato ma che può avere conseguenze anche oltre la perdita delle informazioni. Chi si appropria dell'identità di un'altra persona può infatti utilizzarla per compiere atti illeciti, esponendo il proprietario inconsapevole a possibili ripercussioni, anche legali. Le garanzie assicurative possono comprendere l'assistenza necessaria per recuperare dati e account, la rimozione di contenuti lesivi pubblicati utilizzando l'identità sottratta e il rimborso di alcune spese collegate alle azioni fraudolente commesse dai responsabili. La tutela può riguardare anche i contenuti pubblicati online e i danni che ne derivano per le persone coinvolte. In caso di cyberbullismo, revenge porn o lesioni alla reputazione digitale, alcune polizze prevedono il monitoraggio del web per individuare i contenuti dannosi, l'attivazione delle procedure necessarie a rimuoverli definitivamente dalla rete e l'assistenza legale per tutelare i diritti della vittima. In determinati casi è previsto anche il rimborso delle spese sostenute per il supporto psicologico. Coperture di questo tipo possono intervenire inoltre quando a essere danneggiata è la reputazione online di un adulto, a condizione che la persona coinvolta non sia un personaggio famoso.

Non tutte le conseguenze di un attacco informatico riguardano direttamente chi lo subisce. Alcune polizze prendono in considerazione anche i danni provocati involontariamente a terzi. Può accadere, per esempio, che un computer infettato da un virus finisca per contagiare altri dispositivi.

Un'ulteriore area di intervento è quella degli acquisti online. La polizza può fornire assistenza per affrontare eventuali controversie contrattuali e prevedere il rimborso dell'importo perso, sempre entro i massimali stabiliti. La copertura può riguardare sia il caso in cui l'oggetto acquistato non venga consegnato, sia quello in cui il bene ricevuto risulti difettoso o non corrispondente a quanto pubblicizzato.

Resta infine il tema del prezzo. Il costo delle polizze cyber cambia da compagnia a compagnia e dipende dalle coperture offerte, dai massimali e dalle franchigie. Poiché nella maggior parte dei casi si tratta di garanzie collegate a un'assicurazione casa, per valutare la spesa occorre considerare il prezzo dell'intero pacchetto e non soltanto quello del modulo informatico. Secondo l'analisi di Facile.it, il costo complessivo parte in generale da circa 140 euro l'anno. (riproduzione riservata)

## CyberGrant: nelle scuole è allarme dati

Le minacce informatiche alle scuole mostrano che la sicurezza digitale non può fermarsi agli accessi. Un account universitario violato è bastato per inviare allarmi bomba a circa seimila istituti. Il rischio più profondo riguarda però i dati che transitano nelle caselle: Pei, certificati, diagnosi e documenti sulla vita familiare di bambini e ragazzi.

«La posta elettronica è fragile: una mail partita non si richiama e il contenuto resta leggibile in ogni casella in cui è arrivato», osserva **Valerio Pastore**, founder di CyberGrant Inc. Anche errori involontari possono



*Valerio Pastore founder CyberGrant*

esporre informazioni sensibili: il Garante ha sanzionato comunicazioni inviate a destinatari non autorizzati con dati sulla salute degli alunni. Per Pastore occorre affiancare alla casella pubblica un canale riservato per i dati dei minori e gli scambi operativi. Servono mittenti identificati, accesso tramite codice monouso, messaggi e allegati cifrati, revoca o scadenza e tracciamento delle aperture. «La protezione deve stare sul contenuto e seguirlo fino a chi lo legge», sottolinea.

CyberGrant sviluppa EmailGrant, uno strumento che cifra messaggi e allegati, consente di revocarli o farli scadere dopo l'invio e richiede un codice monouso ai destinatari esterni. La sicurezza deve riguardare anche i file nei portali e nelle piattaforme dei fornitori, con cifratura e regole sulla gestione degli incidenti. (riproduzione riservata)

## Frodi finanziarie, Equinix: l'innovazione passa da reti e dati Prevenzione con connettività veloce e intelligenza artificiale

Le frodi finanziarie si combattono con infrastrutture che analizzare grandi quantità di dati rapidamente. Per gli operatori finanziari, individuare transazioni sospette prima che siano completate è una sfida crescente: deepfake, identità sintetiche e phishing generato dall'intelligenza artificiale rendono più sofisticate le tecniche criminali. Machine learning e analisi predittiva devono quindi poggiare su reti affidabili, scalabili e a bassa latenza. «La sfida del settore non è più soltanto comprendere il potenziale dell'AI, ma riuscire ad utilizzarla in modo efficace, sicuro e scalabile», osservano **Iiro Stubin**, principal, global Technical Solutions di Equinix, e Leland Cheuk, director, Solution Marketing della società. Servono «i dati corretti, nei luoghi giusti e con la velocità necessaria» per intervenire.

Un ostacolo è la frammentazione delle informazioni tra data center privati, cloud pubblici, ambienti ibridi e multicloud, applicazioni e partner esterni. La dispersione complica una visione unitaria. Per Stubin e Cheuk, contrastare le frodi significa anche affrontare «una questione di modernizzazione della rete».



*Iiro Stubin principal, global technical solutions Equinix*

La strategia indicata si basa su un nucleo di dati autorevole e controllato dalle organizzazioni, interconnessioni private ad alte prestazioni tra sistemi It, cloud e partner, e infrastrutture edge sicure, che avvicinino l'elaborazione alle fonti informative. Ridurre la distanza tra dati e capacità di calcolo permette di contenere la latenza e sostenere analisi e decisioni in tempo reale.

Gli esempi citati sono Block, che nel 2025 ha annunciato sistemi Nvidia Dgx Gb200 in un data center Equinix per addestrare modelli di AI generativa, e Outseer, attiva nella prevenzione delle frodi digitali, presente in molti mercati attraverso la piattaforma Equinix. (riproduzione riservata)