Sicurezza e frodi informatiche in Banca

[A cura di Maria Ferrucci, CERTFin]

Il Report "Sicurezza e Frodi Informatiche in Banca" viene realizzato annualmente dal CERTFin - CERT (Computer Emergecy Response Team) Finanziario Italiano - e fornisce una fotografia aggiornata del livello di rischio cyber e delle frodi e truffe informatiche nel settore finanziario italiano allo scopo di aiutare banche e operatori finanziari a comprendere l'evoluzione delle minacce e dove rafforzare prevenzione, controlli e investimenti.

A seguire si riportano i principali contenuti del Rapporto 2026, che raccoglie i dati segnalati da 35 organizzazioni rappresentative di oltre il 90% del settore.

Iniziative di awareness, formazione e investimenti

Dalla rilevazione emerge una progressiva diffusione della cultura della sicurezza all'interno dell'intera organizzazione. La formazione "interna" su frodi e attacchi informatici coinvolge ormai in modo sistematico il personale di filiale (100% dei rispondenti) e, con livelli molto elevati, anche i team specialistici di sicurezza, il Top Management, l'Help Desk, il Back Office e il Contact Center, consolidando l'attenzione verso le strutture maggiormente esposte al rapporto con la clientela e alla gestione degli eventi operativi più sensibili.

Oltre alla formazione "interna", gli istituti rivolgono particolare attenzione alle iniziative di sensibilizzazione verso la clientela. L'analisi delle tematiche affrontate mostra una forte concentrazione sui contenuti più direttamente collegati ai meccanismi di frode oggi prevalenti, tra cui social engineering, uso sicuro degli strumenti di pagamento e rischi legati agli investimenti online. Anche la frequenza delle iniziative è significativa: il 78% delle organizzazioni sul segmento delle persone fisiche (c.d. "Retail") e il 69% sul segmento delle imprese (c.d. "Corporate") realizzano attività con frequenza inferiore ai sei mesi.

Il 77% degli istituti ha attivato, inoltre, formazione o sensibilizzazione verso i fornitori ICT, con temi più legati alla relazione tra terza parte e istituto: dall'identificazione e segnalazione degli incidenti, alla protezione dei dati e ai requisiti di sicurezza, fino a normativa di settore, continuità operativa e disaster recovery.

Il peso strategico che il tema della sicurezza riveste per il settore finanziario è confermato anche dal livello degli investimenti, con una quota media di spesa IT dedicata alla sicurezza pari al 6,45% nel 2025 e una stima dell'8% per il 2026. Aumenta, inol-

tre, il budget di sicurezza destinato alla prevenzione e al contrasto delle frodi, con il 13,5% del totale della spesa IT.

Il report 2026 ha per la prima volta approfondito i principali ambiti tecnologici sui quali si concentreranno prevalentemente le iniziative di investimento in materia di cybersicurezza e resilienza operativa nel prossimo biennio (**Figura 1**): emerge che gli investimenti in cybersicurezza si concentreranno soprattutto su resilienza operativa digitale, soluzioni antifrode e gestione delle identità.

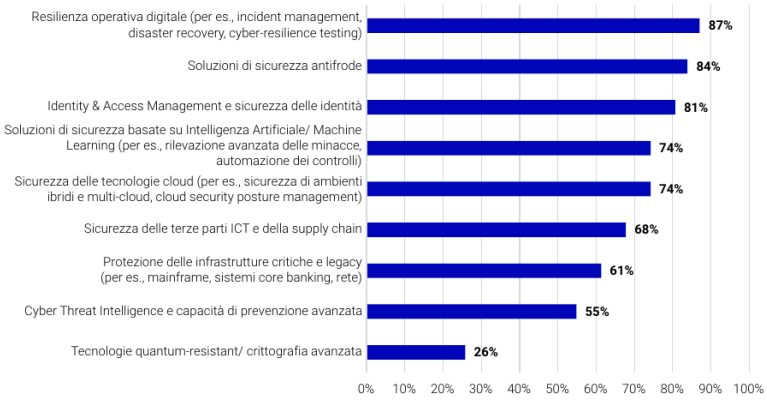

Figura 1 - Principali ambiti tecnologici di investimento nel prossimo biennio *(Fonte: CERTFin, Report Sicurezza e frodi informatiche in banca, maggio 2026)*

Dimensionamento delle frodi e strumenti di pagamento

Tra gli strumenti di pagamento preferiti dai frodatori per la realizzazione dell'attacco, nel segmento Retail il bonifico istantaneo nazionale è il principale (40% dei tentativi di frode in termini di numerosità), seguito dal bonifico ordinario nazionale (30%). Nel segmento delle imprese, invece, il bonifico ordinario nazionale prevale con il 53% degli eventi anomali registrati dal campione. Con riferimento all'efficacia dell'attacco (rapporto tra operazioni effettive e totale transazioni anomale), il bonifico istantaneo nazionale presenta una quota di operazioni effettive più alta rispetto all'ordinario, sia nel segmento Retail che nel Corporate.

Le vittime "più mature" (oltre i 45 anni) rappresentano oltre il 70% del totale, con gli over 60 al 43%, mentre le microimprese vengono colpite in oltre la metà degli attacchi.

Guardando all'efficacia dei presidi di prevenzione e contrasto, emerge che la quota prevalente delle transazioni anomale viene intercettata prima che possa produrre effetti economici, sia con riferimento alla numerosità che agli importi economici associati agli eventi, come si evince dalla **Figura 2**. Si registra, inoltre, un forte aumento degli importi recuperati, che crescono di oltre il 50% passando da 23 a 35 milioni di euro, anche grazie al Protocollo di collaborazione antifrode tra PSP italiani attivato dal CERTFin nel 2020.

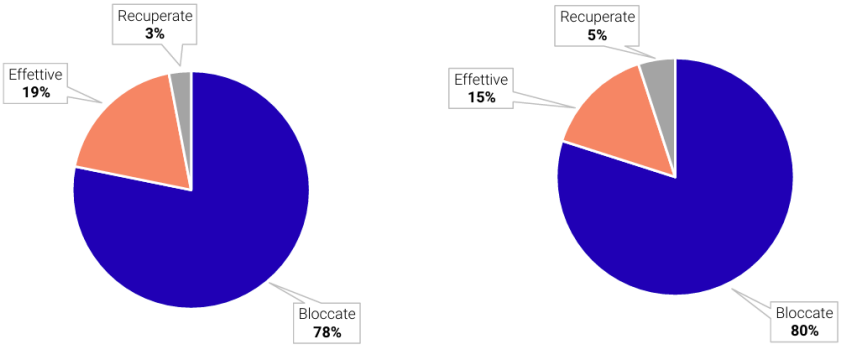

Figura 2 - Ripartizione percentuale delle tipologie di transazioni anomale (bloccate, recuperate ed effettive) – analisi sul numero di accadimenti (complessivo Retail e Corporate) (*Fonte: CERTFin, Report Sicurezza e frodi informatiche in banca, maggio 2026)*

Inoltre, le transazioni anomale si concentrano nettamente sul segmento Retail, che rappresenta la quasi totalità degli eventi (95%) e la maggior parte degli importi (84%). Il Corporate, pur incidendo molto meno in termini di numerosità, presenta tuttavia transazioni mediamente di valore più elevato.

Le transazioni fraudolente mostrano, infine, una crescente dimensione internazionale. All'interno dello Spazio Economico Europeo (SEE), Malta emerge come principale destinazione, seguita da Lituania e Germania, mentre fuori dallo SEE prevale il Regno Unito, seguito da Svizzera e Stati Uniti. Particolarmente significativo è l'aumento degli importi diretti all'estero, più che raddoppiati rispetto all'anno precedente (113 milioni di euro). Si segnala la necessità, pertanto, di una maggiore collaborazione transfrontaliera.

© Clusit 2026

Dinamiche e modalità operative delle frodi informatiche

Con un trend in aumento rispetto all'anno precedente, anche nel 2025 si conferma la prevalenza della manipolazione del pagatore tra le modalità operative di realizzazione della frode (81% nel Retal e 70% nel Corporate). Tale tecnica prevede un'attività manipolatoria posta in essere dal frodatore ai danni del pagatore, finalizzata a indurlo a emettere in buona fede un ordine di pagamento o a impartire un'istruzione di pagamento verso un conto che egli ritiene appartenere a un beneficiario legittimo. Emissione di un ordine di pagamento da parte del frodatore e modifica di un ordine legittimo (entrambe "operazioni non autorizzate" compiute direttamente dal frodatore) occupano rispettivamente il 18% e l'1% nel Retail e il 24% e il 6% nel segmento delle imprese.

Per quanto riguarda i canali o vettori di primo contatto, nel Retail il 46% delle frodi effettive origina ancora da telefonate e SMS, ma il dato è in calo rispetto a circa il 60% della rilevazione precedente e all'87,5% di due anni prima. Le chiamate telefoniche, invece, pesano per il 36% del totale: 24% riconducibile a spoofing del numero chiamante, 9% a spoofing di numeri verdi e 3% a chiamate senza alterazione. Gli SMS incidono per il 10%, metà dei quali con alias falsificato. Al di fuori del canale telco, i social media raggiungono il 22% e le instant messaging app il 10%, confermando uno spostamento verso ambienti meno "controllabili" dal prestatore di servizi di pagamento (psp). Sempre più si manifesta, quindi, l'esigenza di rafforzare la collaborazione tra più settori nel contrasto alle frodi e truffe digitali.

La finalizzazione delle frodi Retail è dominata dal social engineering (ingegneria sociale o impersonificazione), schema che prevede lo sfruttamento di leve emotive, urgenza, pressione psicologica e fiducia artificiale per manipolare le vittime e realizzare la frode, con il 77% dei casi. Di questi i falsi investimenti costituiscono la tipologia più ricorrente (36%), seguiti dai task scam (25%), come rappresentato in **Figura 3**.

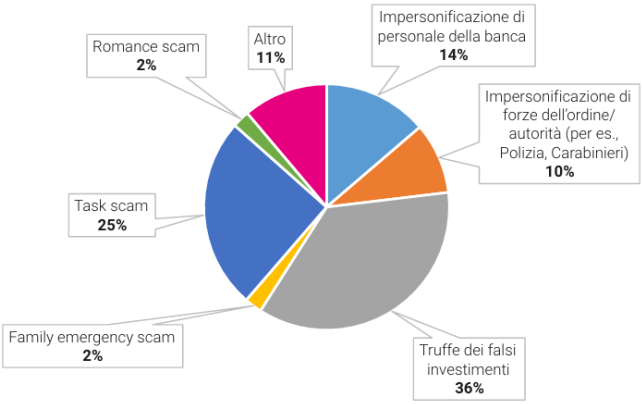

Figura 3 - Distribuzione degli eventi fraudolenti di social engineering nel segmento Retail *(Fonte: CERTFin, Report Sicurezza e frodi informatiche in banca, maggio 2026)*

Nel segmento Corporate il social engineering rappresenta il 37%, mentre la BEC (Business E-mail Compromise), occupa il 23% delle tecniche. Quest'ultima fattispecie è tipica degli attacchi perpetrati verso le imprese, in quanto la finalizzazione della frode si realizza generalmente attraverso l'alterazione o l'intercettazione delle comunicazioni aziendali, allo scopo di indurre l'impresa a eseguire pagamenti verso coordinate fraudolente, sovente nell'ambito di rapporti commerciali apparentemente legittimi. La differenza tra i segmenti suggerisce due diverse superfici di rischio tra i due comparti di clientela: persuasione diretta della persona nel Retail e compromissione dei processi comunicativi e autorizzativi nel Corporate.

Infine, dalla rilevazione del CERTFin emerge che il 96% delle frodi effettive risulta eseguito con Strong Customer Authentication (SCA) correttamente completata, mettendo in evidenza che i presidi di autenticazione forte non vengono elusi in senso tecnico, bensì risultino inefficaci in presenza di un cliente già manipolato e indotto ad autorizzare l'operazione.

Meccanismi di rilevazione e contrasto alle frodi

Tra i metodi adottati per l'individuazione e la segnalazione delle frodi, il controllo delle transazioni effettuato direttamente dalla banca (transaction monitoring interno) continua a rappresentare il principale strumento attraverso il quale vengono inter-

cettate disposizioni di pagamento anomale o fraudolente (57% nel Retail e 58% nel Corporate). Il disconoscimento delle operazioni da parte dei clienti rimane il secondo canale più utilizzato per l'individuazione delle frodi, mentre filiali, canali di infosharing settoriale e servizi di segnalazione specifici acquistati da soggetti terzi rappresentano ulteriori fonti di segnalazione sono rappresentate.

Per quanto riguarda gli strumenti utilizzati per valutare la legittimità delle operazioni all'interno dell'organizzazione, dalla rilevazione emerge che la maggior parte degli istituti tende a utilizzare almeno dieci indicatori differenti nella valutazione delle operazioni, tra cui indirizzi IP, browser e identificativi dei device (93% dei rispondenti), seguiti dalla tipologia di dispositivo, dal Paese destinatario della transazione e dalla presenza di un nuovo beneficiario (87% dei rispondenti).

Con riferimento agli strumenti tecnologici adottati dalle organizzazioni per monitorare e individuare potenziali attacchi informatici diretti verso la propria clientela, ai primi due posti figurano monitoraggio delle transazioni anomale effettuate tramite Internet banking e tramite mobile app. Interessante, inoltre, menzionare l'utilizzo di tecnologie di Artificial Intelligence, alla base – in media – del 25% di tali strumenti.

Infine, rispetto alle contromisure utilizzate per limitare le frodi sui bonifici ordinari e istantanei, emerge un quadro caratterizzato da un ampio ricorso a presidi di prevenzione e intercettazione con un livello di adozione sostanzialmente elevato, che vede al primo posto il blocco delle operazioni verso IBAN segnalati come sospetti, indicato dalla quasi totalità dei rispondenti, seguito dagli alert verso il cliente e dall'applicazione di limiti operativi (**Figura 4**).

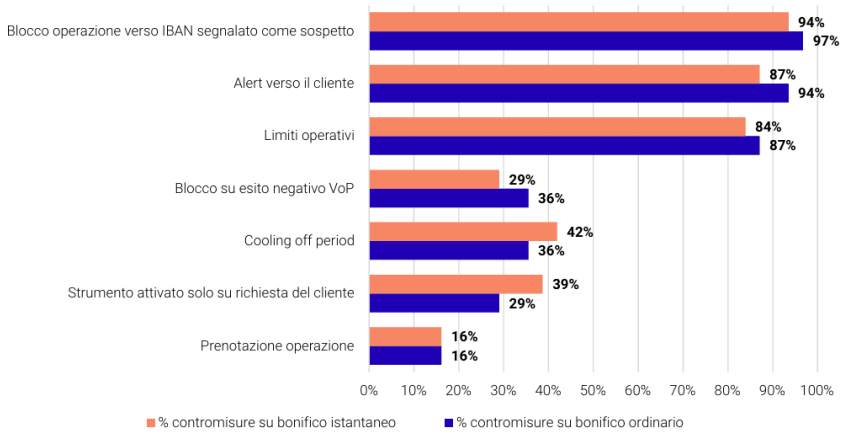

Figura 4 - Distribuzione contromisure bonifici ordinari e istantanei *(Fonte: CERTFin, Report Sicurezza e frodi informatiche in banca, maggio 2026)*

Cybersecurity

La sezione cybersecurity evidenzia una riduzione di alcune minacce "classiche" e, parallelamente, un aumento del rischio "indiretto". Nel 2025 sono stati rilevati infatti 76 data breach, con una crescita del 27% rispetto all'anno precedente. In particolare, il 31% delle organizzazioni dichiara di avere subito un breach diretto, contro il 23% della precedente rilevazione, mentre il 35% segnala almeno un breach indiretto riconducibile a fornitori o supply chain. Tale dato sottolinea la necessità di estendere i controlli sull'intera catena di fornitura.

Per quanto riguarda la distribuzione degli incidenti (**Figura 5**), il social engineering, incluso il phishing, è al primo posto con quasi la metà degli accadimenti, seguito dagli attacchi DDoS. La prevalenza della dinamica dell'ingegneria sociale anche tra gli incidenti cyber conferma che il fattore umano attraversa sia la dimensione delle frodi sia quella della sicurezza informatica tradizionale.

© Clusit 2026

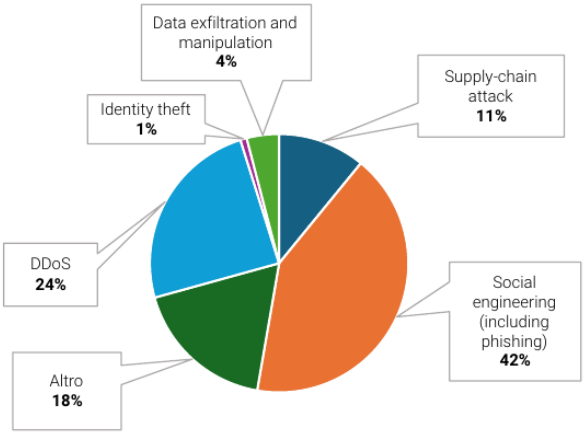

Figura 5 -Distribuzione degli incidenti di sicurezza rilevati nel campione *(Fonte: CERTFin, Report Sicurezza e frodi informatiche in banca, maggio 2026)*

Sul fronte dei DDoS, il 70% degli istituti dichiara di avere rilevato almeno un attacco. Tuttavia, gli attacchi classificati come "gravi" scendono però a due casi, anche grazie al fatto che il 97% disponeva già nel 2025 di contromisure tecnologiche volte a mitigare tali attacchi e che il 70% le ha rafforzate nel corso del 2025.

Nel campione non risultano infezioni ransomware, a fronte del 7% della rilevazione precedente, e non vengono registrati terminali o server danneggiati da ransomware. Il report invita comunque a leggere il dato con cautela, in quanto l'assenza di eventi nel campione non implica la scomparsa della minaccia e può convivere con una riallocazione dell'azione criminale verso fornitori e soggetti della supply chain.

Infine, per la prima volta all'interno del Report viene approfondita anche la dimensione geopolitica del rischio cyber, in considerazione della crescente instabilità dello scenario internazionale. Tra i dati più significativi, emerge che il 56% degli istituti ha integrato il rischio cyber geopolitico nei propri processi di risk assessment e che il 90% delle organizzazioni dispone di un processo strutturato di threat intelligence volto a presidiare le minacce di natura geopolitica.

Conclusioni

Nel complesso, la rilevazione CERTFin 2026 evidenzia un settore bancario che intercetta una quota elevata delle transazioni anomale e investe in modo crescente nel rafforzamento della sicurezza digitale. Il principale cambio di paradigma riguarda però la natura dell'attacco: la tecnologia continua a essere essenziale, ma una parte sempre più rilevante delle perdite nasce da operazioni correttamente autenticate e volontariamente autorizzate da clienti manipolati. È sempre più necessaria, quindi, una risposta coordinata che coinvolga non solo le organizzazioni del settore ma anche clienti, fornitori e altri settori.

© Clusit 2026