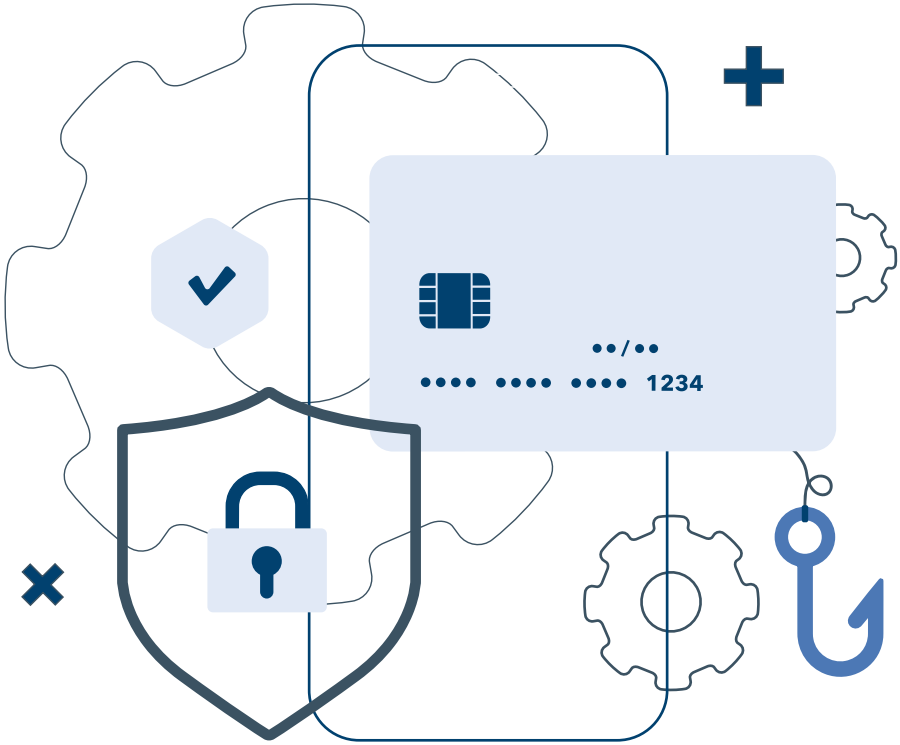
SICUREZZA DEI PAGAMENTI

Strumenti e buone pratiche per prevenire le frodi nelle PMI



cdp

NOTA AL LETTORE

Questo manuale nasce con un obiettivo dichiarato: mettere nelle mani di chi gestisce ogni giorno i pagamenti di un'impresa uno strumento di lavoro, non un documento da archiviare.

Non è un rapporto statistico né un testo normativo. Là dove i rapporti istituzionali descrivono il fenomeno delle frodi con dati e statistiche e le norme prescrivono obblighi ai prestatori di servizi di pagamento, questo manuale risponde a una domanda diversa e molto concreta: che cosa deve fare un'impresa per non finire dentro quelle statistiche.

Per questo è organizzato per scenari operativi, calibrato sulla dimensione dell'impresa e corredato di strumenti pronti all'uso: checklist, procedure di verifica, modelli di comunicazione, percorsi di escalation.

I dati citati provengono da fonti istituzionali aggiornate — in particolare i rapporti della Banca d'Italia e del Comitato Pagamenti Italia, le rilevazioni di CERTFin, dell'Agenzia per la Cybersicurezza Nazionale e del Clusit. Le fonti puntuali sono indicate nel testo e raccolte in appendice.

A cura di
Nicola Vanin, Daniele Spelta, Davide Vittorio Cappelletti

SICUREZZA DEI PAGAMENTI

Strumenti e buone pratiche per prevenire le frodi nelle PMI

Prefazione

La trasformazione digitale è oggi una delle principali leve di sviluppo e competitività per l'economia italiana. Tecnologie, dati e nuovi servizi stanno ridefinendo il modo in cui le imprese operano, innovano e competono, aprendo nuove opportunità sui territori.

Per le piccole e medie imprese, che rappresentano l'ossatura del nostro sistema produttivo, cogliere appieno queste opportunità significa anche saper affrontare con consapevolezza i rischi che accompagnano la crescente digitalizzazione dei processi aziendali.

Tra questi, la sicurezza dei pagamenti riveste un'importanza cruciale.L'evoluzione delle minacce informatiche e delle tecniche di frode dimostra che la protezione delle transazioni non dipende soltanto dalle tecnologie adottate, ma anche dalla diffusione di competenze adeguate, dall'efficacia dei processi e da una solida cultura della prevenzione.

In linea con la propria missione e con le priorità del Piano Strategico 2025-2027,CDP è al fianco delle imprese per sostenerne lo sviluppo e rafforzare la competitività del Paese. Un impegno che oggi si traduce in un'offerta sempre più ampia di soluzioni finanziarie, servizi e iniziative per investire in innovazione e crescita.

In questo contesto, promuovere una maggiore consapevolezza dei rischi digitali significa mettere a disposizione del tessuto imprenditoriale conoscenze e competenze utili a rafforzarne la resilienza e ad accompagnarne i percorsi di trasformazione.Questo manuale nasce con un obiettivo concreto: offrire alle PMI un supporto pratico per riconoscere i principali rischi connessi ai pagamenti e adottare comportamenti più sicuri nella gestione quotidiana delle proprie attività.

Perché rendere le imprese più sicure significa anche renderle più solide e innovative e, allo stesso tempo, contribuire a costruire un'economia più forte e preparata ad affrontare le sfide del futuro.

Dario Scannapieco
Amministratore Delegato e Direttore Generale
Cassa Depositi e Prestiti

Indice

INTRODUZIONE

Finalità

Ogni giorno, in Italia, le imprese spostano denaro: pagano fornitori, ricevono incassi, regolano stipendi e imposte. La quasi totalità di questi movimenti avviene oggi per via digitale, attraverso i servizi di *home banking* aziendale e le piattaforme di gestione dei pagamenti. È un'infrastruttura quotidiana e in larga parte invisibile, sulla quale poggia la continuità operativa di qualunque attività economica.

Proprio per questo è divenuta uno degli obiettivi privilegiati della criminalità economica. Nella grande maggioranza dei casi il punto debole non risiede nella tecnologia bancaria, bensì nella catena di decisioni e di processi attraverso cui un ordine di pagamento nasce, viene autorizzato ed eseguito. È in quella catena che si inserisce la frode contemporanea. Ed è su quella catena che questo manuale intende agire.

La finalità è circoscritta e, per questo, raggiungibile: ridurre la probabilità che un'impresa subisca una frode sui pagamenti e contenere il danno quando un tentativo di frode vada a buon fine. Non si propone l'azzeramento del rischio, che sarebbe un obiettivo irraggiungibile, ma propone la definizione di un metodo di minimizzazione, applicabile da subito, indipendente dalla dimensione dell'impresa e dal suo grado di maturità tecnologica.

Frode e truffa: una distinzione necessaria

Nel linguaggio corrente i due termini si usano come sinonimi. Per chi gestisce pagamenti, invece, la differenza è sostanziale, perché determina chi sopporta la perdita. Conviene fissarla con precisione prima di procedere.

DEFINIZIONI · I TERMINI ESSENZIALI

Frode (operazione non autorizzata).
Qualcuno dispone un pagamento al posto del titolare, senza il suo consenso. È la sostituzione del dispositore: il criminale si impossessa di credenziali o strumenti e ordina lui l'operazione. In questo caso operano, di norma, le tutele e i rimborsi previsti dalla disciplina.

Truffa (manipolazione del pagatore).
È il titolare stesso a disporre il pagamento, ingannato. È il raggiro del dispositore: nessuno sostituisce nessuno, il pagatore agisce di propria mano in buona fede. Poiché l'operazione risulta autorizzata, le tutele automatiche non si applicano e il recupero è arduo.

Social engineering.
L'insieme delle tecniche di manipolazione psicologica con cui si induce una persona a compiere un'azione — disporre un bonifico, comunicare un codice. È il motore della truffa.

BEC (Business Email Compromise).
La compromissione o l'imitazione della posta aziendale per dirottare un pagamento. È la forma di truffa più rilevante per le imprese.

SCA (Strong Customer Authentication).
L'autenticazione forte introdotta dalla PSD2: due o più fattori indipendenti per validare l'identità del pagatore.

La distinzione non è accademica. Nella frode in senso proprio, il pagatore è vittima passiva e la legge tende a tutelarlo; nella truffa è parte attiva, sebbene ingannata, e la tutela viene meno. È una soglia sottile, ma è la soglia su cui si decide chi paga.

L'inversione

Vi è un dato di tendenza che spiega meglio di ogni altro perché un manuale come questo serve oggi più di ieri. Negli ultimi anni il rapporto tra frode e truffa si è **rovesciato.** L'autenticazione forte introdotta dalla PSD2 ha reso assai più difficile la frode tecnica — sottrarre credenziali e disporre il pagamento al posto del titolare. I criminali, di conseguenza, hanno spostato il proprio sforzo dove la barriera tecnologica non arriva: la persona.

I numeri sono eloquenti. Su cento transazioni fraudolente confermate nel settore, **novantanove avvengono a valle di un'autenticazione forte regolarmente completata:** non perché la SCA abbia fallito, ma perché è il cliente legittimo, manipolato, a portarla a termine. Circa l'82% delle operazioni fraudolente è eseguito direttamente dal titolare; e nel segmento retail l'86% delle frodi è riconducibile a manipolazione tramite ingegneria sociale, in crescita di circa un terzo su base annua[1].

La tecnologia, in altri termini, ha fatto il proprio lavoro: ha blindato la porta. Il criminale ha smesso di forzarla e ha cominciato a *bussare, convincendo qualcuno ad aprirla dall'interno.* È una transizione che riconfigura il problema: la difesa non è più soltanto questione di sistemi, ma di processi e di persone. Ed è esattamente il terreno su cui un'impresa, anche piccola, può intervenire con efficacia — perché processi e persone sono ciò che essa governa direttamente.

Il peso delle PMI

Tra le grandi economie avanzate, l'Italia è quella in cui le piccole e medie imprese pesano di più, e di gran lunga.

99%	**63%**	**76%**
delle imprese italiane sono PMI	del valore aggiunto nazionale	dell'occupazione

[1] Fonti: ECB, World Economic Forum, CERTFin (rilevazioni 2025).

Le PMI costituiscono circa il 99% delle imprese italiane. Ma l'elemento che distingue il nostro Paese è un altro: secondo il McKinsey Global Institute, le piccole e medie imprese italiane generano il **63% del valore aggiunto** e il **76% dell'occupazione**, valori superiori alla media delle economie avanzate, dove le PMI si collocano intorno al 50% del prodotto e al 40% dell'occupazione[2].

Ne deriva una conseguenza che merita di essere enunciata chiaramente: in Italia, colpire le piccole e medie imprese significa colpire l'economia reale nella sua parte più ampia. Non si tratta di un comparto marginale, ma del tessuto connettivo del sistema produttivo. La sicurezza dei pagamenti delle PMI cessa così di essere un problema aziendale privato e assume la natura di una questione di interesse generale.

Un'esposizione anomala

Alla centralità economica delle PMI si aggiunge un secondo fattore, che rende il contesto italiano più critico di quello dei principali partner europei. L'Italia è tra i Paesi più colpiti al mondo dalla criminalità informatica, in misura sproporzionata rispetto al proprio peso economico e demografico.

Nel 2025 il Paese ha concentrato il **9,6% degli incidenti cyber gravi rilevati a livello mondiale,** in crescita del 42% sull'anno precedente; gli attacchi fondati su phishing e ingegneria sociale — la materia prima della frode sui pagamenti — sono aumentati del 75%[3].

Il confronto con Francia e Germania è istruttivo. Quelle economie presentano una struttura meno frammentata, con una quota maggiore di valore concentrata in imprese di grande dimensione, per loro natura più presidiate. L'Italia, al contrario, somma due circostanze che altrove non coincidono con la stessa intensità: **la più elevata esposizione alla minaccia** e **la più elevata dipendenza da imprese di piccola dimensione,** che sono anche le meno attrezzate a fronteggiarla. È una sovrapposizione che fa della prevenzione nel segmento corporate una priorità di natura specificamente nazionale.

Va inoltre considerato un mutamento di natura qualitativa. La frode ha cessato di essere

[2] Fonti: ISTAT, Rapporto annuale; McKinsey Global Institute, «A microscope on small businesses», 2024.
[3] Fonte: Clusit, Rapporto sulla Sicurezza ICT in Italia, edizione 2026 (dati 2025).

un fenomeno artigianale e si è **organizzata su scala industriale:** chi attacca non è più, di norma, il singolo truffatore, ma una struttura che opera come un'impresa, con strumenti automatizzati, servizi acquistabili a basso costo, banche dati di vittime già pronte all'uso. Per chi si difende, la conseguenza pratica è una sola: gli attacchi sono più frequenti, più curati e più credibili di un tempo. Ne consegue una riflessione che vale per ogni impresa, grande o piccola: la sicurezza dei pagamenti **non è una questione da lasciare all'informatico.** Non si tratta di un problema tecnico da delegare a chi gestisce i computer, ma di una scelta gestionale che riguarda chi guida l'azienda e chi, ogni giorno, autorizza i pagamenti. È una responsabilità che si esercita con le procedure e con le persone, prima ancora che con la tecnologia.

Difese fragili

Il terzo elemento attiene allo stato di preparazione. Le piccole e medie imprese italiane affrontano questo scenario con difese mediamente modeste e con un atteggiamento che resta, nella maggior parte dei casi, reattivo: ci si occupa della sicurezza dopo aver subito un danno, e di rado prima.

La rilevazione più autorevole, il Cyber Index PMI promosso da Agenzia per la Cybersicurezza Nazionale, Confindustria e Generali, indica che **quasi una PMI su quattro ha subito almeno una violazione informatica nell'ultimo triennio,** dato triplicato rispetto alla rilevazione precedente. A fronte di una minaccia in crescita, il livello di maturità nella gestione del rischio rimane insufficiente, in particolare nelle realtà di minori dimensioni[4].

La ragione è di ordine strutturale. Un intermediario bancario dispone di un centro operativo di sicurezza, di obblighi di vigilanza e di esercitazioni periodiche di crisi. Una piccola impresa dispone, di norma, di un antivirus, di una rete non segmentata e di una credenziale sul gestionale. Per chi conduce l'attacco, il rapporto tra il rischio e il rendimento atteso è, nel secondo caso, incomparabilmente più favorevole. La frode, come ogni attività economica illecita, segue il percorso di minore resistenza.

[4] Fonte: Cyber Index PMI (ACN, Confindustria, Generali), edizione 2025.

Il quadro normativo e le PMI

Vi è infine una circostanza di ordine normativo che completa il quadro. La principale disciplina europea in materia di sicurezza informatica, la **direttiva NIS2** — recepita in Italia con il decreto legislativo 138 del 2024 — adotta come criterio generale l'esclusione delle piccole imprese: gli obblighi gravano in via ordinaria sulle realtà che superano le soglie della media dimensione, ossia oltre cinquanta addetti o dieci milioni di euro di fatturato.

La conseguenza è che la maggior parte delle PMI italiane **resta al di fuori del perimetro degli obblighi diretti,** pur rappresentando la componente più esposta e meno difesa del sistema. Non esiste, allo stato, un quadro di *compliance* di sicurezza cogente e specifico per l'impresa non finanziaria. Sussistono soltanto leve indirette, tra cui il dovere degli amministratori di dotarsi di «adeguati assetti organizzativi» sancito dall'articolo 2086 del Codice civile.

È in questo spazio che il presente manuale si colloca. Non surroga un obbligo inesistente: offre alle imprese un percorso volontario, ordinato e proporzionato, per costruire autonomamente i presidi che la legge non impone ma che la realtà delle minacce rende necessari. Va peraltro osservato che, lungo le catene di fornitura, le PMI sono sempre più spesso tenute di *fatto* a innalzare la propria postura: i committenti di maggiori dimensioni, soggetti alla NIS2, devono presidiare i rischi derivanti dai propri fornitori, e chi non garantisce standard minimi rischia l'esclusione dalle filiere. Ciò che oggi è facoltativo tende, per questa via, a diventare condizione di mercato.

Impianto del manuale

Il volume è concepito per essere consultato, prima ancora che letto. Ogni capitolo muove da una situazione concreta e conduce a uno strumento utilizzabile.
Tre criteri ne definiscono l'impianto.

- **ORDINAMENTO PER SCENARI.** Non un'esposizione di principi, ma la descrizione di ciò che accade — una richiesta di cambio IBAN, un ordine urgente dal vertice — e di come occorre rispondervi.

- **CALIBRAZIONE DIMENSIONALE.** Le medesime procedure sono declinate in forme diverse per la micro-impresa, la piccola impresa e la media impresa strutturata.

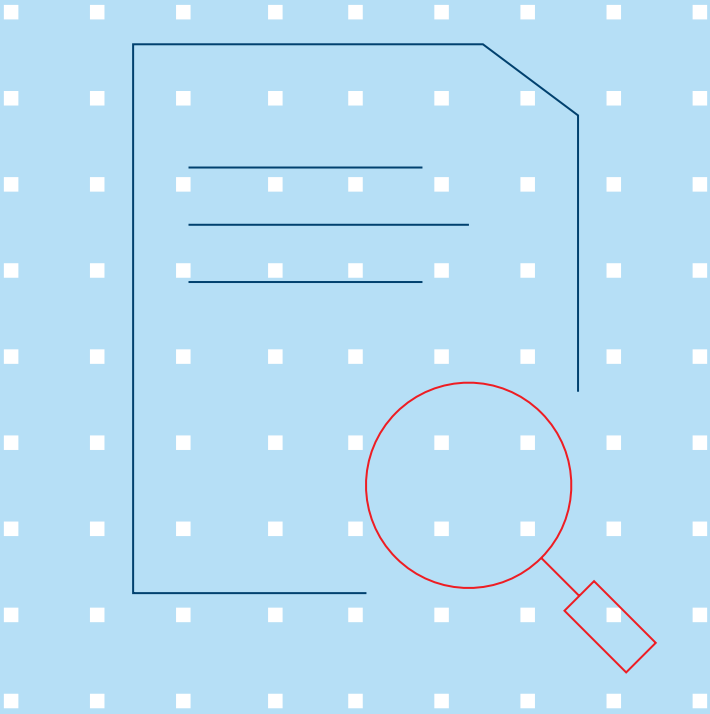
- **STRUMENTI OPERATIVI.** Liste di controllo, modelli, schemi decisionali e percorsi di escalation, destinati all'applicazione immediata.

Lungo l'intero testo ricorrono dei riquadri **CASO**: brevi scenari verosimili, ispirati a frodi realmente avvenute e opportunamente anonimizzati. Ne costituiscono la componente esemplificativa, e mostrano come i principi enunciati si traducano nella pratica quotidiana.

CASO · Anatomia di una frode su fattura

Una PMI manifatturiera del Nord-Est riceve, da un indirizzo identico a quello del fornitore tedesco abituale, la comunicazione di un nuovo IBAN sul quale saldare una fattura di 48.000 euro. L'addetta amministrativa, in rapporto consolidato con quel fornitore, dispone il bonifico. Il conto era controllato da terzi, che avevano violato la casella del fornitore alcune settimane prima. Una sola regola — la verifica di ogni cambio di coordinate tramite un recapito già noto — avrebbe interrotto la sequenza prima del pagamento.

1. CAPIRE IL RISCHIO



Questa prima parte ha una funzione preliminare: definire con precisione il terreno. Prima di ogni procedura occorre comprendere *la logica di chi attacca, la dimensione del fenomeno e la distribuzione del rischio*. I dati che seguono non hanno funzione allarmistica; servono a orientare le difese verso i punti in cui sono effettivamente necessarie.

1.1 La logica del frodatore

La frode contemporanea sui pagamenti è raramente un evento di natura tecnica. Il frodatore, nella maggioranza dei casi, non viola i sistemi dell'intermediario: **induce una persona a disporre il pagamento in prima persona.** È un'inversione che merita attenzione, poiché sposta il fronte difensivo. L'obiettivo non è la macchina, ma la trama di fiducia e di consuetudini su cui si regge il lavoro di chi amministra i pagamenti.

Le leve impiegate sono ricorrenti e, una volta riconosciute, prevedibili: l'urgenza, che comprime il tempo della verifica; l'autorità, che invoca una gerarchia; la riservatezza, che isola il destinatario dal confronto con i colleghi; la familiarità, che si appoggia a un mittente o a un fornitore già noto. L'identificazione di queste leve costituisce il primo presidio, giacché esse rappresentano la traccia comune a quasi ogni tentativo.

1.2 Le tre categorie di frode

Le autorità europee, attraverso le linee guida dell'Autorità Bancaria Europea, distinguono tre categorie di frode sui pagamenti. Non è una classificazione fine a sé stessa: conoscerla aiuta a capire dove, lungo il percorso di un pagamento, ci si può difendere.

EMISSIONE NON AUTORIZZATA

Il frodatore dispone un pagamento al posto del titolare, dopo essersi impossessato dello strumento o delle credenziali — numeri di carta, PIN, codici di accesso all'home banking. Il titolare non ha dato alcun consenso.

MODIFICA DELL'ORDINE

Il frodatore intercetta un ordine di pagamento legittimo e ne altera il contenuto lungo il percorso, ad esempio attraverso un programma malevolo installato sul dispositivo, oppure interviene sui sistemi prima che il pagamento venga eseguito.

MANIPOLAZIONE DEL PAGATORE

È la categoria più insidiosa e, per le imprese, la più rilevante. In essa **è il titolare a disporre il pagamento,** in buona fede, perché tratto in inganno. Vi appartengono le truffe via e-mail, le finte telefonate, la frode del finto amministratore delegato (la cosiddetta CEO fraud) e le frodi sulle fatture. Poiché l'operazione risulta formalmente autorizzata dal titolare, le tutele previste per le operazioni non autorizzate non si attivano, e il recupero delle somme diventa assai più difficile.

CASO · La fattura modificata

Uno studio di consulenza riceve dal proprio fornitore di software una fattura ricorrente, in tutto identica a quelle dei mesi precedenti salvo una riga: le nuove coordinate bancarie, motivate da un «aggiornamento dell'istituto».

Ogni elemento appare coerente — logo, impaginazione, importo. Il pagamento viene disposto. Soltanto tre settimane più tardi, alla telefonata di sollecito del fornitore autentico, emerge che la sua casella di posta era stata compromessa e la fattura intercettata e alterata. Le somme erano già state prelevate da un conto estero. Nessun sistema interno allo studio era stato violato: era bastato un dettaglio modificato su un documento atteso.

1.3 La dimensione del fenomeno

I dati istituzionali più recenti giustificano l'attenzione qui proposta. Conviene leggerli su due livelli distinti: quello generale della criminalità informatica e quello specifico delle frodi sui pagamenti.

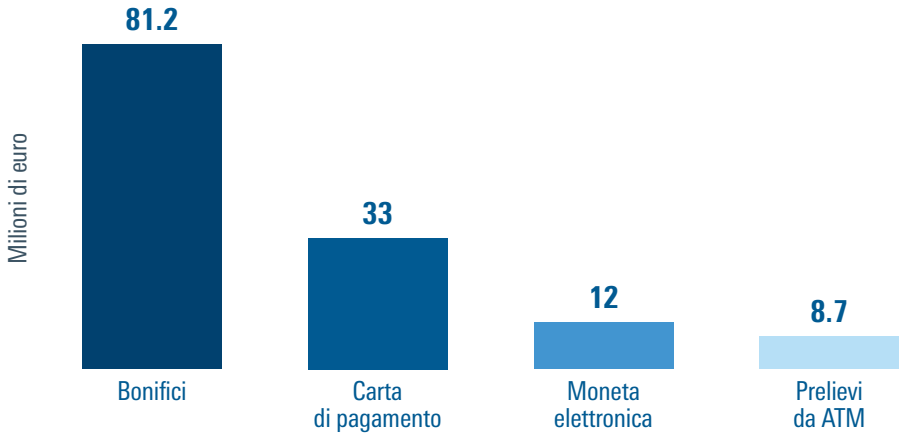
IL QUADRO DEL CYBERCRIME

Nel 2025 l'Italia ha concentrato il **9,6% degli incidenti cyber gravi su scala mondiale,** con una crescita del 42% sull'anno precedente; gli attacchi di phishing e ingegneria sociale sono aumentati del 75% (Clusit, 2026). È una pressione che investe in misura crescente le imprese e che individua nelle PMI il bersaglio meno protetto.

IL QUADRO DEI PAGAMENTI

Sul piano specifico, i dati della Banca d'Italia relativi al primo semestre 2025 indicano nel **bonifico lo strumento con il maggior valore di operazioni fraudolente**. A fronte di una pluralità di strumenti di pagamento, il valore delle frodi si concentra in misura nettamente prevalente su di esso.

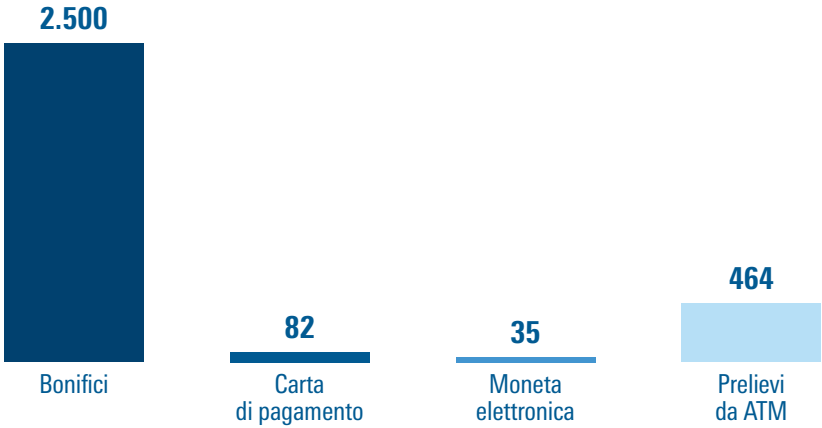
Valore delle operazioni fraudolente per strumento (€ milioni)



Elaborazione su dati Banca d'Italia – Comitato Pagamenti Italia, I semestre 2025.

Il dato sul valore complessivo, tuttavia, racconta solo una parte. L'elemento che dovrebbe interessare più da vicino un'impresa è **quanto costa una singola frode.** E qui il divario tra gli strumenti diventa abissale: la frode media su un bonifico vale circa trenta volte quella su una carta di pagamento.

Importo medio di una singola operazione fraudolenta (€)



Elaborazione su dati Banca d'Italia – Comitato Pagamenti Italia, I semestre 2025.

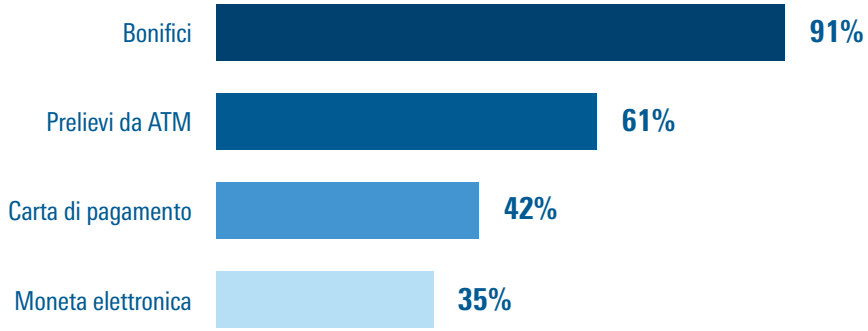
La ragione è intuitiva: una carta ha massimali contenuti, un bonifico no. Per un'impresa, il messaggio è che il pericolo non si misura nella frequenza degli attacchi, ma nel **valore unitario di quelli che vanno a segno.** Una sola frode su bonifico può pesare quanto centinaia di frodi su carta.

Vi è infine la fattispecie prevalente. Per i bonifici, la frode più diffusa è ormai la *manipolazione del pagatore* — circa il 74% del valore — e per le imprese il dato si accentua: le rilevazioni di CERTFin indicano che, nel segmento corporate, una quota assai rilevante delle frodi si conclude attraverso la *Business Email Compromise,* ossia la compromissione o l'imitazione della posta aziendale[5].

[5] Fonti: Banca d'Italia – Comitato Pagamenti Italia, I semestre 2025; CERTFin, rilevazioni sul segmento corporate.

Un ultimo dato merita di essere fissato, poiché smentisce una convinzione assai diffusa: nel caso dei bonifici, **il 91% del valore delle perdite da frode permane in capo al cliente,** e non all'intermediario.

Quota delle perdite da frode a carico del cliente, per strumento



Elaborazione su dati Banca d'Italia – Comitato Pagamenti Italia, I semestre 2025.

La ragione è tecnica ma dirimente: quando è il titolare a disporre l'operazione — come accade nella manipolazione — le tutele previste per le operazioni non autorizzate non trovano applicazione. In termini concreti, nella maggioranza dei casi il costo di una frode su bonifico grava sull'impresa. È questa la combinazione che rende il fenomeno tanto insidioso: lo strumento più colpito è anche quello dalla frode più costosa, ed è quello su cui la perdita resta, quasi sempre, a chi paga.

1.4 Da dove proviene il rischio

Per difendersi conviene sapere da dove arriva l'attacco. Pur nella varietà degli scenari concreti — che la Parte II tratterà uno per uno — i canali attraverso cui un tentativo di frode raggiunge l'impresa sono pochi e ricorrenti. La frode contemporanea non si inventa ogni volta una strada nuova: ne percorre alcune, collaudate, e le combina. Conoscerle consente di alzare la guardia nei punti giusti, anziché disperdere l'attenzione.

- **LA POSTA ELETTRONICA.** È il canale principale e il più redditizio per chi attacca. Opera in due modi: con l'imitazione, creando un indirizzo quasi identico a quello reale che inganna una lettura distratta; oppure con la compromissione, prendendo il controllo della casella autentica di un fornitore o di un collega e inserendosi in conversazioni già in corso. Nel secondo caso non vi è alcun dettaglio fuori posto — il messaggio arriva davvero dal mittente atteso — e per questo è la forma più difficile da riconoscere. Si deve tenere conto che la PEC non è immune da questi rischi e non garantisce l'identità del mittente.

- **IL TELEFONO E I MESSAGGI.** Quasi sei frodi su dieci iniziano con una telefonata o un SMS. Il telefono aggiunge ciò che l'e-mail non ha: una voce,un tono rassicurante o autorevole, la pressione dovuta a un'urgenza immediata che non lascia margine per riflettere. Un SMS che sembra provenire dalla banca, una chiamata di un finto tecnico o di un finto incaricato sono efficaci proprio perché la conversazione dal vivo abbassa la diffidenza e riduce l'impulso di effettuare una verifica a freddo.

- **I CANALI EMERGENTI.** Social media e applicazioni di messaggistica crescono rapidamente come punto di primo contatto. Sono particolarmente insidiosi nelle imprese piccole, dove il confine tra account personale e aziendale è labile: un messaggio che arriva sul profilo privato del titolare elude del tutto i controlli previsti per i canali aziendali.

- **I DISPOSITIVI E GLI ACCESSI.** Un computer infettato da un programma malevolo o una credenziale sottratta aprono la porta direttamente, senza bisogno di ingannare nessuno. È il canale più «tecnico» e, oggi, meno frequente degli altri — proprio perché l'autenticazione a più fattori lo ha reso più

arduo — ma resta rilevante e, quando riesce, particolarmente difficile da individuare in tempo[6].

Un punto accomuna i quattro canali e merita di essere reso esplicito: nella grande maggioranza dei casi essi non servono a *scavalcare* le difese tecniche dell'impresa, ma a *convincere una persona ad agire*. Il canale è il mezzo; l'obiettivo è sempre la decisione di chi sta davanti allo schermo o al telefono.

A questi canali corrispondono alcuni punti deboli ricorrenti: i momenti in cui il processo sicuro collegato al pagamento fallisce. Non sono vulnerabilità tecnologiche, ma passaggi del processo in cui manca una verifica. Tre, in particolare, ritornano in quasi ogni frode.

- **IL CAMBIO DELLE COORDINATE.** È il singolo punto di rottura più sfruttato. Una variazione di IBAN comunicata via e-mail e recepita senza un controllo su un canale indipendente consente di dirottare un pagamento dovuto, legittimo nell'importo e nella causale, verso un conto controllato dal frodatore. L'impresa crede di pagare il proprio fornitore, e lo sta facendo davvero — solo, sul conto sbagliato.

- **L'AUTORIZZAZIONE SOLITARIA.** Quando una sola persona può condurre un pagamento dall'inizio alla fine — disporlo e confermarlo — senzache nessun altro lo veda, viene a mancare il controllo incrociato che intercetterebbe l'inganno. È la condizione tipica della micro-impresa, ma si ritrova anche in realtà più grandi quando le procedure sono informali.

- **L'URGENZA NON VERIFICATA.** Quasi ogni frode impone fretta e scoraggia il controllo: «paga subito», «è riservato», «non coinvolgere nessuno». L'urgenza è una leva deliberata, perché comprime il tempo in cui una verifica sarebbe possibile. Una richiesta che, insieme al denaro, chiede anche di rinunciare a controllare è per tali motivi sospetta.

Quattro canali, tre punti di rottura. Su questo schema — semplice, ma sorprendentemente costante nel tempo e tra i Paesi — si regge la quasi totalità delle frodi sui pagamenti che colpiscono le imprese. È una buona notizia, in fondo: un numero

[6] Riferimenti: ECB, World Economic Forum, CERTFin (rilevazioni 2025).

limitato di varchi è anche un numero limitato di punti da presidiare. La Parte II declinerà lo schema negli scenari concreti; per ora basti trattenere il principio che li riassume tutti: **la frode entra dove la verifica manca oppure è evitabile.**

1.5 Il caso dei pagamenti istantanei

Un'attenzione particolare merita il bonifico istantaneo, perché concentra in sé due tendenze destinate ad aggravare il rischio per le imprese: una di natura tecnica, l'altra di natura strutturale.

Sul piano tecnico, l'istantaneo è **irrevocabile e immediato.** Il denaro raggiunge il conto del beneficiario in pochi secondi, in qualunque momento del giorno, e non esiste, di fatto, una finestra utile per accorgersi dell'errore e bloccare l'operazione. Nel bonifico ordinario un margine, sia pure ridotto, talvolta esiste; nell'istantaneo no. Questo trasforma un tentativo andato a segno in una perdita pressoché certa e definitiva, e sposta tutto il peso della difesa a *monte del pagamento:* sulla verifica, non sul recupero. Quando l'ordine parte è troppo tardi.

Sul piano strutturale, l'uso dell'istantaneo è destinato a crescere rapidamente. Le recenti evoluzioni normative europee ne hanno favorito la diffusione — equiparandone le condizioni a quelle del bonifico ordinario e rimuovendo i precedenti limiti di importo — al punto che il pagamento istantaneo è stato riconosciuto come strumento di riferimento dei pagamenti europei. Più imprese lo adotteranno, più aumenterà l'esposizione complessiva. Le rilevazioni di settore già lo confermano: in alcuni Paesi **fino al 60% delle frodi è riconducibile a pagamenti istantanei,** e il valore medio di una frode su questo strumento è in costante aumento, su livelli sensibilmente superiori a quelli del bonifico ordinario[7].

La conseguenza per un'impresa è netta e va enunciata senza ambiguità: **sul bonifico istantaneo non esiste rete di sicurezza a valle.** L'unica difesa efficace è la verifica prima di disporre, ad oggi supportata (ma non pienamente risolta) nei sistemi di internet banking dalla verifica VOP (Verification of Payee). È un punto che ritornerà, in forma operativa, negli scenari della Parte II e nella governance dei pagamenti della Parte III.

[7] Riferimenti: ECB, World Economic Forum, CERTFin (rilevazioni 2025); quadro europeo sui pagamenti istantanei.

1.6 La distribuzione del rischio

L'esposizione non è uniforme, né per intensità né per tipologia di scenario. Una mappatura commisurata alla dimensione dell'impresa consente di concentrare gli sforzi dove più servono. Costituisce il presupposto dell'intero manuale e sarà ripresa, in termini operativi, nella Parte III.

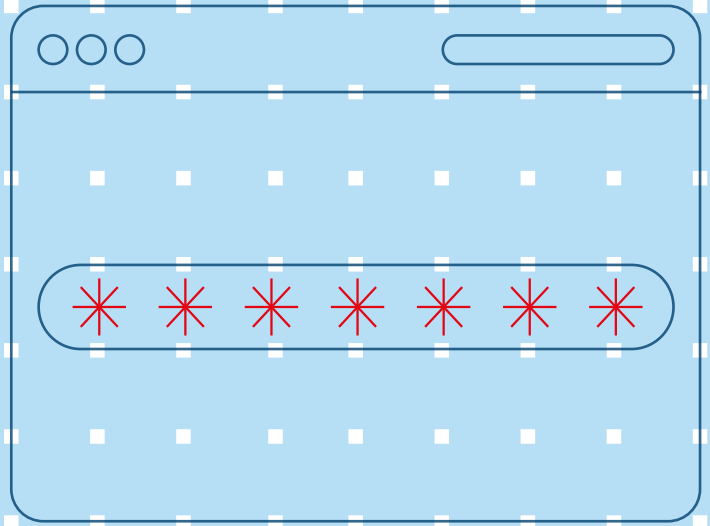
- **MICRO-IMPRESA.** Una sola persona, di norma il titolare, concentra tutti i poteri dispositivi. Ne derivano massima rapidità e assenza di controllo incrociato: lo scenario più pericoloso è la richiesta urgente che elude ogni verifica.

- **PICCOLA IMPRESA**. Compare una funzione amministrativa, ma le procedure restano informali. Lo scenario tipico è la frode sulla fattura del fornitore, che trae vantaggio proprio dall'assenza di una verifica strutturata dei cambi di coordinate.

- **MEDIA IMPRESA STRUTTURATA.** Esistono una funzione amministrativa articolata e una catena autorizzativa; tuttavia la maggiore complessità amplia la superficie d'attacco — più persone, più caselle, più deleghe. Qui assumono rilievo la separazione dei compiti e la doppia autorizzazione.

Nelle pagine seguenti ciascun profilo troverà procedure calibrate sulla propria realtà. La sicurezza dei pagamenti non si presta a una misura unica: è un assetto che va adattato all'impresa cui si applica.

2. GLI SCENARI OPERATIVI



2.1 Il cambio dell'IBAN di un fornitore

È lo scenario più frequente e, in valore, il più dannoso per le imprese. Si riceve la comunicazione che un fornitore abituale ha cambiato le proprie coordinate bancarie: una e-mail, talvolta una lettera su carta intestata, che chiede di indirizzare i pagamenti futuri — o una fattura già emessa — verso un nuovo IBAN. La richiesta arriva nel contesto di un rapporto reale, su una fornitura reale, per un importo plausibile. Tutto torna, tranne il conto di destinazione, che appartiene al frodatore.

La compromissione può avvenire in due modi: il frodatore ha violato la casella di posta del fornitore e scrive dal suo indirizzo autentico, inserendosi nella corrispondenza; oppure imita l'indirizzo con una variazione minima, difficile da cogliere. Nel primo caso non esiste alcun dettaglio tecnico fuori posto: è per questo che la difesa non può fondarsi sull'aspetto del messaggio, ma deve poggiare su una verifica esterna al canale da cui la richiesta proviene.

Dal 2025 le imprese dispongono di un aiuto in più. Le banche sono ora tenute a offrire un servizio di **verifica del beneficiario** — indicato anche con la sigla inglese *VoP, Verification of Payee* — che, prima della conferma di un bonifico, confronta il nome del titolare del conto di destinazione con l'IBAN inserito e segnala le eventuali discrepanze. Poiché un IBAN fraudolento è quasi sempre intestato a un soggetto diverso dal fornitore atteso, una *mancata corrispondenza* tra nome e conto è un campanello d'allarme prezioso. È uno strumento utile, ma non infallibile — i criminali ricorrono talvolta a conti intestati a nomi di comodo simili a quello atteso — e per questo affianca la verifica diretta con il fornitore, senza sostituirla.

Conviene comprendere perché questo schema è tanto efficace. Quando i criminali violano la casella di posta di un fornitore — ciò che si chiama *presa di controllo dell'account* — non ottengono solo un indirizzo da cui scrivere: ottengono l'archivio delle fatture, gli importi ricorrenti, il calendario dei pagamenti, perfino il tono delle conversazioni. La richiesta di cambio IBAN che ne deriva non è un tentativo alla cieca, ma un messaggio calibrato su informazioni vere, inserito nel momento esatto in cui un pagamento è atteso. È questo che lo rende quasi indistinguibile da una comunicazione legittima — e che impone di non fidarsi mai dell'aspetto, ma solo di una verifica condotta su un canale indipendente.

LA PROSPETTIVA DELL'ATTACCANTE

Il suo lavoro comincia molto prima della richiesta, e altrove. Il bersaglio iniziale non è l'impresa che pagherà, ma un anello più debole della sua filiera — un fornitore, un cliente, uno studio. Violata quella casella di posta, l'attaccante non la legge a mano: imposta filtri automatici su parole chiave come «fattura», «pagamento», «IBAN», «coordinate», «scadenza», e lascia che siano i messaggi stessi a segnalarsi. In pochi giorni, senza fatica, ricostruisce la mappa dei pagamenti: chi paga chi, con quale cadenza, per quali importi, con quale tono.

Poi aspetta. La pazienza, qui, è una virtù professionale: osserva per settimane, impara il ritmo delle scadenze e lo stile delle persone, e sceglie la fattura giusta — un importo alto ma non anomalo, coerente con la storia del rapporto — e il momento giusto, quello in cui quel pagamento è atteso e una richiesta di conferma delle coordinate appare del tutto naturale.

A quel punto decide come inserirsi, e ha due strade. Può registrare un dominio quasi identico a quello reale — una lettera cambiata, un «.it» al posto di un «.com», un carattere che a colpo d'occhio non si distingue — e scrivere da lì. Oppure, caso ben più insidioso, può operare direttamente dalla casella autentica che controlla, inserendosi in una conversazione già aperta: il messaggio parte davvero dal mittente atteso, prosegue un carteggio reale, cita documenti veri. Nessun filtro lo ferma, nessun sospetto lo precede.

È qui la sua forza, e insieme il suo limite. La sua forza: non fabbrica nulla di falso, devia soltanto un pagamento che sarebbe partito comunque, e un singolo colpo ben piazzato ripaga settimane di attesa. Il suo limite: tutto l'inganno poggia sull'abitudine a trattare per iscritto. L'unica mossa che non ha modo di controllare è una telefonata al fornitore, su un numero già noto, per chiedere conferma a voce. È esattamente ciò su cui conta che nessuno faccia.

SEGNALI D'ALLARME

- Una variazione di IBAN comunicata via e-mail, soprattutto se presentata come urgente o accompagnata da un sollecito di pagamento.
- Un IBAN estero, o intestato a un soggetto diverso dal fornitore, quando in precedenza il conto era nazionale e coerente.
- Piccole differenze nell'indirizzo del mittente, nella firma, nel tono della comunicazione rispetto agli scambi abituali.
- La richiesta di non telefonare per confermare, o l'indicazione di un nuovo recapito telefonico «per qualsiasi verifica».

COSA FARE

Verifica rapida

1. Non utilizzare i recapiti contenuti nella comunicazione che annuncia il cambio.
2. Telefonare al fornitore su un numero già noto e usato in passato, e farsi confermare a voce la variazione.
3. Prestare attenzione all'esito della verifica del beneficiario (VoP) che la banca mostra al momento del pagamento: se segnala che il nome non corrisponde all'IBAN, fermarsi.
4. Sospendere il pagamento fino a conferma avvenuta: nessuna urgenza giustifica di saltare questo passo.

Procedura ordinaria

1. Stabilire come regola fissa che ogni modifica di coordinate sia validata su un canale diverso da quello della richiesta (telefono verso un numero in anagrafica).
2. Registrare la variazione in anagrafica fornitori solo dopo la conferma, annotando chi ha verificato e quando.
3. Per i primi pagamenti sul nuovo IBAN, valutare un importo ridotto di prova quando la natura della fornitura lo consente.

Escalation

1. Se il pagamento è già partito, contattare immediatamente la banca per tentare il richiamo delle somme: i primi minuti sono decisivi.
2. Informare il fornitore reale, la cui casella potrebbe essere compromessa e usata anche verso altri clienti.
3. Procedere con la denuncia e con le segnalazioni dovute (si veda la Parte V).

CASO · La fattura modificata

Un'azienda agricola riceve dal fornitore di mangimi una e-mail con la richiesta di aggiornare l'IBAN per la fattura in scadenza. Il messaggio proviene dall'indirizzo corretto del fornitore e cita correttamente numero e importo della fattura. L'addetto aggiorna l'anagrafica e paga 26.000 euro. La casella del fornitore era stata violata e i criminali ne monitoravano la posta da settimane, in attesa di una fattura su cui inserirsi. La verifica telefonica su un numero già noto — quello del commerciale con cui l'azienda parlava ogni settimana — avrebbe smascherato la frode in trenta secondi.

2.2 La richiesta urgente dal vertice

Conosciuta anche come *frode del finto amministratore delegato,* colpisce chi, all'interno dell'impresa, ha facoltà di disporre pagamenti — il personale amministrativo, il responsabile finanziario, talvolta lo stesso titolare di una controllata. Il frodatore si presenta come una figura apicale, reale e riconoscibile, e richiede un bonifico straordinario, urgente e riservato: un'acquisizione in via di definizione, un pagamento sbloccato all'ultimo, un'operazione «che solo tu puoi gestire».

La forza dello schema non sta nella tecnologia, ma nella combinazione di tre leve psicologiche: l'*autorità* di chi impartisce l'ordine, l'*urgenza* che impedisce di riflettere, la *riservatezza* che isola la vittima e le impedisce di chiedere conferma ai colleghi. La gerarchia, in questo schema, è un'arma: disobbedire a un superiore costa, e il frodatore conta esattamente su questo.

Anche qui la credibilità nasce da un lavoro preparatorio. Prima di colpire, il frodatore studia l'impresa: chi è l'amministratore delegato, chi gestisce i pagamenti, come sono strutturate le comunicazioni interne. Molte di queste informazioni sono pubbliche — il sito aziendale, i profili sui social — e altre provengono da una casella di posta già compromessa, magari quella di un fornitore o di un collega. Quando arriva, la richiesta cita i nomi giusti e i toni giusti: sembra autentica perché è *costruita su dati reali.* È la ragione per cui non ci si può affidare alla sola impressione di familiarità, ma occorre una verifica indipendente.

LA PROSPETTIVA DELL'ATTACCANTE

Prima di scrivere, studia. L'organigramma e i ruoli li ricava da fonti aperte — il sito aziendale, i profili professionali, le notizie —; il tono, la firma, le formule ricorrenti li copia da e-mail intercettate. Quando la richiesta arriva, **sa già chi comanda, chi paga e come si scrivono tra loro:** non deve fingere una relazione, la conosce.

La sua arma è la combinazione di tre leve. L'**autorità**, perché una richiesta che sembra venire dal vertice inibisce la verifica; l**'urgenza,** perché la fretta spegne il pensiero critico; la **segretezza,** che è la più sottile. Non è teatralità: la riservatezza imposta («non parlarne con nessuno finché non torno») serve a un solo scopo, *isolare la vittima dall'unico controllo che teme davvero* — la domanda a un collega.

Sceglie anche il terreno temporale con cura: il venerdì pomeriggio, la vigilia di una chiusura, un momento in cui il dirigente vero è irraggiungibile — dettaglio che spesso ricava da un post o da un messaggio di fuori sede. Conta sull'asimmetria gerarchica: disobbedire a un superiore costa, chiedergli conferma sembra sfiducia. Per questo l'unica difesa che regge non è il fiuto, ma una regola che rende *normale e dovuto verificare,* a prescindere da chi firma la richiesta.

SEGNALI D'ALLARME

- Una richiesta di pagamento che proviene «dall'alto» ma arriva per iscritto, via e-mail o messaggio, anziché attraverso i canali abituali.
- L'insistenza sulla segretezza: non parlarne con colleghi, non seguire le procedure ordinarie «vista l'eccezionalità».
- L'urgenza estrema, con scadenze di poche ore e la pressione a completare l'operazione prima di un termine.
- La destinazione insolita: un beneficiario nuovo, spesso estero, e un importo elevato rispetto all'operatività corrente.

COSA FARE

Verifica rapida

1. Confermare la richiesta con il presunto mittente di persona o su un suo recapito noto (es. chiamando il mittente direttamente), mai rispondendo al messaggio ricevuto.

2. Considerare la riservatezza richiesta non come un vincolo, ma come un motivo in più per verificare.
3. Non lasciarsi condizionare dall'urgenza: un'operazione legittima regge una pausa di pochi minuti per un controllo.

Procedura ordinaria

1. Stabilire che nessun pagamento straordinario possa essere disposto sulla sola base di un'e-mail o di un messaggio, a prescindere dal mittente apparente.
2. Introdurre, per i pagamenti oltre una certa soglia, il principio del doppio controllo — in inglese four eyes: chi dispone il pagamento e chi lo approva devono essere due persone diverse, così che nessuno possa portare a termine da solo un'operazione (si veda la Parte III).
3. Comunicare apertamente, a tutti i livelli, che la verifica di una richiesta del vertice è dovuta e gradita, mai una mancanza di fiducia.

Escalation

1. Se il pagamento è stato eseguito, contattare immediatamente la banca per il tentativo di richiamo e bloccare eventuali operazioni successive.
2. Informare senza indugio la persona di cui è stata usurpata l'identità e i vertici aziendali.
3. Conservare i messaggi ricevuti e procedere con denuncia e segnalazioni (si veda la Parte V).

CASO · Un messaggio dall'amministratore delegato

La responsabile amministrativa di una media impresa riceve un messaggio, apparentemente dall'amministratore delegato in viaggio all'estero, che annuncia un'acquisizione riservata e chiede un bonifico urgente di 90.000 euro a un nuovo fornitore, raccomandando la massima discrezione fino al rientro. Il tono e la firma sono convincenti. Prima di disporre, la responsabile chiama il cellulare dell'amministratore — non per sfiducia, ma perché è la regola interna per ogni pagamento straordinario. L'amministratore cade dalle nuvole. Il bonifico non parte. La regola, applicata senza eccezioni, aveva fatto il suo lavoro.

2.3 La telefonata della finta banca o del finto tecnico

Il frodatore telefona presentandosi come operatore della banca — spesso dell'«ufficio sicurezza» o «antifrode» — o come tecnico informatico. Annuncia un problema urgente: un addebito sospetto da bloccare, un tentativo di accesso da respingere, un aggiornamento di sicurezza da completare. L'obiettivo è uno solo: indurre l'interlocutore a comunicare codici di accesso o codici usa e getta (gli OTP ricevuti via SMS), oppure a disporre un'operazione «per mettere in sicurezza il conto».

Due elementi rendono lo schema insidioso. Il primo è che il numero visualizzato può coincidere con quello reale della banca: esistono tecniche che falsificano il chiamante, perciò l**a provenienza apparente di una telefonata non prova nulla.** Il secondo è la regia emotiva: chi chiama si presenta come colui che vuole proteggervi, e così trasforma la diffidenza naturale in collaborazione. Vale un principio semplice e senza eccezioni: la banca non chiede mai codici, password od OTP, né chiede mai di spostare denaro su un «conto sicuro».

C'è un terzo elemento, spesso sottovalutato, che spiega perché certe telefonate risultano così convincenti. La compromissione della casella di un fornitore o di una controparte non serve solo a dirottare i pagamenti via e-mail: mette in mano al frodatore una **conoscenza dettagliata dell'impresa** — fatture in corso, importi, nomi delle persone, rapporti aperti. Con questo bagaglio, la telefonata non è più generica: è un attacco mirato a chi gestisce i pagamenti, che cita un numero di fattura reale, un fornitore reale, una scadenza reale. La vittima si fida proprio perché «questo qui sa tutto». Riconoscere che le informazioni vere, in mano a un estraneo, non garantiscono la sua identità è il salto di consapevolezza decisivo.

LA PROSPETTIVA DELL'ATTACCANTE

Dietro la telefonata c'è spesso una struttura, non un individuo: postazioni, copioni collaudati, obiezioni già previste e, sullo schermo, i **dati veri della vittima** — nome, banca, magari un'operazione reale recente, ottenuti da una violazione o da una casella compromessa. È questo che trasforma una telefonata generica in un attacco mirato: chi chiama «sa cose», e sapere cose, per la vittima, equivale a essere legittimo.

La falsificazione del numero è solo l'apri-pista: costa pochi euro e serve a **superare i primi dieci secondi di diffidenza,** quelli in cui la vittima decide se stare al gioco. Da lì entra in scena la regia emotiva. Prima l'allarme — un addebito sospetto, un accesso anomalo, un conto a rischio —; poi la figura rassicurante che «è qui per aiutare». Spavento e sollievo, in rapida successione, disattivano il controllo meglio di qualunque argomento.

Il resto è una corsa contro il tempo. Ogni minuto in cui tiene la vittima in linea gioca per lui; l'istante in cui lei *riaggancia per verificare* è quello in cui perde. Per questo la pressione non cala mai: una finestra che si chiude, un blocco imminente, un codice «da confermare subito». L'unica contromisura che disinnesca l'intero schema è banale e per lui fatale: chiudere e richiamare la banca per conto proprio, sui recapiti dell'app o della filiale — non su quelli che lui stesso ha fornito.

SEGNALI D'ALLARME

- Una telefonata «dalla banca» che segnala un problema urgente e chiede di agire immediatamente.
- La richiesta di comunicare codici di accesso, password o codici usa e getta (OTP) ricevuti via SMS.
- L'invito a spostare i fondi su un «conto sicuro» o «conto di transito» per proteggerli.

COSA FARE

Verifica rapida

1. Chiudere la conversazione e contattare la banca per conto proprio, usando i

recapiti presenti nell'home banking o nell'app, oppure rivolgendosi direttamente al personale della filiale.
2. Non comunicare mai codici, password o OTP: nessun operatore legittimo li chiede al telefono.
3. Non eseguire alcuna operazione dettata durante la chiamata, per quanto urgente venga presentata. È buona prassi non rispondere mai 'si' o 'confermo' in una chiamata di questo tipo.

Procedura ordinaria

1. Istruire chiunque gestisca i pagamenti sul principio che la banca non chiede mai codici né di spostare denaro, e che conoscere dettagli riservati non prova l'identità di chi chiama.
2. Individuare un punto di contatto interno cui segnalare telefonate sospette, così da avvisare rapidamente gli altri.
3. Concordare con la banca quali siano i suoi canali ufficiali e diffidare di qualunque altro.

Escalation

1. Se sono stati comunicati codici o eseguite operazioni, contattare subito la banca sui canali ufficiali per bloccare conto e disposizioni in corso.
2. Modificare immediatamente le credenziali di accesso eventualmente compromesse.
3. Procedere con denuncia e segnalazioni (si veda la Parte V).

CASO · L'ufficio antifrode che non esisteva

Il titolare di una piccola impresa riceve la telefonata di un sedicente operatore dell'ufficio antifrode della sua banca: sul display compare proprio il numero della filiale. L'operatore conosce un bonifico realmente disposto nei giorni precedenti — informazione che lo fa apparire autentico — e, «per bloccare un addebito sospetto», chiede di leggere il codice appena arrivato via SMS. Il titolare lo detta. Quel codice autorizzava, in realtà, un bonifico predisposto dal frodatore. Una sola contromisura avrebbe retto: chiudere la chiamata e contattare la banca per conto proprio, con i recapiti dell'home banking o della filiale, da cui sarebbe emerso che nessun addebito sospetto era mai esistito.

2.4 L'applicazione o il programma da installare

Dopo un primo contatto telefonico, il frodatore induce la vittima a **installare un'applicazione o un programma:** una finta app della banca, un finto aggiornamento di sicurezza, o un software di «assistenza remota» che — si dice — serve al tecnico per risolvere il problema. Una volta installato, lo strumento intercetta credenziali e codici, oppure consente al frodatore di vedere lo schermo e comandare il dispositivo a distanza, disponendo operazioni mentre la vittima è ancora al telefono.

Questo scenario merita un'attenzione particolare nelle piccole e medie imprese, per una ragione concreta. Le PMI raramente forniscono ai collaboratori telefoni o computer aziendali; e quando lo fanno, di rado dispongono di strumenti per controllare centralmente quali applicazioni vi vengono installate. Ne consegue che lo **stesso dispositivo personale** usato per le app di tutti i giorni è anche quello con cui si accede all'home banking aziendale, senza alcun filtro su ciò che vi si installa. La superficie di rischio si concentra così su un singolo telefono, fuori da ogni presidio. La prudenza su ciò che si installa diventa, in questo contesto, la prima linea di difesa.

LA PROSPETTIVA DELL'ATTACCANTE

Cerca i dispositivi che nessuno governa, e nelle piccole imprese ne trova in abbondanza. Il telefono personale usato anche per il lavoro è **terreno libero**: nessuna regola su ciò che vi si installa, nessun controllo centrale, nessuna separazione tra l'app della banca e tutto il resto. È la superficie ideale, perché la sua debolezza non è tecnica ma organizzativa — e quindi invisibile a chi la usa.

Non forza nulla: **si fa invitare.** Un pretesto tecnico — un aggiornamento, un problema da risolvere, un'assistenza premurosa — e la vittima installa da sé lo strumento che la tradirà: un'app che intercetta i codici, un programma di controllo remoto che consegna il dispositivo. L'inganno non aggira una difesa, *ne prende in prestito le chiavi,* offerte spontaneamente.

E una volta dentro non ha fretta. Può osservare l'operatività, imparare le abitudini, attendere l'operazione giusta. È la differenza che lo rende pericoloso: non un colpo

mordi-e-fuggi, ma una presenza silenziosa che sceglie il momento. Ciò che teme è tutto ciò che riduce quel terreno libero — un dispositivo dedicato ai pagamenti, la regola di non installare nulla su richiesta altrui, la diffidenza verso ogni «assistenza» non cercata.

SEGNALI D'ALLARME

- L'invito, al telefono o via messaggio, a installare un'app o un programma per «risolvere un problema» o «aggiornare la sicurezza».
- App proposte tramite link diretti, allegati o fonti diverse dagli store ufficiali (App Store, Google Play).
- La richiesta di installare software di «assistenza remota», che consente a un terzo di vedere e comandare il dispositivo.
- App che, una volta avviate, chiedono permessi sproporzionati: accesso agli SMS, ai contatti, o il controllo dello schermo.

COSA FARE

Verifica rapida

1. Non installare nulla su indicazione di chi ha telefonato o scritto: nessun tecnico legittimo lo chiede in questo modo.
2. **Scaricare le applicazioni soltanto dagli store ufficiali, verificando editore e recensioni. In caso di dubbio contattare immediatamente il servizio clienti della banca.**
3. Non concedere mai a sconosciuti l'accesso remoto al proprio dispositivo.

Procedura ordinaria

1. Per quanto possibile, tenere distinto il dispositivo usato per i pagamenti aziendali da quello di uso personale.
2. Limitare allo stretto necessario le app installate sul dispositivo che accede all'home banking, e rivedere periodicamente i permessi concessi.
3. Mantenere sempre aggiornati sistema operativo e applicazioni, attingendo solo agli store ufficiali.
4. Se l'impresa fornisce i dispositivi, valutare strumenti che permettano di governare le applicazioni installabili.

Escalation

1. Se è stata installata un'app sospetta o concesso un accesso remoto, scollegare subito il dispositivo dalla rete e contattare la banca.
2. Disinstallare l'applicazione, cambiare le credenziali da un dispositivo sicuro e controllare i movimenti del conto.
3. Far esaminare il dispositivo prima di riutilizzarlo per i pagamenti; procedere con denuncia e segnalazioni (Parte V).

CASO · L'app per «mettere in sicurezza» il conto

Dopo la telefonata di un finto tecnico della banca, il titolare di una ditta individuale viene convinto a installare sul proprio telefono — lo stesso che usa per l'internet banking — un'applicazione di assistenza remota, «così il tecnico può sistemare tutto da solo». Da quel momento il frodatore vede lo schermo in tempo reale e legge i codici in arrivo. Nel giro di pochi minuti dispone due bonifici mentre il titolare, ancora al telefono, crede che si stia risolvendo il problema. Sul quel telefono non esisteva alcuna separazione tra uso personale e aziendale, né alcun controllo sulle installazioni.

2.5 La finta fattura fuori dal Sistema di Interscambio

A differenza del cambio IBAN, dove la fattura è autentica e sbagliato è solo il conto, qui la richiesta di pagamento è in sé illegittima: una fattura per beni mai ordinati, un finto rinnovo di un dominio o di un'iscrizione a un registro, un sollecito per un abbonamento mai sottoscritto. In Italia, però, questo schema incontra un ostacolo strutturale che conviene conoscere e sfruttare a proprio vantaggio.

Tra imprese italiane la fattura è **elettronica e obbligatoria,** e transita per il **Sistema di Interscambio (SdI)** dell'Agenzia delle Entrate, che la veicola, la registra e la recapita nel cassetto fiscale del destinatario. Un frodatore non può emettere una fattura elettronica valida a nome di un fornitore: gli mancano l'identità fiscale e l'accesso al sistema. Di conseguenza ripiega su documenti che *imitano* una fattura ma non sono mai passati dallo SdI — un PDF allegato a un'e-mail, un modulo cartaceo, un sollecito dall'aspetto ufficiale. Ed è proprio questo il punto debole dell'inganno e la cartina di tornasole per l'impresa: **una richiesta di pagamento che non corrisponde a una fattura elettronica realmente ricevuta tramite lo SdI è, per ciò stesso, sospetta.**

Resta qualche ambito in cui la verifica va condotta con più attenzione, perché la fattura elettronica non si applica o si applica diversamente: i fornitori esteri, alcuni regimi particolari, i pagamenti verso soggetti non imprenditori. In questi casi vale comunque il principio generale del riscontro interno: nessun pagamento senza un ordine che lo giustifichi e senza la conferma di aver ricevuto il bene o il servizio.

LA PROSPETTIVA DELL'ATTACCANTE

Qui non punta sulla precisione, ma sui grandi numeri. Invia migliaia di richieste pressoché identiche, con importi **calibrati sotto la soglia dell'attenzione** — piccoli abbastanza da non richiedere un'autorizzazione, plausibili abbastanza da sembrare routine — e una grafica che imita un ente ufficiale o un fornitore di servizi. Non gli serve ingannare tutti: gli basta che una minima frazione paghi senza guardare.

La sua è una scommessa lucida. Sa perfettamente di **non poter emettere una fattura elettronica valida:** gli mancano l'identità fiscale e l'accesso al Sistema di

Interscambio. Per questo ripiega su ciò che una fattura la *imita* soltanto — un PDF, un modulo, un sollecito cartaceo — e punta tutto sul fatto che l'impresa non sappia che proprio questo lo smaschera: se non è passato dallo SdI, non è una fattura.

L'economia dell'attacco spiega la sua persistenza. Con un costo di invio prossimo allo zero, il modello resta in profitto anche se paga *un'impresa su mille.* È un gioco di volumi, non di abilità, e per questo si combatte non con l'astuzia del singolo, ma con una regola meccanica: nessun pagamento senza una fattura elettronica ricevuta via SdI e un ordine che la giustifichi.

SEGNALI D'ALLARME

- Una «fattura» o richiesta di pagamento arrivata solo via e-mail o su carta, che non trova riscontro tra le fatture elettroniche ricevute via SdI.
- Finti rinnovi o iscrizioni (domini, registri, elenchi) che imitano la grafica di enti ufficiali ma non transitano dai canali fiscali.
- Importi contenuti e scadenze ravvicinate, calibrati per scoraggiare la verifica e indurre un pagamento «di routine».
- Fornitori sconosciuti, non presenti in contabilità né nell'anagrafica aziendale.

COSA FARE

Verifica rapida

1. Verificare che la richiesta corrisponda a una fattura elettronica realmente ricevuta tramite lo SdI e a un ordine effettivo: una «fattura» mai transitata dal sistema è già un segnale.
2. Diffidare dei finti rinnovi e solleciti ricevuti via e-mail o posta, anche quando l'aspetto è ufficiale.
3. In caso di dubbio, sospendere il pagamento e verificare in contabilità chi avrebbe disposto l'ordine.

Procedura ordinaria

1. Adottare il principio «nessun pagamento senza fattura elettronica e senza ordine»: riconciliare ogni pagamento con la fattura ricevuta via SdI e con la merce o il servizio effettivamente ricevuti.

2. Centralizzare la ricezione e il riscontro delle fatture, evitando che singoli dispongano pagamenti senza controllo.
3. Per i fornitori esteri e i casi fuori dalla fattura elettronica, definire una verifica rafforzata prima del primo pagamento.

Escalation

1. Se il pagamento è già avvenuto, contattare la banca e valutare le possibilità di recupero.
2. Segnalare il tentativo internamente, per mettere in guardia chi gestisce gli altri pagamenti.
3. Procedere con denuncia e segnalazioni (si veda la Parte V).

CASO · Il rinnovo che non esisteva

L'ufficio amministrativo di una piccola impresa riceve, via e-mail, un sollecito dall'aspetto ufficiale per il rinnovo annuale dell'iscrizione a un «registro nazionale delle imprese»: importo 280 euro, scadenza ravvicinata, grafica che imita quella di un ente pubblico. La cifra modesta e l'apparenza di routine inducono a pagare senza controlli. Non esisteva alcun registro né alcuna iscrizione, e — dettaglio decisivo — non esisteva alcuna fattura elettronica: la richiesta non era mai transitata dallo SdI, perché non poteva. Bastava chiederselo. Il principio «nessun pagamento senza fattura elettronica e senza ordine» l'avrebbe fermata.

2.6 L'accesso non riconosciuto all'home banking

Cambia, in questo scenario, la natura dell'attacco. Non si tratta più di indurre l'impresa a disporre un pagamento, ma che sia il **frodatore a entrare nel conto** e a operare. Va detto subito: è un caso meno frequente degli altri. I dati della Banca d'Italia mostrano che la grande maggioranza delle frodi passa oggi per la manipolazione del pagatore, non per l'accesso abusivo. Ma non è un caso da escludere, e quando riesce il danno è pieno: chi entra può disporre operazioni, aggiungere beneficiari, modificare i massimali o abilitare un proprio dispositivo per autorizzare i pagamenti futuri.

Conviene però sgombrare il campo da un equivoco diffuso: **per entrare nel conto non bastano nome utente e password.** L'autenticazione forte (la SCA di cui si è detto) richiede un secondo fattore — il token app, un codice monouso — e senza quello le sole credenziali non aprono nulla. Le password sottratte — da una violazione di dati, dal riuso tra servizi personali e aziendali, da una pagina di accesso falsificata — sono il punto di partenza dell'attacco, non il suo esito. Per arrivare in fondo, il frodatore deve aggirare anche il secondo fattore.

È qui che tornano le tecniche viste negli scenari precedenti, perché **l'accesso abusivo è quasi sempre il risultato di un altro inganno andato a segno.** Il frodatore può indurre la vittima a installare una falsa applicazione o a concedere l'accesso remoto al dispositivo, e di lì intercettare i codici o operare dal suo stesso telefono (scenario 2.4). Può tentare la registrazione fraudolenta di un proprio dispositivo — il *malicious enrollment* — facendosi approvare l'attivazione dalla vittima. Può manipolarla al telefono perché comunichi un codice o approvi una notifica che crede legata ad altro (scenario 2.3). Sui codici via SMS, può ricorrere alla sostituzione fraudolenta della SIM. In tutti questi casi il vero bersaglio non è la password, ma il secondo fattore: è lì che si decide se l'accesso riesce. Ed è la ragione per cui le difese che seguono guardano soprattutto a quel fronte.

LA PROSPETTIVA DELL'ATTACCANTE

Le credenziali, di norma, non le ruba: le compra. I mercati clandestini rivendono per pochi euro le password uscite dalle grandi violazioni, e strumenti automatici le riprovano su centinaia di servizi in cerca di una corrispondenza. Il riuso della stessa password tra posta personale e home banking aziendale fa il resto: una sola chiave, compromessa altrove, apre più porte del previsto.

Ma sa che la password, da sola, non basta più. L'autenticazione forte gli sbarra la strada, e il vero ostacolo diventa il secondo fattore. Per questo il suo lavoro cambia natura: non più «bucare» un sistema, ma convincere una persona ad aprirgli la porta. Farsi dettare un codice, farsi approvare una notifica che la vittima crede legata ad altro, indurla ad autorizzare — senza capirlo — la registrazione di un nuovo dispositivo.

Quest'ultima mossa è la più preziosa per lui: abilitare un proprio telefono come strumento valido significa smettere di dipendere dalla vittima e poter operare a piacimento. È la ragione per cui i due presìdi che più lo ostacolano sono un secondo fattore robusto e una regola semplice, applicata senza eccezioni: non si approva mai ciò che non si è avviato in prima persona.

SEGNALI D'ALLARME

- Notifiche di accesso al conto da luoghi, orari o dispositivi che non si riconoscono.
- L'arrivo di un codice usa e getta (OTP) che nessuno ha richiesto: è il segnale che qualcuno sta tentando di accedere o di autorizzare un'operazione.
- La comparsa di nuovi beneficiari, dispositivi autorizzati o massimali modificati senza che l'impresa li abbia disposti.
- L'improvviso mancato arrivo degli SMS abituali della banca, possibile spia di una sostituzione fraudolenta della SIM.

COSA FARE

Verifica rapida

1. Non ignorare mai le notifiche di accesso o di operazione: sono il primo e spesso unico avviso tempestivo, verificando contestualmente la sorgente della notifica.

In caso di dubbi, non cliccare su eventuali link e contattare il servizio clienti della banca.
2. Se arriva un OTP non richiesto, non inserirlo e non comunicarlo a nessuno; significa che un tentativo è in corso.
3. Al primo dubbio, cambiare la password da un dispositivo sicuro e controllare beneficiari, massimali e dispositivi autorizzati.

Procedura ordinaria

1. Attivare tutte le notifiche disponibili su accessi e operazioni, e leggerle.
2. Usare una password robusta e diversa per ogni servizio — mai la stessa tra usi personali e home banking aziendale — appoggiandosi a un gestore di password.
3. Mantenere attiva l'autenticazione a più fattori e rivedere periodicamente l'elenco dei beneficiari e dei dispositivi autorizzati, rimuovendo quelli non più in uso.

Escalation

1. Se si sospetta un accesso non autorizzato, contattare immediatamente la banca per bloccare l'operatività del conto.
2. Far esaminare il dispositivo alla ricerca di programmi malevoli prima di riutilizzarlo, e cambiare le credenziali da un dispositivo sicuro.
3. Verificare le operazioni recenti e procedere con denuncia e segnalazioni (si veda la Parte V).

CASO · La notifica delle tre di notte

Il titolare di una piccola impresa riceve, nel cuore della notte, una richiesta di approvazione di accesso che non ha avviato. La password dell'home banking la usava da anni, identica, anche per la posta personale e per alcuni acquisti online, uno dei quali aveva subìto una violazione di dati: di lì i criminali l'avevano ottenuta. Ma la password, da sola, non bastava — serviva il secondo fattore, e quella richiesta notturna era proprio il tentativo di ottenerlo, inducendolo ad approvare. Il titolare non approva e, al mattino, avvisa la banca e cambia le credenziali. L'accesso non riesce. Se avesse toccato «approva» credendo a un disguido, avrebbe aperto lui stesso la porta: è questa la conferma che il secondo fattore è la vera barriera, e che non si approva mai ciò che non si è avviato.

2.7 La carta aziendale

La carta di pagamento aziendale presenta un profilo di rischio diverso dal bonifico: le singole frodi valgono molto meno, ma sono più frequenti e più difficili da notare. I dati della carta — numero, scadenza, codice di sicurezza — possono essere sottratti in molti modi: una pagina di pagamento contraffatta, un negozio online compromesso, una violazione di dati presso un esercente, una richiesta ingannevole. Una volta ottenuti, vengono usati per acquisti non autorizzati.

Ciò che rende questo scenario sfuggente è la sua **discrezione.** I frodatori procedono spesso con un piccolo addebito di prova — pochi euro — per verificare che la carta sia attiva, prima di colpire con importi maggiori o con addebiti ricorrenti camuffati da abbonamenti. In un'impresa, dove la carta è usata da più persone e per molte spese, una piccola voce estranea passa facilmente inosservata. Va però ricordato un dato a favore dell'impresa: sulle carte le tutele per le operazioni non autorizzate sono più ampie che sui bonifici, e una contestazione tempestiva consente, nella maggioranza dei casi, il riaccredito. La rapidità con cui ci si accorge dell'addebito diventa, perciò, la prima difesa.

LA PROSPETTIVA DELL'ATTACCANTE

Per l'attaccante i dati di una carta sono una **merce**, e come ogni merce si raccolgono, si impacchettano e si rivendono. Spesso chi li sottrae — da un sito compromesso, da una violazione, da un terminale manomesso — non è chi li userà: esiste una filiera, e ogni passaggio vuole la sua garanzia di qualità. Da qui il **microaddebito di prova:** pochi centesimi, un piccolo acquisto insignificante, il cui unico scopo è certificare che la carta è «viva» e attiva. Una carta verificata vale di più, e viene rivenduta o usata con priorità. È il motivo per cui un addebito minimo e inspiegabile non è mai davvero trascurabile: spesso è l'annuncio di ciò che seguirà.

Poi si muove in fretta, contro il rischio del blocco, e predilige gli **addebiti ricorrenti camuffati da abbonamenti:** piccoli, regolari, dall'aspetto legittimo. Contano su una sola debolezza — che una voce modesta e periodica *non venga mai riconciliata* con una spesa reale. La sua economia è quella dei tanti piccoli importi, invisibili singolarmente; le uniche difese che la spezzano sono la notifica su ogni transazione e l'abitudine a controllare, senza trascurare nulla.

SEGNALI D'ALLARME

- Piccoli addebiti di pochi euro, sconosciuti e apparentemente insignificanti: spesso sono transazioni di prova.
- Addebiti ricorrenti non riconosciuti, camuffati da abbonamenti o servizi mai sottoscritti.
- Richieste di comunicare numero, scadenza o codice di sicurezza della carta via e-mail, telefono o messaggio.
- Transazioni effettuate da Paesi o esercenti del tutto estranei all'attività dell'impresa.

COSA FARE

Verifica rapida

1. Controllare con regolarità i movimenti della carta, prestando attenzione anche agli importi minimi.
2. Bloccare la carta — oggi è possibile in autonomia dall'app — al primo addebito che non si riesce a ricondurre a una spesa nota.
3. Non comunicare mai a nessuno il codice di sicurezza, il PIN o il numero completo della carta.

Procedura ordinaria

1. Attivare le notifiche su ogni transazione, così da accorgersi in tempo reale di un addebito anomalo.
2. Impostare massimali di spesa coerenti con l'uso effettivo e disattivare le funzioni non necessarie (ad esempio i pagamenti dall'estero, se non servono).
3. Per gli acquisti online e gli abbonamenti, preferire carte dedicate o virtuali, con plafond limitato e separate da quelle di uso corrente.
4. Assegnare le carte nominativamente e tenere traccia di chi le utilizza, evitando carte condivise senza controllo.

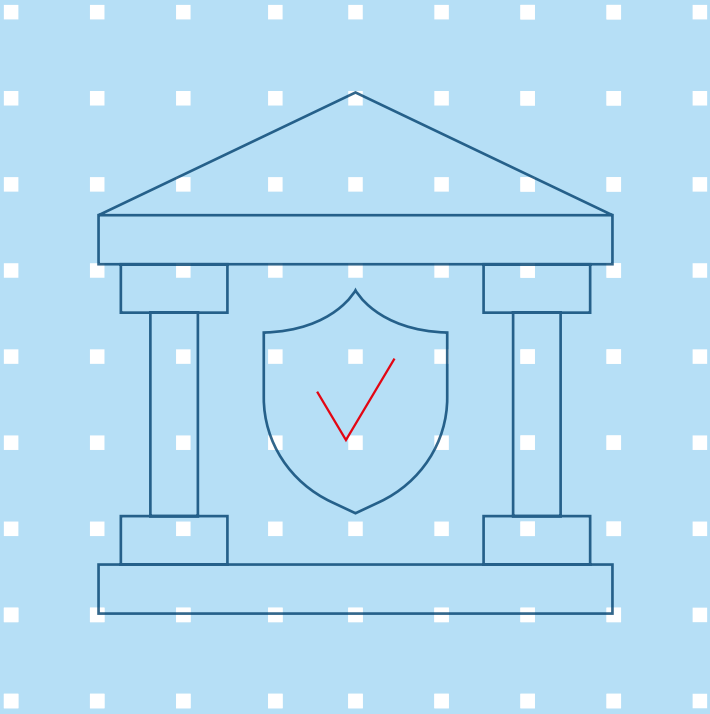
Escalation

1. Al rilevamento di un addebito non riconosciuto, bloccare la carta e contestare l'operazione alla banca nei tempi più rapidi possibili.
2. Richiedere la riemissione della carta con nuove coordinate quando i dati risultano compromessi.
3. Conservare le evidenze e procedere, ove necessario, con denuncia e segnalazioni (si veda la Parte V).

CASO · I tre euro che annunciavano il resto

Sull'estratto della carta aziendale di una piccola impresa compare un addebito di poco più di tre euro, presso un esercente online sconosciuto. Nessuno vi presta attenzione: una cifra simile non vale il tempo di una verifica. Due giorni dopo, dalla stessa carta partono tre addebiti per oltre duemila euro complessivi. Quel piccolo importo era una transazione di prova, con cui i frodatori avevano accertato che la carta era attiva. Le notifiche su ogni transazione, e l'abitudine a non trascurare nemmeno gli importi minimi, avrebbero trasformato quei tre euro in un campanello d'allarme anziché in un preavviso ignorato.

3. LA GOVERNANCE INTERNA DEI PAGAMENTI



Perché serve una governance, non solo attenzione

Nei capitoli precedenti è emersa una circostanza scomoda: oggi il frodatore non aggredisce i sistemi, aggredisce le persone. Fa leva sull'urgenza, sull'autorità, sulla fiducia, sulla fretta. È qui che questa parte interviene alla radice. Di fronte a un attacco costruito per manipolare una persona, chiedere a quella persona di «stare più attenta» non è una strategia. L'attenzione è una risorsa finita; il frodatore lavora esattamente per esaurirla, scegliendo il momento peggiore — la chiusura di bilancio, il venerdì sera, l'assenza del titolare. Una difesa che dipende dalla lucidità del singolo nel momento sbagliato è una difesa destinata, prima o poi, a cedere.

La governance dei pagamenti rovescia l'impostazione. Non si propone di rendere le persone infallibili — obiettivo irraggiungibile — ma di costruire un processo che **regga anche l'errore o l'inganno di una singola persona.** La sicurezza smette così di essere una prestazione richiesta all'individuo e diventa una proprietà del processo: qualcosa che non si deve ricordare di fare, perché è il modo stesso in cui il lavoro è organizzato a produrla. È la differenza tra affidare la solidità di un edificio alla prudenza di chi lo abita e affidarla a come l'edificio è costruito.

Questo è il principio che gli specialisti chiamano *security by design* — la sicurezza incorporata nel processo fin dalla sua progettazione, e non aggiunta in un secondo momento come un correttivo. Ha una conseguenza pratica immediata: ciò che nella Parte II era una verifica da ricordare caso per caso, qui diventa una regola stabile, parte del processo. Non «mi raccomando, controlla i cambi di IBAN», ma un processo nel quale un cambio di IBAN non può tradursi in un pagamento senza che un secondo passaggio lo validi. La reazione diventa architettura.

Resta un'obiezione legittima, soprattutto per chi è piccolo: «tutto questo è roba da grande impresa». Non è così, ed è il secondo principio di questa parte: la **proporzionalità.** Nessuna delle misure che seguono è una taglia unica. Per ciascuna esiste una forma piena, adatta a chi ha una struttura, e un equivalente minimo, alla portata di chi lavora da solo. La micro-impresa non può separare i compiti tra persone diverse, ma può introdurre un secondo occhio esterno — il commercialista — attivare le notifiche e tenere bassi i massimali. L'obiettivo resta identico per tutti; cambia solo il modo di raggiungerlo.

E quell'obiettivo si riassume in una frase, che attraversa l'intera parte: ***nessuno deve poter fare tutto da solo, senza che nessun altro veda.***

LA PROSPETTIVA DELL'ATTACCANTE

L'attaccante non aggredisce l'impresa nel suo insieme: cerca il punto in cui l'impresa ha **concentrato tutto.** La persona che richiede, autorizza ed esegue da sola un pagamento; l'account condiviso che rende ogni operazione non attribuibile a nessuno; la delega temporanea mai revocata, di cui più nessuno ricorda l'esistenza. Sono questi i varchi che cerca, perché gli consentono di ottenere molto ingannando poco.

Ragiona, come sempre, in termini di costo. Dove i poteri sono divisi, il suo lavoro raddoppia: deve ingannare due persone, in due momenti, sullo stesso inganno — e mantenere la finzione coerente attraverso un secondo paio d'occhi che non ha motivo di fidarsi. Il rischio di essere scoperto cresce, il vantaggio atteso cala.

Il risultato è che, davanti a una separazione dei compiti reale, molto spesso *semplicemente rinuncia* e *cambia bersaglio.* La governance non lo rende impossibile in assoluto; lo rende sconveniente — e per un'attività che vive di margini e di volumi, sconveniente è quasi sempre sufficiente.

Le sezioni che seguono non sono un elenco di adempimenti separati: sono modi diversi di applicare questo stesso principio. Lo si ritroverà, di volta in volta, nella separazione dei compiti, nel controllo di più persone, nei limiti ai poteri, negli strumenti di autorizzazione, nella verifica delle richieste. Un solo principio, declinato lungo l'intera catena del pagamento.

3.1 La separazione dei compiti

Il primo modo per non dipendere da una persona sola è scomporre il pagamento nelle sue funzioni e affidarle a soggetti distinti. È il principio della separazione dei compiti — in inglese *segregation of duties,* spesso abbreviato in SoD — e poggia su un'idea elementare: nessuno dovrebbe trovarsi a controllare il proprio operato. Un pagamento attraversa quattro funzioni, che idealmente non dovrebbero concentrarsi nelle stesse mani.

Funzione	In cosa consiste
Richiesta	Chi origina la spesa: ordina la fornitura, riceve la fattura, propone il pagamento.
Autorizzazione	Chi approva il pagamento, verificandone la legittimità prima dell'esecuzione.
Esecuzione	Chi dispone materialmente l'operazione sull'home banking.
Registrazione	Chi contabilizza e riconcilia il pagamento con la documentazione.

La regola d'oro è che chi dispone un pagamento non dovrebbe poterlo anche approvare e riconciliare. Quando queste funzioni si sommano in una sola persona, viene a mancare ogni controllo naturale: la stessa mano che crea l'operazione la convalida e ne verifica l'esito. È la condizione ideale perché una frode — o un errore — passi inosservata.

CALIBRAZIONE PER DIMENSIONE

Nella media impresa la separazione piena è possibile e va perseguita. Nella piccola impresa si possono almeno tenere distinte la richiesta e l'autorizzazione.Nella micro-impresa, dove una sola persona fa tutto, la separazione tra individui è impossibile: subentrano allora i *controlli compensativi.* Un secondo occhio esterno — tipicamente il commercialista — che riveda periodicamente i movimenti; le notifiche bancarie attive su ogni operazione, che fanno da revisione in tempo reale; massimali contenuti, che limitano il danno di un singolo errore. Non è la stessa cosa di una separazione formale, ma ne riproduce la funzione: introdurre uno sguardo che non coincide con chi ha disposto.

3.2 Il controllo four eyes

Se i compiti sono separati, il passo successivo è esigere l'accordo di più persone sulle operazioni che contano. È il principio *four eyes* — alla lettera «quattro occhi» —, per cui un pagamento richiede l'intervento di due persone diverse: una che lo dispone e una, distinta, che lo approva. Il vantaggio è diretto: un singolo individuo, anche se manipolato o infedele, non può portare a termine l'operazione da solo. Perché la frode riesca dovrebbe ingannare due persone contemporaneamente — un ostacolo molto più alto.

Per le operazioni di maggior rilievo — importi elevati, nuovi beneficiari, pagamenti verso l'estero — alcune imprese adottano il controllo *six eyes:* una terza persona aggiunge un'ulteriore verifica. Non è necessario applicarlo a tutto; è ragionevole riservarlo alle operazioni che, per importo o natura, comporterebbero il danno maggiore.

Sul piano pratico, questo controllo si traduce nei **profili dell'home banking:** le banche consentono di assegnare a ciascun utente un ruolo diverso — chi può solo predisporre un'operazione e chi può autorizzarla — così che la separazione non resti sulla carta, ma sia imposta dal sistema. È il punto in cui la regola organizzativa diventa un vincolo tecnico, e per questo più difficile da aggirare.

Anche qui vale la proporzionalità. Per la micro-impresa il secondo paio d'occhi non deve necessariamente essere un dipendente: può essere un soggetto esterno di fiducia che convalida le operazioni sopra una certa soglia. L'essenziale è che, oltre un certo importo, *nessun pagamento parta sulla decisione di una persona sola.*

3.3 Profili, deleghe e soglie

Perché il controllo four eyes funzioni, i poteri di ciascuno vanno definiti con precisione: chi può fare cosa, e fino a quale importo. È la materia delle deleghe e dei profili autorizzativi, e governarla bene significa mettere un tetto, per costruzione, al danno che una singola operazione può produrre.

I PROFILI

Sull'internet banking aziendale conviene distinguere almeno tre profili: il **dispositore**, che predispone le operazioni ma non le rende definitive; l'**autorizzatore**, che le approva; e il profilo di **sola lettura**, per chi deve consultare i movimenti senza operare — ad esempio il commercialista. Assegnare a ciascuno solo ciò che gli serve è una forma di sicurezza: meno poteri del necessario significa meno danno possibile in caso di compromissione.

LE DELEGHE

Le deleghe a operare vanno conferite per iscritto, con un perimetro chiaro: a chi, per quali operazioni, entro quali limiti di importo. Una delega vaga è una delega pericolosa. E va gestito il loro ciclo di vita: una delega concessa per una necessità temporanea, e mai revocata, diventa un potere dormiente di cui nessuno ricorda l'esistenza — finché qualcuno non lo sfrutta.

LE SOGLIE

Le soglie di importo stabiliscono quando scattano controlli più stringenti: oltre un certo valore, il controllo four eyes; oltre un valore superiore, i six eyes o una verifica esterna. Nel fissarle conviene tenere a mente i dati della Parte I: l'importo medio di una frode su bonifico si aggira intorno alle migliaia di euro, non alle decine. Una soglia tarata troppo in alto lascia passare proprio le operazioni nella fascia in cui le frodi si concentrano.

LA REVISIONE PERIODICA

Profili, deleghe e soglie non sono decisioni da prendere una volta sola. Almeno una volta l'anno andrebbero riviste: chi ha cambiato ruolo, chi ha lasciato l'impresa, quali deleghe non servono più. Un accesso o una delega che sopravvivono alla persona o alla ragione che li giustificavano sono tra i varchi più silenziosi e più frequenti.

3.4 Gli strumenti di autorizzazione: dal token all'identità digitale

I poteri definiti dai profili si esercitano attraverso uno strumento che autorizza l'operazione e ne conferma l'autore. È ciò che comunemente si chiama *token*, ed è il secondo elemento dell'autenticazione forte richiesta dalla normativa europea (la SCA, *Strong Customer Authentication*): oltre a qualcosa che si *sa* — la password —, serve qualcosa che si *ha* o che si *è*.

COS'È OGGI UN TOKEN, E PERCHÉ STA CAMBIANDO

Conviene chiarire un equivoco diffuso. Il token non è più, se non in misura decrescente, un oggetto fisico — la chiavetta che genera codici, il lettore di carta. Sempre più è **parte integrante del proprio profilo digitale** quindi legato alla persona e al proprio dispositivo: un profilo sicuro, attivato dentro l'applicazione della banca sul telefono, che conferma l'operazione combinando il possesso del dispositivo e un fattore personale — l'impronta, il volto o un codice noto solo al titolare. Non è più «una cosa che porti con te», ma «un'identità che sei», ancorata a uno strumento personale.

Molte imprese vivono con disagio l'abbandono del token fisico o del token SMS, percepito come un cambiamento imposto e scomodo. Vale la pena spiegare perché il passaggio non solo è inevitabile, ma è nell'interesse dell'impresa. Per farlo conviene distinguere i tre strumenti, che spesso vengono confusi sotto la stessa parola.

- **Il token SMS è fragile.** È il codice monouso inviato con un messaggio. Può essere intercettato, e soprattutto è esposto alla sostituzione fraudolenta della SIM, con cui un criminale dirotta su di sé i messaggi della vittima. Per questo è considerato il fattore più debole e viene progressivamente abbandonato.

- **Il token fisico è costoso e scomodo.** È l'oggetto — la chiavetta che genera codici, il lettore di carta. Si smarrisce, si rompe, va sostituito, non si aggiorna; è una cosa in più da custodire, e quando manca blocca l'operatività.

- **Il token in-app funziona in modo diverso, e migliore.** È il token generato dentro l'applicazione della banca. Non produce un codice da leggere e digi-

tare: quando si dispone un'operazione, l'app riceve una notifica sul telefono; aprendola e autenticandosi — con l'impronta, il volto o un codice personale — si vede il dettaglio dell'operazione, importo e beneficiario, e la si approva con un tocco. Niente codice da trascrivere, e soprattutto i dati reali dell'operazione appaiono davanti agli occhi nell'istante decisivo: chi autorizza vede «stai per pagare 90.000 euro a questo IBAN» prima di confermare. È una difesa diretta contro la manipolazione, perché anche chi è stato ingannato ha sotto gli occhi ciò che sta realmente autorizzando.

In altre parole, il passaggio al token app non toglie sicurezza all'impresa: gliene aggiunge. Resistere significa restare legati a strumenti più deboli e comunque destinati a essere dismessi.

LE REGOLE D'USO, E COME ATTIVARLO BENE

Proprio perché il token è oggi legato alla persona, le regole sul suo uso diventano più stringenti, non meno. La prima vale per tutti: il token è personale e non si condivide mai. Prestarlo non equivale a passare una chiave, ma a cedere la propria identità autorizzativa: con essa un altro opera a nome del titolare, e ogni tracciabilità si perde. Per questo ogni persona deve avere il proprio, mai uno condiviso tra più collaboratori.

Le altre regole dipendono dal tipo di strumento, e conviene non confonderle. Con il **token SMS** o il **token fisico**, che generano un numero, la regola è una sola: **quel codice non si comunica a nessuno,** per nessun motivo — non alla banca, non a un tecnico, non a chi telefona. Con il **token app,** dove non c'è alcun codice ma si approva una notifica, la regola cambia di conseguenza: **non si approva mai una richiesta che non si è generata in prima persona.** Se arriva una notifica di approvazione mentre non si sta disponendo alcuna operazione, è il segnale che qualcun altro sta tentando di operare con il proprio profilo: la richiesta va rifiutata, e vanno cambiate immediatamente le credenziali di accesso.

Sull'attivazione valgono poche cautele essenziali: installare l'applicazione solo dagli store ufficiali e attivare il token solo seguendo le istruzioni ricevute dalla banca per i canali ufficiali, mai su indicazione di una telefonata o di un messaggio; usare un dispositivo personale, protetto da codice di sblocco e biometria, e mantenerlo aggiornato; in caso di cambio o smarrimento del telefono,

disattivare tempestivamente il token sul vecchio dispositivo e riattivarlo sul nuovo attraverso la banca.

PIÙ DISPOSITIVI E BIOMETRIA

Le banche consentono spesso di abilitare il servizio su più dispositivi — il cosiddetto *multidevice*. È comodo, ma vale un principio: ogni dispositivo abilitato è una porta d'accesso in più, e va protetto con la stessa cura. Conviene tenere abilitati solo i dispositivi effettivamente in uso e rimuovere quelli dismessi.

Merita inoltre capire come funziona la biometria — l'impronta o il riconoscimento del volto — perché non tutte le soluzioni offrono lo stesso grado di sicurezza. Nella maggior parte dei casi la banca si appoggia alla **biometria del dispositivo:** l'impronta o il volto gestiti dal telefono. In questo caso il riconoscimento vale per chiunque sia registrato su quel dispositivo: se vi sono memorizzate più impronte o più volti — per esempio di familiari — ciascuno di essi può sbloccare l'app. La biometria del dispositivo, in altre parole, conferma che chi opera ha accesso a quel telefono, non che è proprio il titolare. Alcune banche, ancora poche, adottano invece una **biometria legata all'identità del cliente** e gestita dai propri sistemi (in gergo tecnico CIAM, da *Customer Identity and Access Management*): qui è verificata l'identità della persona, ed è un livello di protezione superiore. È utile sapere quale delle due adotta la propria banca; se è quella del dispositivo, è bene che sul telefono usato per i pagamenti sia registrata soltanto la propria impronta o il proprio volto.

Ne discende una raccomandazione netta: **non attivare il token su dispositivi condivisi** — un tablet alla reception, un computer comune, un telefono usato da più persone. Su un dispositivo condiviso il token diventa accessibile ad altri, la responsabilità delle operazioni non è più attribuibile a una persona sola e, se la biometria è quella del device, più individui possono autorizzare i pagamenti. Il token deve risiedere su un dispositivo personale, custodito dal solo titolare.

C'è infine un rischio che merita attenzione specifica: la **registrazione fraudolenta di un dispositivo** (in inglese *malicious enrollment*). Se un frodatore riesce ad abilitare un proprio telefono come token valido sul profilo della vittima, da quel momento può autorizzare operazioni come se fosse il titolare. L'attivazione di un nuovo dispositivo richiede però quasi sempre una conferma — un codice o l'approvazione di una notifica —:

ed è esattamente il punto in cui l'attacco si può fermare. Per questo una notifica che segnala l'abilitazione di un nuovo dispositivo non va mai ignorata, e una richiesta di approvare l'attivazione di un dispositivo che non si sta registrando in prima persona va sempre rifiutata. Vale, ancora una volta, la regola di fondo del token app: non si approva mai ciò che non si è avviato.

3.5 Il protocollo di comunicazione e le verifiche out-of-band

Anche con ruoli, controlli e strumenti al loro posto, il canale in cui la frode tenta di entrare resta lo "human factor", ovvero la richiesta che arriva. È il momento più delicato, ed esige una regola di comportamento chiara, valida per tutti e in ogni circostanza.

La regola è questa: per verificare una richiesta che comporta un pagamento o una modifica, si usa **sempre un canale diverso da quello con cui la richiesta è arrivata.** È ciò che si definisce verifica *out-of-band* — «fuori banda», cioè su un canale separato e indipendente. Se la richiesta giunge via e-mail, si verifica per telefono; se giunge per telefono, si richiama su un recapito certo. Il motivo è semplice: un frodatore che controlla un canale controlla anche le risposte che vi transitano, e una verifica condotta sullo stesso canale finisce per chiedere conferma proprio a chi sta ingannando.

Ne discende un divieto preciso, che conviene fissare come abitudine: **non si usano mai i recapiti contenuti nella richiesta stessa.** Non il numero in calce all'e-mail, non il link «per verificare», non il telefono indicato nella comunicazione che annuncia il cambio. Quei recapiti, se la richiesta è fraudolenta, portano diritti al frodatore. Si usano invece i contatti già noti e raccolti in precedenza: per questo è utile mantenere una rubrica dei recapiti dei fornitori e dei referenti, validata in tempi non sospetti e tenuta separata dalla corrispondenza corrente.

La verifica out-of-band non va fatta su ogni operazione — sarebbe paralizzante — ma è obbligatoria nei casi a maggior rischio, che conviene definire in anticipo: ogni variazione di coordinate bancarie; ogni richiesta urgente o riservata proveniente dal vertice; i pagamenti sopra le soglie definite; i nuovi beneficiari. In questi casi la verifica non è un eccesso di zelo: è parte della procedura.

Per i beneficiari del tutto nuovi, infine, è buona prassi — dove le informazioni sono accessibili — estendere la verifica dalla singola richiesta al soggetto: un controllo proporzionato sulla solidità e sull'affidabilità del fornitore prima del primo pagamento — l'esistenza effettiva dell'attività, la coerenza dei recapiti, una presenza verificabile — completa la verifica del canale con quella della controparte, e con essa la difesa dal lato antifrode.

3.6 L'anagrafica dei fornitori

La verifica condotta una volta va resa permanente, perché non debba ripetersi a ogni pagamento. È la funzione dell'anagrafica dei fornitori: il registro dei beneficiari e delle loro coordinate, che — se governato bene — fa sì che i dati di pagamento siano validati a monte e non più rimessi in discussione al momento di ogni bonifico.

Due regole la rendono efficace. La prima: i dati di un nuovo fornitore si validano all'inserimento, verificandone le coordinate alla fonte, e ogni **modifica successiva** — un cambio di IBAN, in particolare — si tratta con la stessa cautela di un nuovo inserimento, con verifica out-of-band e doppio controllo. La seconda: ogni variazione lascia traccia — chi l'ha disposta, quando, su quale base — così che l'anagrafica non sia un dato modificabile in silenzio, ma un registro con una storia. È qui che il servizio di verifica del beneficiario offerto dalla banca, di cui si è detto, trova il suo complemento naturale: lo strumento tecnico e la disciplina interna si rafforzano a vicenda.

Vi è infine un ulteriore aspetto che merita attenzione, perché rovescia la prospettiva: l'anagrafica non è soltanto lo strumento della difesa, ma può essere essa stessa un bersaglio. Chi ottenesse accesso al gestionale potrebbe modificare un IBA senza bisogno di alcuna e-mail persuasiva: il pagamento successivo partirebbe da sé, verso il conto sbagliato, senza che nessuno abbia ricevuto una richiesta da valutare — e nessuna verifica out-of-band potrebbe scattare, semplicemente perché una richiesta non c'è stata. Pertanto è opportuno trattare l'accesso in modifica all'anagrafica come un potere, e non come una funzione amministrativa qualsiasi: riservato a poche persone individuate, distinto — dove la struttura lo consente — da chi dispone materialmente i pagamenti, sempre tracciato e oggetto di controllo four eyes. È la separazione dei compiti e dei doveri applicata ai dati, prima ancora che alle operazioni.

3.7 Le basi: identità e credenziali

Tutto quanto precede presuppone una condizione che spesso si dà per scontata e che invece va affermata con chiarezza: ogni persona deve essere identificabile, e le sue credenziali devono essere davvero solo sue. Senza questo, l'intera impalcatura si svuota — la separazione dei compiti diventa una finzione se due persone usano lo stesso accesso, e il controllo four eyes non ha senso se non si sa chi ha fatto cosa. Le regole che seguono sono elementari, persino ovvie; proprio per questo sono tra le più disattese.

- **UN PROFILO PER OGNI PERSONA.** Niente account condivisi, neppure sull'home banking: ciascuno deve avere il proprio profilo, con le proprie credenziali. Un accesso condiviso rende impossibile sapere chi ha disposto un'operazione e vanifica ogni tracciabilità.

- **PASSWORD ROBUSTE, DIVERSE, NON RIUTILIZZATE.** Ogni servizio deve avere la sua, e quella dell'home banking aziendale non deve mai coincidere con password usate altrove, tantomeno per usi personali. Un gestore di password consente di averne molte, complesse e diverse, senza doverle ricordare.

- **AUTENTICAZIONE A PIÙ FATTORI SEMPRE ATTIVA.** Dove è disponibile un secondo fattore oltre alla password, va attivato e mantenuto: è la barriera che regge anche quando una password viene sottratta.

- **CREDENZIALI E TOKEN NON SI COMUNICANO.** Nessuno — né un collega, né un presunto tecnico, né la banca — ha motivo di chiedere le proprie credenziali o il codice del token. Una simile richiesta è, di per sé, il segnale di un tentativo di frode.

- **REVOCA IMMEDIATA ALL'USCITA** Quando una persona lascia l'impresa o cambia mansione, i suoi accessi e le sue deleghe vanno revocati subito. Un profilo attivo che non corrisponde più a nessuno è una porta lasciata aperta.

3.8 Dispositivi e canali

I presìdi valgono quanto il dispositivo su cui si esercitano. L'ultimo anello della governance riguarda gli strumenti e i canali con cui si accede ai pagamenti, e qui le piccole imprese scontano una fragilità già richiamata: lo stesso telefono o computer personale serve spesso anche per l'attività aziendale, senza separazioni né controlli.

- **MOBILE BANKING, CON COGNIZIONE.** L'accesso da telefono è comodo e, se il dispositivo è protetto e aggiornato, non meno sicuro di altri. Va però usato su un dispositivo personale e custodito, mai su apparecchi condivisi o pubblici, e con il blocco schermo sempre attivo.

- **SEPARARE, PER QUANTO POSSIBILE.** Tenere distinto il dispositivo usato per i pagamenti da quello di uso quotidiano riduce l'esposizione. Dove non è possibile, conviene almeno limitare le applicazioni installate su quel dispositivo allo stretto necessario.

- **AGGIORNARE, E INSTALLARE SOLO DAGLI STORE UFFICIALI.** Sistema operativo e applicazioni vanno tenuti aggiornati; le app si scaricano esclusivamente dagli store ufficiali. Gli aggiornamenti correggono proprio le falle che gli attacchi sfruttano.

- **ATTENZIONE ALLE RETI.** Evitare di operare sui pagamenti da reti pubbliche e non protette. Nel dubbio, è preferibile usare la connessione dati del proprio telefono.

La governance secondo la dimensione

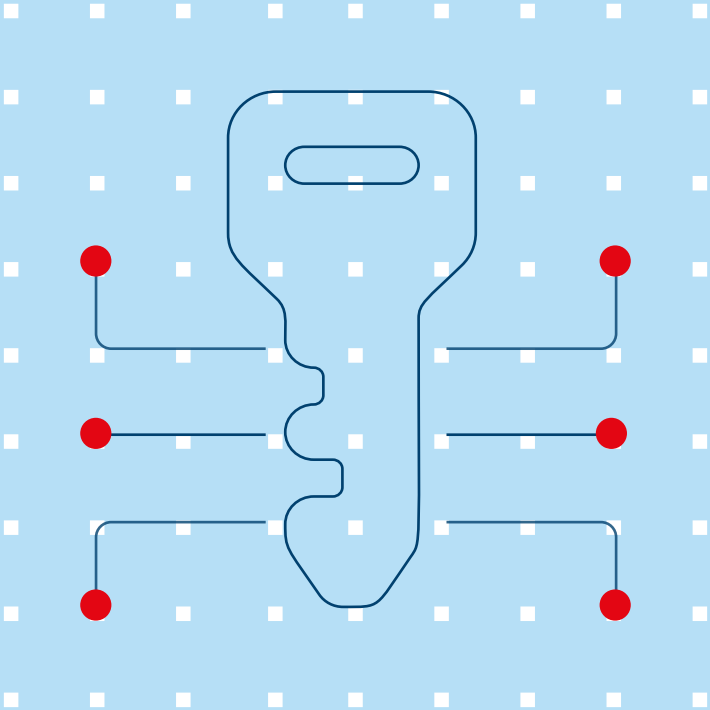
Le misure di questa parte non si applicano allo stesso modo a tutte le imprese. La tabella che segue riassume, per i tre profili, ciò che è realistico e prioritario adottare in ciascun ambito. L'obiettivo, come si è detto, è il medesimo per tutti; cambia la forma con cui lo si raggiunge.

Ambito	Micro	Piccola	Media
Separazione compiti	Secondo occhio esterno	Richiesta e autorizzazione distinte	Separazione piena delle funzioni
Four eyes	Verifica esterna sopra soglia	*Four eyes* sopra soglia	*Four eyes; six eyes* nei casi critici
Soglie e profili	Massimali bassi	Profili distinti, soglie definite	Profili, deleghe e soglie formalizzati
Token	Personale, token app	Personale, per ruolo	Personale, per ruolo
Verifiche	Sempre per cambi IBAN	*Out-of-band* nei casi a rischio	Protocollo formalizzato

CASO · *Four eyes*, novantamila euro

Una media impresa riceve la richiesta di un bonifico urgente, apparentemente dal direttore generale, verso un nuovo beneficiario estero. L'addetto che la riceve ha il profilo di solo dispositore: può predisporre l'operazione, non renderla definitiva. La prepara, e l'operazione passa, come da procedura, all'autorizzatore. Questi nota il beneficiario nuovo e l'importo sopra soglia, e applica la verifica *out-of-band* prevista per questi casi: una telefonata al direttore su un numero noto. La frode emerge in un minuto. Nessuno, quel giorno, è stato più attento del solito. È stato il processo — profili distinti, soglia, verifica obbligatoria — a fermare il pagamento. Esattamente ciò per cui era stato costruito.

4. GLI STRUMENTI A DISPOSIZIONE DELL'IMPRESA



La sicurezza dei pagamenti è una responsabilità condivisa. La banca mette a disposizione una serie di strumenti di protezione; l'impresa deve attivarli, usarli bene e presidiare la parte che le compete — i propri sistemi, la propria posta, i propri dispositivi. Le parti precedenti hanno spiegato *perché* servono certi presìdi e come organizzarli; questa parte è la mappa concreta degli strumenti e della linea che separa ciò che fa la banca da ciò che spetta all'impresa. Molti temi sono già stati trattati: qui si raccolgono in forma operativa, come una cassetta degli attrezzi da tenere a portata di mano.

4.1 Gli strumenti che offre la banca

La banca mette a disposizione, di norma gratuitamente, un insieme di strumenti che riducono in modo sostanziale il rischio. Il problema, nella maggior parte dei casi, non è la loro assenza, ma il fatto che restino inattivi: ogni protezione comporta un piccolo attrito — un avviso in più, un passaggio in più — e davanti all'attrito la comodità tende a prevalere, finché non accade qualcosa. È una falsa economia, perché il fastidio risparmiato oggi si paga, moltiplicato, il giorno di una frode. Conviene perciò conoscere questi strumenti e verificare, uno per uno, che siano davvero accesi.

- **L'AUTENTICAZIONE FORTE E IL TOKEN APP.** È il presidio cardine: assicurarsi che sia attivo e, dove possibile, preferire il token app al token SMS, per le ragioni viste nella Parte III.

- **LE NOTIFICHE E GLI AVVISI.** Avvisi in tempo reale su accessi, operazioni e modifiche. Vanno attivati tutti: sono spesso il primo e più tempestivo segnale di qualcosa che non va.

- **LA VERIFICA DEL BENEFICIARIO (VOP).** Il controllo che confronta nome e IBAN prima di un bonifico. Quando segnala una mancata corrispondenza, va presa sul serio (si veda lo scenario 2.1).

- **I LIMITI E I MASSIMALI.** Tetti di importo per operazione, per giornata, per canale. Impostarli coerenti con l'uso reale limita il danno di qualunque operazione fraudolenta.

- **I PROFILI E LE DELEGHE.** La possibilità di assegnare ruoli distinti — chi dispone, chi autorizza, chi consulta — su cui poggia la separazione dei compiti (Parte III).

- **IL BLOCCO RAPIDO.** La possibilità di sospendere in autonomia, dall'app, una carta o l'operatività in caso di sospetto. Sapere in anticipo dove si trova questa funzione fa risparmiare minuti preziosi.

Nessuno di questi strumenti è efficace se resta inattivo. Conviene perciò una verifica periodica, e soprattutto un confronto diretto con il proprio referente in banca. La sezione che chiude questa parte propone le domande da porgli.

LA PROSPETTIVA DELL'ATTACCANTE

La frode, come ogni attività economica, segue il **percorso di minore resistenza.** L'attaccante confronta di continuo lo sforzo richiesto con il guadagno atteso, e sceglie di conseguenza. Un'impresa che ha attivato notifiche, massimali coerenti, verifica del beneficiario e doppia autorizzazione non gli oppone un muro invalicabile: gli oppone un conto economico sfavorevole.

Ed è quasi sempre abbastanza. Davanti a un bersaglio presidiato, di norma non insiste: **passa a quello accanto,** che quei presìdi non li ha attivati. Gli strumenti della banca non lo rendono impotente — lo rendono *antieconomico* —, e per chi si difende è esattamente ciò che conta. Non occorre essere imprendibili; basta essere più costosi da colpire di chi ci sta intorno.

4.2 Biometria e autenticazione adattiva

Due strumenti meritano un approfondimento, perché incidono direttamente sul modo in cui un pagamento viene protetto e perché sono spesso fraintesi: la biometria e l'autenticazione che si adatta al rischio.

LA BIOMETRIA

L'impronta e il riconoscimento del volto sono diventati il modo più comune di confermare la propria identità. La loro forza è di sostituire qualcosa che si sa — un codice, che si può carpire o farsi dettare — con qualcosa che si è, un tratto fisico assai più difficile da sottrarre. Ma proprio questa natura impone una cautela che le password non richiedono: un dato biometrico **non si può cambiare.** Una password compromessa si sostituisce; un'impronta, no. Per questo conta come viene custodita: le implementazioni serie conservano il dato biometrico unicamente sul dispositivo e non lo trasmettono alla banca — un punto che, se interessa, vale la pena chiedere.

Resta valida la distinzione vista nella Parte III: la biometria del dispositivo riconosce chiunque vi sia registrato, mentre quella legata all'identità del cliente verifica proprio la persona. Sapere quale adotta la propria banca aiuta a capire quanto, davvero, quella biometria stia proteggendo.

L'AUTENTICAZIONE CHE SI ADATTA AL RISCHIO (STEP-UP)

Non tutte le operazioni comportano lo stesso rischio, e non avrebbe senso applicare a ciascuna lo stesso livello di verifica. Consultare il saldo non equivale a disporre un bonifico verso un nuovo beneficiario estero. Da questa osservazione nasce il principio dell'autenticazione adattiva, o *step-up authentication*: il sistema della banca «innalza» il livello di verifica — chiedendo un fattore aggiuntivo — quando l'operazione lo merita, e lo lascia leggero quando il rischio è basso.

È una protezione che lavora in silenzio a favore del cliente, e per due ragioni. La prima: concentra l'attrito dove serve davvero — l'importo anomalo, il beneficiario mai visto, l'operazione fuori dalle abitudini —, lasciando fluide le operazioni ordinarie. La seconda, più sottile: impone un passaggio in più proprio nei momenti che il frodatore predilige, quelli in cui sta tentando qualcosa di insolito. Là dove un'operazione anomala scivolerebbe via, lo *step-up*

la rallenta e chiede una conferma ulteriore. Non tutte le banche la offrono, o la offrono con lo stesso grado di finezza; ma è bene sapere che esiste, perché si combina con i presìdi interni dell'impresa. La banca innalza l'autenticazione sulle operazioni a rischio; l'impresa, sulle stesse fasce, innalza i propri controlli — il four eyes, le verifiche out-of-band. Due difese che scattano sugli stessi segnali, e che insieme rendono molto più stretto il varco. Dove disponibile, conviene chiedere quali operazioni attivano la verifica rafforzata.

4.3 Ciò che spetta all'impresa

Gli strumenti della banca proteggono il conto e l'operazione di pagamento. Restano fuori dal loro perimetro le porte da cui la frode entra più spesso, e che competono interamente all'impresa: la posta, i dispositivi, le reti, gli accessi. È la parte di sicurezza che nessuna banca può presidiare al posto del cliente.

- **LA POSTA ELETTRONICA AZIENDALE**. È il canale principale della frode sulle imprese. Va protetta con autenticazione a più fattori, password robuste e attenzione ai segnali di compromissione: è dalla casella violata che nascono le frodi su fattura e molte richieste fraudolente.

- **I DISPOSITIVI.** Telefoni e computer usati per i pagamenti vanno tenuti aggiornati, protetti da blocco e biometria, e per quanto possibile separati dagli usi personali (si vedano gli scenari 2.4 e la sezione 3.8).

- **LE RETI E GLI ACCESSI REMOTI.** Evitare di operare da reti pubbliche; gestire con cautela gli accessi da remoto, che ampliano la superficie esposta.

- **LE CREDENZIALI E GLI ACCESSI.** Un profilo per persona, password diverse e non riutilizzate, revoca immediata all'uscita: le basi descritte nella sezione 3.7.

La linea di confine è semplice da ricordare: **la banca protegge il pagamento, l'impresa protegge il punto da cui il pagamento parte.** Trascurare la seconda metà significa lasciare aperta la porta a monte di ogni difesa bancaria.

4.4 Cosa la banca non chiederà mai

Esiste uno strumento di difesa che non costa nulla, non va attivato e funziona contro quasi tutte le frodi che abbiamo visto: sapere con certezza che cosa la propria banca non farà mai. La grande maggioranza dei tentativi si smaschera su questo solo metro. Vale la pena impararlo a memoria e diffonderlo a chiunque, in azienda, abbia a che fare con i pagamenti.

LA BANCA NON CHIEDERÀ MAI

- Non chiede mai password, PIN o codici usa e getta (OTP), per nessun motivo e attraverso nessun canale.
- Non chiede mai di approvare una notifica sull'app per «verifiche», «controlli di sicurezza» o «storno» di operazioni.
- Non chiede mai di spostare il denaro su un «conto sicuro» o «conto di transito» per proteggerlo.
- Non chiede mai di installare applicazioni o software di assistenza per «risolvere un problema».
- Non invia link per «verificare» o «sbloccare» il conto chiedendo di inserire le credenziali.
- Non impone scadenze di pochi minuti minacciando il blocco immediato del conto.

Qualunque richiesta rientri in questo elenco è, per definizione, un tentativo di frode — a prescindere da quanto sia convincente la voce, ufficiale il numero o credibile il messaggio. Non c'è eccezione che tenga: di fronte a una di queste richieste, la risposta corretta è una sola, sospendere e verificare attraverso i canali ufficiali.

4.5 Pronti a parlare con la banca

Molti degli strumenti descritti vanno richiesti, attivati o configurati con l'aiuto del proprio referente. Un confronto periodico con la banca è esso stesso una misura di sicurezza. Ecco le domande utili da porre.

- Quali strumenti di protezione antifrode offrite, e quali sono attivi sul mio rapporto?
- Come attivo tutte le notifiche su accessi e operazioni?
- Offrite la verifica del beneficiario (VoP)? Come si presenta al momento del bonifico?
- Posso impostare limiti e massimali per operazione, giornata e canale? Con quali valori?
- Posso configurare profili distinti per disporre e autorizzare i pagamenti, e una doppia autorizzazione sopra soglia?
- Come blocco rapidamente una carta o l'operatività in caso di sospetto, e quali sono i vostri recapiti ufficiali per le emergenze?
- Offrite una verifica rafforzata (step-up) per le operazioni a rischio, e quali la attivano?
- Come gestite il passaggio al token app, e cosa devo fare in caso di cambio o smarrimento del telefono?
- Se disconosco un'operazione, a chi devo rivolgermi e quali informazioni mi verranno chieste?

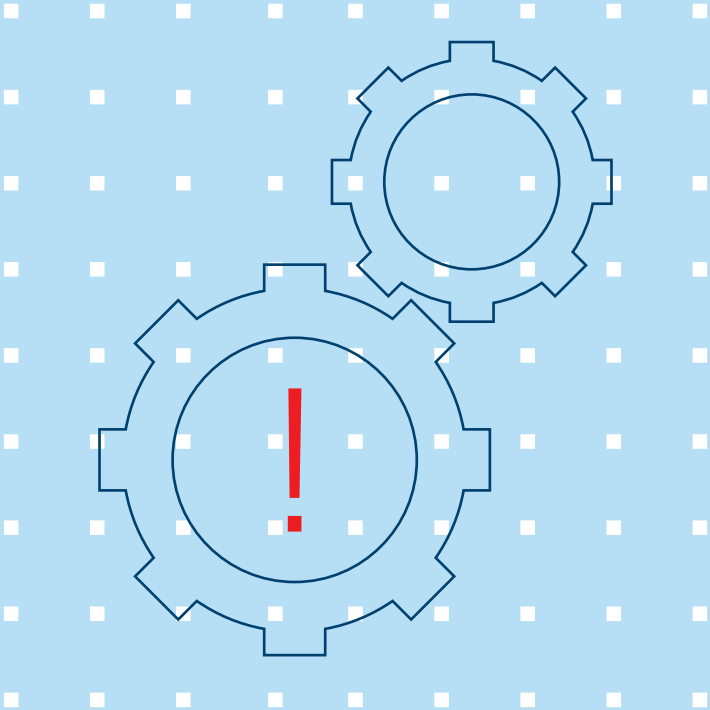
Vale la pena preparare quel confronto anziché improvvisarlo. È utile che vi partecipi, insieme al titolare, anche la persona che materialmente dispone i pagamenti: è lei che userà gli strumenti di cui si parla, ed è lei che si accorgerà per prima se qualcosa non funziona. È opportuno portare un elenco di chi opera sui conti e con quali poteri, perché è il punto di partenza per configurare profili e soglie in modo coerente con la realtà dell'impresa. a memoria.

CASO · La verifica che ha bloccato il bonifico

L'ufficio amministrativo di una piccola impresa sta per saldare una fattura di 31.000 euro verso un fornitore abituale, con cui lavora da anni e che non aveva mai dato problemi. Pochi giorni prima era arrivata una e-mail, apparentemente ordinaria, che comunicava un cambio di coordinate bancarie: stesso tono delle comunicazioni precedenti, firma corretta, riferimenti coerenti alla fattura in scadenza. Al momento di confermare il bonifico, però, la banca segnala che il nome del titolare del conto di destinazione non corrisponde all'IBAN inserito. L'addetta si ferma, evita di procedere per abitudine e telefona al fornitore su un numero già presente in rubrica, non su quello indicato nella mail. Scopre così che nessun cambio di coordinate era mai stato richiesto: la casella del fornitore era stata violata e l'attaccante aveva intercettato la conversazione sulla fattura. La verifica del beneficiario non aveva impedito l'errore da sola — è stata la telefonata a chiuderlo —, ma aveva acceso il dubbio nel momento esatto in cui serviva. Strumento della banca e verifica dell'impresa, insieme, avevano fatto la differenza.

Nei giorni successivi l'impresa fece un'altra cosa, meno visibile ma altrettanto utile: rilesse l'anagrafica dei fornitori per verificare che nessun'altra coordinata fosse stata modificata di recente, e avvisò il fornitore della compromissione, che poté così allertare gli altri clienti. Da allora ogni variazione di IBAN viene confermata per telefono prima di essere registrata. Non è una procedura complessa: è una telefonata, decisa una volta e applicata sempre.

5. GESTIONE DELL'INCIDENTE



Fin qui il manuale ha parlato di prevenzione. Ma nessuna difesa è perfetta, e va messo in conto che un tentativo, prima o poi, vada a segno — per una distrazione, una circostanza sfortunata, un inganno particolarmente curato. Ciò che distingue un danno contenuto da una perdita piena non è, a quel punto, la bravura nell'evitare la frode, ma la **rapidità e l'ordine della reazione.** La prevenzione riduce la probabilità che accada; la gestione dell'incidente riduce il danno quando accade. Sono le due metà della stessa difesa.

Nei pagamenti la variabile dominante è il tempo. Una volta partito un bonifico — tanto più se istantaneo —, i fondi vengono spostati in pochi minuti su una catena di altri conti, i cosiddetti conti di passaggio, e di lì prelevati: oltre una certa soglia di tempo il recupero diventa quasi impossibile. La finestra utile per intervenire si misura in minuti, non in giorni. È la ragione per cui la reazione **non si improvvisa: si prepara.** Chi sa già chi chiamare, con quali recapiti, e chi fa cosa, guadagna i minuti che fanno la differenza. Chi deve cominciare a cercarli nel momento del panico, li perde.

Tre regole guidano l'intera reazione, e conviene tenerle a mente prima ancora di leggere i dettagli: agire *in fretta*, per non lasciare scappare i fondi; agire *in ordine,* seguendo una sequenza decisa a mente fredda; e *non distruggere le tracce,* perché serviranno per il recupero e per la denuncia. Le pagine che seguono organizzano la reazione per orizzonti temporali.

LA PROSPETTIVA DELL'ATTACCANTE

Il suo piano non finisce con il bonifico: quella è appena la metà del lavoro. La **rete dei conti di passaggio** — i cosiddetti muli — è pronta prima ancora che la frode parta, e serve a spezzare la tracciabilità: appena i fondi arrivano, vengono frammentati, spostati su altri conti e prelevati, spesso nel giro di poche ore. In questa fase il suo alleato più efficace è il **silenzio della vittima.** L'imbarazzo, l'incredulità, la speranza che si risolva da sé: ogni ora persa a esitare è un'ora in cui lui mette i fondi al sicuro. Conta sul fatto che chi ha sbagliato tenda a nascondersi, non a reagire.

È per questo che l'unica mossa che il suo piano non assorbe bene è la *reazione immediata:* la chiamata alla banca nei primissimi minuti, il disconoscimento avviato subito, la denuncia sporta senza attendere. La velocità della vittima è l'unica variabile che lui non controlla — ed è precisamente quella su cui si gioca il recupero.

5.1 Le prime due ore

È la fase che decide quasi tutto. L'obiettivo è uno: fermare l'emorragia e mettere in sicurezza ciò che resta, nell'ordine giusto e senza perdere tempo in valutazioni che possono attendere. Le azioni vanno compiute il più rapidamente possibile, idealmente in parallelo.

- **Contattare subito la banca e disconoscere l'operazione.** È la prima telefonata, su un recapito ufficiale già noto: chiedere il blocco dell'operazione e il tentativo di richiamo delle somme, e il blocco di ogni ulteriore disposizione. Contestualmente si avvia il disconoscimento, l'atto formale con cui si dichiara di non riconoscere l'operazione (vi è dedicata la sezione che segue). Più si è tempestivi, più alte sono le probabilità di recuperare.
- **Sporgere denuncia senza attendere.** Avvisare le autorità e presentare denuncia è una priorità immediata, non un adempimento da rimandare: la Polizia Postale è il riferimento per le frodi informatiche. Presentarla subito ha anche un vantaggio pratico — consente di allegarne copia al disconoscimento, rafforzando la propria posizione.
- **Bloccare ciò che è compromesso.** Sospendere il conto, la carta o gli accessi coinvolti; se si sospetta un programma malevolo o un accesso remoto, scollegare immediatamente il dispositivo dalla rete per impedire ulteriori operazioni.
- **Cambiare le credenziali.** Da un dispositivo sicuro e non compromesso, modificare le credenziali di accesso eventualmente carpite, e verificare che non siano stati aggiunti beneficiari o abilitati nuovi dispositivi.
- **Preservare le evidenze.** È il passo più controintuitivo e più importante: non cancellare nulla. Conservare le e-mail (con le loro intestazioni complete), i messaggi, gli SMS, le schermate, i riferimenti delle operazioni Non «ripulire» né reinstallare il dispositivo compromesso. Quelle tracce servono al recupero, al disconoscimento e alla denuncia; distruggerle, anche in buona fede, indebolisce tutto.
- **Avvisare chi deve sapere.** Informare il titolare o il responsabile, e chiunque altro operi sui pagamenti: la stessa frode può essere tentata in parallelo su più persone dell'impresa.

5.2 Il disconoscimento

Quando un'operazione non viene riconosciuta, lo strumento formale per contestarla alla banca si chiama **disconoscimento:** con esso l'impresa dichiara di non riconoscere come

propria un'operazione e ne chiede la restituzione. È il canale ufficiale attraverso cui si attiva la tutela, e va avviato il prima possibile, in parallelo alle altre azioni immediate.

FRODE O TRUFFA: PERCHÉ LA DISTINZIONE CONTA QUI

È in questa fase che la distinzione vista nell'introduzione diventa concreta, perché incide sull'esito. Se l'operazione è stata disposta da altri senza il consenso del titolare — una *frode,* cioè un'operazione non autorizzata —, la disciplina prevede in linea di principio la restituzione delle somme, salvo i casi di colpa grave o dolo del cliente. Se invece è stato il titolare stesso a disporre il pagamento, sia pure ingannato — una *truffa*, cioè una manipolazione —, le tutele automatiche di norma non si applicano, e il recupero dipende dalla tempestività del blocco e dall'esito delle verifiche. Questo quadro, però, è in evoluzione. Il nuovo regolamento europeo sui servizi di pagamento — la *PSR,* destinata ad aggiornare la cornice della PSD2 — è orientato ad ampliare le tutele anche in alcune ipotesi oggi scoperte, come determinati casi di impersonificazione della banca. È bene perciò informarsi sullo stato della normativa al momento del fatto: le tutele effettivamente applicabili potrebbero risultare più ampie di quelle qui descritte, e conviene non darle per escluse a priori.

LA MEMORIA, E COME PREPARARLA

Nell'ambito del disconoscimento la banca chiede di norma all'impresa un resoconto scritto dell'accaduto — una **memoria** — sulla cui base conduce poi le proprie verifiche. Prepararla con cura non è un adempimento burocratico: è il modo in cui l'impresa rappresenta la propria posizione, e una memoria chiara e documentata è la base di una tutela solida. Conviene che sia:

- **Cronologica e chiara:** cosa è successo, quando, come è arrivata la richiesta fraudolenta e quali passaggi si sono susseguiti, in ordine di tempo.
- **Circostanziata:** accompagnata dalle evidenze raccolte — le e-mail con le intestazioni complete, i messaggi, le schermate, i riferimenti delle operazioni contestate.
- **Accompagnata dalla denuncia:** allegare copia della denuncia già presentata rafforza il resoconto ed è la ragione per cui conviene sporgerla subito.

Vale la pena avere chiaro, in conclusione, ciò che spetta all'impresa in questo processo: **segnalare e disconoscere senza ritardo, fornire un resoconto accurato e completo,**

conservare e trasmettere le evidenze, presentare la denuncia. È la parte di competenza dell'impresa, e quanto più è curata e tempestiva, tanto più solido ne risulta il presupposto della tutela.

5.3 Le prime quarantotto ore

Avviati il disconoscimento e la denuncia, restano i passaggi che danno seguito alla reazione e che aiutano a chiudere le falle ancora aperte.

- **Segnalare l'incidente.** Per gli incidenti di natura informatica, il CSIRT Italia — la struttura nazionale presso l'Agenzia per la Cybersicurezza Nazionale — è il punto di riferimento in caso di imprese con obbligo di segnalazione. Contribuisce anche a proteggere altri da attacchi analoghi.
- **Avvisare i terzi coinvolti.** Se la frode è passata dalla casella compromessa di un fornitore o di un cliente, avvisarlo: la stessa compromissione viene usata, di norma, verso più controparti. Se sono coinvolti dati personali, valutare con un consulente gli obblighi di notifica previsti dalla normativa sulla protezione dei dati.
- **Coinvolgere i consulenti.** Il commercialista per i profili contabili e fiscali, un legale per le azioni di recupero, e — se serve — un tecnico per esaminare i dispositivi compromessi prima di rimetterli in uso.
- **Ricostruire l'accaduto.** Mettere in fila, con calma, come la frode è entrata e quali sistemi e persone ha toccato. Serve a chiudere le falle ancora aperte e a impostare la fase successiva.

5.4 Dopo: imparare dall'incidente

Passata l'emergenza, resta la domanda che più conta per il futuro: **dove ha ceduto la catena?** Ogni frode che va a segno indica, con precisione, il punto in cui mancava una verifica — un cambio di coordinate non controllato, un'autorizzazione lasciata a una sola persona, una credenziale condivisa. Individuarlo senza cercare un colpevole, ma una causa, è il primo passo per non ripetere l'esperienza. Da lì, l'aggiornamento dei presìdi: correggere la procedura che si è rivelata debole, rivedere soglie e profili, rafforzare la formazione sul

tipo di inganno subìto. È il momento in cui la gestione dell'incidente si ricongiunge alla prevenzione, e l'esperienza dolorosa di una frode diventa la difesa contro la prossima. Vale, anche qui, il principio della Parte III: la reazione, una volta compresa, diventa architettura. Un'ultima avvertenza, di metodo. La reazione descritta funziona se è stata preparata: i recapiti raccolti in anticipo, i ruoli assegnati, la sequenza nota a chi opera.

5.5 A chi rivolgersi

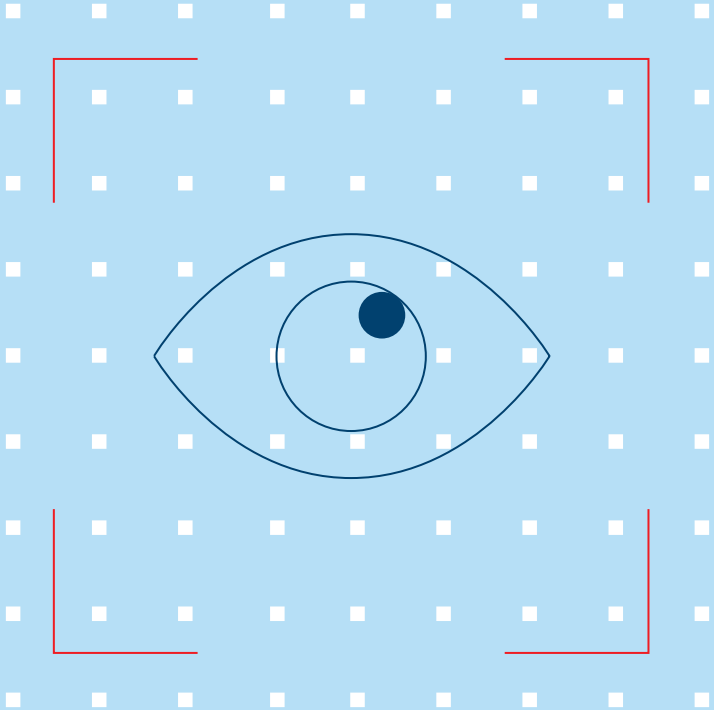
Conviene preparare in anticipo una rubrica con i recapiti certi, da tenere accessibile anche quando i sistemi aziendali non lo fossero. Lo schema seguente indica chi contattare e per cosa; i recapiti puntuali andranno raccolti e verificati dall'impresa, e sono richiamati nell'appendice dei contatti.

Situazione	Chi contattare
Pagamento fraudolento appena disposto	La propria banca, sui recapiti ufficiali di emergenza, per il blocco e il richiamo dei fondi
Frode subìta, da denunciare	La Polizia Postale (denuncia)
Incidente informatico (accessi, malware)	Il CSIRT Italia, presso l'Agenzia per la Cybersicurezza Nazionale
Profili contabili, fiscali e legali	Commercialista e legale di fiducia
Dati personali coinvolti	Un consulente, per valutare gli obblighi di notifica

CASO · Le prime due ore

Un'impresa di servizi si accorge, a metà mattina, che un bonifico di 54.000 euro è partito verso un IBAN sbagliato a seguito di una richiesta fraudolenta. L'addetta non perde tempo: chiama subito la banca sul numero di emergenza che l'impresa teneva annotato, ottiene il blocco del tentativo di accredito e l'avvio del richiamo dei fondi, mentre il titolare sporge denuncia nel pomeriggio. Grazie alla rapidità, gran parte della somma — non ancora prelevata dai conti di passaggio — viene bloccata e recuperata. La differenza non l'ha fatta una tecnologia, ma il fatto che l'impresa sapeva già chi chiamare e in quale ordine agire. Le stesse due ore, spese a cercare un numero e a decidere il da farsi, avrebbero avuto un esito molto diverso.

6. IL FATTORE UMANO



Un'apparente contraddizione attraversa questo manuale. La Parte III ha sostenuto che non ci si può affidare all'attenzione delle persone, e che la difesa va incorporata nel processo. Questa parte, invece, parla di persone. Le due cose non si contraddicono: si completano. Il processo è la prima linea, perché non dipende dalla lucidità del singolo in un dato momento; ma il processo è **fatto di persone,** sono loro ad applicarlo, e persone consapevoli lo applicano meglio e resistono quando l'inganno arriva. La tecnologia e le procedure spostano molto; l'ultimo metro, però, lo percorre sempre un essere umano.

Conviene perciò dire con chiarezza una cosa che toglie peso e aiuta a ragionare: **cadere in un inganno ben costruito non è una questione di intelligenza.** Le frodi moderne sono progettate da professionisti per sfruttare meccanismi mentali che appartengono a tutti, e che si attivano soprattutto sotto pressione. Chiunque, nel momento sbagliato, può abbassare la guardia. Riconoscere questo non è una resa: è il presupposto per costruire difese — culturali, non solo tecniche — che reggano davvero.

LA PROSPETTIVA DELL'ATTACCANTE

Non sceglie le vittime più ingenue — un errore comune è crederlo. Sceglie i **momenti più fragili:** la fine di una giornata lunga, il venerdì, la corsa di una chiusura fiscale, l'assenza del titolare. E sceglie le persone più **isolate**, quelle che in quel momento non hanno accanto un collega a cui girare un dubbio. La vulnerabilità che sfrutta non è un tratto della persona, ma una condizione del contesto.

Perché per lui la manipolazione non è un colpo di fortuna: è un *processo*. Ha copioni che affina, ruoli che si dividono, varianti che mette alla prova per capire quale funziona meglio, percentuali di successo da migliorare. Ragiona come chi ottimizza una campagna, non come chi tenta un azzardo.

Contro un avversario così metodico, la difesa non può essere l'attenzione del singolo nel momento peggiore — che è proprio quello che lui ha scelto. Può esserlo solo una cultura condivisa, in cui verificare è normale e chiedere aiuto non è debolezza: qualcosa che **non dipende dallo stato d'animo di una persona sola.**

6.1 Le leve della manipolazione

La frode che colpisce le persone — l'*ingegneria sociale,* in inglese *social engineering* — non agisce a caso. Preme alcuni pulsanti psicologici precisi, gli stessi che regolano molte delle nostre decisioni quotidiane. Conoscerli è il primo antidoto, perché un meccanismo riconosciuto perde gran parte della sua forza.

- **L'autorità.** Tendiamo a obbedire a chi percepiamo come legittimo o superiore. È la leva del finto amministratore delegato e della finta banca: il solo presentarsi come tali abbassa la nostra resistenza.

- **L'urgenza.** La fretta spegne il pensiero critico. «Subito, o si perde tutto» non è un'informazione, è uno strumento: serve a comprimere il tempo in cui una verifica sarebbe possibile.

- **La fiducia e la familiarità.** Abbassiamo la guardia davanti a ciò che sembra noto: un logo conosciuto, il nome di un fornitore abituale, il tono di un collega. È il motivo per cui le caselle compromesse sono così efficaci.

- **La paura.** La minaccia di una conseguenza — il conto bloccato, una sanzione, un danno — spinge ad agire d'impulso, saltando i controlli proprio quando servirebbero di più.

Il punto più utile da trattenere riguarda la loro **combinazione**. Quando una richiesta attiva contemporaneamente più di queste leve — un'autorità che impone urgenza e chiede riservatezza —, non è una coincidenza: è la firma della manipolazione. Quella sovrapposizione, più di qualunque dettaglio tecnico, è il segnale che impone di fermarsi e verificare.

6.2 Quando l'inganno parte da un contesto autentico

Le leve appena descritte diventano molto più potenti quando il frodatore non deve costruire da zero un contesto credibile, ma può inserirsi in uno vero. È la frontiera più insidiosa dell'inganno contemporaneo, e va compresa perché manda in crisi le difese fondate sull'intuito.

Il punto di partenza è che il frodatore raramente attacca l'impresa di petto. Più spesso compromette un anello della catena di cui l'impresa si fida: **un fornitore, un cliente, un consulente, un partner.** Violata la casella di posta di una di queste terze parti, ne osserva la corrispondenza anche per settimane — chi scrive a chi, su quali pratiche, con quali importi e scadenze — e attende il momento opportuno. La fiducia che lega le imprese tra loro, di norma una risorsa, diventa così il veicolo dell'attacco. Ne discende una verità scomoda: la sicurezza di un'impresa dipende anche da quella dei suoi interlocutori, sui quali non ha alcun controllo. Un fornitore con la posta mal protetta è un rischio per tutti i suoi clienti.

La tecnica più raffinata che ne deriva è il **dirottamento della conversazione** (in inglese *thread hijacking*). Invece di inviare un messaggio nuovo — che potrebbe insospettire — il frodatore **risponde a un carteggio reale e già in corso,** con tutto lo storico della conversazione sotto. Il messaggio arriva dal mittente atteso, dentro uno scambio che il destinatario riconosce, e cita dettagli veri perché veri sono. È in quel punto — dove ogni cosa torna — che viene inserita la richiesta fraudolenta: il cambio di IBAN, l'urgenza improvvisa, la nuova coordinata «per il prossimo pagamento».

L'effetto è che quasi tutti i segnali d'allarme tradizionali svaniscono: nessun mittente sconosciuto, nessun contesto inventato, nessun errore grossolano di lingua o di grafica. L'inganno non si presenta travestito da estraneo; *arriva dentro l'atteso.* È qui che gran parte della formazione tradizionale mostra il proprio limite, e che questa parte si ricongiunge alla governance. Insegnare a «diffidare dell'inatteso» funziona contro le frodi rozze, non contro quelle che si innestano nel familiare: se l'inganno indossa il volto di una conversazione autentica, non «puzzerà» affatto, e il giudizio del momento — «questa e-mail non mi convince» — non scatterà.

La conseguenza è netta: contro l'inganno che parte da un contesto vero, l'unica difesa affidabile è quella **strutturale,** che scatta a prescindere dall'impressione. La verifica out-of-band su ogni cambio di coordinate non è la reazione a un messaggio sospetto; è una regola che vale anche — e soprattutto — quando il messaggio sembra perfetto. La cultura della verifica, in altre parole, deve proteggere non dall'evidentemente falso, ma dal perfettamente credibile.

6.3 La cultura della verifica

Se l'inganno può indossare il volto del familiare, la verifica non può restare un istinto occasionale: deve diventare **cultura**, cioè il modo normale e atteso di lavorare. Negli scenari è tornata più volte una frase — nessuna richiesta legittima viene mai compromessa da una verifica —, ma perché quel principio funzioni non basta enunciarlo. In un'impresa dove fermarsi a controllare è visto come perdita di tempo o segno di sfiducia, le verifiche salteranno proprio quando servono. In un'impresa dove verificare è la prassi, il frodatore perde la sua arma migliore.

Il fattore decisivo, qui, è il **vertice.** La cultura della verifica si costruisce o si distrugge dall'alto. Se il titolare o il responsabile si spazientisce quando un collaboratore chiede conferma di una sua richiesta, insegna a tutti che verificare è sbagliato — e apre la strada alla frode del finto vertice, che su quella reticenza conta. Se invece incoraggia la verifica, e accetta per primo di esservi sottoposto, la rende legittima. Conviene dirlo in modo esplicito a chi gestisce i pagamenti: fermarsi a verificare è dovuto e gradito, non sarà mai considerato un intralcio né una mancanza di fiducia.

C'è poi un ulteriore aspetto organizzativo del doppio controllo che per chi lavora è forse il più prezioso. Il four eyes non protegge soltanto l'impresa da frodi esterne (ed interne): protegge la persona. Chi opera sapendo che nessun pagamento può partire dalla sua sola decisione ha, di fronte a qualunque pressione, una via d'uscita semplice e inattaccabile: «non dipende da me, la procedura richiede una seconda approvazione». È una frase che disinnesca l'urgenza, scoraggia il frodatore e solleva il singolo dal peso di decidere da solo nel momento peggiore. La separazione dei compiti, vista da qui, non è un vincolo imposto alle persone: è una tutela che l'impresa offre loro.

6.4 Formazione e simulazioni

La consapevolezza non si improvvisa: si costruisce con la formazione. Ma una formazione che funzioni ha alcune caratteristiche che la distinguono dall'adempimento dimenticato il giorno dopo. Deve essere *concreta* — fondata su scenari reali come quelli della Parte II, non su principi astratti —; *continua,* perché le tecniche di frode evolvono e una formazione di tre anni fa è in parte superata; e *calibrata sui ruoli,* perché chi di-

spone i pagamenti ha bisogno di sapere cose diverse da chi si occupa d'altro. L'obiettivo non è trasformare ognuno in un esperto, ma far sì che chi opera riconosca i segnali e sappia cosa fare. Uno strumento particolarmente efficace è la **simulazione.** Inviare deliberatamente, all'interno dell'impresa, finte e-mail fraudolente o finte richieste urgenti — l'*urgenza simulata* — permette di allenare le persone in condizioni reali ma sicure, e di misurare quanto i presìdi reggono. L'errore commesso in una simulazione è gratuito; quello commesso davanti a una frode vera, no. Vale però una regola ferma: la simulazione **serve a formare,** non a punire. Chi vi incappa va accompagnato e istruito, mai messo alla berlina — altrimenti l'unica lezione appresa sarà nascondere l'errore la volta successiva, che è esattamente l'opposto di ciò che serve.

6.5 Il valore di dirlo subito

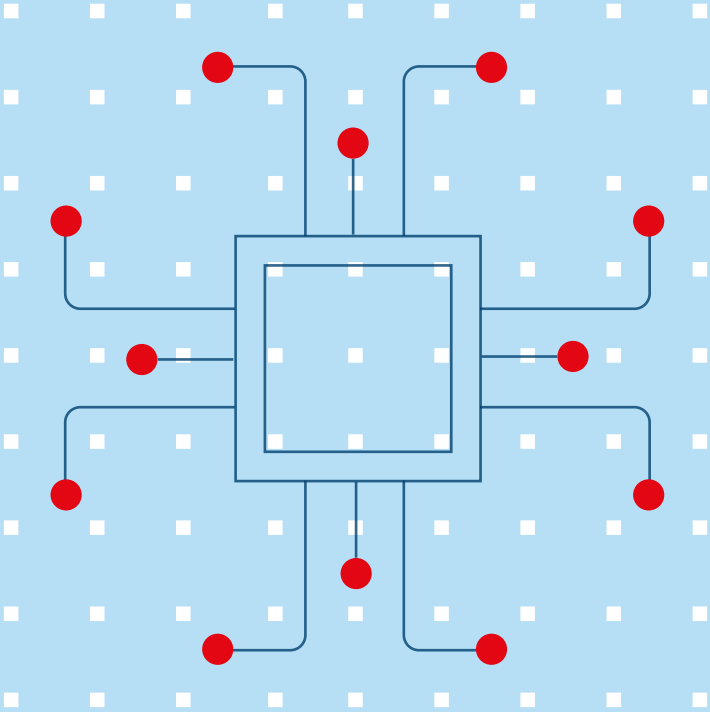
C'è un ultimo tratto della cultura aziendale che incide sulla sicurezza più di quanto si creda, e si lega direttamente alla gestione dell'incidente. L'errore più costoso, di fronte a una frode, raramente è cadere nell'inganno: è **tacerlo.** Per paura, per vergogna, nella speranza che si sistemi da sé, chi ha sbagliato spesso aspetta — e in quell'attesa si bruciano i minuti che, come si è visto nella Parte V, decidono se i fondi si recuperano.

Per questo un'impresa che voglia davvero proteggersi deve costruire un clima in cui segnalare un proprio errore, o anche solo un dubbio, sia **sicuro** e **incoraggiato.** Chi alza la mano per dire «forse ho sbagliato» va ringraziato, non rimproverato, perché sta regalando all'impresa il tempo per reagire. La sicurezza, in ultima analisi, non è fatta di persone che non sbagliano mai — non esistono —, ma di persone che, quando qualcosa va storto, lo dicono subito.

CASO · L'e-mail che era già stata vista

Un'impresa aveva svolto, qualche mese prima, una semplice simulazione interna: una finta e-mail del titolare che chiedeva un bonifico urgente e riservato. Diversi collaboratori, allora, ci erano cascati — senza conseguenze, ma con una discussione franca su cosa fosse andato storto. Quando arrivò la richiesta vera, costruita quasi allo stesso modo, l'addetta amministrativa ebbe un'esitazione precisa: l'aveva già vista. Si fermò, telefonò al titolare su un numero noto, e la frode si fermò lì. Non era diventata un'esperta di sicurezza; aveva semplicemente riconosciuto uno schema che le era già stato mostrato, in un contesto in cui sbagliare era stato permesso.

7. LE FRODI POTENZIATE DALL'INTELLIGENZA ARTIFICIALE



Tutto ciò che si è detto finora resta valido. Questa parte non descrive una minaccia nuova, ma un **salto di scala e di credibilità** delle minacce già note. L'intelligenza artificiale generativa non ha inventato la frode del finto amministratore delegato o la richiesta urgente: le ha rese enormemente più convincenti, più rapide da produrre e più economiche da lanciare. È bene conoscerne i contorni, senza allarmismo ma senza sottovalutazione, perché è la direzione verso cui il fenomeno si sta muovendo.

Per coglierne la portata occorre andare oltre l'aspetto più appariscente — la voce o il video falsi — e fermarsi sull'implicazione di fondo, che è di natura economica. Per molto tempo le frodi più sofisticate hanno richiesto competenze, tempo e mezzi: bisognava saper scrivere in una lingua impeccabile, conoscere la vittima, costruire un inganno su misura. Erano barriere — tecniche ed economiche — che limitavano il numero di chi poteva permettersi quel tipo di attacco. L'intelligenza artificiale ha abbattuto quelle barriere.

È questo il punto che merita di essere còlto fino in fondo: l'**IA abbassa il costo e la difficoltà del crimine finanziario**. Ciò che prima richiedeva un gruppo organizzato e competente, oggi è alla portata di un singolo, con strumenti acquistabili a poco prezzo e nessuna competenza specialistica. È nata una vera e propria offerta di «frode come servizio»: kit, modelli e strumenti automatizzati, venduti o affittati, che chiunque può impiegare. La conseguenza non è solo che le frodi diventano più credibili, ma che diventano **più numerose**, perché si è allargata enormemente la platea di chi può commetterle. Gli osservatori di mercato concordano su una previsione netta: nei prossimi anni le perdite da frodi rese possibili dall'IA cresceranno a ritmi che non hanno precedenti, trainate proprio da questa accessibilità[8].

LA PROSPETTIVA DELL'ATTACCANTE

Per l'attaccante l'intelligenza artificiale è, prima di ogni altra cosa, un **abbattimento di costi**. Dove serviva un madrelingua per un testo credibile, ora basta un modello; dove serviva un imitatore per una voce, bastano pochi secondi di audio pubblico; dove serviva un falsario, basta un software. Ciò che un tempo richiedeva competenze rare, e quindi costose, oggi è alla portata di chiunque.

[8] Riferimenti: analisi di mercato e di società di consulenza sull'impatto dell'IA generativa nelle frodi finanziarie, 2024-2025.

La conseguenza più profonda non è che le frodi diventano più sofisticate, ma che la **sofisticazione si democratizza**. La qualità che un tempo distingueva il crimine organizzato dal truffatore improvvisato è ora compresa nel prezzo di un kit, venduto o affittato a chi non saprebbe costruirla. La platea di chi può colpire, e colpire bene, si allarga enormemente.

Il suo calcolo cambia di conseguenza: **più tentativi, più credibili, allo stesso costo** Ma — ed è ciò che conta per chi si difende — cambia lo strumento, non la struttura dell'inganno. L'obiettivo resta convincere una persona a disporre un pagamento che non dovrebbe; e le difese che valgono restano quelle che agiscono a valle della credibilità, verificando i fatti invece di giudicare le apparenze.

7.1 La voce clonata

La prima applicazione, e oggi la più diffusa, è la clonazione della voce. A partire da pochi secondi di audio — una telefonata, un messaggio vocale, un intervento a una conferenza reperibile in rete — è possibile generare una voce sintetica che riproduce in modo convincente quella di una persona reale: il timbro, la cadenza, perfino l'intonazione. Quella voce può poi essere usata, in una telefonata, per impartire un ordine di pagamento urgente che sembra provenire dal titolare o da un dirigente.

È l'evoluzione diretta della frode del finto vertice e del vishing visti nella Parte II, con un'aggravante: viene a mancare proprio l'elemento su cui istintivamente ci si affidava — il riconoscimento della voce. «L'ho sentito, era lui» non è più una prova. Già nel 2019 un'impresa europea del settore energetico fu indotta a versare circa 220.000 euro da una telefonata che riproduceva la voce del proprio amministratore delegato; oggi gli strumenti per farlo sono alla portata di chiunque, e non richiedono competenze tecniche né investimenti significativi.

7.2 Il volto falsificato: i deepfake in video

Lo stesso principio si applica alle immagini e ai video. Un *deepfake* è un video sintetico che riproduce il volto e i movimenti di una persona reale, fino a poterla far comparire, in tempo reale, in una videochiamata. È la frontiera più impressionante e più inquietante del

fenomeno, perché abbatte l'ultima difesa intuitiva rimasta: vedere il proprio interlocutore. Il caso che ha segnato uno spartiacque è avvenuto a inizio 2024. Un dipendente della sede di Hong Kong di una nota società di ingegneria fu invitato a una videoconferenza con quello che credeva essere il direttore finanziario del gruppo, basato nel Regno Unito, e altri colleghi. Tutti i partecipanti, tranne lui, erano **ricostruzioni artificiali**, generate a partire da video e audio pubblicamente disponibili dei dirigenti reali. Convinto dalla scena, il dipendente eseguì quindici bonifici per circa 25 milioni di dollari. La frode emerse soltanto quando, in un secondo momento, contattò la sede centrale[9].

Quel caso insegna due cose. La prima è che l'attacco non era partito dal video: era cominciato con una banale e-mail che annunciava una «transazione riservata» — esattamente lo schema della frode del vertice —, e il dipendente, inizialmente, ne aveva diffidato. È stata la videochiamata, con la sua parvenza di prova inoppugnabile, a vincere la sua cautela. La seconda è che nessun sistema era stato violato: non un accesso forzato, non un programma malevolo. L'attacco non è passato per la rete, ma **attraverso una persona**. E si è chiuso, alla fine, con l'unica difesa che ha tenuto: una verifica indipendente, condotta su un altro canale.

7.3 Testi perfetti, su larga scala

Meno spettacolare, ma forse più insidiosa nel quotidiano, è l'applicazione dell'IA alla parola scritta. Le e-mail fraudolente di un tempo si riconoscevano spesso per gli errori di lingua, le frasi sgrammaticate, il tono incerto. Quel segnale d'allarme è scomparso. Oggi un'IA produce in pochi istanti messaggi impeccabili, nella lingua e nel registro giusti, calibrati sul destinatario; e può farlo per migliaia di bersagli contemporaneamente, a costo quasi nullo. Si stima che la grande maggioranza delle e-mail di phishing contenga ormai testo generato dall'IA, e che questi messaggi ottengano tassi di successo sensibilmente più alti di quelli scritti a mano[10]. Unita alla compromissione di una casella autentica e al dirottamento di una conversazione reale — i meccanismi descritti nella Parte VI —, questa capacità rende l'inganno scritto quasi indistinguibile da una comunicazione legittima. È la conferma definitiva di un principio già incontrato: la difesa non può più poggiare sulla ricerca dell'errore o sull'impressione di autenticità, perché errori non ce ne sono più e l'autenticità è simulabile.

[9] Fonti: CNN Business e Polizia di Hong Kong, 2024.

[10] Riferimenti: analisi di settore su phishing e contenuti generati da IA, 2025.

7.4 Uno sguardo al futuro: le identità sintetiche

Vale la pena, in chiusura, alzare lo sguardo su un fenomeno che oggi tocca soprattutto banche e intermediari, ma la cui logica è destinata a riguardare più da vicino anche le imprese. Finora si è parlato di frodatori che imitano una persona reale; lo stadio successivo è la costruzione di **identità che non esistono**, le cosiddette identità sintetiche.

Il meccanismo combina frammenti di dati veri — sottratti da violazioni e reperibili a basso costo — con dati inventati, fino a comporre una «persona» del tutto plausibile: un nome, una storia, dei documenti, perfino una presenza credibile in rete. L'intelligenza artificiale rende questo assemblaggio rapido e convincente, generando documenti, volti e profili coerenti che superano i controlli superficiali. È, secondo più osservatori, tra le forme di frode in più rapida crescita, e la sua insidia sta in un punto preciso: i sistemi di verifica tradizionali sono fatti per accertare che un'identità *esista*, non che sia *reale*.

Per un'impresa la rilevanza è duplice e indiretta, ma concreta. Un'identità sintetica può presentarsi come un **nuovo cliente** che non pagherà mai, o come un **fornitore inesistente** costruito ad arte per emettere richieste di pagamento credibili. Senza voler trasformare l'imprenditore in un investigatore, il principio difensivo resta quello che attraversa l'intero manuale: la verifica di chi si ha di fronte — un nuovo fornitore, una nuova controparte — non può fermarsi all'apparenza dei documenti, ma deve poggiare su riscontri indipendenti prima che un rapporto si traduca in un pagamento. È la stessa logica della verifica del beneficiario e del riscontro in anagrafica, applicata all'identità di chi entra nel giro d'affari.

Non è una ragione per allarmarsi, ma per restare informati: è un fronte in evoluzione, su cui banche e autorità stanno costruendo nuove difese, e di cui conviene seguire gli sviluppi senza farsi cogliere impreparati.

7.5 Cosa cambia, e cosa non cambia

Di fronte a tutto questo la reazione istintiva è lo sgomento: se la voce, il volto e le parole si possono falsificare, di che cosa ci si può ancora fidare? La risposta, però, è più rassicurante di quanto sembri, e costituisce il filo che lega questa parte all'intero manuale. L'**IA cambia gli strumenti dell'inganno, non la sua struttura**. Per quanto perfetta sia la voce o il video, l'obiettivo resta sempre lo stesso: convincere una persona a disporre un

pagamento, di norma con urgenza, riservatezza e verso una destinazione nuova.

E proprio perché la struttura non cambia, non cambiano nemmeno le difese. Una voce clonata che chiede un bonifico urgente resta una richiesta da verificare su un canale indipendente. Un video del direttore che ordina una «transazione riservata» non supera il controllo a quattro occhi né la conferma su un recapito noto. Una mail perfetta che annuncia un cambio di IBAN cede, comunque, di fronte a una telefonata di verifica. **Le difese strutturali costruite nelle parti precedenti — separazione dei compiti, controllo four eyes, verifica out-of-band, soglie — non vengono indebolite dall'intelligenza artificiale: ne diventano, anzi, l'unica risposta adeguata**, perché funzionano a prescindere da quanto l'inganno sia convincente.

Cambia, semmai, l'intensità con cui vanno applicate. Se «l'ho visto e sentito» non è più una garanzia, allora la verifica indipendente non è più un di più riservato ai casi dubbi: diventa la regola anche quando ogni cosa appare in ordine. È bene, infine, che chi opera sappia che queste tecnologie esistono — perché un inganno che non si immagina possibile è molto più efficace —, e che concordi un dettaglio semplice ma prezioso: una parola o una domanda di sicurezza, nota solo alle persone reali, che nessuna voce clonata potrà conoscere.

CASO · La voce del titolare

L'addetta amministrativa di una piccola impresa riceve una telefonata dal titolare, riconoscibilissimo nella voce: chiede con urgenza un bonifico a un nuovo fornitore, mentre è «in riunione e non può parlare a lungo». Tutto torna, persino il tono brusco di chi ha fretta. Ma la regola interna, per i pagamenti a nuovi beneficiari, non fa eccezioni: si verifica sempre con un messaggio sul canale concordato. L'addetta scrive al titolare la domanda convenuta. La risposta non arriva — perché il vero titolare era davvero in riunione, ignaro di tutto, e la voce al telefono era stata clonata da un suo intervento pubblico. La tecnologia era nuova; la difesa che l'ha fermata era quella di sempre.

NOTA DI CHIUSURA

Questo manuale ha attraversato il rischio e i suoi scenari, la governance interna e gli strumenti, la gestione dell'incidente, il fattore umano e le frodi potenziate dall'intelligenza artificiale. Un percorso ampio, che però ruota intorno a un'idea sola, e conviene riaffermarla con semplicità: la sicurezza dei pagamenti non è un prodotto che si acquista né una tecnologia che si installa. È un modo di lavorare.

Le tecniche dei frodatori cambieranno ancora — la voce e il volto falsificati di oggi saranno superati da altro domani —, ma la struttura dell'inganno resta quella di sempre: convincere una persona a disporre un pagamento che non dovrebbe. Per questo le difese che contano non sono quelle più sofisticate, ma quelle più **costanti**: separare i compiti, verificare su un canale indipendente, non lasciare che nessuno decida da solo, dubitare con metodo anche di ciò che sembra perfetto. Poche regole, applicate sempre.

Non serve essere una grande impresa per difendersi bene. Serve proporzione e costanza: scegliere i presìdi adatti alla propria dimensione e tenerli vivi nel tempo. Se questo manuale lascia una sola convinzione, è che la sicurezza dei pagamenti è alla portata di qualunque impresa decida di farne una pratica quotidiana, e non un pensiero rimandato al giorno in cui sarà troppo tardi.

A | Glossario

Una raccolta dei termini tecnici usati nel manuale, in forma sintetica. I riferimenti normativi sono raccolti nell'Appendice B.

ACCOUNT TAKEOVER (presa di controllo dell'account). La situazione in cui un frodatore ottiene il controllo della casella di posta o del profilo di una persona, e la usa per condurre o agevolare la frode.

AUTENTICAZIONE FORTE (SCA). Dall'inglese Strong Customer Authentication. La verifica dell'identità che combina almeno due fattori tra qualcosa che si sa (una password), qualcosa che si ha (un dispositivo) e qualcosa che si è (un dato biometrico).

BEC (Business Email Compromise). La compromissione o l'imitazione della posta aziendale per inserirsi nelle comunicazioni e indurre pagamenti fraudolenti.

BIOMETRIA. Il riconoscimento basato su un tratto fisico, come l'impronta o il volto. Può essere gestita dal dispositivo o, in soluzioni più avanzate, legata all'identità del cliente presso la banca (CIAM).

CEO FRAUD (frode del finto amministratore delegato). L'inganno in cui il frodatore si finge una figura apicale per ordinare un pagamento urgente e riservato.

CIAM (Customer Identity and Access Management). La gestione dell'identità del cliente da parte dei sistemi della banca; nella biometria, indica un riconoscimento legato alla persona e non solo al dispositivo.

CONTI DI PASSAGGIO (money mule). Conti, spesso intestati a prestanome, su cui i fondi frodati transitano rapidamente per renderne difficile il recupero.

DEEPFAKE. Un video o un'immagine sintetica, generata dall'intelligenza artificiale, che riproduce in modo realistico il volto e i movimenti di una persona reale.

DISCONOSCIMENTO. L'atto formale con cui il cliente dichiara alla banca di non riconoscere un'operazione e ne chiede la restituzione.

FOUR EYES / SIX EYES. Il controllo che richiede l'intervento di due (four eyes) o tre (six eyes) persone diverse per autorizzare un'operazione.

IDENTITÀ SINTETICA. Un'identità del tutto inesistente, costruita combinando dati reali sottratti e dati inventati, fino ad apparire una persona vera.

INGEGNERIA SOCIALE (social engineering). L'insieme delle tecniche che manipolano le persone — facendo leva su autorità, urgenza, fiducia, paura — anziché aggirare i sistemi tecnici.

INSTANT PAYMENT (bonifico istantaneo). Un bonifico eseguito in pochi secondi e irrevocabile: una volta partito, non può essere fermato.

MALICIOUS ENROLLMENT (registrazione fraudolenta di un dispositivo). L'abilitazione, da parte di un frodatore, di un proprio dispositivo come strumento valido per autorizzare i pagamenti della vittima.

MFA (autenticazione a più fattori). L'uso di più fattori indipendenti per accedere o autorizzare, così che la sottrazione di uno solo non basti.

OTP (codice usa e getta). Un codice valido una sola volta, generato o inviato per confermare un'operazione.

OUT-OF-BAND. La verifica condotta su un canale diverso e indipendente da quello con cui è arrivata la richiesta.

PHISHING, VISHING, SMISHING. L'inganno condotto, rispettivamente, via e-mail, per telefono e via SMS, per carpire dati o indurre azioni.

SECURITY BY DESIGN. Il principio per cui la sicurezza è incorporata nel processo fin dalla sua progettazione, e non aggiunta in seguito.

SEPARAZIONE DEI COMPITI (SoD). Dall'inglese segregation of duties. La suddivisione delle funzioni di un pagamento tra persone diverse, così che nessuno controlli sé stesso.

SIM SWAP (sostituzione fraudolenta della SIM). La tecnica con cui un criminale dirotta su di sé il numero di telefono della vittima, intercettandone i messaggi, inclusi gli OTP.

SISTEMA DI INTERSCAMBIO (SDI). Il sistema dell'Agenzia delle Entrate attraverso cui transitano le fatture elettroniche tra imprese italiane.

SPOOFING. La falsificazione dell'identità del mittente — il numero di telefono, l'indirizzo e-mail — per apparire un soggetto legittimo.

STEP-UP AUTHENTICATION. L'autenticazione che si innalza, richiedendo un fattore aggiuntivo, quando un'operazione presenta un rischio maggiore.

THREAD HIJACKING (dirottamento della conversazione). L'inserimento del frodatore in un carteggio di posta reale e già in corso, per rendere credibile la richiesta fraudolenta.

TOKEN (SMS, FISICO, APP). Lo strumento che autorizza un'operazione: un codice via SMS, un oggetto fisico che genera codici, o l'applicazione della banca che approva tramite notifica.

TRUFFA E FRODE. Nel linguaggio di questo manuale, la frode è l'operazione disposta da altri senza il consenso del titolare; la truffa è il pagamento disposto dal titolare stesso, ma ingannato (manipolazione).

VOP (VERIFICATION OF PAYEE). La verifica del beneficiario: il confronto, prima di un bonifico, tra il nome del titolare del conto e l'IBAN indicato.

B | Quadro normativo essenziale

Una mappa sintetica delle principali norme che fanno da sfondo alla sicurezza dei pagamenti. Alcune sono in evoluzione: per i dettagli e lo stato di applicazione conviene fare riferimento alle fonti ufficiali al momento della consultazione.

PSD2 e autenticazione forte

La seconda Direttiva europea sui servizi di pagamento (PSD2) ha introdotto, tra l'altro, l'obbligo dell'autenticazione forte del cliente (SCA) per l'accesso ai conti e per le operazioni di pagamento. È la base normativa del secondo fattore — il token — di cui si è parlato nel manuale.

PSD3 E PSR

La cornice della PSD2 è in corso di aggiornamento attraverso una nuova direttiva (PSD3) e un regolamento sui servizi di pagamento (PSR). Tra gli obiettivi figura il rafforzamento della lotta alle frodi, con un'attenzione anche ad alcune ipotesi di truffa oggi meno tutelate, come determinati casi di impersonificazione della banca. Trattandosi di norme in iter, è bene verificarne lo stato e i contenuti effettivi al momento dell'applicazione.

IPR — Regolamento sui pagamenti istantanei

Il regolamento europeo sui pagamenti istantanei ha favorito la diffusione del bonifico istantaneo, equiparandone le condizioni a quelle del bonifico ordinario, e ha reso disponibile il servizio di verifica del beneficiario (VoP) prima della disposizione di un bonifico.

DORA — Resilienza operativa digitale

Il regolamento sulla resilienza operativa digitale (DORA) rafforza i presìdi di sicurezza e continuità del settore finanziario. Riguarda direttamente gli intermediari, ma incide sull'intero ecosistema in cui le imprese operano.

NIS2 — Sicurezza delle reti e dei sistemi

La direttiva NIS2, recepita in Italia, eleva i requisiti di cybersicurezza per numerosi settori. Adotta come criterio generale l'esclusione delle imprese di piccola dimensione, che restano perciò, di norma, fuori dagli obblighi diretti — pur essendo, come si è visto, tra le più esposte.

GDPR — Protezione dei dati personali

Il regolamento europeo sulla protezione dei dati (GDPR) disciplina il trattamento dei dati personali. In caso di frode che coinvolga dati personali può rilevare, tra l'altro, in tema di obblighi di notifica delle violazioni: un aspetto da valutare con un consulente.

C | Fonti

I dati e i riferimenti citati nel manuale provengono dalle fonti elencate di seguito. Per le pubblicazioni periodiche conviene fare riferimento all'edizione più recente al momento della consultazione.

- Banca d'Italia — Comitato Pagamenti Italia, rilevazioni sulle operazioni di pagamento fraudolente.
- CERTFin — rilevazioni e analisi sulle frodi nel settore finanziario.
- Clusit — Rapporto sulla sicurezza ICT in Italia.
- Cyber Index PMI — Agenzia per la Cybersicurezza Nazionale, Confindustria, Generali.
- McKinsey Global Institute — analisi sul peso economico delle piccole e medie imprese; ISTAT.
- Banca Centrale Europea (ECB) e World Economic Forum — analisi sulle frodi nei pagamenti e sull'ingegneria sociale.
- Analisi di mercato e di società di consulenza sull'impatto dell'intelligenza artificiale generativa nelle frodi finanziarie.

D | Contatti utili

Conviene preparare in anticipo una rubrica con i recapiti certi, accessibile anche quando i sistemi aziendali non lo fossero. La tabella indica i soggetti di riferimento; i recapiti puntuali vanno verificati sui canali ufficiali e aggiornati periodicamente, e qui lasciati da completare.

Soggetto	Quando rivolgersi	Recapito
La propria banca	Pagamento fraudolento, blocco e richiamo fondi, disconoscimento	[da inserire: numero di emergenza e filiale]
Polizia Postale	Denuncia di frode informatica	[da inserire: recapito ufficiale]
CSIRT Italia (ACN)	Segnalazione di incidente informatico	[da inserire: recapito ufficiale]
Garante per la protezione dei dati personali	Coinvolgimento di dati personali	[da inserire: recapito ufficiale]
Commercialista e legale	Profili contabili, fiscali e azioni di recupero	[da inserire: recapiti di fiducia]


cdp