



PROFESSIONE BANCARIA

Cyber Security, truffe e Social Engineering: la nuova frontiera del rischio bancario.

Contesto

Negli ultimi anni il mondo delle prevenzioni frodi si è evoluto molto rapidamente. Le minacce informatiche sono diventate sempre più subdole, facendo leva non solo sulle abilità degli hacker ma soprattutto agendo sulla *vulnerabilità emotiva*, sulla *velocità di attacco* e soprattutto sulla *fiducia*. L'aumento della digitalizzazione dei processi industriali e l'incremento delle tensioni geopolitiche hanno incrementato la vulnerabilità dei sistemi infrastrutturali così come l'integrazione della GenAi nei processi aziendali creando una vera e propria impennata di cyberattacchi verso grandi aziende e Pubblica Amministrazione. Secondo gli ultimi dati presentati dall'Agenzia per Cybersicurezza Nazionale (ACN), il 2025 è stato caratterizzato da una crescita del volume di attività criminali (oltre 2.729 eventi), con una media mensile in aumento del 38%. La diffusione dei sistemi generativi ha pertanto creato terreno fertile per massimizzare efficacia ed efficienza degli attacchi.

Analisi

Per quanto riguarda le tecniche di attacco esse possono partire da diversi vettori, per questo motivo analizziamole attentamente. Il *social engineering* è una tecnica di attacco cyber basata sullo studio del comportamento delle persone con il fine di manipolarne e carpire informazioni confidenziali. Il procedimento si basa sulla manipolazione psicologica usata dai criminali informatici per ingannare le persone agendo sulle vulnerabilità cognitive e le relazioni della vittima per ottenere dati sensibili come accessi e informazioni con il fine unico di indurle a compiere azioni che ne compromettano la sicurezza (password, informazioni sui conti correnti). La manipolazione segue pattern ben definiti: il criminale *raccoglie informazioni* sulla vittima studiandone abitudini e vulnerabilità con il fine di costruire una relazione di fiducia apparente, sfruttando specifiche leve emotive per ottenere ciò che vuole. Di solito si fingono figure istituzionali come ad esempio dirigenti aziendali, funzionari bancari o autorità governative, sfruttando così il naturale rispetto verso le posizioni di potere. L'*urgenza* come, ad esempio, il blocco di un account impedisce alla vittima di riflettere razionalmente spingendola ad agire impulsivamente, la *fiducia* costruita nel corso del tempo la induce ad operare portando così a termine il progetto criminale.



Impatto sul settore

Cyber security nel settore finanziario

La Cyber security nel settore finanziario non riguarda più soltanto la capacità di difendere infrastrutture, server e applicazioni da attacchi informatici diretti. Una parte sempre più rilevante del rischio nasce dalla capacità degli attaccanti di manipolare non solo le procedure ma soprattutto le persone. È il terreno del *social engineering*: *phishing*, *vishing*, *impersonificazione* di colleghi, clienti o autorità, falsi messaggi urgenti e tecniche psicologiche finalizzate a ottenere informazioni, autorizzazioni o accesso a sistemi e dati. In questo scenario, l'identità digitale diventa una vera superficie di attacco: non è quindi necessario "bucare" un sistema quando è possibile convincere qualcuno che la richiesta ricevuta sia legittima. Sinteticamente possiamo delineare tre macro-ambiti relativi alle minacce esterne: il primo inerente alla compromissione dei sistemi informatici, il secondo relativo a frodi e il terzo alle truffe. Per quanto riguarda invece le minacce interne, il focus si concentra essenzialmente sul trasferimento all'esterno di dati sensibili. I livelli di sofisticazione diventano sempre più evoluti: si parte così da messaggi provenienti da sconosciuti, fino ad arrivare a profili social falsi e da messaggi provenienti da nostri conoscenti (l'attaccante è in grado di variare il numero del mittente con uno proveniente dalla nostra rubrica telefonica). Un esempio avvenuto di recente è la cosiddetta "*truffa della ballerina*" dove la vittima riceve un messaggio da un contatto fidato della sua rubrica (che è stato a sua volta truffato) il cui contenuto richiede di votare per una giovane ballerina in un concorso di danza allegando una foto ed un link cliccando sul quale si apre una pagina che richiede l'inserimento del numero di telefono e un codice ricevuto via sms attraverso il quale i truffatori possono così entrare nel profilo WhatsApp agendo con richieste di denaro urgente. Altra tecnica molto utilizzata di recente sono i *video deepfake* costruiti attraverso l'intelligenza artificiale mediante software non particolarmente evoluti e pertanto di facile accesso, attraverso i quali si riescono a replicare immagini di una persona replicandone voce, movimenti e tratti somatici. Il recente caso che ha coinvolto la banca digitale inglese *Revolut* rappresenta un esempio particolarmente significativo di questa evoluzione. Secondo le ricostruzioni pubblicate a settembre 2026, gli attaccanti avrebbero utilizzato una casella PEC riconducibile alla Prefettura di Reggio Calabria per presentarsi come autorità e ottenere informazioni riservate su clienti della banca.

Cyber security nel settore bancario

Per il settore bancario, il social engineering introduce un rischio che attraversa contemporaneamente cyber security, frodi, privacy, compliance e rischio operativo. Una richiesta fraudolenta può infatti apparire formalmente corretta, provenire da un canale realmente esistente e utilizzare informazioni vere, rendendo più difficile distinguere l'attacco da una normale attività operativa. Il problema non riguarda soltanto la sottrazione diretta di denaro: informazioni anagrafiche, documenti, numeri di telefono, dati finanziari e storico delle transazioni possono diventare strumenti per attacchi successivi, furti d'identità e frodi più sofisticate. Il caso *Revolut* mostra inoltre come una compromissione esterna possa produrre conseguenze su un intermediario che, dal punto di vista tecnico, non è necessariamente stato direttamente violato. È una dinamica particolarmente rilevante per banche e fintech, perché la sicurezza non può più essere valutata esclusivamente guardando il proprio perimetro IT: occorre considerare anche fornitori, autorità, partner, canali di comunicazione e identità digitali che interagiscono con l'organizzazione. Anche sul piano delle controversie con la clientela, il tema è concreto: una decisione dell'Arbitro Bancario Finanziario del marzo 2026 ha esaminato un caso di social hacking nel quale la vittima era stata contattata tramite un falso SMS bancario e successivamente convinta da un sedicente operatore a effettuare operazioni di pagamento.



Cosa cambia per i lavoratori

La principale conseguenza per chi lavora in banca è che la sicurezza informatica diventa una responsabilità operativa quotidiana, non più esclusivamente una competenza dell'ufficio IT o della funzione Security. Ogni dipendente che gestisce dati, autorizzazioni, pagamenti, richieste di clienti o comunicazioni con soggetti esterni può diventare un punto di ingresso per un attacco. Diventa quindi fondamentale sviluppare una cultura del *"trust but verify"*: verificare l'identità del richiedente attraverso canali indipendenti; non considerare sufficiente la presenza di un dominio o di una firma apparentemente ufficiale; prestare particolare attenzione alle richieste urgenti o anomale; non aggirare le procedure previste per velocizzare un'operazione; segnalare tempestivamente anomalie e tentativi di manipolazione. Nel caso Revolut, proprio l'utilizzo di un canale istituzionale apparentemente autentico dimostra quanto sia importante verificare non soltanto "da dove arriva" una richiesta, ma anche chi è realmente autorizzato a formularla e se la richiesta è coerente con il processo previsto. La formazione del personale dovrà quindi evolvere: non solo corsi sul phishing, ma esercitazioni su scenari realistici, impersonificazione, deepfake, vishing, compromissione di account e abuso di identità digitali.

Cosa significa per te

La lezione che arriva dai nuovi casi di social engineering è semplice: la sicurezza non coincide con l'assenza di una vulnerabilità tecnica. Un'organizzazione può avere sistemi adeguatamente protetti e, allo stesso tempo, essere esposta se un attaccante riesce a sfruttare la fiducia riposta in un'identità, in un canale o in una procedura. Per il settore bancario questo significa rafforzare contemporaneamente tecnologia, processi e persone. Operativamente, ogni istituto dovrebbe continuare a investire in costante monitoraggio, ma anche nella verifica indipendente delle richieste sensibili, nella segregazione delle autorizzazioni, nella formazione continua del personale, nei test di social engineering e nella capacità di condividere rapidamente gli indicatori di compromissione. Su queste tematiche il 22 e 23 settembre a Milano presso Allianz MiCo si è inaugurato un nuovo evento dedicato alla sicurezza: *WeSec - Il salone della Sicurezza*, promosso da ABI e organizzato da [ABISevizi](#) proprio per promuovere una cultura della sicurezza sempre più integrata, condivisa e orientata al futuro. Instabilità geopolitica, accelerazione tecnologica, minacce cyber, truffe, rischi fisici e vulnerabilità delle infrastrutture sono fenomeni sempre più interconnessi, che richiedono competenze integrate e una collaborazione sempre più stretta tra settore pubblico e privato. Ed è proprio su questo cambio di prospettiva che si gioca una parte importante della cyber resilience bancaria dei prossimi anni.

Claudia Mastrorilli