

Milano, 23 Settembre 2026



Le Frodi e le Truffe verso le PMI

Rischi, Strategie di Difesa Aziendale

Inquadramento normativo, vettori d'attacco e protocolli operativi di prevenzione



I VALORI DEL GRUPPO



TERRITORIALITÀ



MUTUALITÀ



MODERNITÀ

Le BCC contribuiscono al benessere delle comunità e allo sviluppo locale, attraverso un'azione attiva di responsabilità sociale. **Si distinguono per la scelta di costruire il bene comune.**



IL RADICAMENTO SUL TERRITORIO



111

BCC



>2.400

Sportelli



>920.000

Soci



1.700

Comuni presidiati



>5Mln

Clienti



>22.000

Dipendenti



Le PMI nel Mirino dei Cyber-Criminali: Falsi Miti vs Real



Facciamo luce su ciò che sembra vero, ma potrebbe non esserlo

"I nostri sistemi IT e antivirus ci proteggono da qualsiasi attacco."

REALTA' OPERATIVA

Oltre il 70% degli attacchi finanziari sfrutta l'ingegneria sociale e il fattore umano, scavalcando del tutto i firewall e i software di sicurezza.

"La mia azienda è troppo piccola per interessare i cyber-criminali."

REALTA' OPERATIVA

Le PMI sono il target primario perché considerate l'anello debole della catena di fornitura (Supply Chain) e contengono risorse finanziarie significative con difese ridotte.

"I pagamenti bancari disposti per errore sono sempre revocabili o rimborsabili."

REALTA' OPERATIVA

In caso di manipolazione del pagatore (truffa), il recupero dei fondi e il rimborso da parte dell'istituto di credito sono estremamente complessi e non automatici.

Inquadramento Giuridico: Frode Informatica vs Truffa (CERTFin)



FRODE INFORMATICA (Art. 640-ter c.p.)

Target dell'Attacco: Alterazione o accesso abusivo a sistemi informatici, dati, carte o portali di home banking.

Azione della Vittima: Operazione NON Autorizzata. La transazione avviene a totale insaputa del titolare del conto.

Esempi Tassonomia: Malware (Man-in-the-Browser), Account Takeover (ATO), SIM Swap, Card Relay Attack, BIN Attack.

Profili di Responsabilità: La responsabilità ricade prevalentemente sul PSP (banca), salvo prova di colpa grave dell'utente.

TRUFFA (Art. 640 c.p.)

Target dell'Attacco: Manipolazione psicologica della vittima mediante inganno, artifici e raggiri (Social Engineering).

Azione della Vittima: Manipolazione del Pagatore. La vittima esegue o autorizza personalmente l'operazione di pagamento.

Esempi Tassonomia: Business Email Compromise (BEC), CEO Fraud, Invoice Fraud (falsa fattura), Truffa da Filiale.

Profili di Responsabilità: Il PSP può dimostrare l'assenza di responsabilità avendo eseguito l'ordine conforme disposto dal cliente.

Schemi di Truffa: Manipolazione del Pagatore (Art. 640 c.p.)



BEC / CEO Fraud

Inganno basato su e-mail che simulano i vertici aziendali per richiedere un bonifico urgente e riservato. Utilizza anche Deepfake audio/video su app di messaggistica.

Invoice Fraud (Fattura)

Il truffatore si sostituisce al fornitore reale intercettando le e-mail commerciali e notifica un falso cambio di coordinate IBAN per il saldo delle fatture.

Truffa da Filiale

La vittima viene persuasa al telefono a recarsi in banca fornendo un 'copione' falso allo sportello (es. acquisto auto) per non far insospettire il personale bancario.

Bank Impersonation

Finti operatori antifrode contattano l'azienda segnalando un presunto attacco in corso e guidano la vittima a compiere 'bonifici di messa in sicurezza'.

Schemi di Frode: Compromissioni Tecniche (Art. 640-ter c.p.)



Account Takeover (ATO)

Sottrazione delle credenziali di accesso al portale bancario aziendale tramite phishing, malware o aggiunta fraudolenta di nuovi dispositivi autorizzati.

Malware & MITB

Software malevoli (Man-in-the-Browser) che modificano l'IBAN in tempo reale durante la digitazione del bonifico, mantenendo visibile a schermo il dato corretto.

SIM Swap Scam

Duplicazione fraudolenta della SIM telefonica aziendale ottenuta con social engineering sull'operatore telco per intercettare SMS, OTP e notifiche bancarie.

BIN Attack

Attacco informatico automatizzato tramite script bot che testano in massa combinazioni di carte per individuare quelle reali da usare su e-commerce poco protetti.

Tattiche Ibride e Ingegneria Sociale Evoluta

Attacchi Multicanale (Phishing/Smishing + Vishing)

L'attacco si avvia con un'e-mail o SMS di allerta ed è seguito immediatamente da una chiamata di un finto operatore che guida la vittima nell'errore.

CLI Spoofing & SMS Spoofing

Mascheramento del numero chiamante o dell'ALIAS SMS per farli coincidere perfettamente con la numerazione verde o il nome ufficiale della banca.

Falso Supporto Tecnico (Remote Tools)

L'attaccante persuade l'utente a installare software di assistenza remota (AnyDesk, TeamViewer) ottenendo il controllo diretto del PC aziendale.

NFC Card Relay Attack & Quishing

Intercettazione contactless dei dati delle carte via app malevole e utilizzo di codici QR ingannevoli per reindirizzare su siti di phishing.

Tattiche Ibride e Ingegneria Sociale Evoluta

Attacchi Multicanale (Phishing/Smishing + Vishing)

L'attacco si avvia con un'e-mail o SMS di allerta ed è seguito immediatamente da una chiamata di un finto operatore che guida la vittima nell'errore.

CLI Spoofing & SMS Spoofing

Mascheramento del numero chiamante o dell'ALIAS SMS per farli coincidere perfettamente con la numerazione verde o il nome ufficiale della banca.

Falso Supporto Tecnico (Remote Tools)

L'attaccante persuade l'utente a installare software di assistenza remota (AnyDesk, TeamViewer) ottenendo il controllo diretto del PC aziendale.

NFC Card Relay Attack & Quishing

Intercettazione contactless dei dati delle carte via app malevole e utilizzo di codici QR ingannevoli per reindirizzare su siti di phishing.

Vulnerabilità Strutturali nell'Organizzazione delle PMI

1

Concentrazione dei Poteri Operativi

La gestione finanziaria ed esecutiva ruota attorno a un'unica persona, senza segregazione dei compiti e controlli incrociati.

2

Assenza di Procedure Out-of-Band

Mancanza di protocolli codificati per verificare i cambi di IBAN dei fornitori tramite chiamata a numeri storici in anagrafica.

3

Processi di Autorizzazione Informali

Accettazione di richieste di bonifico d'urgenza veicolate via e-mail o app di messaggistica senza verifiche aggiuntive.

4

Carenza di Formazione e Consapevolezza

Assenza di sessioni formative e simulazioni di phishing destinate al personale contabile ed amministrativo.

Strategia di Prevenzione Integrata: I 3 Pilastri della Difesa

PILASTRO PROCEDURALE

Adozione della regola 'Out-of-Band'

Obbligo interno di confermare qualsiasi variazione di IBAN ricevuta via mail contattando il fornitore al telefono ufficiale già presente in anagrafica. Azzerare l'Invoice Fraud e la BEC.

PILASTRO TECNOLOGICO

Verification of Payee (VoP) & Presidi PSP

Sfruttamento dei servizi di verifica della corrispondenza IBAN-Intestatario primadell'invio (VoP) e uso di autenticazione forte su dispositivi dedicati e segregati.

PILASTRO UMANO

Formazione Continua e Culture Building

Programmi di simulazione periodica di Phishing/Vishing per il personale e creazione di un protocollo chiaro e non colpevolizzante per la segnalazione immediata.

Gestione dell'Incidente: Checklist di Risposta Rapida

PASSO 1: BLOCCO IMMEDIATO (Minuti 0 - 15)

Contattare tempestivamente la filiale o la centrale antifrode del PSP per bloccare le credenziali di accesso e richiedere il recall immediato del bonifico.



PASSO 2: ISOLAMENTO TECNOLOGICO

Scollegare dalla rete aziendale (Wi-Fi e LAN) i dispositivi coinvolti (PC, smartphone) per congelare le evidenze informatiche e forensi.

PASSO 3: DENUNCIA E NOTIFICA LEGALE

Sporgere formale denuncia alla Polizia Postale ed effettuare la notifica di Data Breach al Garante Privacy/DPO qualora vi sia stata esfiltrazione di dati.

PASSO 4: DOSSIER E GESTIONE CONTENZIOSO

Predisporre un dossier dettagliato con log, e-mail e orari per l'analisi delle responsabilità e la gestione delle contestazioni bancarie (es. ABF).

L'impegno del Gruppo Bancario Cooperativo Iccrea

Il percorso avviato negli ultimi anni ha portato alla costruzione di un ecosistema di sicurezza integrato, in cui innovazione tecnologica, prevenzione e centralità del cliente operano in modo sinergico. Il nostro motto oggi è... **'Rafforzare la fiducia che ci unisce'**

Valori per il Gruppo

FORMAZIONE DIFFUSA



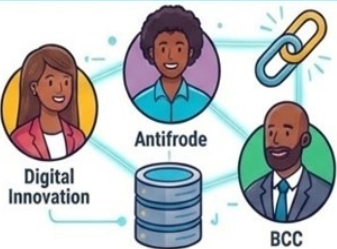
Cybersecurity e antifrode per tutti i livelli del Gruppo e per la clientela: la sicurezza è cultura condivisa.

REFERENTE ANTIFRODE PER OGNI BCC



Un presidio operativo dedicato su tutto il territorio per garantire tempestività e coordinamento.

MAGGIORE COORDINAMENTO DIGITALE



Sinergia rafforzata tra Digital Innovation & Multichannel e BCC

La condivisione proattiva della cultura - Creati 5 Corsi Antifrode ad Hoc

175 Referenti antifrode formati in modalità webinar (durata corso 3,5 ore - 13 eventi - totale 612 ore di formazione)

2100 Esponenti formati in modalità webinar (durata corso 2,5 ore - 22 eventi - totale 5250 ore di formazione)

19977 Dipendenti formati in modalità e-learning (durata corso 1 ora - 19977 eventi - totale 19977 ore di formazione)

Vademecum distribuiti per la diffusione culturale e informativa

Rete Nazionale di 112 Fraud Manager

Creata una rete di coordinamento in real time dei Fraud Manager di ogni singola BCC su tutto il territorio nazionale e contrattualizzazione del servizio antifrode con tutte le BCC con modello unico e standard condivisi

Sinergia e Coordinamento infra Gruppo

Collaborazione proattiva e dinamica con le Unità Operative come SOC; Sicurezza delle Informazioni; Digital Marketing; Comunicazione Istituzionale e Interna; Risk Operating Officer; Compliance; BCC Sinergia; BCC Sistemi Informatici e tutte le Legal Entities del Gruppo.

Milano, 23 Settembre 2026



Grazie