

PROTEGGERE I CLIENTI DIGITALI DALLA SVOLTA «ANALOGICA» DEI FRODATORI

Modelli, prospettive e nuovi approcci all'evoluzione degli scenari di frode



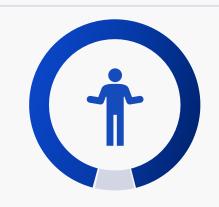
SCENARIO

EVOLUZIONE DELLE FRODI: DAL DIGITALE ALL'ANALOGICO



67%

Delle frodi utilizza come primo punto di contatto un canale analogico (Telefonata/SMS)



92%

Delle frodi è portata a termine tramite manipolazione dell'utente

(+65% rispetto al 2022)

COSA CI DICONO

- → I frodatori introducono elementi analogici per «rompere» la catena dei controlli digitali della banca
- L'utente è l'«anello debole», fattore determinante della transazione fraudolenta



EVOLVERE LA RISPOSTA DELL'ANTIFRODE

LA SFIDA: ESTENDERE IL FOCUS SUL SINGOLO CLIENTE

L'attenzione del frodatore si è spostata dalla banca al cliente.

L'antifrode deve aumentare il livello di protezione del cliente finale, assicurandogli la stessa resilienza fornita alla banca





CONTRASTARE I NUOVI SCENARI DI FRODE

EVOLVERE IL MODELLO TRADIZIONALE



APPROCCIO

- Estendere metodologie e tecnologie innovative anche sul device del Cliente per rafforzare i controlli ed abilitare nuovi processi nel rispetto di vincoli normativi (es. DORA, privacy, PSD2)
- Mettere il cliente al centro del processo, integrando prodotti e canali in ottica omni-channel
- Supportare l'operatività del Servizio Antifrode fino al contatto diretto con il Cliente (tramite chiamata) mediante team di lavoro dedicati, scalabili e specializzati
- Integrare l'approccio deterministico «rule based» mediante l'adozione di Advanced Analytics basati su Indicatori di Rischio Comportamentali



CONTRASTARE I NUOVI SCENARI DI FRODE

EVOLVERE IL MODELLO TRADIZIONALE



CONTINUOUS IMPROVEMENT

- → Aumentare la capacità di resilienza del team Antifrode per rispondere più efficacemente alle continue evoluzioni dei fenomeni fraudolenti
- → Tecnologie, Processi, Persone e Dati devono essere intimamente integrati per difendere il Cliente
- → l'Approccio **end-to-end** è in grado di raccogliere il valore della «**lesson learned**» in tutte le sue componenti



CONTRASTARE I NUOVI SCENARI DI FRODE

EVOLVERE IL MODELLO TRADIZIONALE



SHARING AND COLLABORATION

- → La collaborazione tra Istituti di Credito, Istituzioni, Autorità Competenti è fondamentale per la realizzazione di un contrasto efficace
- → La condivisione tempestiva di esperienze ed informazioni tra istituti Bancari fornisce maggiore consapevolezza e conoscenza degli scenari di frodi
- → La presenza di player in grado di supportare più realtà Bancarie facilita la raccolta e l'elaborazione di informazioni, dati, casi di frode per renderli immediatamente fruibili





Raccolta preliminare informazioni (phishing, smishing, dark web)



Telefonata o sms alla vittima (con o senza spoofing n. banca)



Il frodatore spinge la vittima a compiere un'azione



User manipulation



Effettuare un bonifico online o presso un ATM verso un conto di «servizio»



Condividere credenziali o altre forme di autenticazione



Recarsi su una pagina fake della banca e/o installare un'applicazione La vittima completa il bonifico

Il frodatore usa le credenziali fornite per portare a termine una transazione

Il frodatore registra l'APP della vittima su un suo dispositivo ed utilizzarla per transazioni

La vittima inserisce credenziali o altre info di autenticazione, che il frodatore usa a scopo malevolo

Il frodatore controlla il dispositivo della vittima per rubare il denaro



Frode portata a termine



Raccolta preliminare informazioni (phishing, smishing, dark web)



Telefonata o sms alla vittima (con o senza spoofing n. banca)



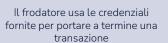
Il frodatore spinge la vittima a compiere un'azione



Effettuare un bonifico online o presso un ATM verso un conto di «servizio»



Condividere credenziali o altre forme di autenticazione



La vittima completa il bonifico

Il frodatore registra l'APP della vittima su un suo dispositivo ed utilizzarla per transazioni



Frode portata a termine

COLLABORATION & SHARING

→ Fraud Intelligence

DATA

→User Behavior Analytics



Recarsi su una pagina fake della banca e/o installare un'applicazione La vittima inserisce credenziali o altre info di autenticazione, che il frodatore usa a scopo malevolo





Raccolta preliminare informazioni (phishing, smishing, dark web)



Telefonata o sms alla vittima (con o senza spoofing n. banca)



Il frodatore spinge la vittima a compiere un'azione



Effettuare un bonifico online o presso un ATM verso un conto di «servizio»



Condividere credenziali o altre forme di autenticazione



Frode portata a termine



→ Device SDK (Smishing / Spoofing / Vishing)

PROCESS

→Fraud Monitoring&Response

PEOPLE

→ Client Contact Center



Recarsi su una pagina fake della banca e/o installare un'applicazione La vittima inserisce credenziali o altre info di autenticazione, che il frodatore usa a scopo malevolo

La vittima completa il bonifico

Il frodatore usa le credenziali

Il frodatore registra l'APP della

vittima su un suo dispositivo ed

utilizzarla per transazioni



Raccolta preliminare informazioni (phishing, smishing, dark web)



Telefonata o sms alla vittima (con o senza spoofing n. banca)



Il frodatore spinge la vittima a compiere un'azione



Effettuare un bonifico online o presso un ATM verso un conto di «servizio»



Condividere credenziali o altre forme di autenticazione



Il frodatore registra l'APP della vittima su un suo dispositivo ed utilizzarla per transazioni

La vittima completa il bonifico

Il frodatore usa le credenziali



Frode portata a termine

DATA

→ User Behavior Analytics

COLLABORATION & SHARING

→Smart Case Manager



Recarsi su una pagina fake della banca e/o installare un'applicazione La vittima inserisce credenziali o altre info di autenticazione, che il frodatore usa a scopo malevolo





Raccolta preliminare informazioni (phishing, smishing, dark web)



Telefonata o sms alla vittima (con o senza spoofing n. banca)



Il frodatore spinge la vittima a compiere un'azione



Effettuare un bonifico online o presso un ATM verso un conto di «servizio»



Condividere credenziali o altre forme di autenticazione



Frode portata a termine



TECHNOLOGY

→ Fraud Monitoring & Response

DATA

→User Behavior Analytics



Recarsi su una pagina fake della banca e/o installare un'applicazione La vittima inserisce credenziali o altre info di autenticazione, che il frodatore usa a scopo malevolo

La vittima completa il bonifico

Il frodatore usa le credenziali

fornite per portare a termine una

transazione

Il frodatore registra l'APP della

vittima su un suo dispositivo ed

utilizzarla per transazioni





Raccolta preliminare informazioni (phishing, smishing, dark web)



Telefonata o sms alla vittima (con o senza spoofing n. banca)



Il frodatore spinge la vittima a compiere un'azione



Effettuare un bonifico online o presso un ATM verso un conto di «servizio»



Condividere credenziali o altre forme di autenticazione



Frode portata a termine



- → Device Monitoring SDK
- → Identity Checking Solution



Recarsi su una pagina fake della banca e/o installare un'applicazione La vittima inserisce credenziali o altre info di autenticazione, che il frodatore usa a scopo malevolo

La vittima completa il bonifico

Il frodatore usa le credenziali

fornite per portare a termine una

transazione

Il frodatore registra l'APP della

vittima su un suo dispositivo ed

utilizzarla per transazioni



Raccolta preliminare informazioni (phishing, smishing, dark web)



Telefonata o sms alla vittima (con o senza spoofing n. banca)



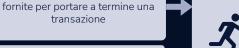
Il frodatore spinge la vittima a compiere un'azione



Effettuare un bonifico online o presso un ATM verso un conto di «servizio»



Condividere credenziali o altre forme di autenticazione



Il frodatore registra l'APP della vittima su un suo dispositivo ed utilizzarla per transazioni

La vittima completa il bonifico

Il frodatore usa le credenziali



Frode portata a termine



- → Device Monitoring SDK
- → Device Security Check



Recarsi su una pagina fake della banca e/o installare un'applicazione La vittima inserisce credenziali o altre info di autenticazione, che il frodatore usa a scopo malevolo





Raccolta preliminare informazioni (phishing, smishing, dark web)



Telefonata o sms alla vittima (con o senza spoofing n. banca)



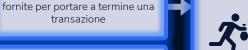
Il frodatore spinge la vittima a compiere un'azione



Effettuare un bonifico online o presso un ATM verso un conto di «servizio»



Condividere credenziali o altre forme di autenticazione



Frode portata a termine

CON IMP

CONTINOUS IMPROVEMENT

- → Policy & Rules Enhancement
- → Checklist Feeding

PROCESS

- → Fraud Monitoring & response
- → Fraud Management Support
- → Automation & Digitalization

PEOPLE

- → Client Contact Center
- → Managed Services

COLLABORATION & SHARING

→ Smart Case Manager

DATA

- → KPI and Alerts
- → Ex-Post Analysis
- → Reports



Recarsi su una pagina fake della banca e/o installare un'applicazione La vittima inserisce credenziali o altre info di autenticazione, che il frodatore usa a scopo malevolo

La vittima completa il bonifico

Il frodatore usa le credenziali

Il frodatore registra l'APP della

vittima su un suo dispositivo ed

utilizzarla per transazioni

Il frodatore controlla il dispositivo della vittima per rubare il denaro

End to end support



FRAUD MANAGED SERVICE

L'APPROCCIO ALFA GROUP

TECHNOLOGY

- → Transaction Monitoring Platform
- → Device Monitoring (SDK)
- → Identity Checking Solution
- → Anti Phishing Tools

DATA

- → KPI & Alert
- → User Behaviour Analytics
- → Ex-Post Analysis
- → Reporting

CONTINUOUS IMPROVEMENT

- → Policy & Rules Enhancement
- → List Automation&Management
- → Managed End-to-end Support



PROCESS

- → Fraud Monitoring & Response
- → Fraud Management Support
- → Automation & Digitalization

PEOPLE

- → Managed Services
- → Client Contact Center

COLLABORATION & SHARING

- → Fraud intelligence
- → SMART Case Management
- → Fraud Network Infosharing



Alfa Group S.p.A.

Via Fiume Giallo, 3 00144 Roma (RM)

(+39) 0652244040 | Fax: (+39) 0652244423

info@alfagroup.it | www.alfagroup.it

ROMA, MILANO, BOLOGNA, PORTO SAN GIORGIO,

AMERSFOORT (NL), LONDRA (UK)

