Agenda

- **Lo scenario delle frodi su Internet e Mobile Banking**
  - Dimensionamento del fenomeno
  - Modalità di realizzazione della frode
  - Focus canale Mobile Banking

- **Le collaborazioni per il contrasto e la prevenzione delle frodi**
  - La cooperazione con la Polizia Postale e delle Comunicazioni
  - Le azioni di sensibilizzazione
  - I network e i progetti di ricerca nazionali e internazionali

La rilevazione ABI Lab sulle frodi realizzate via Internet e Mobile Banking

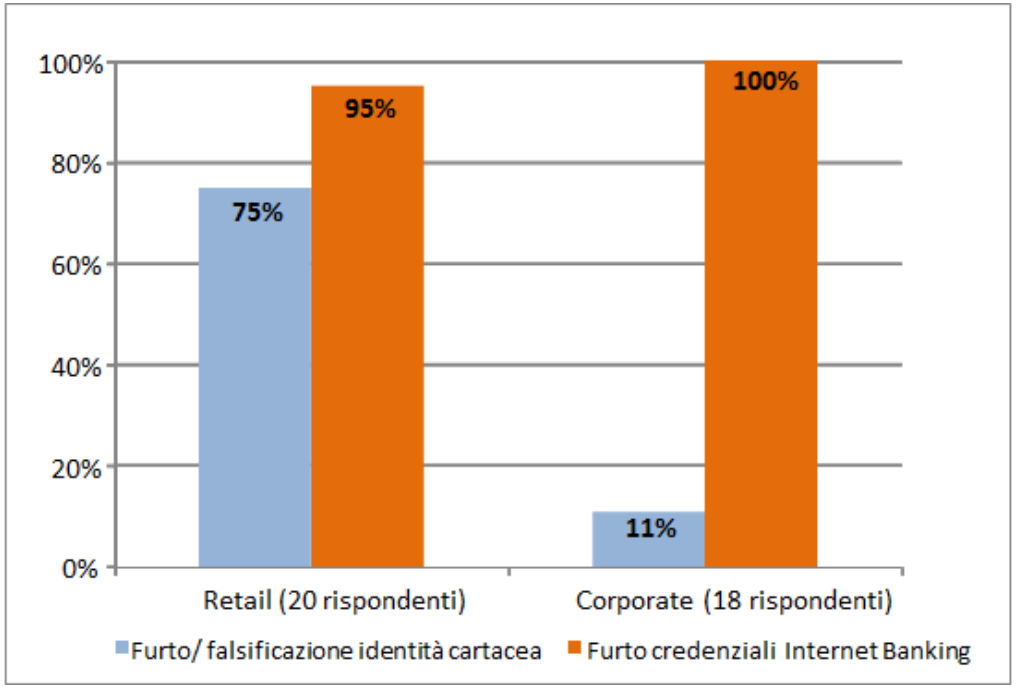
- La **rilevazione** dell'Osservatorio Sicurezza e Frodi Informatiche di ABI Lab ha visto la partecipazione di **25 organizzazioni** operanti nel settore bancario, tra banche, gruppi e outsourcer, per un totale di **153** istituti rappresentativi del **77%** del settore in termini di **dipendenti**
- **I dati si riferiscono al periodo temporale dal 1° Gennaio al 31 Dicembre 2013** e sono stati raccolti in maniera **distinta** per il segmento **Retail** (circa 77% degli account abilitati) e **Corporate** (circa 1,9 milioni account attivi)

Stima accessi al portale di Internet Banking sul campione totale

- **Retail: 873 milioni**
- **Corporate: 281 milioni**

In generale aumento rispetto al 2012

Le tipologie di frode rilevate dalle banche che hanno dichiarato una perdita di credenziali – confronto Retail e Corporate

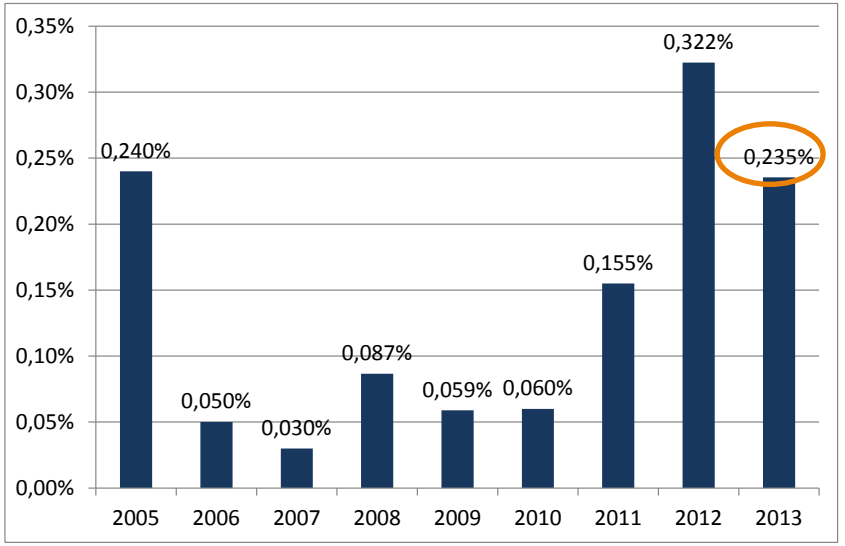


Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

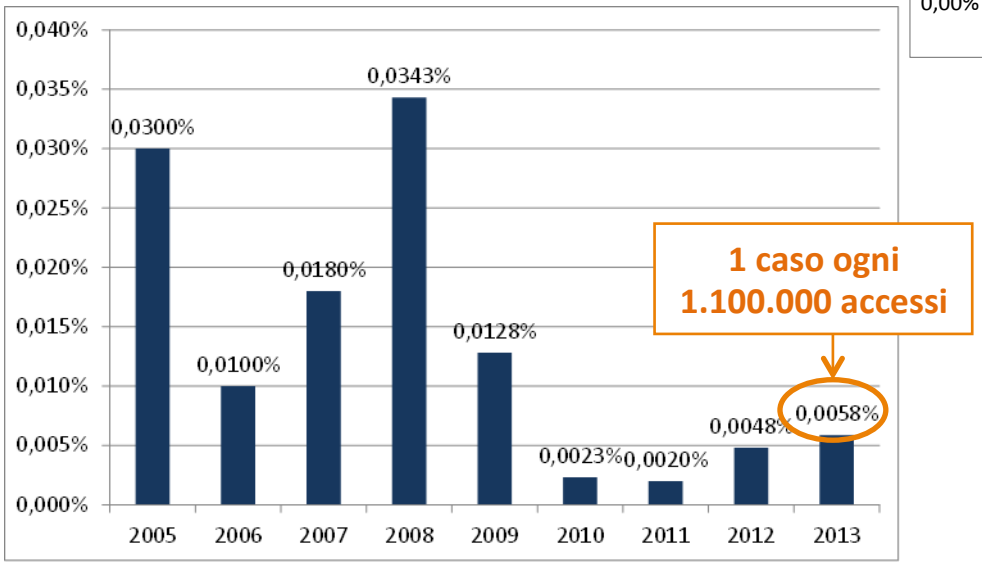
Il fenomeno delle frodi informatiche
Furto di credenziali e danno economico – ambito Retail

- A livello complessivo, nel 2013 si registra una **riduzione** di episodi di **furto di credenziali** di accesso ai servizi di Internet Banking, con un valore pari allo **0,235%**.
- Rapportato al numero di accessi all'Internet Banking, tale % scende a un valore di **0,0036%**, pari a **1 caso di perdita di credenziali ogni 28.000 accessi**.

% clienti attivi Retail vittima di furto di credenziali (trend 2005- 2013)



% clienti attivi Retail che hanno subito un danno economico (trend 2005-2013)



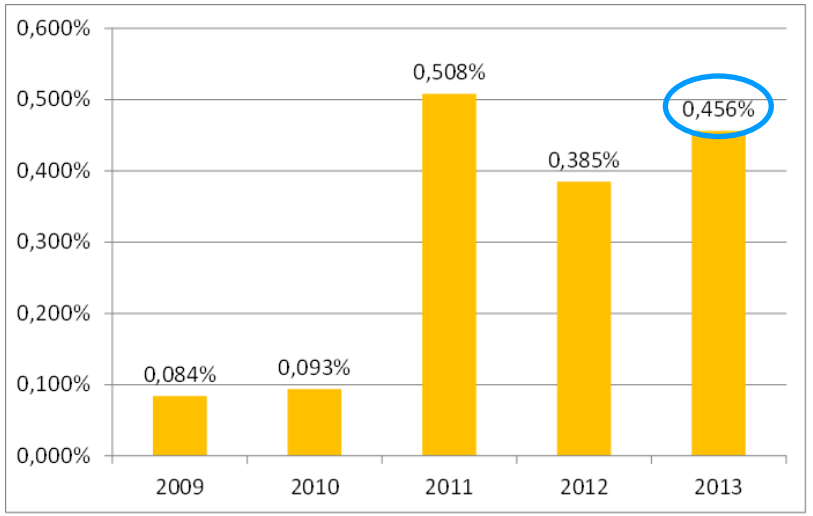
- Dal 2012 al 2013 si registra un lieve **incremento** della percentuale di **clienti** vittima di furto di identità e che conseguentemente hanno **perso denaro**.
- In relazione al totale degli **accessi** stimati all'Internet Banking, la % di clienti che hanno subito un **danno economico** (al lordo di eventuali rimborsi) rimane comunque molto bassa, pari allo **0,00009%**.

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

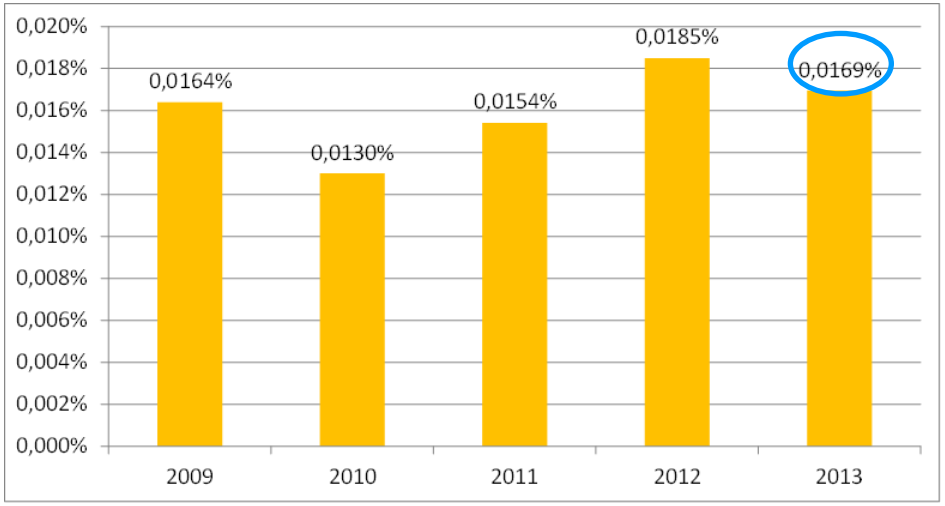
Il fenomeno delle frodi informatiche
Furto di credenziali e danno economico – ambito Corporate

- In relazione al segmento di clientela Corporate, il 2013 ha fatto registrare per il campione complessivo un **aumento** della percentuale dei clienti attivi che hanno **perso le credenziali** (**0,456%**), a conferma dell'**attenzione crescente** dei criminali verso tale segmento di clientela.
- Se rapportato al totale degli **accessi** all'Internet Banking, tale percentuale si riduce allo **0,0032%** (1 caso ogni 31.000 accessi circa).

% clienti attivi Corporate vittima di furto di credenziali (trend 2005- 2013)



% clienti attivi Corporate che hanno subito un danno economico (trend 2005- 2013)

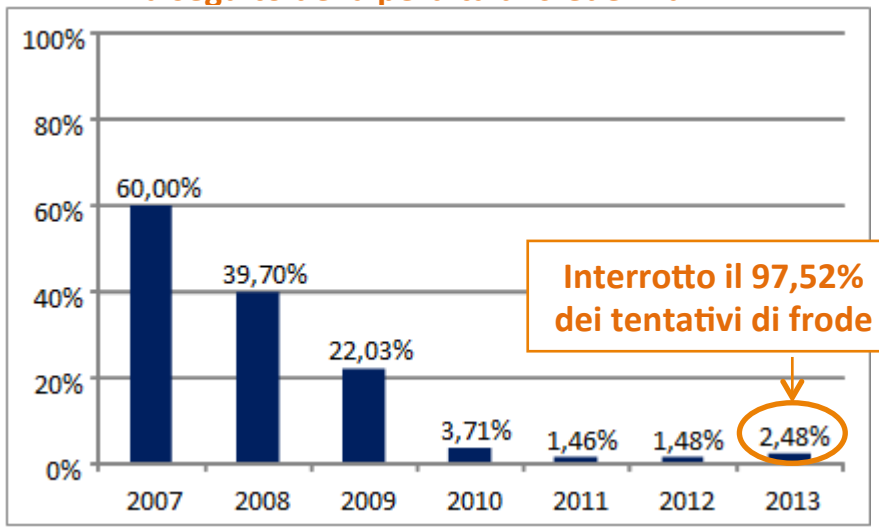


- Al contrario, risulta nel 2013 in lieve **diminuzione** la percentuale relativa dei **clienti** che hanno **perso denaro** (0,0169%), a conferma di una crescente efficacia delle azioni di contrasto e prevenzione.
- In rapporto al **numero di accessi** ai **servizi** di Internet Banking stimati, la percentuale di **casi di perdita di denaro** si attesta intorno allo **0,0001%.**

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

Il fenomeno delle frodi informatiche
Efficacia delle frodi – Confronto segmenti di clientela

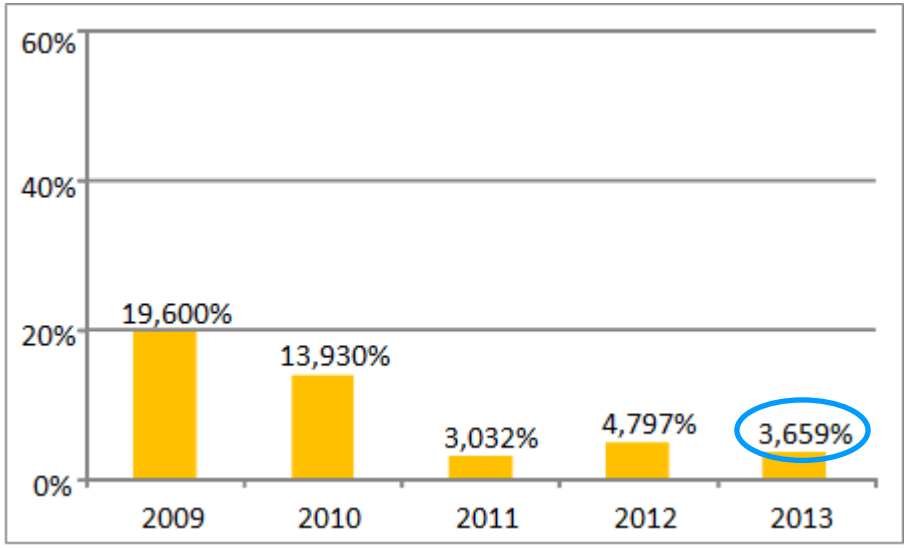
Percentuale di clienti attivi Retail che perde denaro a seguito della perdita di credenziali



- Nonostante il lieve incremento degli episodi di frode, l'**incidenza degli attacchi** rimane comunque **contenuta** (**2,48%**), anche se in lieve **aumento** rispetto al **2012**.
- È sempre più importante **associare** alle **contromisure tecnologiche** di contrasto anche importanti **iniziative di prevenzione** rivolte all'utente

- Dall'analisi svolta emerge un **miglioramento** dell'**efficacia** delle azioni di **contrasto** degli attacchi indirizzati al segmento Corporate: nel 2013, infatti, la percentuale di clienti che ha subito un danno economico a seguito del furto di credenziali è scesa al **3,659%**.
- Per avere una **visione completa** del fenomeno, è opportuno leggere tali informazioni insieme con le analisi sulla **numerosità degli episodi di frode** e sui relativi **volumi anomali** transati.

Percentuale di clienti attivi Corporate che perde denaro a seguito della perdita di credenziali

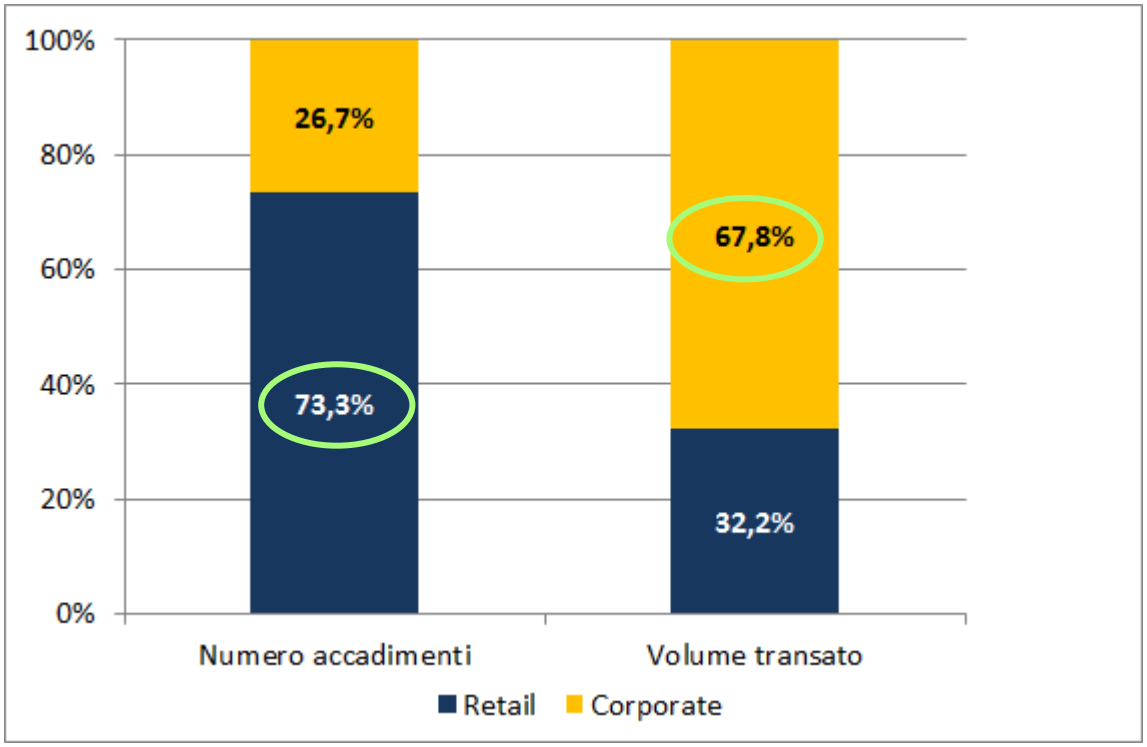


Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

Scenario complessivo transazioni fraudolente
Confronto segmenti di clientela (1/2)

Totale transazioni anomale (bloccate, recuperate ed effettive)

Confronto Retail e Corporate su numero accadimenti e volume transato

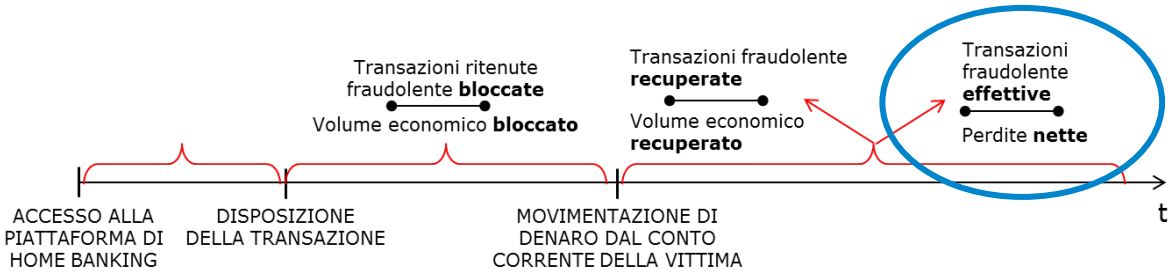


A livello complessivo sul campione:

- Il comparto **Retail** appare soggetto a una **numerosità di attacchi** decisamente **superiore** rispetto al comparto **Corporate,** con un rapporto quasi di **3:1** (73,3% Retail, 26,7% Corporate).
- **La maggiore entità dei volumi economici** transati per l'intero campione di analisi è tuttavia associabile alla clientela **Corporate**, per tutte le fasi della transazione, con un rapporto complessivo di circa **2:1**.

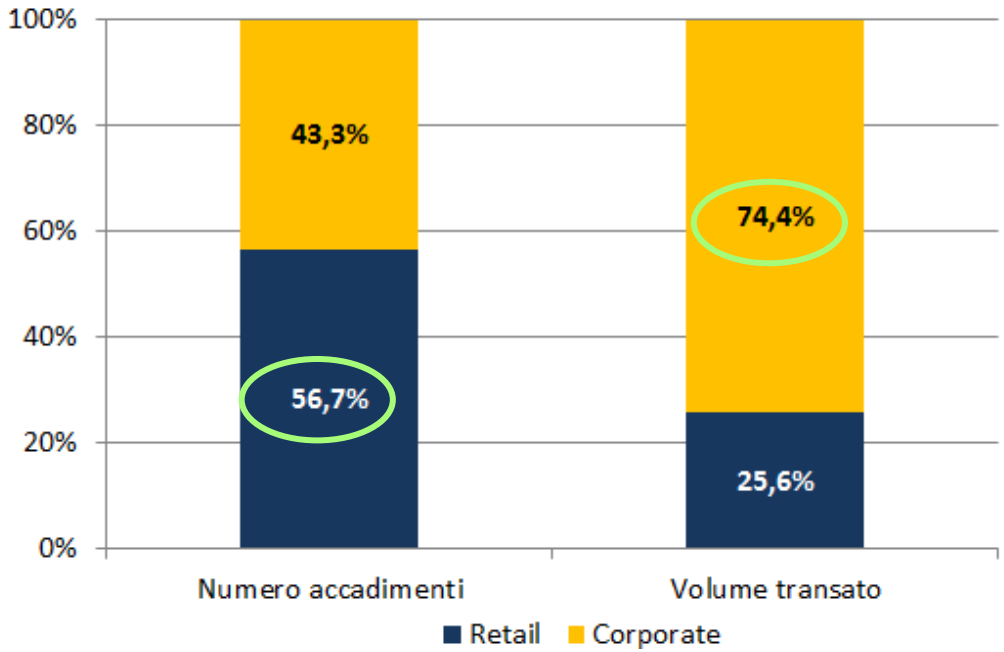
Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

Scenario complessivo transazioni fraudolente
Confronto segmenti di clientela (2/2)



Transazioni fraudolente effettive

Confronto Retail e Corporate su numero accadimenti e volume transato



A livello complessivo sul campione:

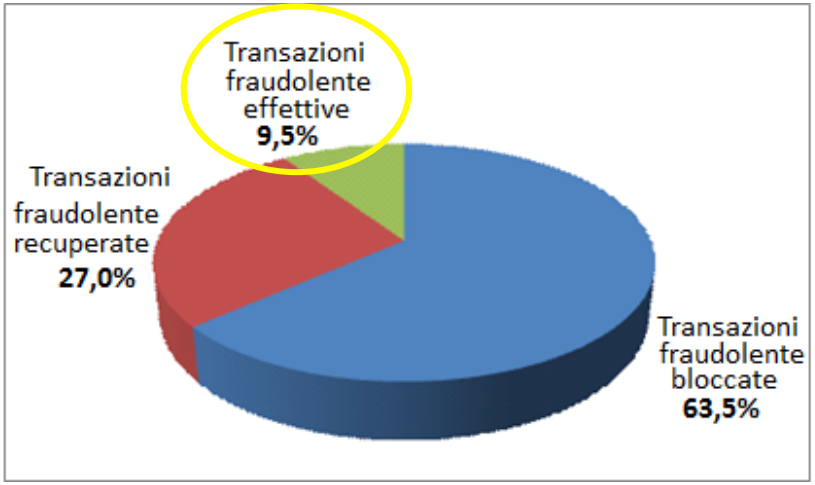
- In relazione al **numero di transazioni effettivamente fraudolente**, la ripartizione percentuale è **maggiormente omogenea** tra i due segmenti di clientela, evidenziando ad ogni modo una leggera **prevalenza del segmento Retail** (56,7%).
- Il rapporto si inverte se si prende come riferimento il **volume economico** associato alle perdite, che è **3 volte maggiore** per il segmento **Corporate**.

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

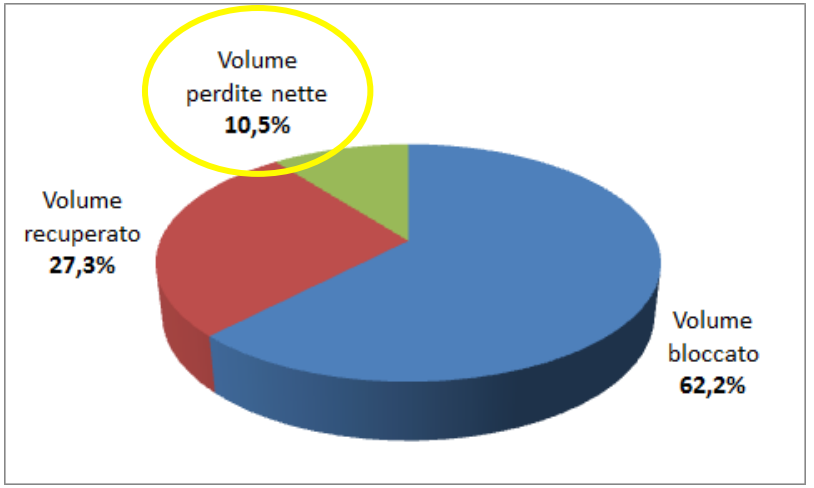
Dettaglio transazioni fraudolente – Clientela Retail

Numero di eventi e volumi economici

Ripartizione percentuale delle tipologie di transazioni anomale rilevate – numero accadimenti



Ripartizione percentuale delle tipologie di transazioni anomale rilevate – volume transato



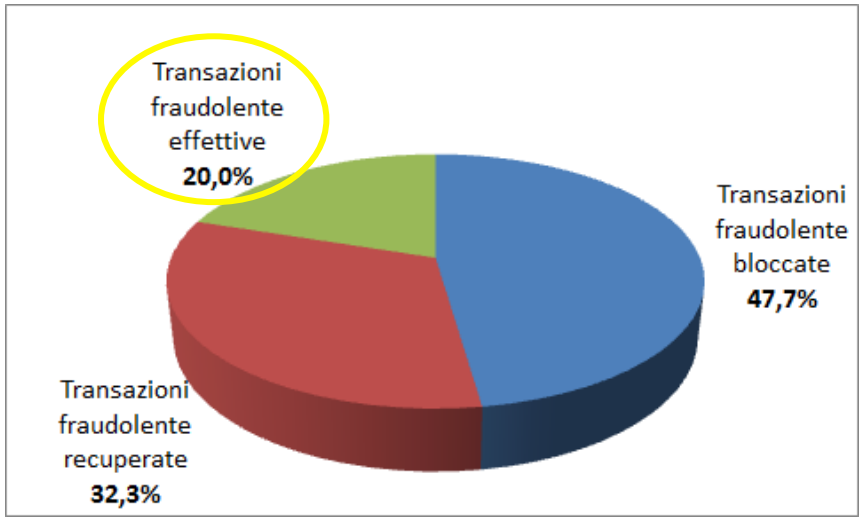
- Rispetto alla stima **totale** delle transazioni effettuate via **Internet Banking** dalla clientela Retail (tra bonifici e ricariche), solo lo **0,0007%** degli accadimenti (pari a 1 su 125.000) ha costituito una **frode effettiva**.
- In relazione al **volume economico** associato al totale delle operazioni **fraudolente**, l'**89,5%** risulta essere relativo alle operazioni **bloccate o recuperate**.

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

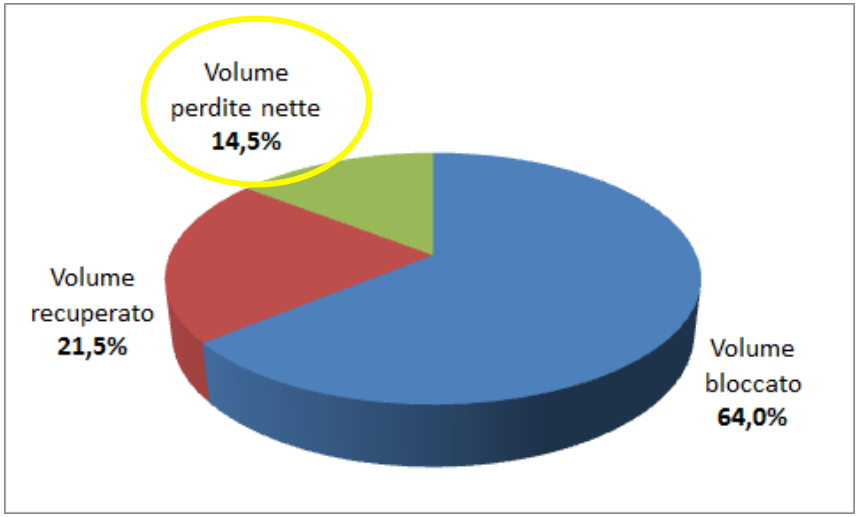
Dettaglio transazioni fraudolente – Clientela Corporate

Numero di eventi e volumi economici

Ripartizione percentuale delle tipologie di transazioni anomale rilevate – numero accadimenti



Ripartizione percentuale delle tipologie di transazioni anomale rilevate – volume transato

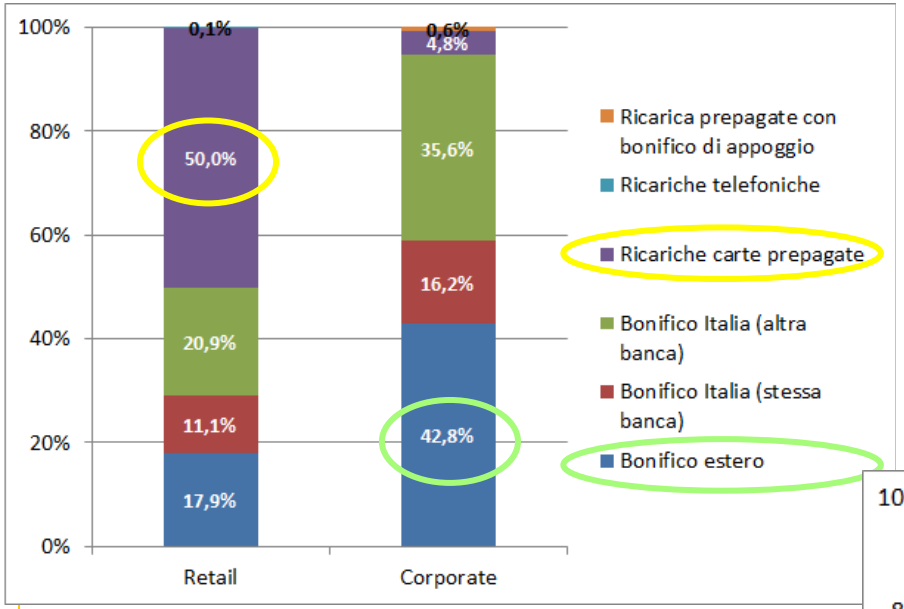


- La percentuale di transazioni **fraudolente effettive** (20%) sul totale delle anomale induce a ragionare sull'introduzione di **modalità e procedure cooperative sempre più tempestive** per fermare transazioni sospette.
- Interessante notare come l'**85,5%** dei **volumi anomali** transati sia stato efficacemente bloccato o recuperato.

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

Modalità di primo trasferimento
Confronto segmenti di clientela

Modalità di primo trasferimento – confronto Retail e Corporate su numero accadimenti



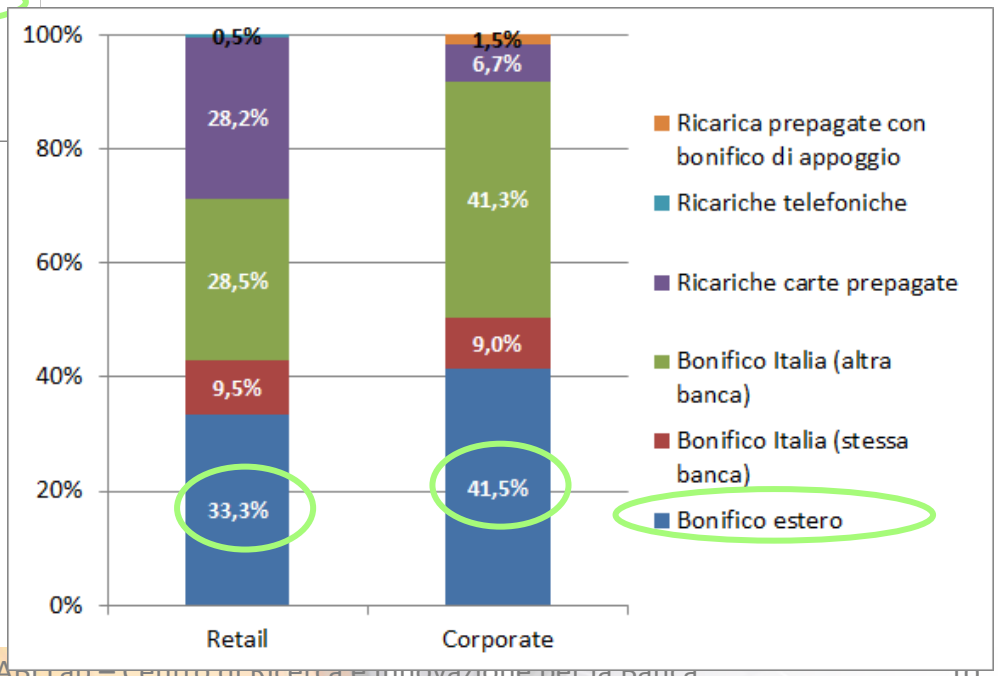
NUMERO ACCADIMENTI

- Clientela **Retail**: si registra per il 2013 un incremento nell'utilizzo delle **ricariche di carte prepagate** come modalità di primo trasferimento del denaro dal conto della vittima (50%).
- Clientela **Corporate**: la modalità di trasferimento illecito di denaro principalmente utilizzata è il **bonifico** (94,6%), in particolare verso l'**estero** (42,8%).

VOLUME TRANSATO

- Clientela **Retail**: le quota percentuale di **denaro** più elevata è associabile alle disposizioni di **bonifico estero** fraudolente (33,3%).
- Clientela **Corporate**: anche per quanto riguarda i volumi sottratti alle vittime, è il **bonifico estero** la modalità principale di **cash out** (41,5%).

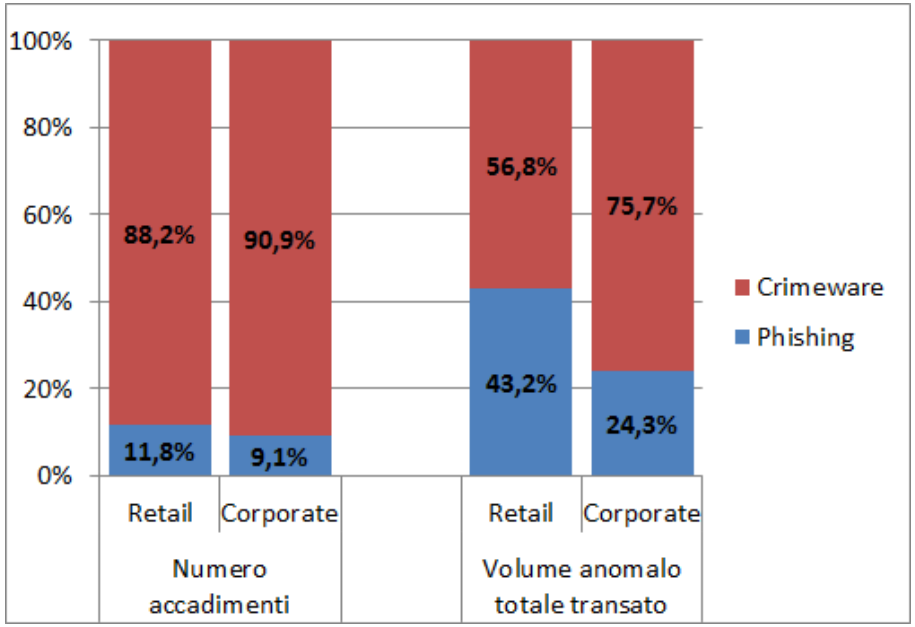
Modalità di primo trasferimento – confronto Retail e Corporate su volume transato



Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

Modalità di realizzazione dell'attacco
Confronto segmenti di clientela

Numero di accadimenti e volume transato per tipologia di attacco



- Clientela **Retail**: in **crescita** nel 2013 la redditività degli attacchi di **phishing**. A livello medio, sono in **aumento** anche attacchi di tipo **man-in-the-browser** (28,1%).
- Clientela **Corporate**: è il **crimeware** il vettore di attacco nettamente più efficace, sia in termini di numero di **accadimenti** che di volume **transato.**
- Per entrambi i segmenti di clientela diviene sempre più **strategico realizzare campagne di sensibilizzazione** e aggiornamento sulle minacce informatiche.

MODALITÀ DI SOTTRAZIONE DELLE CREDENZIALI

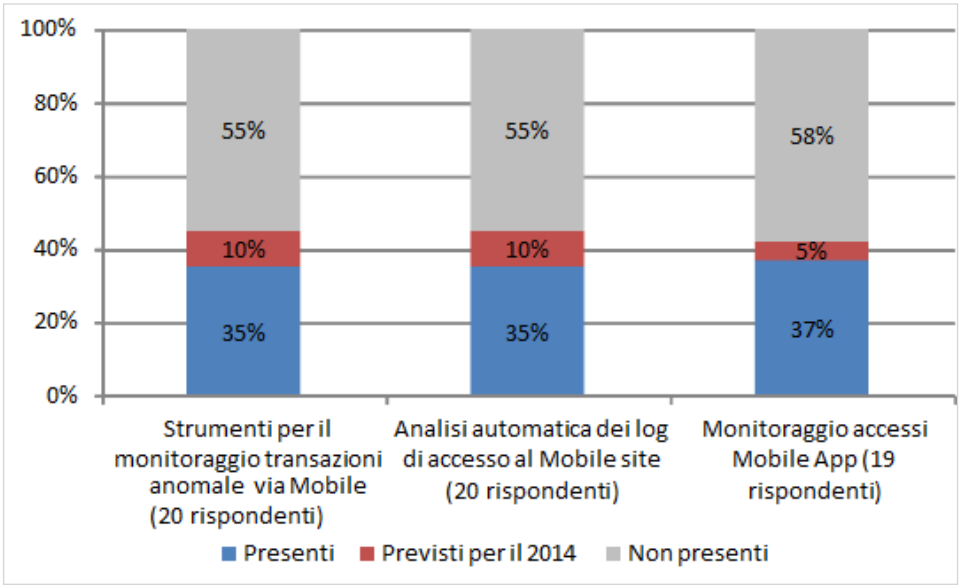
- Clientela **Retail**:
  - Le **credenziali** di **accesso** ai servizi di **Internet Banking** sono state sottratte **esclusivamente dai PC dell'utente**: **non** si riscontrano casi di sottrazione delle credenziali di **accesso** da **device mobili**.
  - L'attenzione dei frodatori si sposta verso i **device mobili solo** quando vengono utilizzati dal cliente per la ricezione dell'**OTP via SMS** necessario per autorizzare la disposizione on line, attraverso meccanismi di **disabilitazione della SIM** e, meno frequentemente, tramite malware scaricati dall'utente. I clienti **vittima** di tali attacchi rappresentano il 7% dei clienti che hanno subito un danno economico e lo **0,0039%** dei clienti che utilizzano il mobile come **tecnologia autorizzativa**.
- Clientela **Corporate**: **sottrazione** delle credenziali **solo da PC utente**.

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

La sicurezza sul canale Mobile

- **Non** si registrano, neanche per il **2013,** casi di **perdita di denaro** a seguito di **attacchi specifici** realizzati sul **canale Mobile** e sui relativi servizi offerti.
- **Solo 1 realtà ha segnalato 1 caso di App Mobile clonata**.

Strumenti tecnologici per il monitoraggio e la rilevazione di attacchi



Iniziative di formazione e sensibilizzazione

- Il **15,8%** del campione ha indicato di aver svolto nel **2013** iniziative di **formazione del personale** sull'incidenza e sulle modalità di perpetrazione delle **frodi** sul canale di **Mobile Banking**, mentre il **10,5%** ha intenzione di **avviarle nel 2014**.
- Infine, il **45,5%** del campione ha indicato di aver svolto nel **2013** iniziative di **sensibilizzazione** della **clientela** specifiche sulle **frodi via Mobile**.

Contromisure tecnologiche

- L'**85,7%** del campione ha introdotto un **secondo livello** di autenticazione.
- Il **95,2%** dei rispondenti prevede l'utilizzo di un **secondo fattore** di autenticazione, nell'**85,7%** dei casi **identico** a quello utilizzato per i servizi di **Internet Banking**.
- La tecnologie di autenticazione più diffusa è l'**OTP via token** (45%), seguita **dall'OTP via numero verde** (15%).

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

Agenda

- **Lo scenario delle frodi su Internet e Mobile Banking**
  - Dimensionamento del fenomeno
  - Modalità di realizzazione della frode
  - Focus canale Mobile Banking

- **Le collaborazioni per il contrasto e la prevenzione delle frodi**
  - La cooperazione con la Polizia Postale e delle Comunicazioni
  - Le azioni di sensibilizzazione
  - I network e i progetti di ricerca nazionali e internazionali

La collaborazione ABI – Banche – Polizia di Stato

- ***Convenzione ABI – Polizia di Stato per la prevenzione dei crimini informatici nel settore bancario italiano***, per la definizione di un piano di **collaborazione** per il contrasto del crimine informatico, prevedendo lo scambio in tempo reale delle informazioni rilevanti.
- ***Lettera Circolare ABI*** "Azioni di sistema in materia di frodi informatiche", che descrive le modalità di partecipazione delle banche al processo di scambio informativo.

Nell'ambito della collaborazione ABI-Banche – Polizia, si inserisce la **partecipazione attiva** di **ABI Lab** nel **progetto europeo OF2CEN,** finalizzato alla **realizzazione** di una **piattaforma** per lo **scambio di informazioni** tra le **banche** e **Forze dell'Ordine** su **frodi online**.

La piattaforma OF2CEN (Online Fraud Cyber Center and Expert Network)

- Possibilità di **inserimento volontario** di **dati** su **transazioni fraudolente, IP sospetti e siti clone**
- **Warning e alert** in caso di **nuove segnalazioni** di operazioni fraudolente
- Sviluppo di un **canale sicuro** per condividere informazioni e garantire la sicurezza della **protezione dei dati**
- **Interfaccia personalizzata** per le esigenze dei diversi attori partecipanti (Polizia, banche, ABI Lab)
- Funzionalità di **estrazione** e **ricerca informazioni** nel database
- **Possibilità** di **analisi statistiche** e **correlazione** delle informazioni presenti nel database

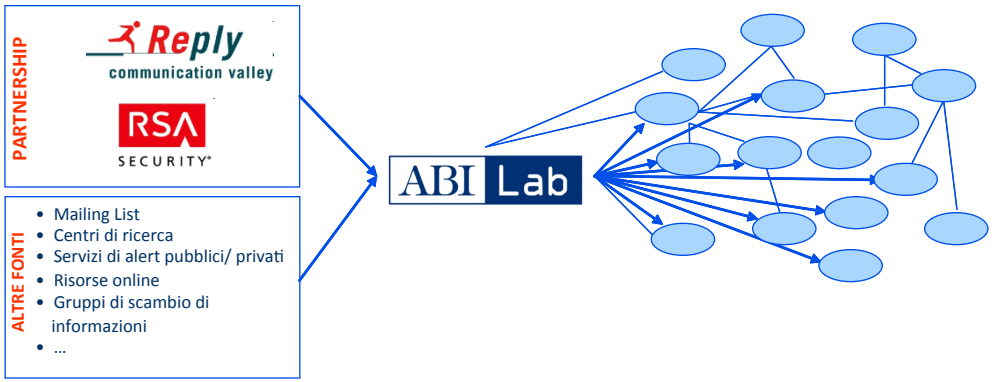
Oggi: utilizzo della piattaforma da banche italiane aderenti all'iniziativa

Prossimi mesi: estensione della piattaforma a banche e Polizie europee, con il supporto di EBF ed Europol

La community presidio.internet di ABI Lab

FI-ISAC italiana per il **monitoraggio** dello scenario delle **frodi informatiche** e per la **collaborazione informale e volontaria** tra gli attori coinvolti nel percorso di **prevenzione e repressione** del cybercrime

Oltre 300 referenti di banche, outsourcer interbancari, Polizia Postale e delle Comunicazioni, Poste Italiane, operatori TLC mobili

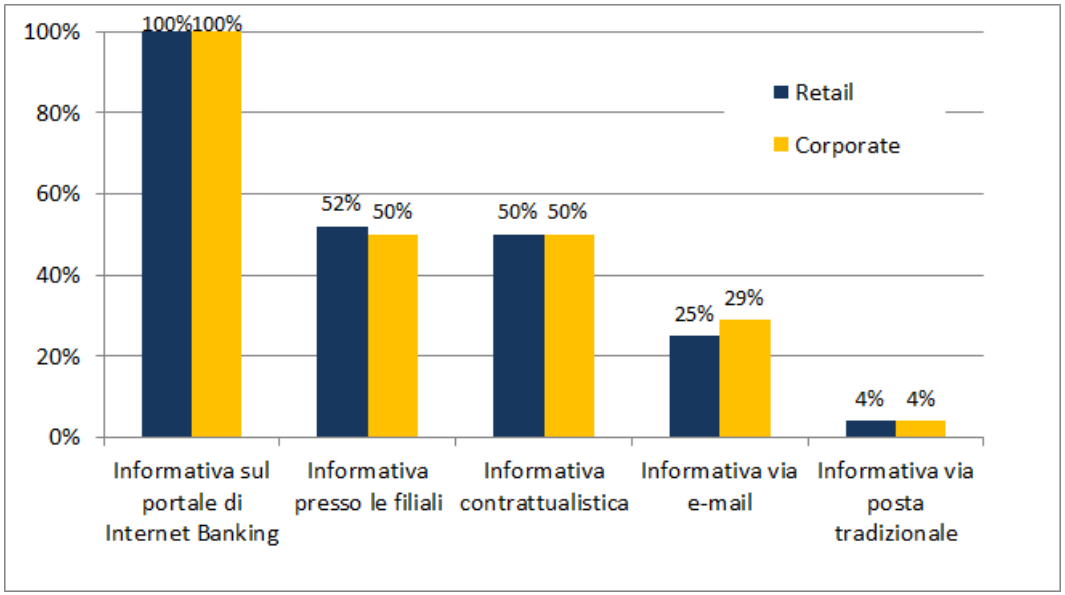


- Tutte le **informazioni** sono **gestite** in accordo alle necessità di **riservatezza e integrità**.
- L'attività di **warning** è corredata dall'invio di **report periodici**, realizzati in collaborazione con i partner tecnologici dell'iniziativa, contenenti informazioni generali sulle principali **minacce informatiche** con **focus** sul settore bancario.

WARNING	Descrizione	1-a-1	1-a-molti	1-a-tutti	encryption
Warning di sistema	Informazioni di dominio pubblico razionalizzate in ottica di evidenziare attacchi all'intero sistema bancario		✓	✓	
Warning generico	Informazioni disponibili pubblicamente o su canali riservati a potenziale impatto diretto sullo sviluppo del fenomeno fraudolento, a bassa criticità	✓	✓	✓	✓
Warning specifico	Informazioni su minacce anche specifiche di singole banche, provenienti anche da fonti private, che richiedono una reazione in tempo reale da parte della struttura di sicurezza.	✓			✓

Le azioni di sensibilizzazione della clientela

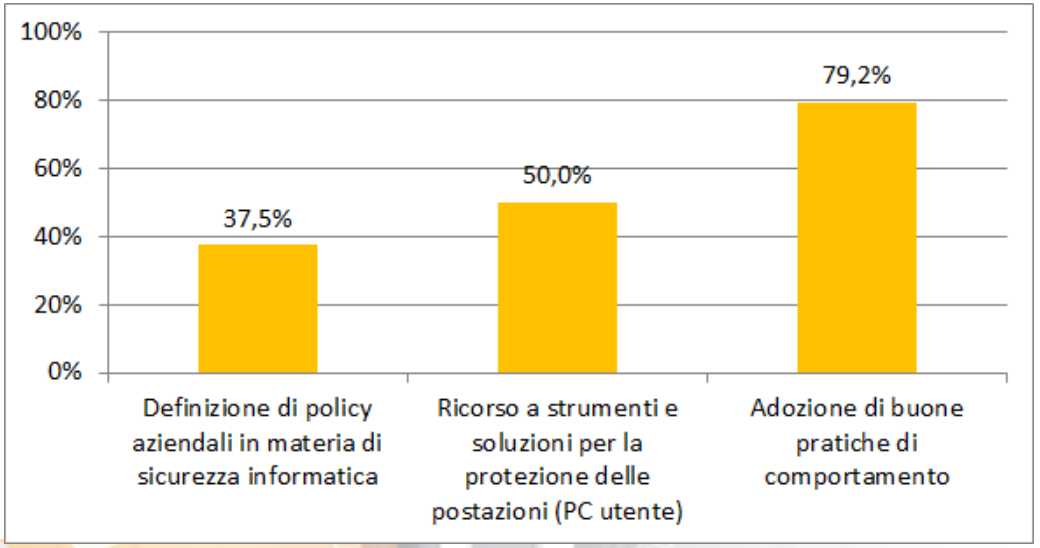
Attività informativa verso la clientela



- Sia per il segmento di clientela Retail che per il Corporate, le banche utilizzano i **diversi canali** disponibili per **aggiornare la clientela** sulle **minacce informatiche** e sulle **buone pratiche** di comportamento.
- L'**importanza** delle azioni di **customer awareness** è confermata anche nelle recenti **raccomandazioni BCE** sulla sicurezza dei pagamenti Internet.

Azioni specifiche di sensibilizzazione clientela Corporate

- Sono **diffuse** a diverso livello nel campione varie **azioni specifiche** per indirizzare la **clientela Corporate** verso un utilizzo più **sicuro dell'Internet Banking**, anche a partire dalle **recenti raccomandazioni** prodotte da ABI Lab, CBI e Polizia Postale e indirizzate alle imprese.



Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

Le collaborazioni nazionali e internazionali di ABI Lab in materia di sicurezza e frodi informatiche

IL DIALOGO CON LE ISTITUZIONI A LIVELLO NAZIONALE

- **Polizia Postale e delle Comunicazioni**
  - Stipula della **Convenzione ABI – Polizia di Stato** per la prevenzione dei crimini informatici nelle banche italiane
- **Banca d'Italia**
  - Dialogo sulle **procedure e tecnologie a garanzia della sicurezza dei pagamenti**, in considerazione della **revisione della PSD** e delle **raccomandazioni BCE**
  - Collaborazione sui temi di **sicurezza e rischio informatico** in relazione alla **Circolare 263** del luglio 2013
- **Autorità Garante per la Protezione dei Dati Personali**
  - Collaborazione sui **temi di sicurezza e privacy, anche** in ordine al **Provvedimento Garante II** e successivi **chiarimenti**
- **Ministero dell'Economia e delle Finanze**
  - Collaborazione ai fini della **realizzazione di un sistema pubblico di prevenzione delle frodi**, con specifico riferimento **al furto d'identità**

LE COLLABORAZIONI ISTITUZIONALI E OPERATIVE A LIVELLO INTERNAZIONALE

- **IT Fraud Working Group** *(Federazione Bancaria Europea)*
- **European FI-ISAC – Financial Institutions Information Sharing and Analysis Centre** *(ENISA)*
- **ISSG/CISEG – Information Security Support Group/ Cybercrime Information Sharing Expert Group** (European Payments Council)
- **EECTF – European Electronic Crime Task Force** *(Poste Italiane, Polizia Postale, USSS)*
- **European Cybercrime Center** *(Europol)*
- **Altri network:**
  - *Membri di Antiphishing WG*
  - *Partecipazione a DCC & Progetti Europei*

Opportunità di gestione sicura dell'identità digitale
Il progetto europeo Stork 2.0

- Tra le nuove opportunità di **identificazione** sicura di utenti da remoto, si inseriscono le potenzialità di innovazione che emergeranno dal **Progetto Europeo STORK (Secure idenTity acrOss boRders linKed) 2.0**.

https://www.eid-stork2.eu/

OBIETTIVO

- Attuare un sistema europeo di riconoscimento dell'identità elettronica che permetta a imprese, cittadini e dipendenti del settore pubblico di **utilizzare la propria eID nazionale in qualsiasi Stato membro**.
- **Testare** l'uso dei documenti in **"real life environments"**, attraverso la predisposizione di progetti **pilota** cross – border e cross – settoriali.

- **ABI Lab** partecipa al **pilota bancario**, nell'ottica di **promuovere** la **diffusione** e l'**utilizzo** dei documenti di **identità elettronica** nei nuovi processi di **identificazione e vendita online**.

Sintesi dei messaggi chiave

- **MONITORAGGIO CONTINUO DELLO SCENARIO:** è sempre più **rilevante** per le banche essere **aggiornate**, anche attraverso attività di **ricerca,** sulle nuove minacce e sulle **peculiarità dei meccanismi di attacco** realizzati nei confronti dei diversi **segmenti** di clientela, in modo da adeguare opportunamente **procedure** e **tecnologie** di rilevazione e contrasto.
  - Focus clientela **Retail**: attenzione ai **potenziali nuovi attacchi verso i device mobili** e alle soluzioni di protezione per le **transazioni su carte** (sia prepagate sia carte di credito in modalità Card Not Present).
  - Focus clientela **Corporate:** attenzione alle **azioni di rilevazione e contrasto** delle **frodi**.

- **NECESSITÀ DI COMPLIANCE AL NUOVO QUADRO NORMATIVO:** numerosi sono i **progetti** in banca, in corso e previsti per il futuro, per **allineare** soluzioni tecnologiche, modelli di ICT governance, policy organizzative e metodologie di valutazione dei rischi informatici al **nuovo quadro normativo**, sempre più attento alle problematiche di sicurezza e alla lotta alle frodi.

- **ATTIVITÀ DI SENSIBILIZZAZIONE DELLA CLIENTELA:** le iniziative di **education e awareness** della clientela rappresentano oramai un elemento imprescindibile del piano di sicurezza delle banche, al fine di incrementare la **fiducia** dell'utente nei nuovi strumenti di pagamento e diffondere **comportamenti diligenti**.

- **AZIONI DI COOPERAZIONE E INFORMATION SHARING:** nell'ottica di rendere sempre più **tempestiva** ed efficace la lotta al crimine informatico, è necessario definire **procedure di cooperazione e information sharing nazionali e internazionali** tra i diversi soggetti interessati nel percorso di attuazione della frode (banche, Forze dell'Ordine e istituzioni di riferimento).

Milano, 28 maggio 2014

ABI Lab
Tecnologia utile

GRAZIE PER L'ATTENZIONE

presidio.internet@abilab.it