Un contesto dinamico in continua evoluzione…

- Il **settore bancario** è un **target** particolarmente **appetibile** per i cybercriminali, per molteplici finalità
  - → **Sottrazione denaro** dai conti delle vittime
  - → Sottrazione e divulgazione del **patrimonio informativo**
  - → Attacchi **dimostrativi** contro l'«istituzione banca»

- Al contempo, lo **scenario** dei possibili **attacchi** è molto **variegato e complesso**, con **meccanismi** in continuo **cambiamento** e **aggiornamento**

Social engineering **Trojan horse** **Pharming** **TCP Attacks**

Root kit **Botnet** **ATM malware** **Intrusion** **Packet Sniffing**

Spoofing **Ransomware** **Session Hijacking** **DDoS**

Man in the browser **SQL injection** **Virus** **Bruce force attack**

Man in the middle **…** **Spear phishing** **Vishing**

Phishing **Smishing**

Data breach **Worm**

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

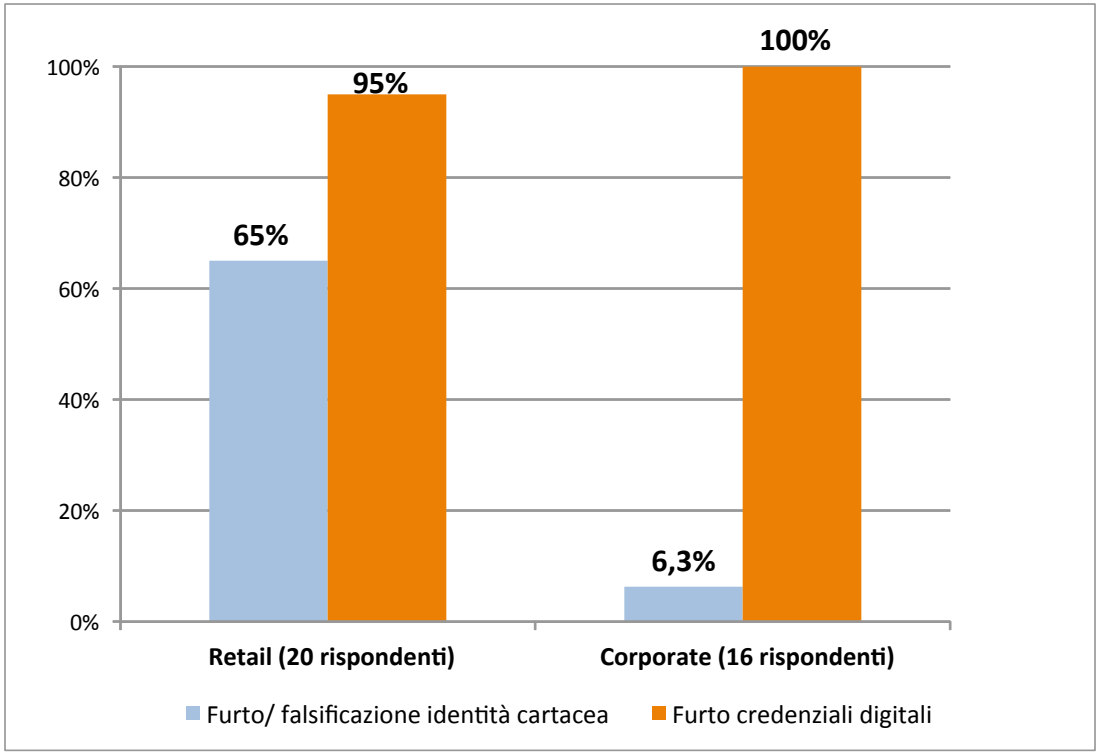
- La **rilevazione** annuale dell'Osservatorio Sicurezza e Frodi Informatiche di ABI Lab ha visto la partecipazione di **25 organizzazioni** operanti nel settore bancario, tra banche, gruppi e outsourcer, per un totale di **140** istituti rappresentativi dell'**80%** del settore in termini di **dipendenti**
- **I dati si riferiscono al periodo temporale dal 1° Gennaio al 31 Dicembre 2014** e sono stati raccolti per il segmento **Retail** (circa 85% degli account abilitati) e **Corporate** (circa 2,1 milioni account attivi)

SU TUTTA LA CLIENTELA

- La sottrazione delle **credenziali digitali** è avvenuta esclusivamente in fase di accesso ai servizi di **Internet Banking**
- Tra le banche che hanno rilevato almeno una tipologia di frode indirizzata alla clientela, praticamente la totalità ha indicato casi di **furto di credenziali digitali**

Le tipologie di frode rilevate dalle banche – confronto Retail e Corporate

(Banche che hanno rilevato almeno un tipo di frode)

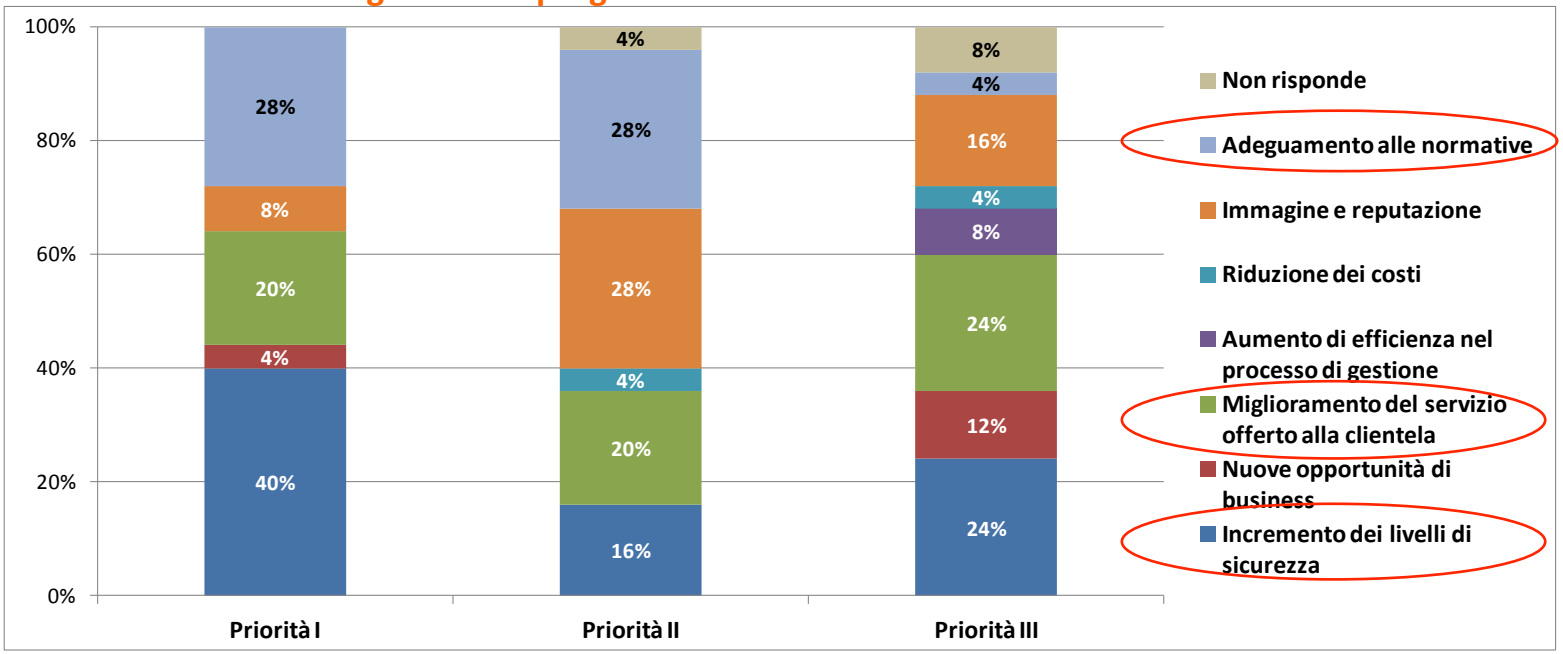


Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2015 (Campione Retail: 20 rispondenti; Campione Corporate: 16 rispondenti)

Trend di spesa per la sicurezza dei canali remoti

- Nel 2014 nessuna realtà ha indicato una diminuzione della spesa per i prossimi 12 mesi
- Circa il **50%** del campione prevede un **aumento medio** (tra 5 e 15%) o **rilevante** (superiore al 15%) per progetti e iniziative lato cliente

Priorità ed esigenze cui i progetti di sicurezza canali remoti devono dare



Principali **priorità alla base degli investimenti**:

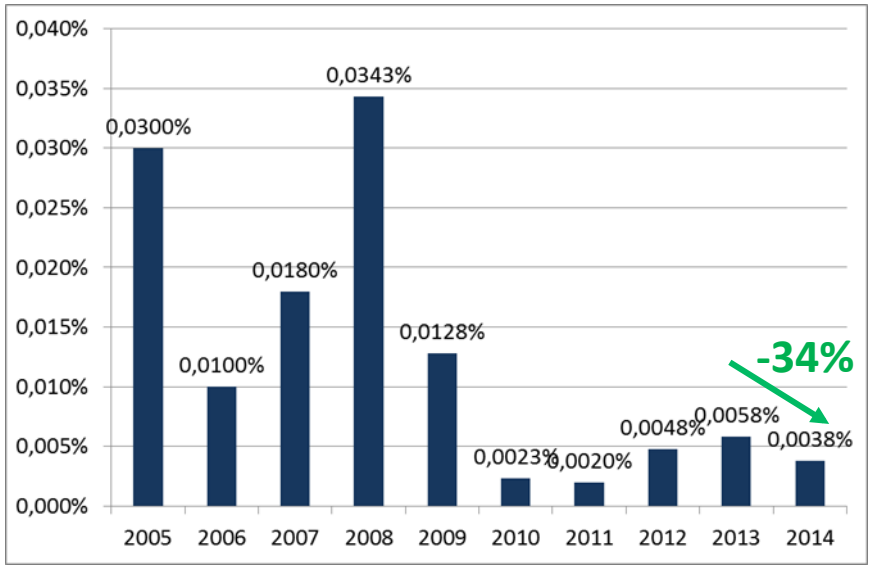
- → Incremento dei **livelli di sicurezza** (40%)
- → Adeguamento alle **normative** (28%)
- → Necessità di tutelare l'**immagine e** la **reputazione** verso l'esterno (28%)
- → Miglioramento del **servizio** offerto alla clientela (20%)

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2015 (Campione: 25 rispondenti)

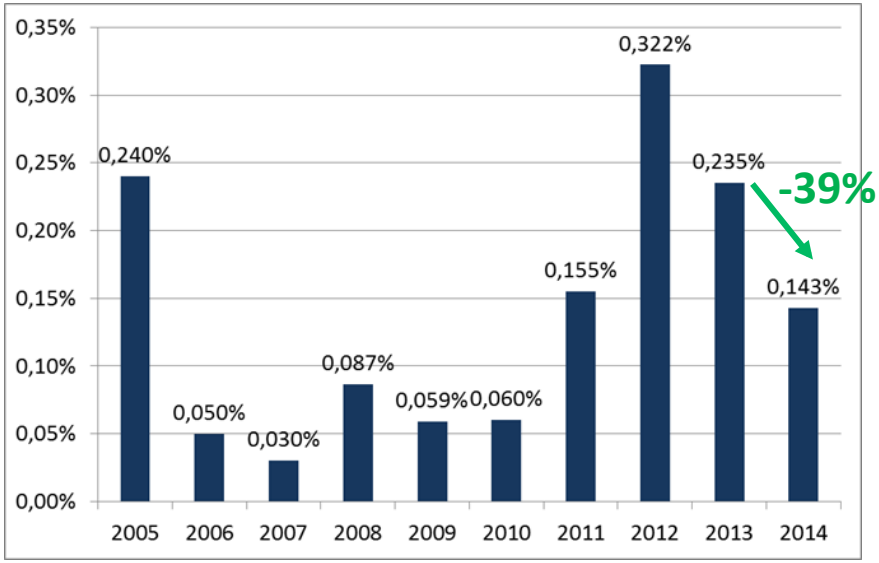
Il fenomeno delle frodi informatiche
Furto di credenziali e danno economico – ambito Retail

- Continua nel **2014** il **trend decrescente** relativo alla percentuale di **clienti attivi** vittima di furto di **credenziali**: il valore è dello **0,143%**, pari a
  - **-39%** rispetto al **2013**
  - **-55%** rispetto al **2012**.
- Il **rapporto** tra numero clienti Retail vittima di **furto di credenziali** e il totale degli **accessi** all'Internet Banking è dello **0,0023%.**

Percentuale di clienti attivi Retail che hanno perso denaro - trend 2005-2014 (campione variabile)



Percentuale di clienti attivi Retail che hanno perso le credenziali - trend 2005-2014 (campione variabile)



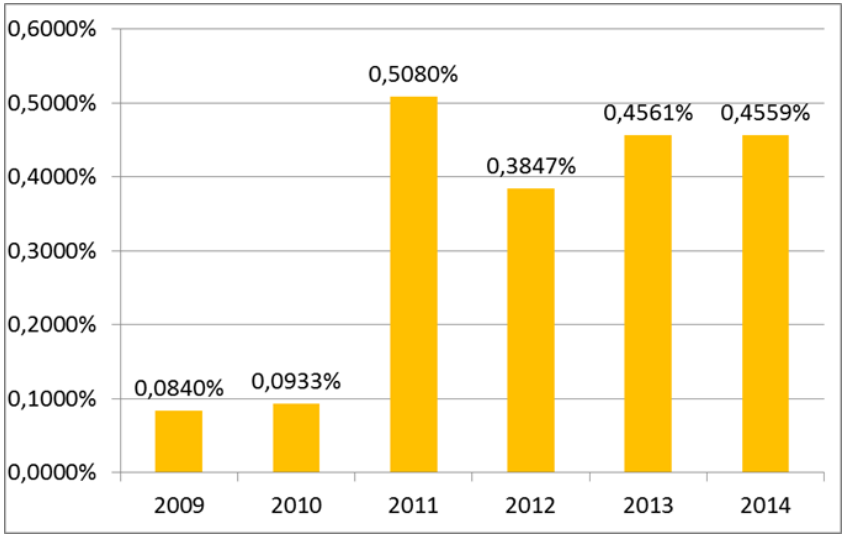
- L'efficacia delle contromisure ha fatto registrare per il 2014 anche una **riduzione** della percentuale di **clienti attivi** che ha subito una frode **con danno economico: 0,0038%, pari -34%** dal 2013.
- In relazione al totale degli **accessi** sul canale Internet Banking stimato per il 2014, la % è dello **0,000059%**, pari a **1 cliente ogni 1.700.000.**

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2015
(Campione: 25 rispondenti)

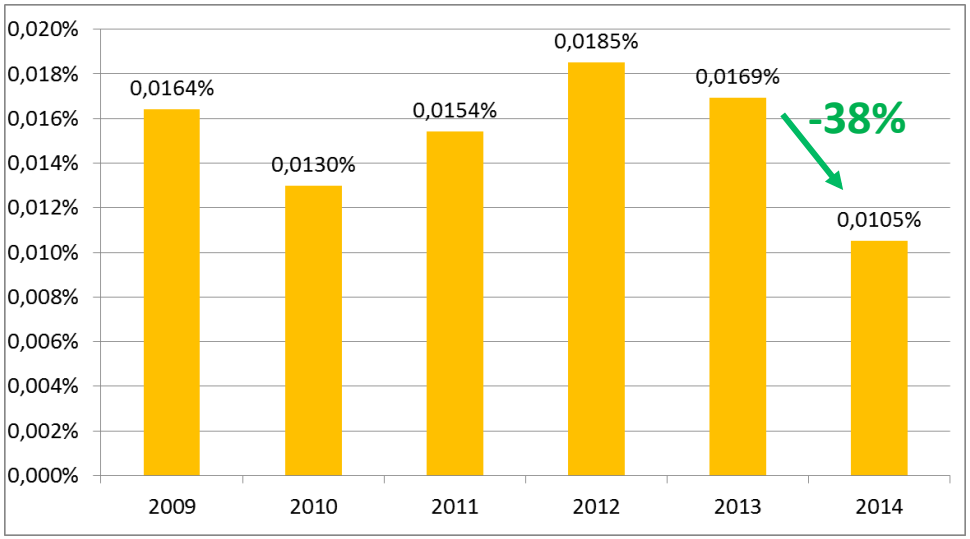
Il fenomeno delle frodi informatiche
Furto di credenziali e danno economico – ambito Corporate

- La **percentuale** clienti attivi vittima di **furto di credenziali** è sostanzialmente **in linea con il 2013**, a testimonianza dell'**elevato indice di rischio** associato a tale segmento di clientela rispetto agli attacchi informatici.
- Rapportando la **% di clienti attivi** vittima di furto di credenziali alla stima degli **accessi** all'Internet Banking, la percentuale si attesta sullo **0,0037%**.

Percentuale di clienti attivi Corporate che hanno perso le credenziali - trend 2009-2014 (campione variabile)



Percentuale di clienti attivi Corporate che hanno perso denaro - trend 2009-2014 (campione variabile)

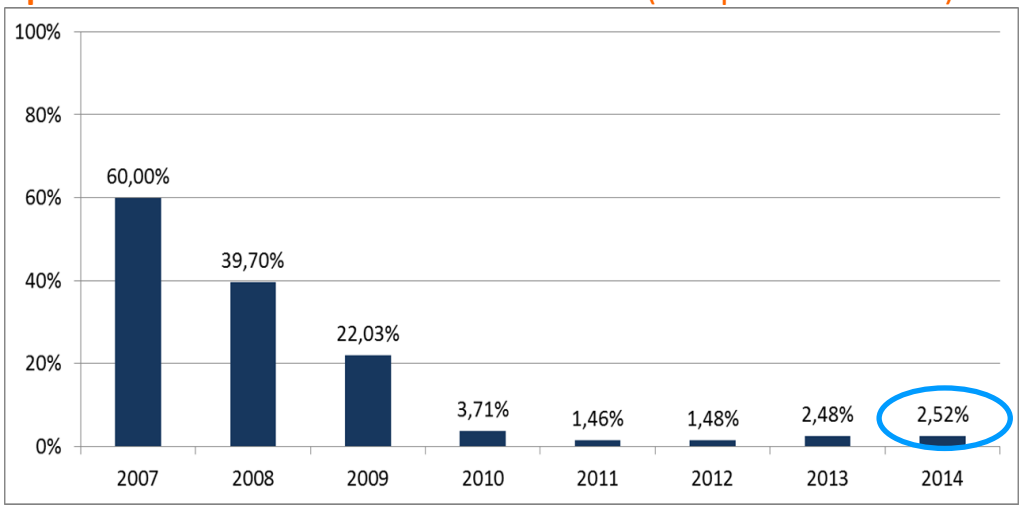


Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2015 (Campione: 25 rispondenti)

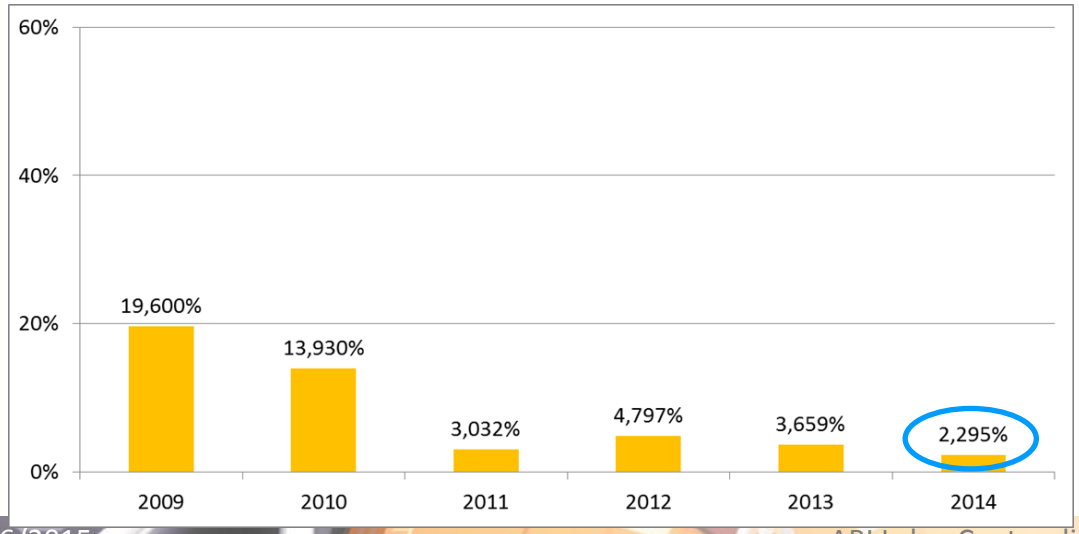
- Nel 2014 si registra una **diminuzione** quasi del **38%** rispetto all'anno precedente dei clienti che a fronte del furto di identità hanno subito un **danno economico**.
- In rapporto al **totale degli accessi** all'Internet Banking, la percentuale di **clienti che ha subito un danno economico** è pari allo **0,00009%.**

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

Percentuale di clienti Retail che perde denaro a seguito della perdita di credenziali - trend 2007-2014 (campione variabile)



Percentuale di clienti attivi Corporate che perde denaro a seguito della perdita di credenziali - trend 2009-2014 (campione variabile)



Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2015
(Campione: 25 rispondenti)

SEGMENTO RETAIL

- L'incidenza degli attacchi, che passa dal 2,48% del 2013 al **2,52% del 2014**, rappresenta **un'efficacia dell'azione di contrasto superiore al 97%.**

SEGMENTO CORPORATE

- **Miglioramento** dell'**efficacia** delle contromisure tecnologiche e di processo: nel 2014, la percentuale di clienti che ha subito un danno economico a seguito del furto di credenziali è scesa al **2,295%**.
- I **volumi economici** associati alle **frodi tentate o effettive** verso le **imprese** rimangono percentualmente **più elevati** rispetto al comparto Retail.

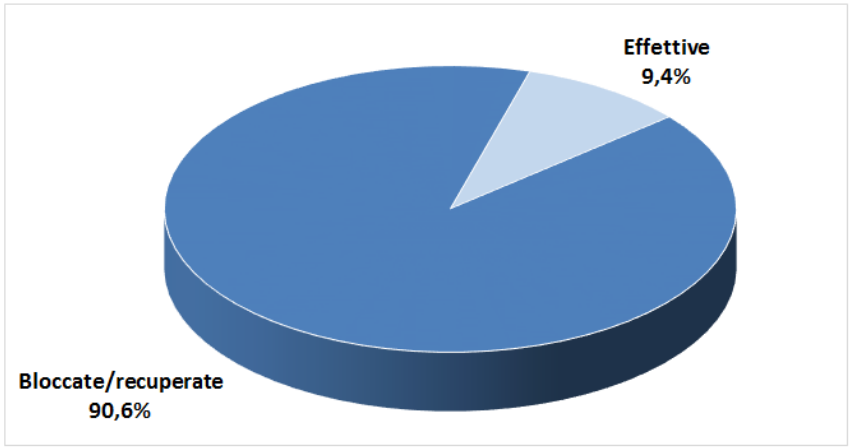
SU TUTTA LA CLIENTELA

- Nel **2014** la **percentuale di clienti attivi** che hanno **perso denaro** è diminuita di circa il **37%**

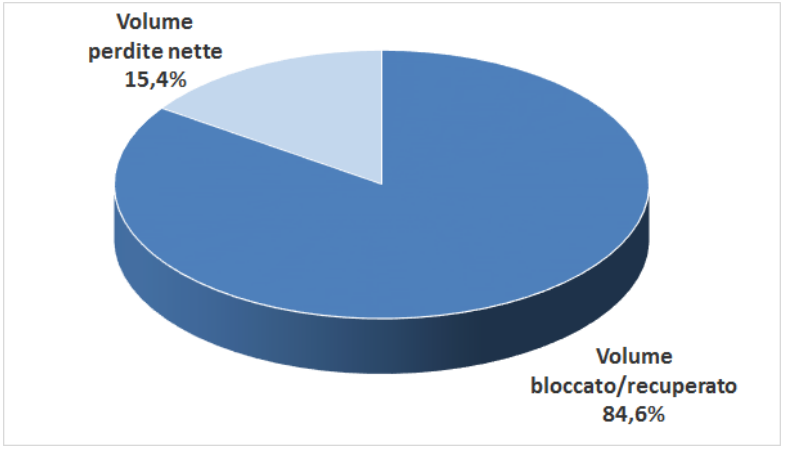
Scenario complessivo transazioni anomale

Numero di eventi e volumi economici – clientela Retail

Ripartizione percentuale delle tipologie di transazioni anomale rilevate – numero accadimenti



Ripartizione percentuale delle tipologie di transazioni anomale rilevate – volume transato (



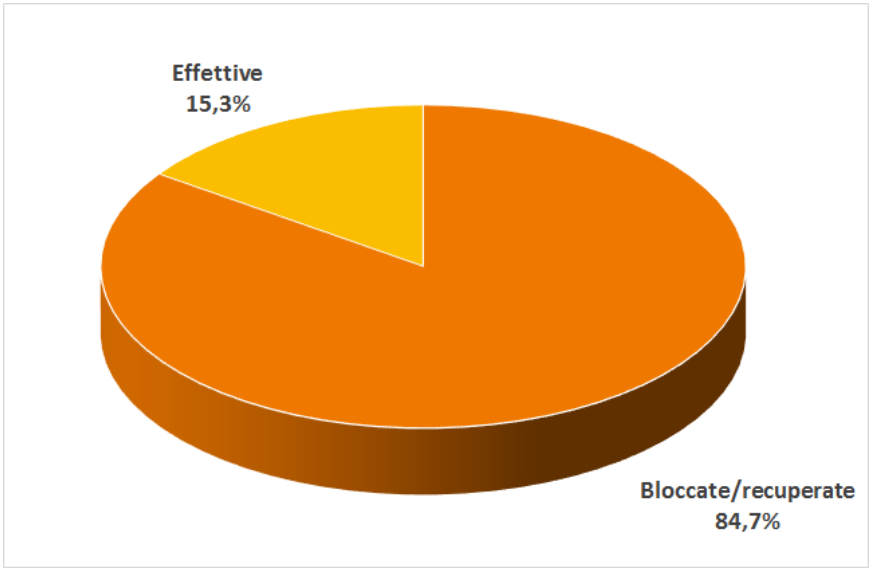
- Per il 2014 solo il **9,4%** ha rappresentato una **transizione fraudolenta** (in termini di **numero di episodi**).
- In relazione al **volume economico anomalo** transato, il **15,4%** è relativo alle transazioni fraudolente effettive**,** mediamente in **lieve aumento** rispetto al **passato**.
- Il vettore di **cash out** più diffuso è rappresentato dai **bonifici** disposti verso l'**estero** (53%), seguito dalle operazioni di **ricarica di carte prepagate** (34,6%).

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2015 (Campione: 25 rispondenti)

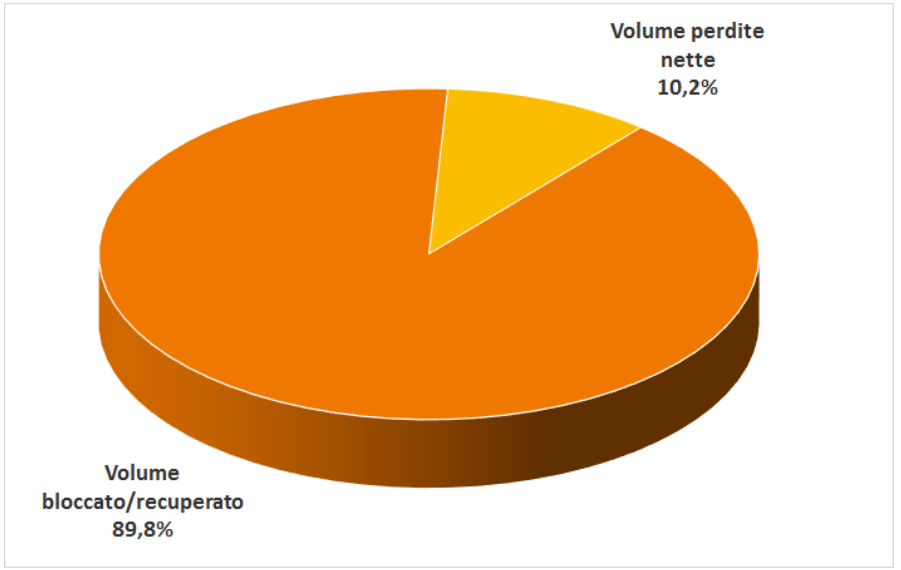
Scenario complessivo transazioni anomale

Numero di eventi e volumi economici – clientela Corporate

Ripartizione percentuale delle tipologie di transazioni anomale rilevate - numero accadimenti



Ripartizione percentuale delle tipologie di transazioni anomale rilevate - volume transato

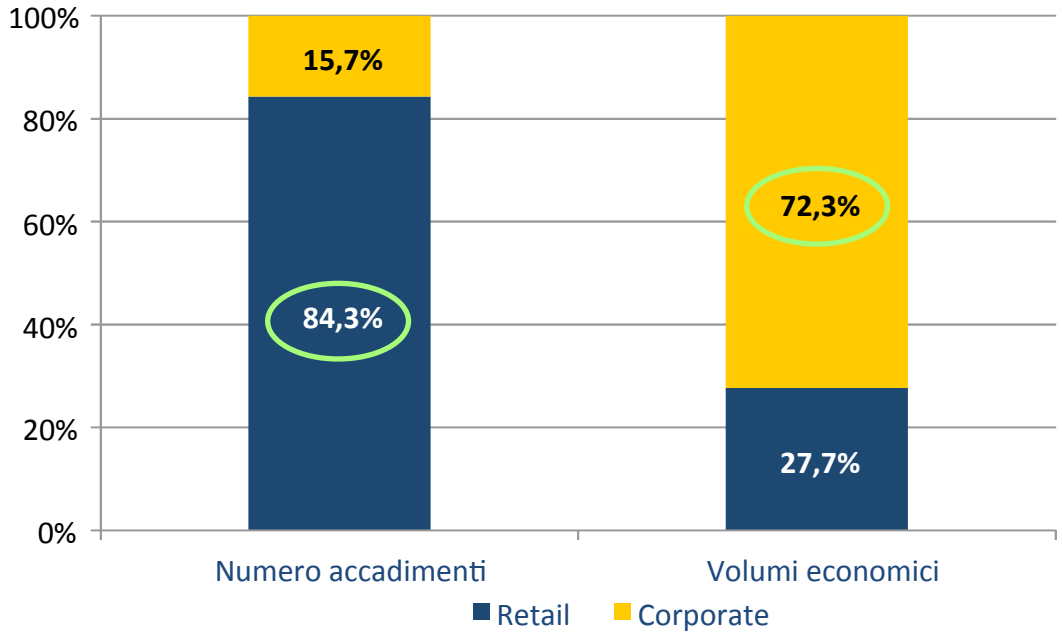


- La pressoché totalità delle **transazioni anomale** in danno alla clientela Corporate è costituita da **bonifici,** di cui **la maggioranza** è verso l'**estero** (63,9%)
- La percentuale di transazioni **fraudolente effettive** (15,3%) nel 2014 è in diminuzione rispetto al 2013
- L'**89,8%** dei **volumi anomali** transati, **più elevati rispetto al Retail**, è stato efficacemente **bloccato o recuperato**.

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2015
(Campione: 25 rispondenti)

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

Totale transazioni anomale (bloccate, recuperate ed effettive) – confronto Retail e Corporate per numero accadimenti e volumi economici

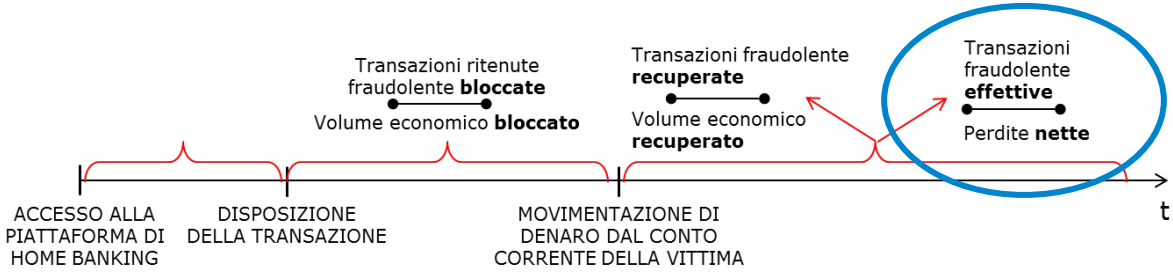


Rispetto al campione totale:

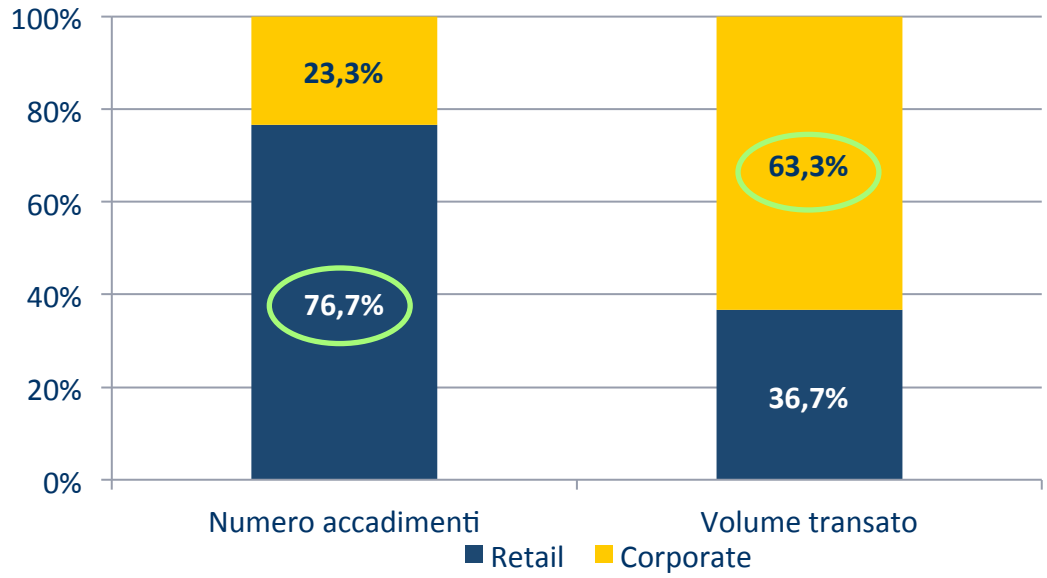
- L'**84,3%** degli attacchi (in termini di numero di episodi) è stato indirizzato alla clientela **Retail**, valore decisamente **superiore** rispetto al comparto **Corporate**.
- **La maggiore entità dei volumi economici** transati per l'intero campione di analisi è tuttavia associabile alla clientela **Corporate**, con un rapporto di quasi **3:1**.

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2015 (Campione: 25 rispondenti)

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



Transazioni fraudolente effettive – confronto Retail e Corporate per numero accadimenti e volume transato

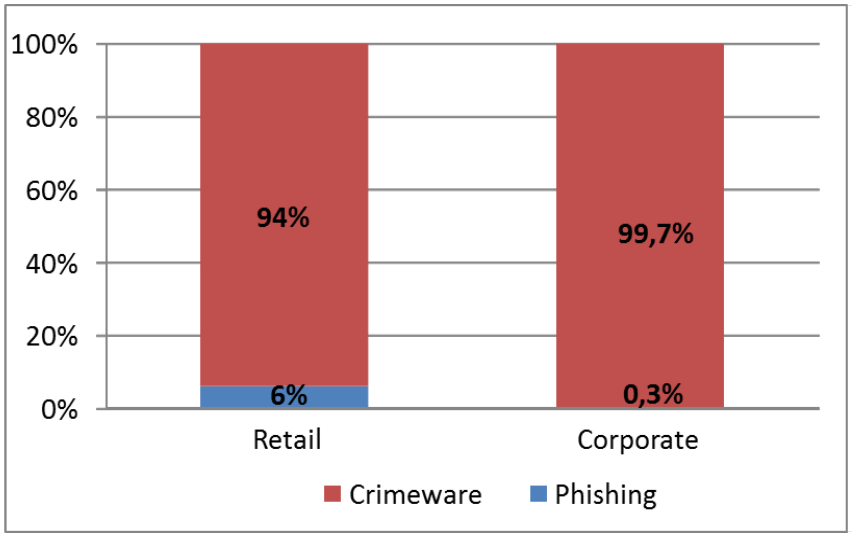


- In relazione al **numero di transazioni effettivamente fraudolente**, la clientela **Retail** risulta maggiormente **colpita** (**76,7%**), rispetto al comparto imprese (23,3%).
- Il rapporto si inverte se si prende come riferimento il **volume economico** associato alle perdite, che è pari al **63,3%** per il segmento **Corporate.**
- In **media,** una **frode effettiva Corporate** ha un **volume 6 volte più elevato** rispetto a una **frode Retail**

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2015 (Campione: 25 rispondenti)

Modalità di realizzazione dell'attacco
Confronto segmenti di clientela

Modalità di realizzazione dell'attacco – confronto Retail e Corporate



SEGMENTO RETAIL

- Solo il **6%** delle operazioni anomale è riconducibile ad attacchi di **phishing tradizionali** (mail «trappola»), ma che mantengono una certa rilevanza in termini di efficacia.

SEGMENTO CORPORATE

- È il **crimeware** il vettore più utilizzato dai frodatori per realizzare un attacco (**99,7%**).
- **Il 60%** degli **attacchi** è **eseguito** dalla **sessione** dell'**utente**

SU TUTTA LA CLIENTELA

- Si rilevano **meccanismi** di sottrazione delle credenziali **ibridi**

MODALITÀ DI SOTTRAZIONE DELLE CREDENZIALI DISPOSITIVE

SEGMENTO RETAIL

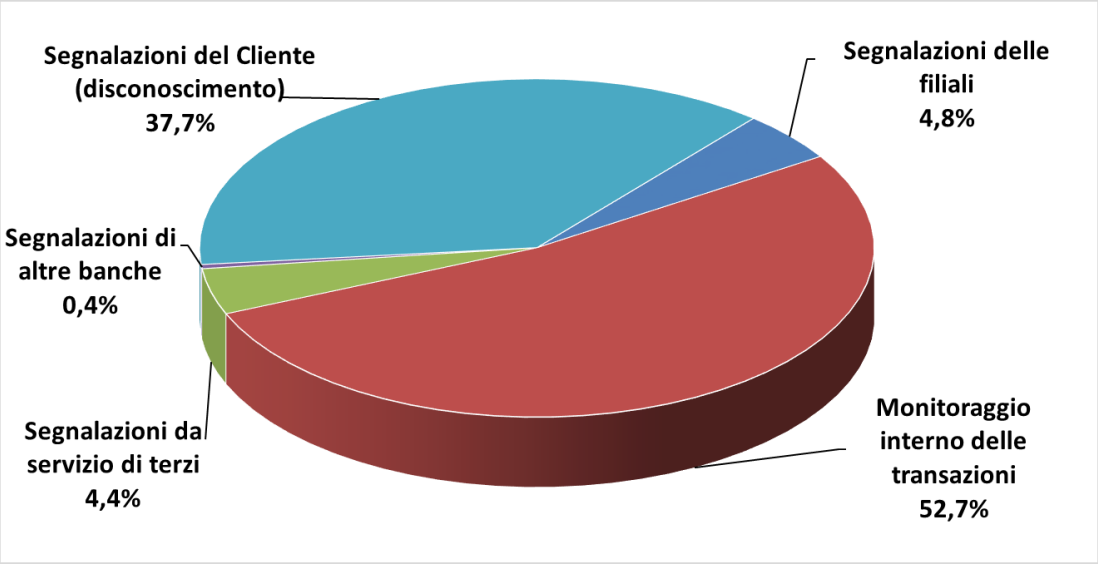
- L'attenzione dei frodatori si sposta verso i **device mobili** di fatto quando vengono utilizzati dal cliente come secondo fattore per la ricezione dell'**OTP via SMS** dispositivi
- Il fenomeno è comunque **contenuto** e **in calo** rispetto al 2013: solo **4** banche hanno rilevato tali episodi, che hanno coinvolto lo **0,0003%** dei **clienti** che utilizzano il telefono come **tecnologia autorizzativa**.

SEGMENTO CORPORATE: **nessun** tipo di **coinvolgimento** di **device mobili**.

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2015 (Campione: 25 rispondenti)

Segnalazione e gestione anomalie transazioni e rete

Segnalazione attraverso cui vengono intercettate le operazioni fraudolente (segmento Retail)*



- Attraverso la definizione di soglie e algoritmi di correlazione in alcuni casi molto complessi, i **sistemi interni di monitoraggio** sono sempre più efficaci nel **rilevare transazioni sospette** (**52,7%**).
- Nel **37,7%** dei casi le segnalazioni provengono dal **cliente** (disconoscimento).

Rilevazioni siti clone

- L'**80%** del campione **contatta** l'Internet Service Provider per bloccare tempestivamente il sito fake

Attacchi DDoS

- Solo il **16%** delle banche rispondenti*** ha rilevato **attacchi DDoS** nel **2014** verso le proprie reti, contrastati nella maggior parte dei casi attraverso l'attivazione di **filtri** del traffico web in entrata, sistemi di **sicurezza interni** o altre soluzioni di sicurezza spesso preventivamente contrattualizzate con i **carrier**.

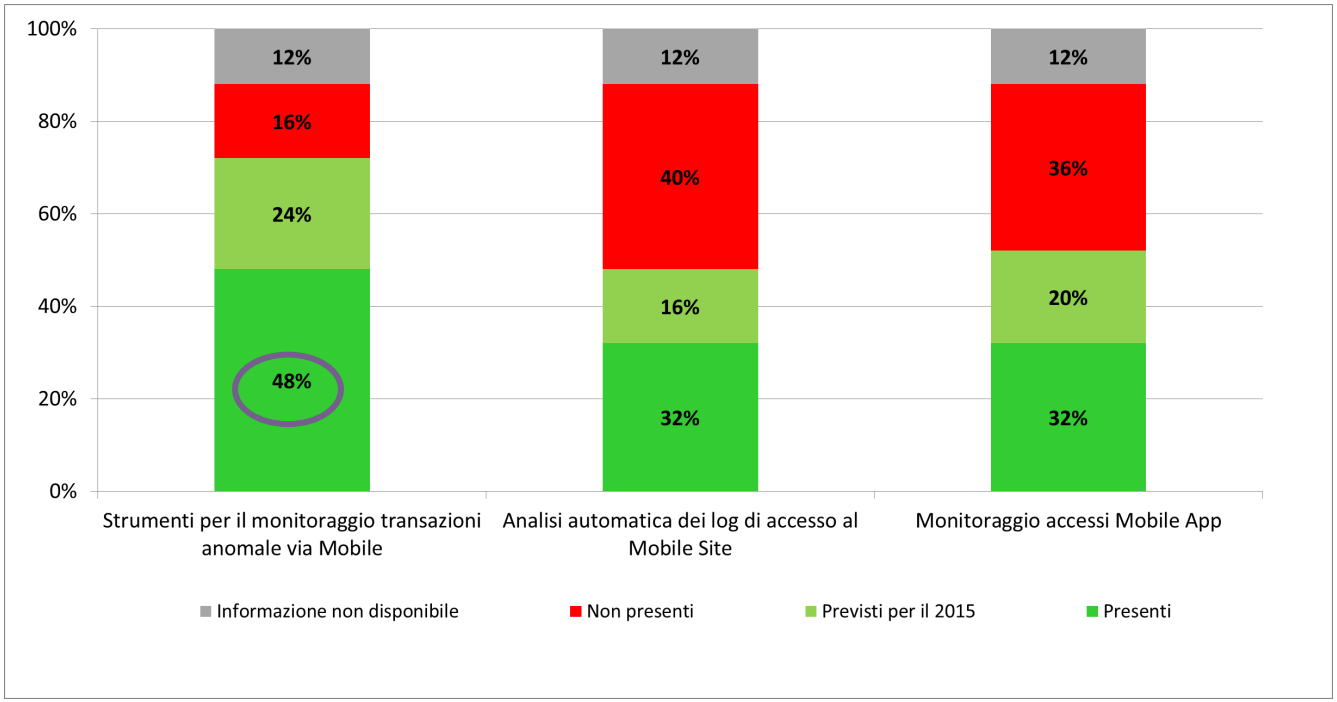
Importanza di promuovere lo scambio di informazioni anche a fini preventivi

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2015
(*Campione Retail: 18 rispondenti, media %; **Campione: 20 rispondenti, media %; ***Campione: 25 rispondenti;)

La sicurezza sul canale Mobile

- **Non** si registrano, neanche per il **2014,** casi di **perdita di denaro** a seguito di **attacchi specifici** realizzati sul **canale Mobile** e sui relativi servizi offerti.
- **Solo 1 realtà ha segnalato casi di App Mobile clonata**.

Strumenti tecnologici per il monitoraggio e la rilevazione di attacchi*



Iniziative di formazione interna**

- Il **39,1%** del campione ha indicato di aver svolto nel **2014** attività di **formazione interna,** mentre il **21,8%** prevede di attuarle durante il 2015

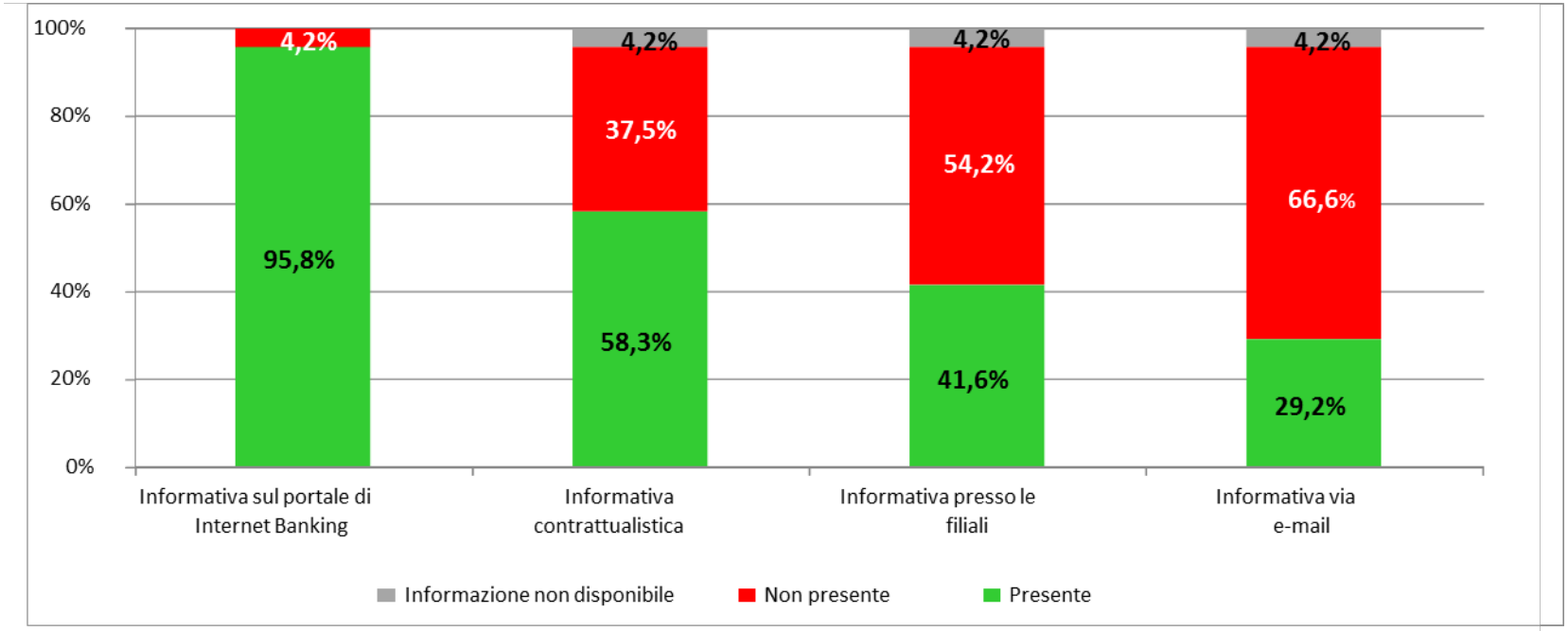
Contromisure tecnologiche*

- L'**88%** del campione adotta per il canale Mobile lo stesso strumenti di secondo fattore offerto per i servizi di Banking.
- La tecnologie di secondo fattore più diffusa è l'**OTP via hardware disconnesso dal PC** (37,5%), seguita **dall'OTP via sms** (20,8%).

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2015
(*Campione: 25 rispondenti; **Campione: 23 rispondenti)

Le azioni di sensibilizzazione della clientela

Attività informativa verso la clientela Retail*



- Le raccomandazioni BCE e le successive linee guida EBA sottolineano l'importanza di svolgere **attività di awareness verso la clientela**, per educarla a un utilizzo corretto dei servizi di Internet Banking e degli strumenti messi a disposizione dalla banca per la sicurezza di accessi e transazioni.
- La quasi totalità di banche intervistate ha svolto **attività informativa** verso la clientela Retail attraverso il proprio **portale di Internet Banking** (95,8%). Risultati analoghi si rilevano per la clientela Corporate.
- Il **12,5%** del campione **informa** il cliente anche attraverso la **App** di Mobile Banking.

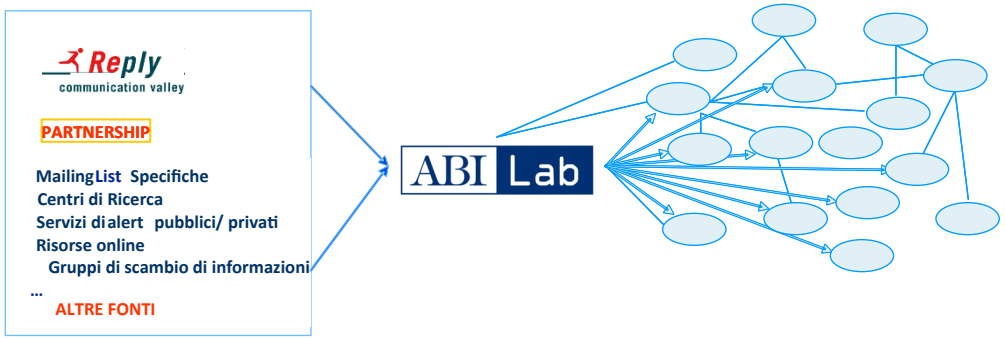
Importanza di sensibilizzare il cliente per poter massimizzare l'efficacia delle contromisure

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2015
(*Campione Retail: 24 rispondenti; **Campione: 23 rispondenti)

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

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 inoltre corredata dall'invio di **report periodici**, realizzati in collaborazione con i partner tecnologici dell'iniziativa, contenenti informazioni generali sulle principali minacce informatiche che insistono 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.	✓			✓

In sintesi…qualche spunto di riflessione

Dinanzi alla **specializzazione** dei **meccanismi** di **attacco** e al **rafforzamento** delle **competenze tecnologiche** e di **processo** da parte dei frodatori, le banche non sono state a guardare, ma hanno definito o rafforzato **presidi strutturati** e al contempo **dinamici**, capaci di rispondere e per quanto possibile di anticipare le mutazioni dei vettori di attacco, al punto che nel **2014 oltre il 97%** degli **attacchi** è stato **bloccato**

next step

PERSEVERARE LUNGO IL PERCORSO INTRAPRESO:

- **Monitoraggio**, **intelligence** e analisi del **rischio**
- Attenzione alle possibili **evoluzioni future** degli attacchi – focus **imprese e nuovi device**

IMPARARE DAGLI ERRORI:

- Guardare con occhio critico e saper trarre delle «**lessons learned**» dagli incidenti e dai casi di frode occorsi

EDUCARE IL CLIENTE:

- Non dimenticare mail di **sensibilizzare** il **cliente** per **massimizzare** l'**efficacia** delle **contromisure** e rafforzare la fiducia dell'utente verso i servizi e gli strumenti offerti

FARE SISTEMA:

- Promuovere e supportare la **cooperazione** e lo **scambio di informazioni**, perché un sistema più forte può essere anche meno appetibile per i cybercriminali

Roma, 05 giugno 2015

ABI Lab
Tecnologia utile

GRAZIE PER L'ATTENZIONE

presidio.internet@abilab.it