Un contesto dinamico in cui si inseriscono le strategie di cybersecurity delle banche…

Società e mercati dipendenti dal cyberspace*

- **65%** degli **utenti Internet** in **EU** ha fatto **acquisti online** nel **2015**
- L'abilitazione del **Digital Single Market** può arricchire il **PIL europeo** di **+415 miliardi** di euro

Incremento dei servizi bancari remoti

- Nel **2015** in **Italia** gli utenti **Retail** che usano l'**HB** sono aumentati del **+12,4%** rispetto al 2014 e gli **accessi** sono in crescita del **+37%****
- **214 milioni** di persone in **Europa** utilizzeranno servizi di **Mobile Banking** entro il **2018*****

Nuove normative con impatti sulla sicurezza

PSD2

Vigilanza Bancaria

RTS EBA su Terze Parti e Strong Authentication

Linee Guida Cyber resilience

Direttiva NIS

…

Evoluzione e specializzazione delle minacce

Ransomware

DDoS for BitCoin

Instant phishing

CEO Fraud

Dridex

…

Data Breach

Avere visibilità del dimensionamento delle frodi informatiche e delle relative azioni di contrasto e prevenzione consente alla singola banca, al settore e agli stakeholder esterni di avere una fotografia del fenomeno e di poterne così individuare margini di miglioramento e punti di forza

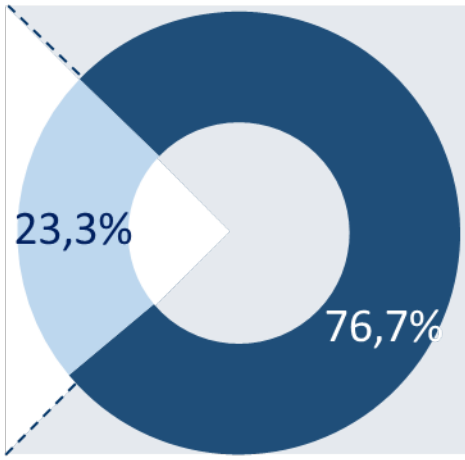
Fonti:* Eurostat 2015, Digital Single Market Strategy, 2015; **ABI, ABI Lab, 2016; ***Forrester Research, EBF Blueprint, 2015

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

- **30 organizzazioni** rispondenti, tra banche, gruppi e outsourcer, per un totale di **142** istituti rappresentativi di dell'**86%** del settore in termini di **dipendenti**
- **Periodo temporale di analisi: 1° Gennaio al 31 Dicembre 2015,** dati raccolti in maniera distinta per segmento **Retail** (circa **84%** degli **account attivi**) e **Corporate** (circa **2 milioni** account **attivi**)

Banche che hanno rilevato casi di frode identitarie – analisi Retail e Corporate

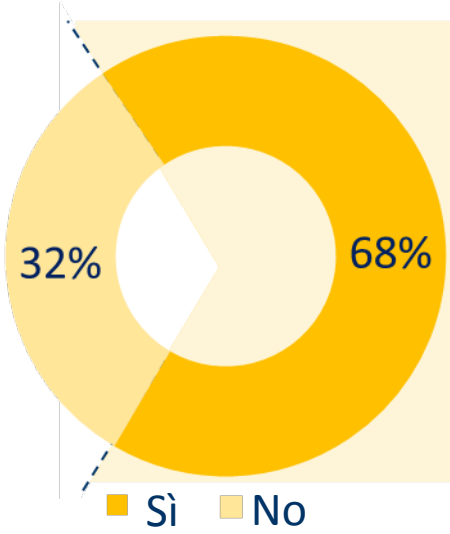
SEGMENTO RETAIL*



Delle banche che hanno detto sì:

- Il **65%** ha rilevato casi di **furto/ falsificazione di identità cartacea**
- Il **96%** ha registrato casi di **furto di credenziali digitali**

SEGMENTO CORPORATE**



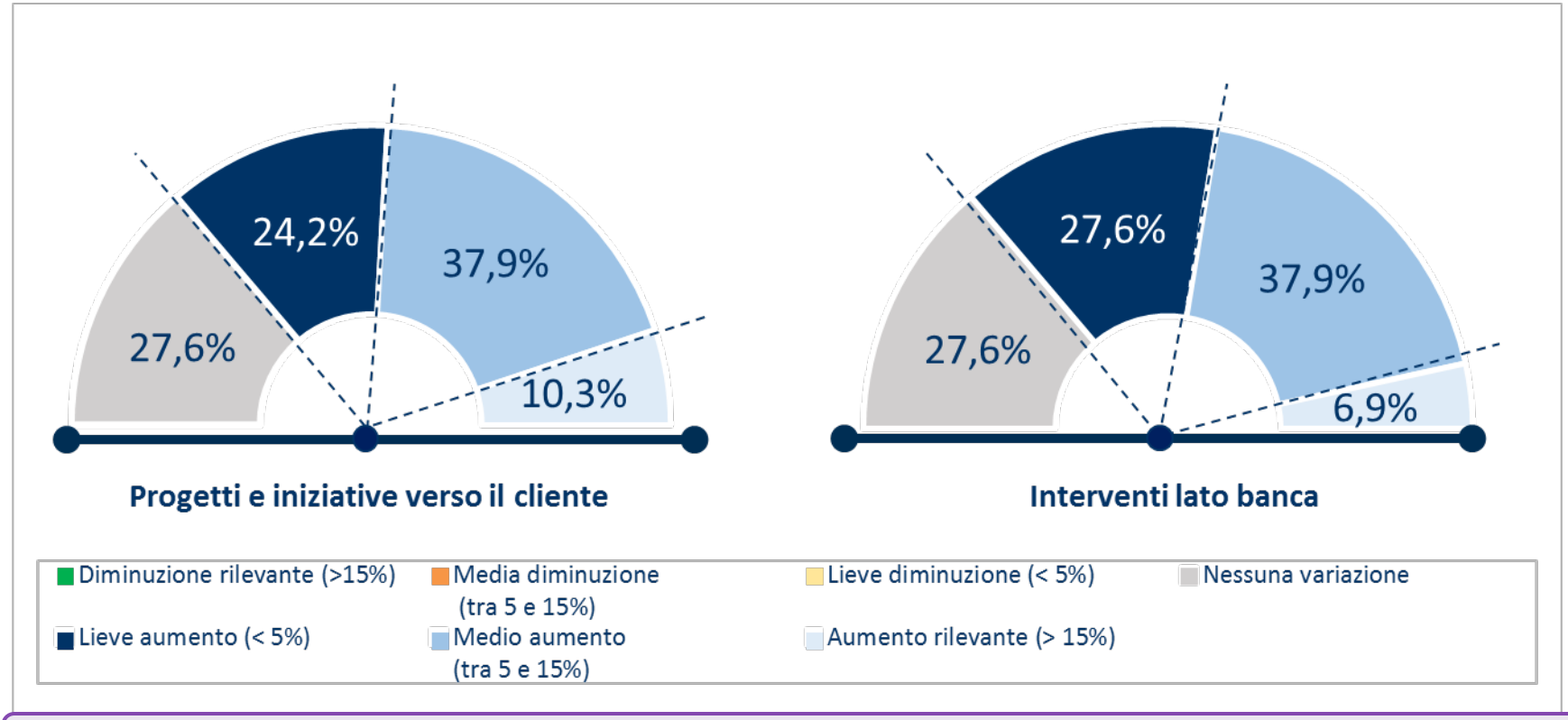
Di queste:

- **TUTTE** hanno registrato casi di **furto di credenziali digitali**
- Il **5,3%** ha segnalato casi di **furto/ falsificazione** di **identità cartacea**

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2016
(*Campione Retail: 30 rispondenti; **Campione Corporate: 28 rispondenti)

Trend di spesa per la sicurezza dei canali remoti

Evoluzione del livello medio di spesa nei prossimi 12 mesi – iniziative su clientela Retail (29 rispondenti)



Nessuna realtà ha indicato una diminuzione della spesa per i prossimi 12 mesi

Principali **esigenze alla base degli investimenti***:

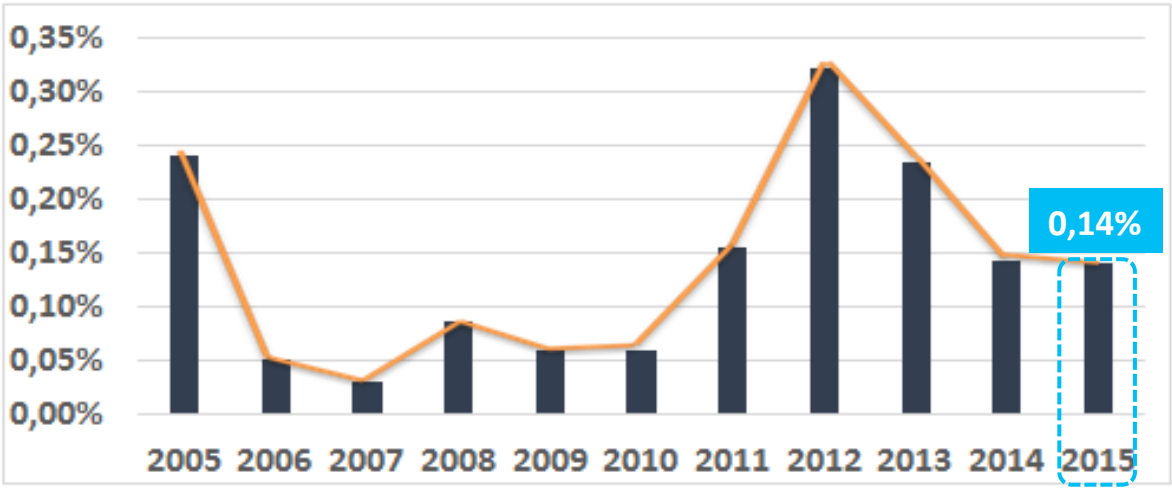
- Incremento dei **livelli di sicurezza** (1° priorità per il 38% del campione)
- Adeguamento alle **normative** (1° priorità per il 31% del campione)
- Miglioramento del **servizio** offerto alla clientela (1° priorità per il 14% del campione)
- Tutela di **immagine e reputazione** verso l'esterno (1° priorità per il 10% del campione)

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2016
Campione: 29 rispondenti

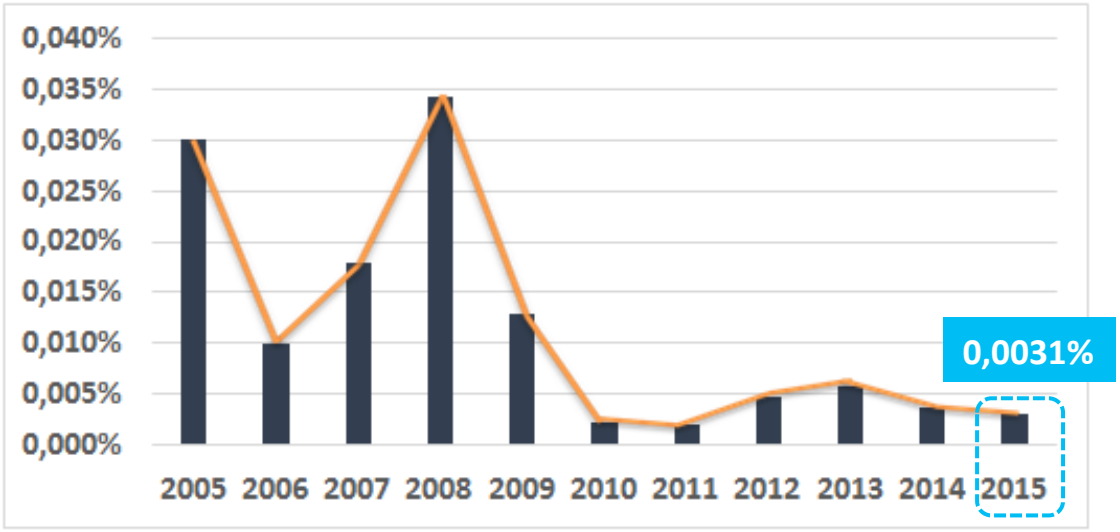
Furto di credenziali e danno economico
Clientela Retail

Percentuale di clienti attivi Retail che hanno perso le credenziali - trend 2005-2015 (campione variabile)

- Il **rapporto** tra numero clienti Retail vittima di **furto di credenziali** e il totale degli **accessi** all'Internet Banking è dello **0,0016% (1 su 62.500)**



Percentuale di clienti attivi Retail che hanno perso denaro - trend 2005-2015 (campione variabile)



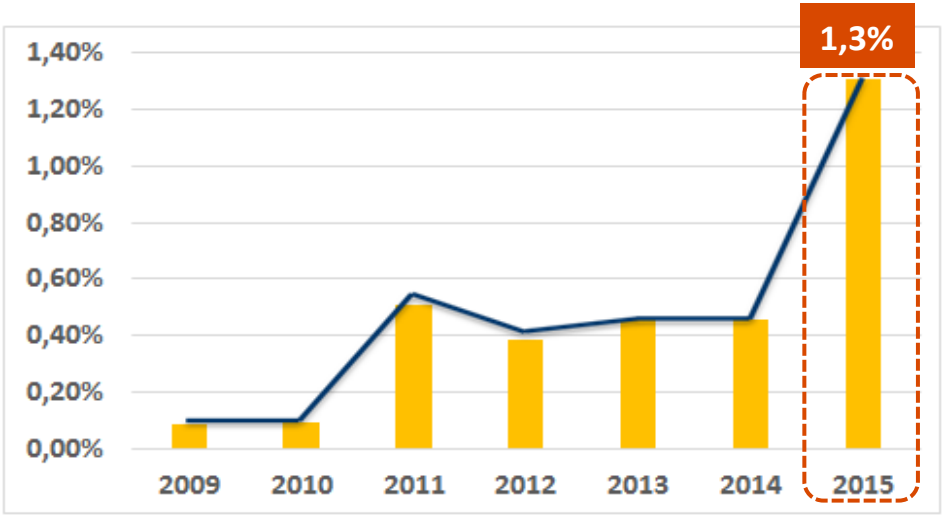
Entrambi i trend sostanzialmente stabili rispetto al 2014

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2016
(Campione: 30 rispondenti)

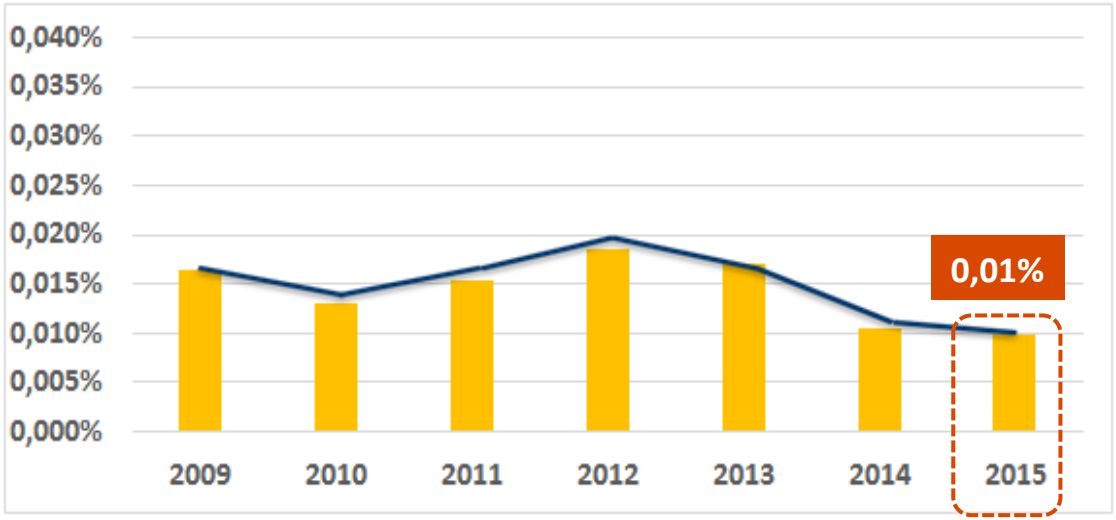
Furto di credenziali e danno economico
Clientela Corporate

Percentuale di clienti attivi Corporate che hanno perso le credenziali - trend 2009-2015 (campione variabile)

- Rapportando la **% di clienti attivi** vittima di furto di credenziali alla stima degli **accessi** all'Internet Banking, la percentuale si attesta sullo **0,0087%**.



Percentuale di clienti attivi Corporate che hanno perso denaro - trend 2009-2015 (campione variabile)



Efficace azione di contrasto a fronte di un elevato indice di rischio

SU TUTTA LA CLIENTELA: lo **0,004%** dei **clienti attivi** ha subito una **perdita di denaro**

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2016 (Campione: 30 rispondenti)

Il percorso di realizzazione di una transazione fraudolenta

Definizioni adottate

Al fine di avere un **linguaggio comune** e di raccogliere **informazioni omogenee** e **confrontabili** tra le diverse banche, sono state condivise e validate le seguenti **definizioni**, adottate nella rilevazione:

Somma delle transazioni fraudolente **bloccate** e **recuperate**

Frodi rilevate e **bloccate** prima che abbiano avuto un impatto economico sul conto corrente della vittima

Frodi "andate a buon fine", per le quali il **cliente** ha subito un **danno economico**, anche parziale (senza considerare eventuali rimborsi).

Transazioni fraudolente **tentate**

Volume economico associato alle transazioni fraudolente **tentate**

Transazioni fraudolente **bloccate**

Volume economico **bloccato**

Transazioni fraudolente **recuperate**

Volume economico **recuperato**

Transazioni fraudolente **effettive**

Volume economico **frodi effettive**

ACCESSO ALLA PIATTAFORMA DI INTERNET BANKING

DISPOSIZIONE DELLA TRANSAZIONE

MOVIMENTAZIONE DI DENARO

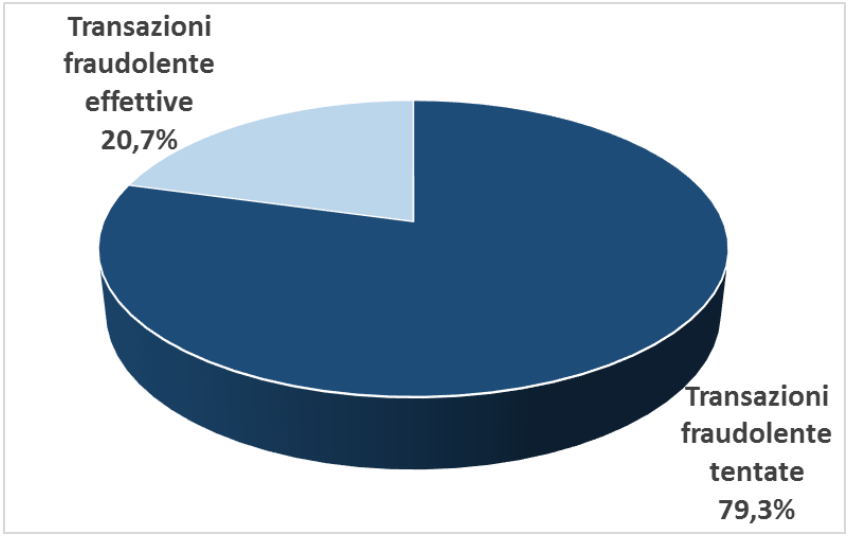
t

Frodi che hanno comportato una movimentazione di denaro dal conto corrente della vittima ma che per le quali è stato possibile **recuperare l'intero importo transato**

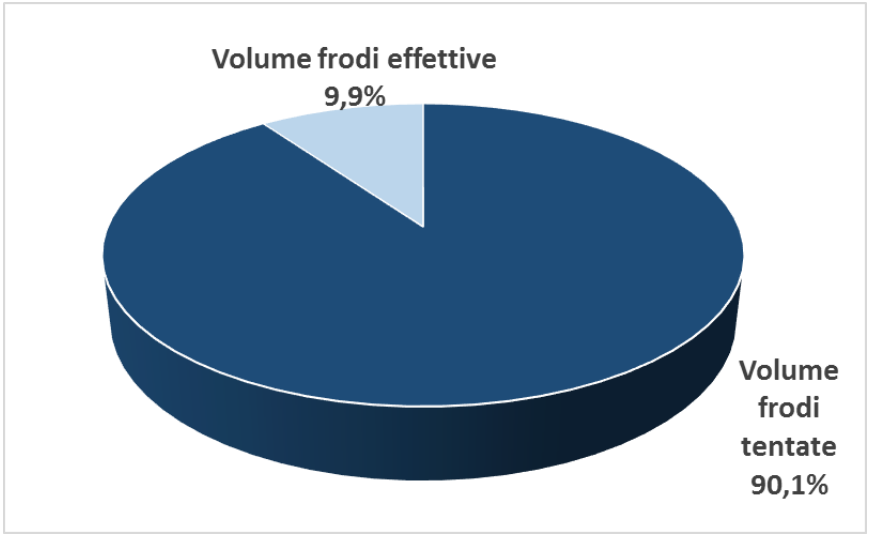
Scenario complessivo transazioni anomale

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 economico



- Il **43,3%** del totale delle **transazioni fraudolente effettive** è rappresentato dalle operazioni di **ricarica di carta prepagata**, il **23%** da **bonifici** disposti **verso un'altra banca italiana**

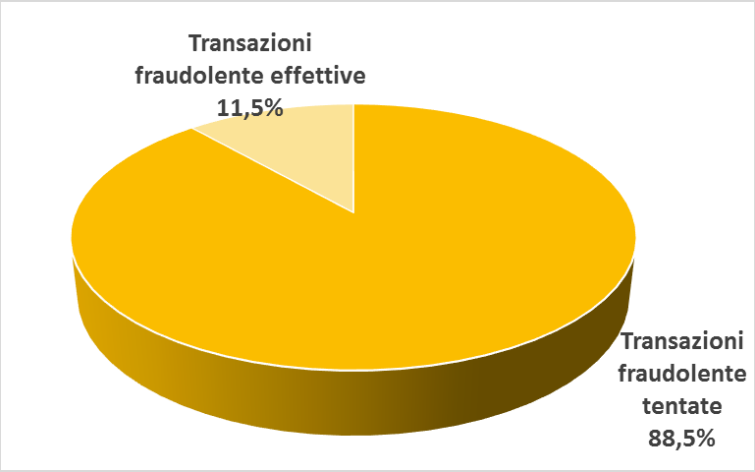
Importanza di un aggiornamento continuo dei criteri alla base delle procedure e degli algoritmi per la rilevazione di anomalie e la generazione di alert

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2016 (Campione: 30 rispondenti)

Scenario complessivo transazioni anomale

Numero di eventi e volumi economici – clientela Corporate

Ripartizione percentuale delle tipologie di transazioni anomale rilevate - numero accadimenti



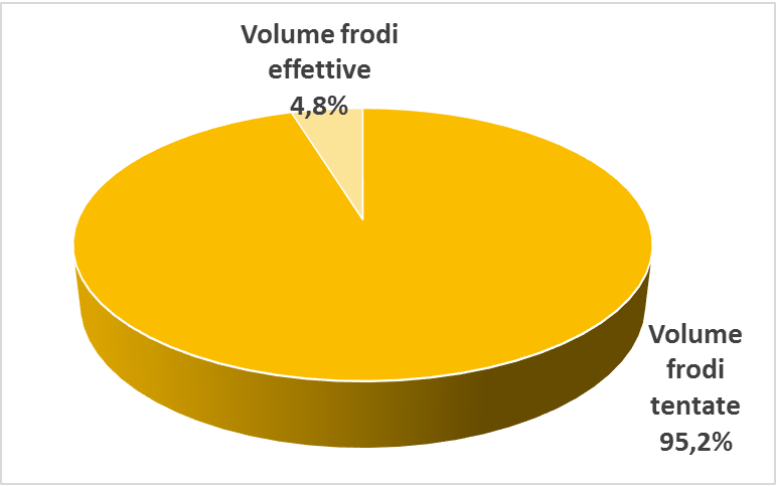
- La pressoché totalità delle **transazioni fraudolente effettive** in danno alla clientela Corporate è costituita da **bonifici,** di cui **la maggioranza** è verso **un'altra banca italiana** (**60,9%**) o verso l'**estero – area SEPA** (**30,7%**)

Importanza di una collaborazione extra-nazionale per l'attività di blocco/recupero della frode

- A fronte dell'incremento del numero di attacchi rispetto al passato, il **numero** di **transazioni effettive** risulta **contenuto**

Le contromisure delle banche hanno limitato il danno potenziale

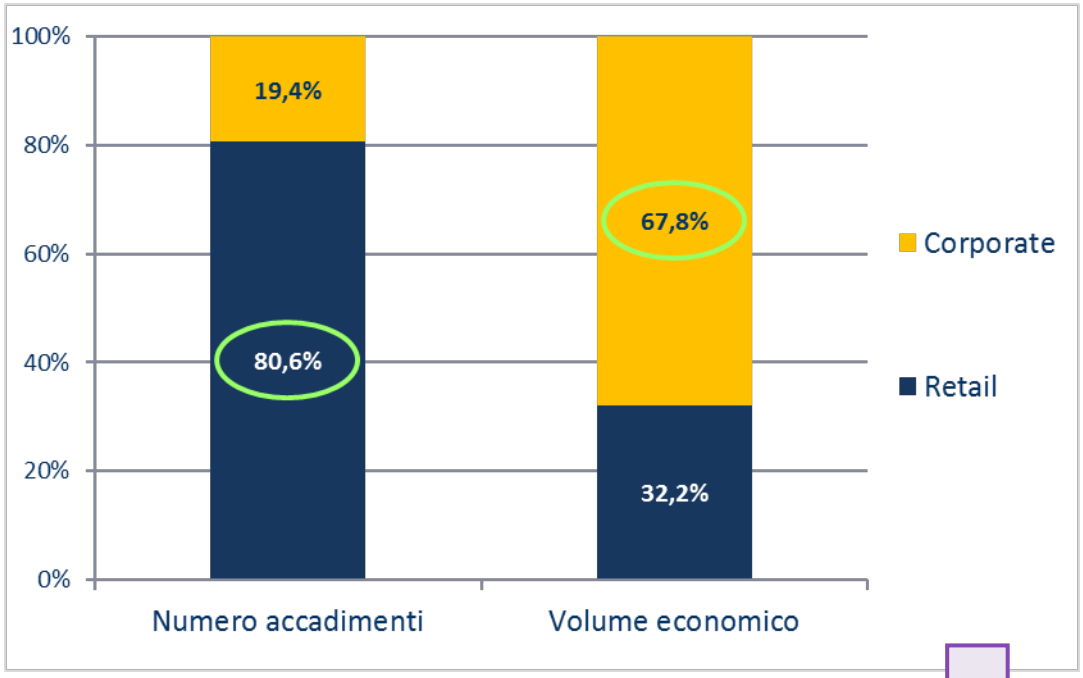
Ripartizione percentuale delle tipologie di transazioni anomale rilevate - volume economico



Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2016 (Campione: 30 rispondenti)

Scenario complessivo transazioni fraudolente
Analisi su tutta la clientela

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



- La clientela **Retail** risulta maggiormente **colpita,** con **rapporto di 4:1** in termini di **numero di accadimenti**
- In **media,** una **frode effettiva Corporate** ha un **volume 9 volte più elevato** rispetto a una **frode Retail**

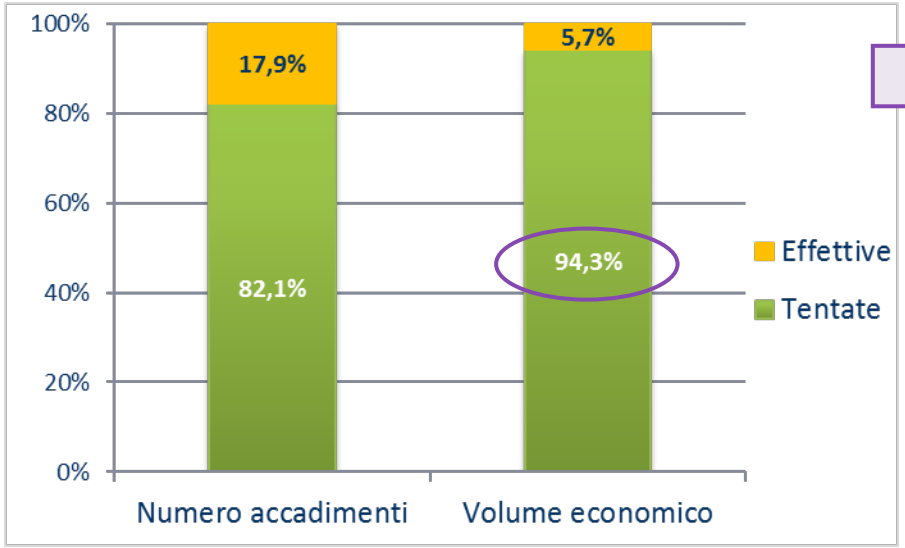
Si osserva una specializzazione dei meccanismi di attacco in base alla clientela e alla tipologia di servizio offerto

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2016 (Campione: 30 rispondenti)

Scenario complessivo transazioni anomale

2015

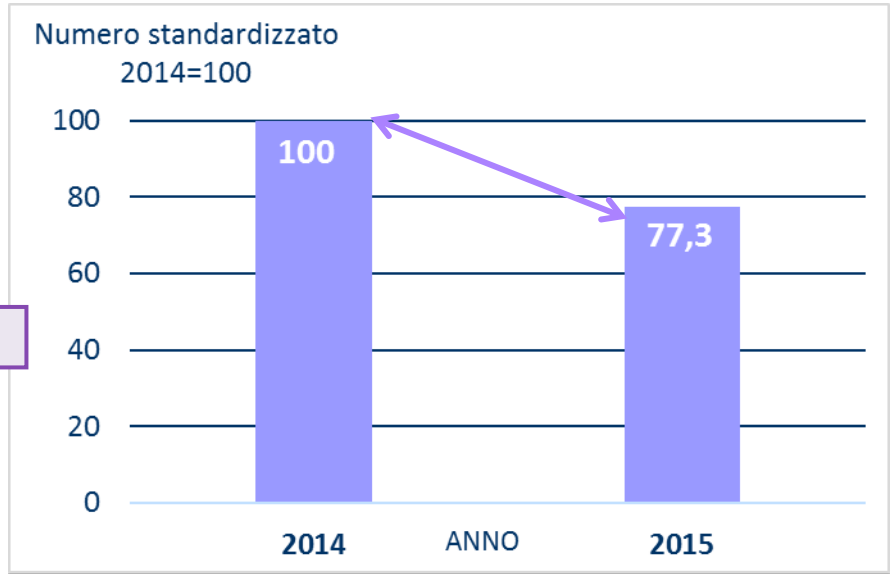
Transazioni anomale – ripartizione % per numero accadimenti e volume transato (Retail e Corporate)



Il **94,3% del volume economico transato è stato efficacemente bloccato**

Trend 2014-2015

Valore standardizzato transazioni anomale in danno a tutta la clientela (campione costante 20 rispondenti)*



Il **numero di transazioni anomale** nel **2015** è **diminuito del 22,7%** rispetto al **2014**

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2016 (Campione: 30 rispondenti)
*Per l'analisi è stato preso come riferimento il totale delle transazioni anomale del 2014 e posto uguale a 100.

Modalità di realizzazione dell'attacco
Confronto segmenti di clientela

È STRATEGICO conoscere i meccanismi di realizzazione di un attacco ed essere aggiornati sulle sue evoluzioni, per individuare le contromisure, cooperare con gli stakeholder interessati e sensibilizzare l'utente

Vettori di attacco e modalità di esecuzione della frode

SEGMENTO RETAIL

- Il **45,2%** del totale dei casi di furto di identità rilevati dalle banche è associato a di **phishing**
- Il **75,2%** delle transazioni è eseguito da una **sessione di log-in del frodatore** a seguito del furto di credenziali* → casi di **instant phishing**

SEGMENTO CORPORATE

- È il **crimeware** il vettore più utilizzato dai frodatori per realizzare un attacco (**91,7%**).
- Il **50%** degli **attacchi** è **eseguito** dalla **sessione** legittima dell'**utente****

Focus device mobili

SEGMENTO RETAIL

- I **device mobili** sono «puntati» dai cybercriminali quando vengono utilizzati dal cliente come secondo fattore per la ricezione dell'**OTP via SMS** dispositivi
- Il fenomeno è comunque **molto contenuto** ma si sta specializzando nelle diverse modalità realizzative: ***
  - → *SIM SWAP*: ha determinato lo **0,74%** delle **frodi effettive** di tutto il campione → *Trend in crescita nel 2016*
  - → *Social Engineering & Malware*: ha determinato lo **0,41%** delle **frodi effettive** su tutto il campione

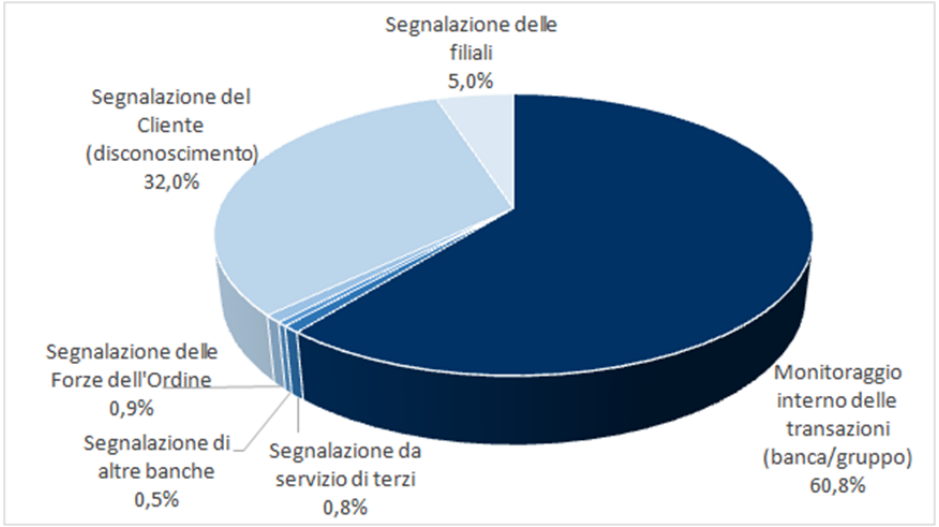
SEGMENTO CORPORATE: **nessun** tipo di **coinvolgimento** di **device mobili**.

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2016
(Campione complessivo: 30 rispondenti; *19 rispondenti; **14 rispondenti; ***20 rispondenti)

Segnalazione e gestione anomalie transazioni e rete

Provenienza della segnalazione

Rilevazione operazioni fraudolente – clientela Retail (andamento medio su 21 rispondenti)



- Gli **strumenti di monitoraggio interni** alla banca si rivelano particolarmente **efficaci** nell'**identificazione** delle **transazioni anomale** (**60,8%**), cui si affianca l'azione di **disconoscimento** da parte del **cliente** (**32%**)

Rilevazione e blocco dei siti clone

- Nel **2015** le banche hanno **oscurato 2025 siti clone***
- L'**87%** del campione** **contatta l'Internet Service Provider** per **bloccare** tempestivamente il **sito clone**

Attacchi DDoS

- Il **20,7%** del campione*** ha rilevato un attacco **DDoS → solo 1 attacco per ogni banca segnalante**
- **Contromisure adottate**: attivazioni di **filtri** e **re-indirizzamento** del **traffico web** in entrata, con modalità stabilite dai **presidi** della banca e/o contrattualizzati con il **carrier**

Il potenziamento dei presidi di cybersecurity di settore – anche in logica CERT – potrà rafforzare ulteriormente lo scambio di informazioni tra banche e con le Forze dell'Ordine

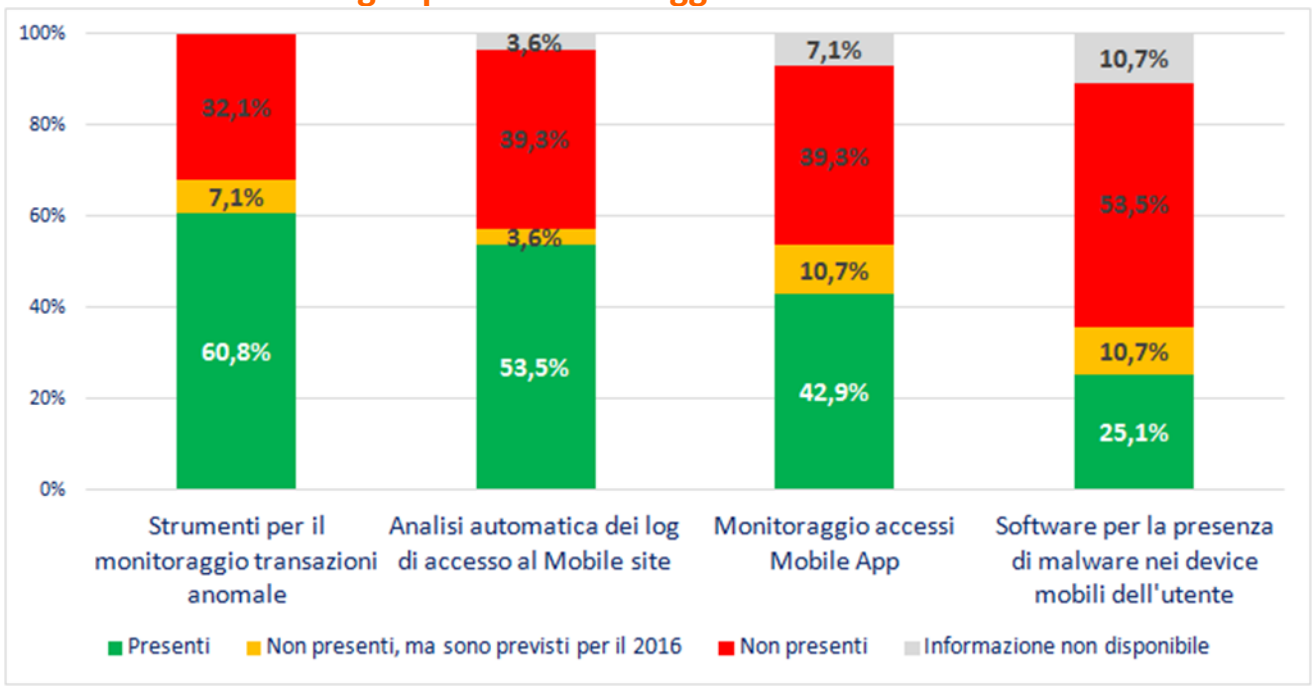
Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2016
(*22 rispondenti; **23 rispondenti; ***29 rispondenti)

La sicurezza sul canale Mobile

Necessità di bilanciare nel Mobile le esigenze di flessibilità e semplicità vs sicurezza → è sempre più importante RESPONSABILIZZARE il cliente rispetto all'uso del device e delle sue funzionalità

- **Non** si registrano per il **2015** casi di **frode** per **attacchi** legati a specifici servizi/piattaforme **Mobile Banking**
- **3 banche** hanno rilevato **App clonate** (non tutte le banche riescono a monitorare tale informazione)

Strumenti tecnologici per il monitoraggio e la rilevazione di attacchi*



Formazione interna specifica su sicurezza Mobile**

- **Effettuata** nel **2015** dal **32%** del campione
- **In previsione** per il **16%** delle banche

Contromisure tecnologiche***

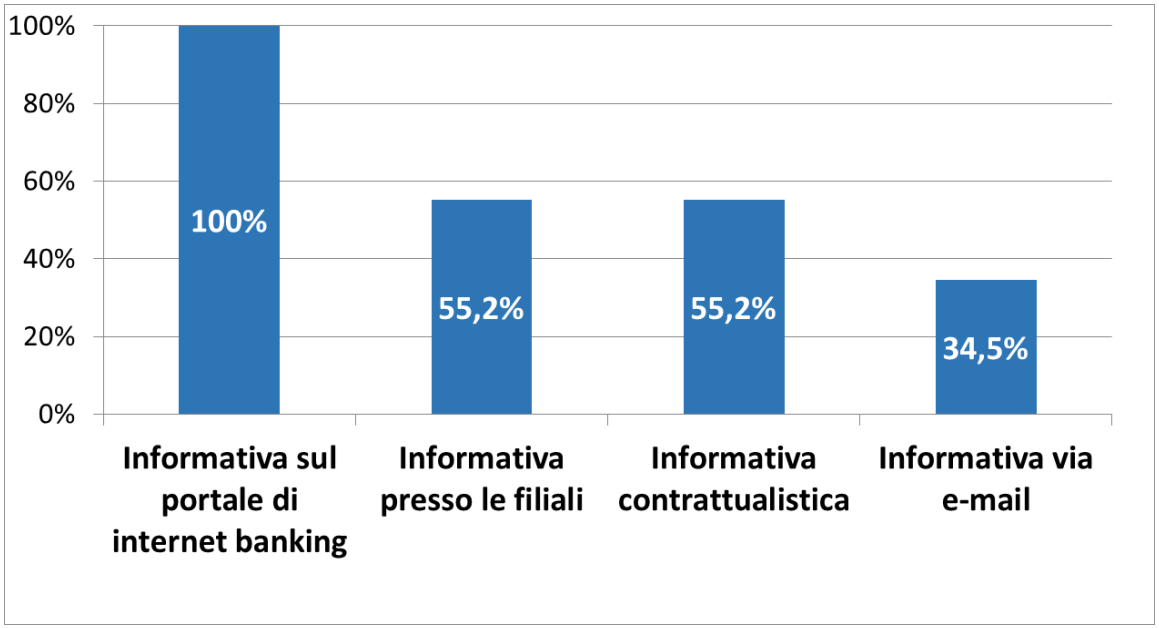
- La tecnologie di secondo fattore più diffuse sono l'**OTP via token** (**40%**), e l'**OTP via sms** (**30%**).

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2016
(Campione: *28 rispondenti; **25 rispondenti; ***30 rispondenti)

Le azioni di sensibilizzazione della clientela

Anche la soluzione tecnologica e la procedura di monitoraggio più evolute possono essere meno efficaci dinanzi a comportamenti negligenti o a una conoscenza non aggiornata dei rischi del cybercrime da parte dell'utente

Attività informativa verso la clientela Retail*



Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2016
(Campione : *29 rispondenti; ** 28 rispondenti)

- Anche a seguito dell'attenzione crescente del regolatore sul tema, **tutte** le **banche** intervistate svolgono attività di **informazione** e **awareness** sui rischi del cybercrime almeno sul proprio **portale di Internet Banking** (100%). Andamento analogo si registra per la clientela Corporate.
- Il **32,1%** del campione** **informa** il cliente rispetto ai rischi sul Mobile anche attraverso la propria **App**.

ABI Lab come national FI-ISAC per le banche sui temi di sicurezza e frodi informatiche

OSSERVATORIO SICUREZZA E FRODI INFORMATICHE

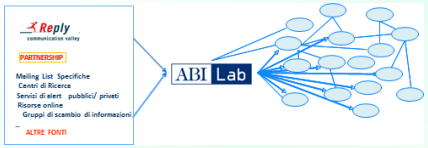
Presidio di settore sui temi di **sicurezza e frodi informatiche**, con un focus su **Internet e Mobile Banking,** attraverso:

- **Attività di Ricerca** ➔ **Survey e bollettini mensili**
  ➔ **Approfondimenti normativi e linee guida**
- **Collaborazioni istituzionali**
- **Workshop e attività di comunicazione**

Tavolo di lavoro composto da:
- *49 banche/outsourcer*
- *Partner ICT*

COMMUNITY PRESIDIO.INTERNET

Community gestita da **ABI Lab** dal 2009 per lo **scambio volontario** di **informazioni** tra **banche** e con la **Polizia Postale** su **frodi** e **attacchi informatici**, in ottica preventiva e di contrasto



Modus operandi:
- *1 to 1*
- *1 to many*
- *1 to all*

Community:
- *167 organizzazioni, 320 referenti*
- *Polizia Postale e delle Comunicazioni*
- *Operatori TLC*

ABI Lab
Tecnologia utile

COLLABORAZIONI INTERNAZIONALI

- **Cybersecurity WG** *(European Banking Federation)*
- **European FI-ISAC – Financial Institutions Information Sharing and Analysis Centre** *(ENISA)*
- **PSSG – *Payment Security Support Group*** (European Payments Council)
- **Advisory Board su financial services e partecipazione a iniziative specifiche per il settore**
- **Partecipazione a progetti di ricerca europei sulla cybersecurity**

Potenziamento collaborazioni istituzionali

Collaborazione con il CERT nazionale

A seguito dell'**accordo operativo** siglato con il **CERT Nazionale** nel **giugno 2015** è stato definito un **set di informazioni** inviate direttamente o per il tramite di ABI Lab alle banche:

- **Indicatori di Compromissione (IoC) relativi ad attacchi rilevati sul web**, relativi a diverse industry e non specifici per il contesto bancario;
- **Attacchi (o tentativi) a danno di singole banche,** rilevate da un sistema di monitoraggio europeo nel quadro del progetto ACDC (http://www.acdc-project.eu/) al quale il CERT Nazionale ha partecipato, e inviate direttamente alle banche
- **Segnalazioni risultanti dall'attività di monitoraggio delle reti Fast Flux:** rilevate nell'ambito del progetto Flux Buster (https://pralab.diee.unica.it/it/FluxBuster) sviluppato da PRA Lab – Università di Cagliari in collaborazione con il CERT Nazionale, che adotta un approccio ad apprendimento automatico per l'identificazione precisa di reti fast flux
- **Ulteriore materiale informativo** proveniente da **fonti esterne** e di supporto per il **settore**

Da settembre 2015 rilevate **141 segnalazioni** del CERT Nazionale, di cui:

- **53** ad **ABI Lab** – veicolate a **referenti** di sicurezza informatica
- **88** direttamente alle **singole banche** – inviate direttamente agli indirizzi di Presidio.Internet

Potenziamento collaborazioni istituzionali

Collaborazione con la Polizia Postale e delle Comunicazioni

In continuità con le azioni già in essere, è stata **rinnovata in data 3 giugno 2015 la convenzione ABI – Ministero dell'Interno** sui temi legati al cybercrime

ABI Lab e **Polizia Postale e delle Comunicazioni** continuano a collaborare **operativamente** e reciprocamente per:

- **Scambiarsi informazioni** su eventi o allarmi legati a minacce specifiche per il settore bancario
- **Informare** in merito a **studi, analisi aggregate e ricerche** in materia di frodi e attacchi informatici
- **Collaborare** a iniziative di **comunicazione**
- **Partecipare** congiuntamente a **progetti di ricerca** in materia di sicurezza informatica e prevenzione frodi

OF2CEN – (Online Fraud Cyber Center and Expert Network) per la definizione di una piattaforma di scambio informazioni tra banche italiane e Polizia Postale su frodi informatiche

Progetto concluso, piattaforma lanciata a fine 2013

EU OF2CEN – (EUropean Online Fraud Cyber Center and Expert Network), per la definizione di una piattaforma e di un modello di partnership tra banche e polizie europee per lo scambio di informazioni relative a frodi e attacchi informatici.

Progetto in corso, con il commitment di EBF ed Europol

In sintesi…

- Le **banche italiane** sono **consapevoli** dei **rischi** del **cybercrime** ed è per questo che **da tempo investono** nella **sicurezza** dei canali remoti e nella protezione dei propri asset IT, per essere pronte a **fronteggiare** e **minimizzare** l'impatto di nuove e possibili **minacce**
- Le **iniziative** in essere e previste hanno l'intento di raggiungere più obiettivi, tra cui:

DISPORRE DI ADEGUATE SOLUZIONI TECNOLOGICHE

→ **adattare soluzioni/strumenti** esistenti in **risposta e prevenzione** ai nuovi modelli di attacco

→ **garantire** la **protezione** degli **accessi** e dell'**identità** degli **utenti** e **monitorare** l'**operatività** online

EDUCARE IL CLIENTE

→ Fare ***awareness*** affinché il cliente sia sempre **aggiornato** e ricorra in maniera **diligente** e **responsabile** a tutti gli strumenti di **pagamento** e di sicurezza offerti dalla banca, in particolare quando usati da **remoto**

FARE INTELLIGENCE

→ **Non ci si può difendere senza conoscere il nemico e le sue mosse**

→ È importante raccogliere le informazioni provenienti da fonti interne/ esterne in maniera **evoluta**, **adattandole** al **contesto** e **modello** di **servizio**

COOPERARE

→ La **cybersecurity non può essere un ambito competitivo** ma deve essere basato sulla **collaborazione** e sullo **scambio tempestivo di informazioni** fra tutti

→ **Più un intero sistema è forte e ben protetto, meno è attraente per i cybercriminali**

Milano, 26 maggio 2016

ABI Lab
Tecnologia utile

GRAZIE PER L'ATTENZIONE

presidio.internet@abilab.it