ABI Lab
Tecnologia utile

Servizi di pagamento nel mercato interno: PSD2 e altri aspetti normativi

Monica Pellegrino, *Research Analyst*, **ABI Lab**

Napoli, 11 Giugno 2013

Il contesto di riferimento

- Continua **evoluzione e sofisticazione delle minacce** e degli attacchi verso i servizi di **Internet e Mobile Banking**, **di pari passo con l'innovazione delle tecnologie** e delle modalità offerte alla clientela per accedere ai prodotti bancari, soprattutto da remoto.
- Crescente **attenzione** da parte delle **istituzioni** di riferimento a livello **nazionale** ed **europeo** in merito ai **rischi informatici** e all'esigenza di garantire **elevati livelli di sicurezza** nella realizzazione di **pagamenti da remoto** e nella **gestione dei dati**, come testimoniato dal recente fermento normativo in materia.

- Le principali evoluzioni normative con impatti sulla gestione della sicurezza e del rischio informatico in banca investono principalmente gli ambiti di:
  - **Sicurezza degli accessi e dei servizi di pagamento**
    - *Payment Service Directive e recepimento a livello nazionale*
    - *Raccomandazioni BCE sulla sicurezza dei pagamenti internet*
    - *Raccomandazioni BCE sulla sicurezza dei servizi di accesso ai conti di pagamento*
  - **Sicurezza nel trattamento di dati e informazioni bancarie**
    - *Provvedimento Autorità Garante per la Privacy per la circolazione delle informazioni bancarie e il trattamento dei dati bancari*
  - **Valutazione del rischio informatico e correlazione con la gestione del rischio operativo**
    - *Disposizioni di vigilanza prudenziale di Banca d'Italia in materia di sistema dei controlli interni, sistema informativo e continuità operativa*

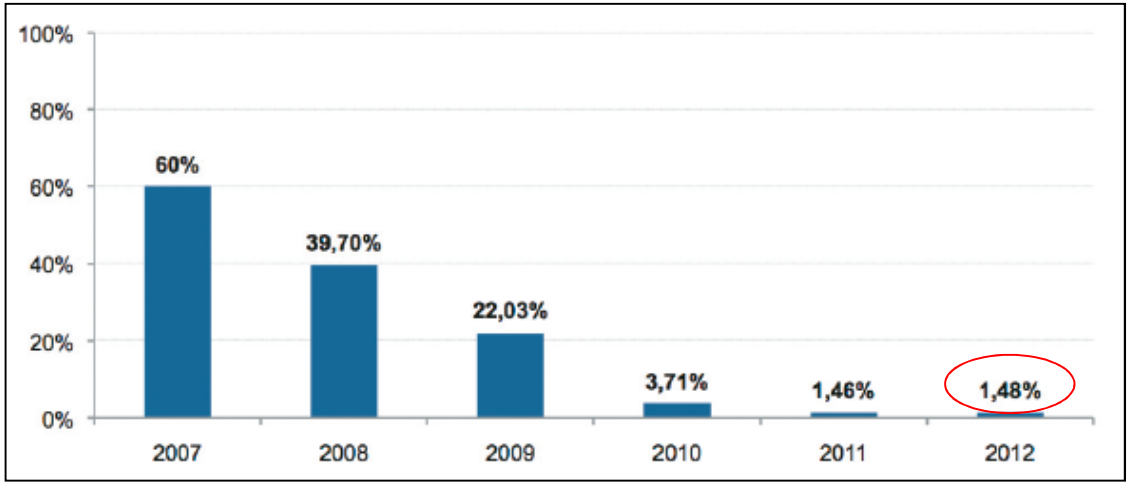
- Tali evoluzioni potranno integrarsi negli **obiettivi più ampi di protezione cibernetica e sicurezza informatica nazionale**, definiti a livello di Sistema **Paese** nell'ambito del **DPCM 23 gennaio 2013**

ABI Lab
Tecnologia utile

Lo scenario delle frodi informatiche via internet nelle banche italiane

Il fenomeno delle frodi informatiche
Perdita di denaro vs perdita di credenziali

Percentuale di clienti che perde denaro a seguito della perdita di credenziali (segmento Retail)

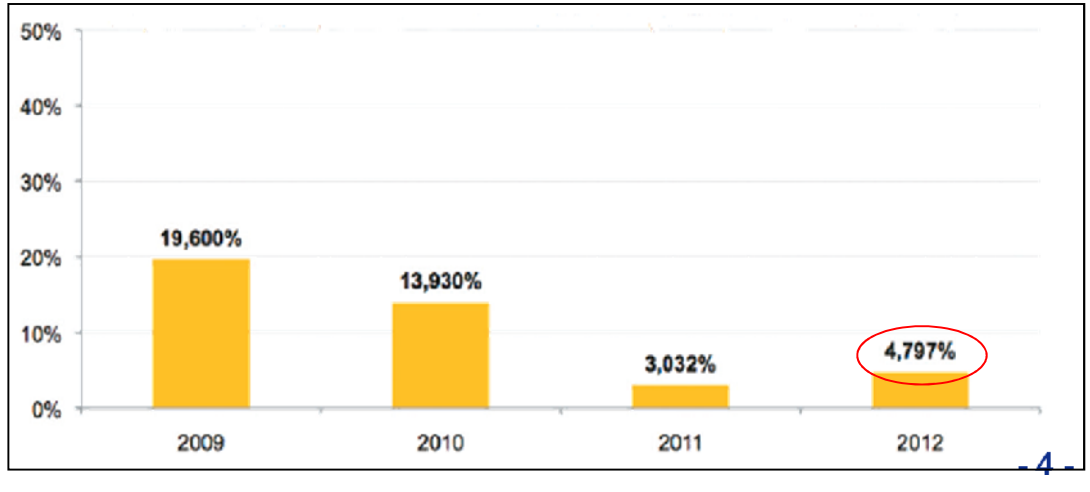


- Nel 2012, a fronte di un notevole incremento degli episodi di furto di identità, l'**efficacia delle azioni di contrasto delle banche** rimane **molto elevata**, consentendo di **interrompere** il **98,5% dei tentativi di frode**.

- La percentuale di **clienti** Corporate cha subito un **danno economico a seguito del furto di credenziali** sale al **4,79%**.

- Tali risultati spingono dunque le banche a ulteriori riflessioni su come potenziare sia le **attività** già avviate di **sensibilizzazione** e **formazione** verso tale clientela.

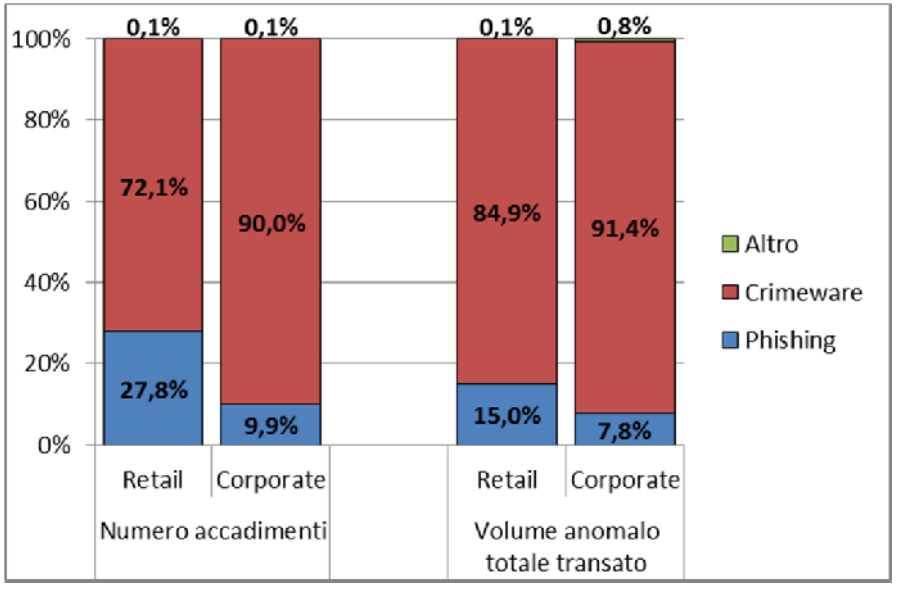
Percentuale di clienti che perde denaro a seguito della perdita di credenziali (segmento Corporate)



Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2013, 29 rispondenti

Modalità di realizzazione dell'attacco
Confronto segmenti di clientela (1/2)

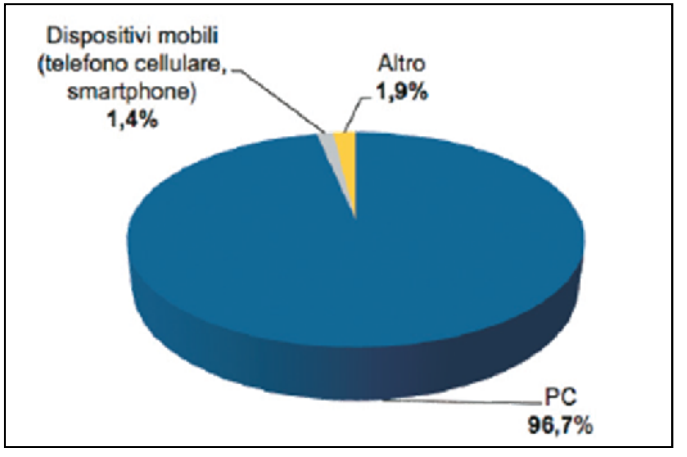
Numero di accadimenti e volume transato per tipologia di attacco



- In linea con quanto già rilevato nel 2011, il **crimeware** si rivela la tipologia di attacco più **efficace** per **entrambi i segmenti di clientela**, sia in termini di **numero di accadimenti** (**72,1%** per il **Retail**, **90%** per il **Corporate**), che di **volume transato** (**84,9%** per il **Retail**, **91,4%** per il **Corporate**).

- Il **PC dell'utente** continua a essere il dispositivo **principalmente compromesso** dai frodatori per il furto di credenziali (sia ambito **Retail** che **Corporate**).
- Con riferimento al solo segmento di **clientela Retail**, per la prima volta nel **2012** si sono registrati eventi di **compromissione di device mobili** (**1,4%**) per realizzare frodi via **Internet Banking,** nella maggior parte dei casi finalizzati a **intercettare in maniera illecita SMS** contenenti i **codici OTP** inviati dalle banche per autorizzare le operazioni di Internet Banking.

Device compromesso per l'attuazione della frode (segmento Retail)

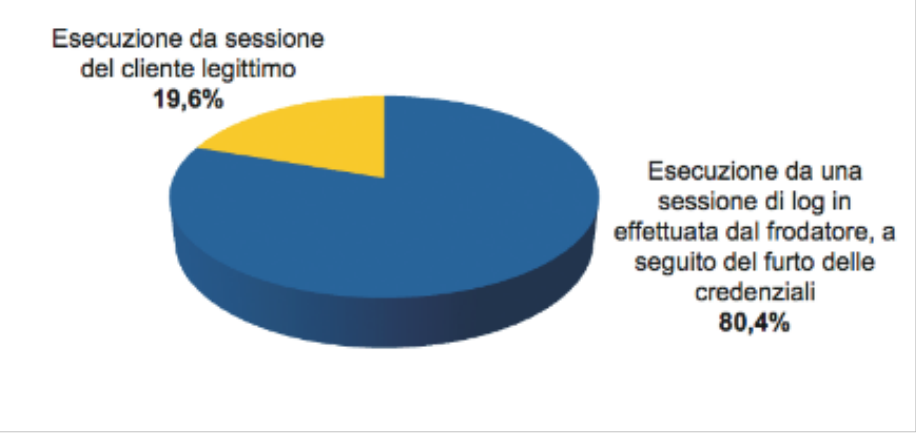


Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2013, 29 rispondenti

Modalità di realizzazione dell'attacco
Confronto segmenti di clientela (2/2)

ABI Lab
Tecnologia utile

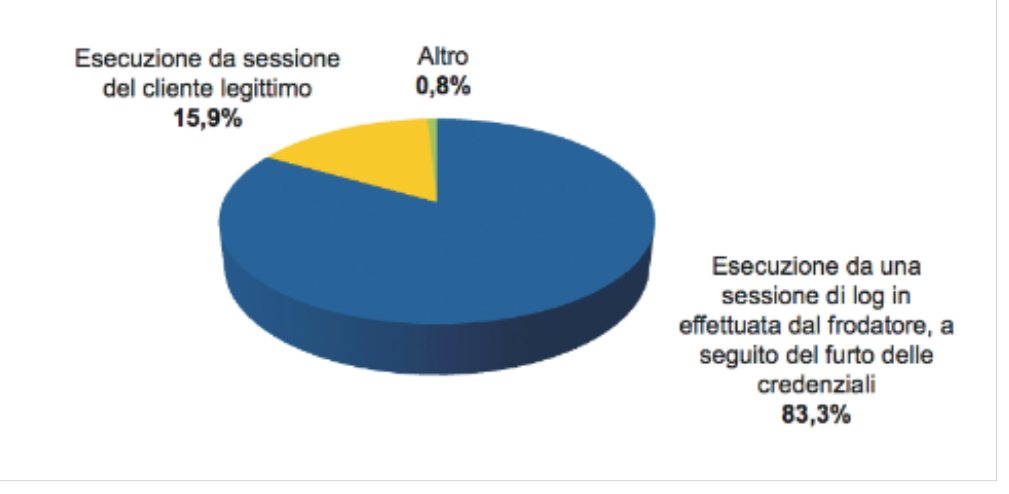
Modalità di esecuzione della frode (segmento Retail)*



- L'**esecuzione della frode** verso la clientela viene realizzata **principalmente** durante una **sessione di login** effettuata direttamente dal frodatore a **seguito di furto di credenziali** (80,4% per il Retail e 83,3% per il Corporate)
- **Non** è **trascurabile**, tuttavia, la percentuale di casi in cui il **frodatore è riuscito a portare a termine un trasferimento di denaro illecito disponendo la transazione da una sessione del cliente legittimo** (19,6% per il Retail e 15,9% per il Corporate)

- Quest'ultima modalità, **molto più complessa da rilevare (anche in fase istruttoria)**, fa leva spesso sulle **vulnerabilità dei device** che in alcuni casi presentano una protezione limitata o addirittura assente.
- Di conseguenza, diviene **strategico** puntare l'attenzione alla **protezione del device e della connessione utente e rendere i clienti sempre più consapevoli** dei rischi del cybercrime e dell'importanza di predisporre adeguati presidi di sicurezza.

Modalità di esecuzione della frode (segmento Corporate)*

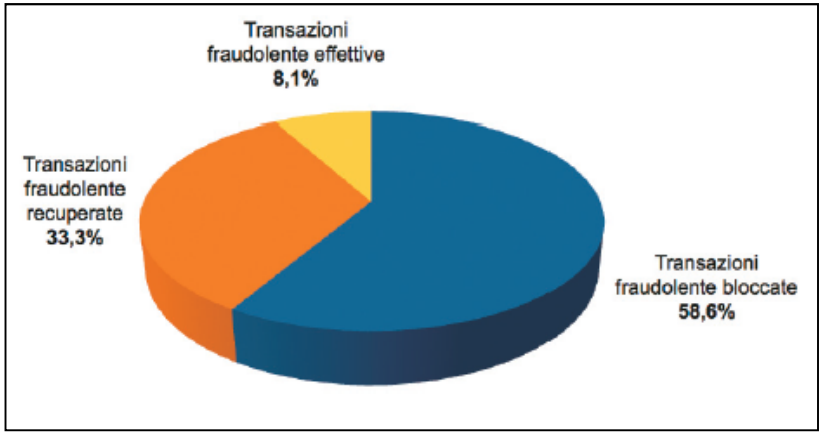


* Andamento medio su un campione di 16 (Retail) e 12 (Corporate) rispondenti

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2013, 29 rispondenti

Numero di eventi e volumi economici
Ambito Retail

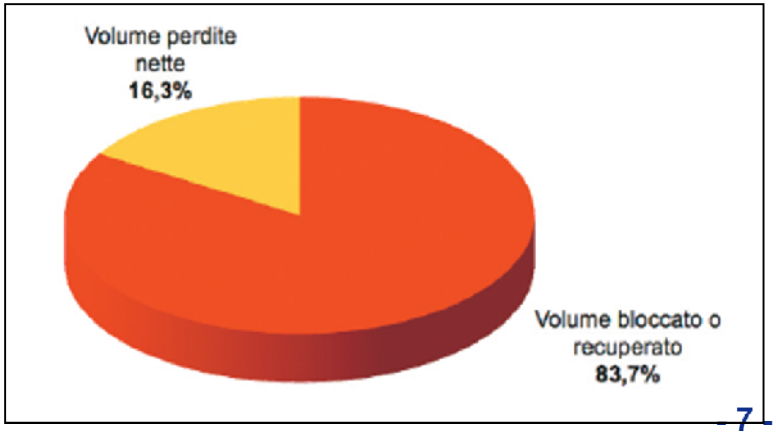
Ripartizione percentuale delle tipologie di transazioni anomale rilevate – numero accadimenti



- In relazione al **volume economico** associato al totale delle operazioni fraudolente, l'**83,7%** risulta essere relativo **alle operazioni bloccate o recuperate**: più in dettaglio, il **57,4%** è stato **bloccato** e il **26,3%** è stato **recuperato**.

- Rispetto alla stima **totale delle transazioni** (**bonifici, ricariche**) **effettuate** via Internet Banking dal campione, solo lo **0,0008%** degli accadimenti (**pari a 1 su 125.000**) ha costituito una **frode effettiva**.

Ripartizione percentuale delle tipologie di transazioni anomale rilevate – volume transato



Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2013, 29 rispondenti

ABI Lab
Tecnologia utile

Sicurezza degli accessi e dei servizi di pagamento

Raccomandazioni BCE in materia di sicurezza dei pagamenti Internet (1/2)

ABI Lab
Tecnologia utile

IL PROCESSO DI EMANAZIONE E LE ATTIVITÀ ABI e ABI Lab

Aprile 2012 — Pubblicazione del documento in consultazione da parte della BCE

- Raccolta dei feedback inviati dalle banche

Maggio 2012 — Termine stabilito da ABI verso le banche la presentazione di osservazioni, commenti e proposte

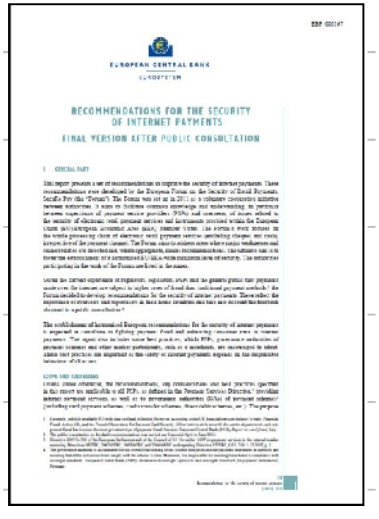
- Stesura del Position Paper ABI

Giugno 2012 — Invio del Position Paper alla BCE

- Analisi dei commenti ricevuti da parte della BCE

59 rispondenti di 17 stati Europei, comprese anche Autorità e Associazioni nazionali e internazionali

Gennaio 2013 — Pubblicazione della versione finale delle raccomandazioni BCE sui pagamenti internet


EUROPEAN CENTRAL BANK

RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

FINAL VERSION AFTER PUBLIC CONSULTATION

Raccomandazioni BCE in materia di sicurezza dei pagamenti Internet (2/2)

ABI Lab
Tecnologia utile

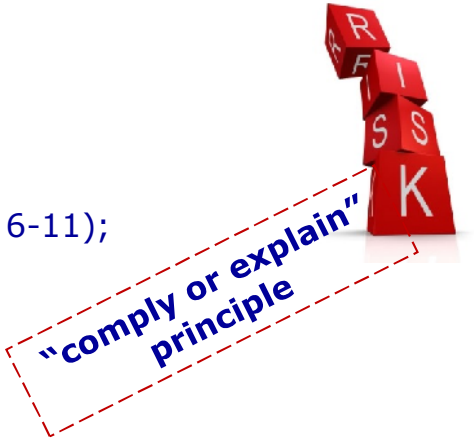
OBIETTIVO GENERALE

- Definire i **requisiti minimi** indirizzati a PSP*, **Autorità di governo** di schemi e sistemi di pagamento ed **e-merchant,** da applicare nell'erogazione di pagamenti tramite cards, credit transfers, e-mandate ed e-money

STRUTTURA del DOCUMENTO

- Le ***14 Recommendations*** rimangono **organizzate in 3 categorie:**
  - Controlli generali (Racc. 1-5);
  - Controlli specifici e misure di sicurezza per i pagamenti internet (Racc. 6-11);
  - Comunicazione con la clientela e customer awareness (Racc. 12-14);

  composte da *Key Considerations* e *Best Practices.*



TEMPI DI IMPLEMENTAZIONE

- A livello nazionale, **le raccomandazioni saranno recepite da Banca d'Italia e inserite nelle Nuove Disposizioni di Vigilanza Prudenziale**.
- La scadenza per il recepimento è prevista per il **1 febbraio 2015**

IMPATTI PER LE BANCHE

- Secondo quanto previsto dai principi guida fondanti le raccomandazioni, sono previste le seguenti attività:
  - Realizzazione di un **assessment specifico** dei **rischi** connessi all'offerta dei servizi di pagamento online (fornite indicazioni di carattere organizzativo e operativo);
  - Introduzione di strumenti di **strong authentication** in fase di accesso ai servizi on line;
  - Implementazione di **procedure efficaci** in merito all'autorizzazione e monitoraggio delle transazioni per identificare comportamenti anomali e prevenire le frodi;
  - Promozione di **iniziative di sensibilizzazione** della **clientela**.

* Banche, istituti di pagamento, istituti di moneta elettronica, Poste e tramite apposite clausole contrattuali anche agli outsorcer coinvolti

Raccomandazioni BCE in materia di sicurezza dei pagamenti Internet

ABI Lab
Tecnologia utile

FOCUS – LA DEFINIZIONE di STRONG AUTHENTICATION

"Second, as a general principle, ***the initiation of internet payments as well as access to sensitive payment data should be protected by strong customer authentication****. For the purpose of this report,* ***sensitive payment data are defined as data which could be used to carry out fraud****. […]*

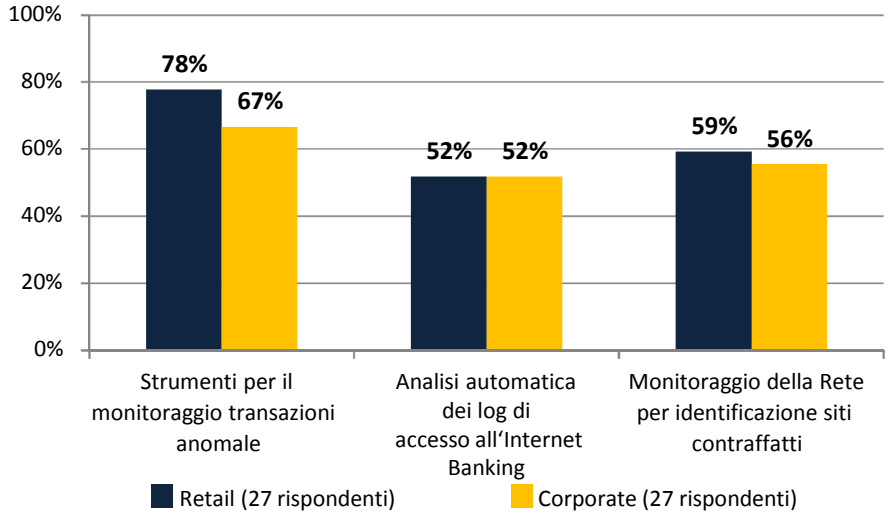
Strong customer authentication *is a* ***procedure based on the use of two or more of the following elements*** *– categorised as knowledge, ownership and inherence:* ***i) something only the user knows****, e.g. static password, code, personal identification number****; ii) something only the user possesses****, e.g. token, smart card, mobile phone;* ***iii) something the user is****, e.g. biometric characteristic, such as a fingerprint. In addition,* ***the elements selected must be mutually independent****, i.e. the breach of one does not compromise the other(s).* ***At least one of the elements should be non-reusable and non-replicable*** *(except for inherence), and not capable of being surreptitiously stolen via the internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data"*

- Uno degli elementi su cui è necessario puntare l'attenzione riguarda la **definizione** adottata di "***strong authentication***" che include anche i requisiti di ***non-reusabilità*** **e** ***non replicabilità*** di almeno uno dei mezzi utilizzati.

- Nella KC 7.1, sono stati al contempo elencati **esplicitamente** i casi in cui i **PSP** possono adottare **misure alternative di autenticazione** della clientela:
  - **pagamenti verso beneficiari sicuri, precedentemente inseriti in apposite white list;**
  - **transazioni tra due account dello stesso cliente presso lo stesso PSP;**
  - **trasferimenti all'interno dello stesso PSP giustificati dalla risk analysis;**
  - **pagamenti di importi ridotti, come previsto nella PSD**.

Lo scenario italiano
Strumenti di monitoraggio e sensibilizzazione clientela

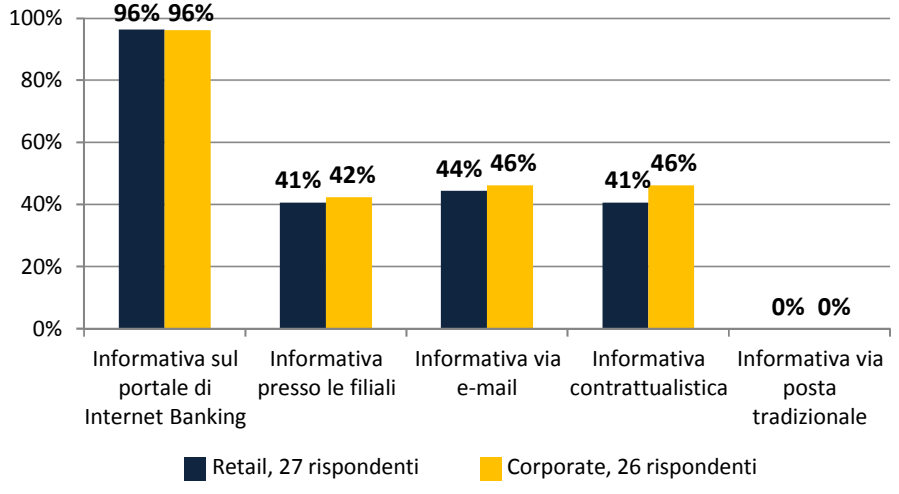
Attività di monitoraggio e dotazione tecnologica



- In linea con quanto già previsto dalle raccomandazioni, sono estremamente **diffuse** presso le banche **attività di carattere informativo** verso la clientela, comunicate principalmente sul **portale Internet Banking** della banca (**96%**) o, in alternativa, via e-mail o riportate nel contratto.
- Nelle **campagne** di informazione e sensibilizzazione sono di solito rappresentati i **rischi** e le **principali minacce** informatiche e viene data **evidenza** degli **strumenti** messi a **disposizione** dalle banche, insieme con una serie di regole e **comportamenti** per l'utente utili a **proteggere i dati** da eventuali attacchi.

- Un **numero sempre maggiore** di **banche** si sta dotando di **strumenti** in grado di **monitorare** costantemente gli accessi all'Internet Banking e di svolgere un **presidio** continuativo della **rete** e delle **operazioni** effettuate dalla clientela, sia **Retail** che **Corporate**.
- In deciso **aumento** anche le banche che partecipano direttamente a **community di information sharing** e a iniziative associative per la **collaborazione intersettoriale**, e che ricorrono a servizi di **segnalazione** ed **early warning** offerto da società esterne.

Attività informativa verso la clientela



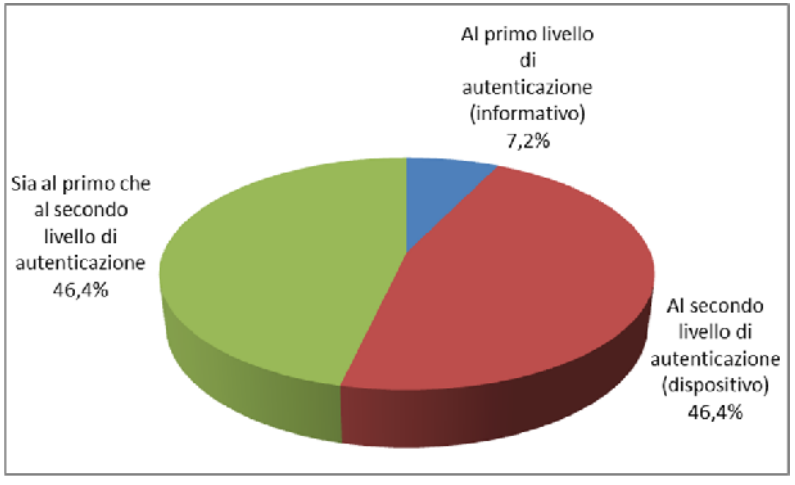
Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2013, 29 rispondenti

Lo scenario italiano
Contromisure tecnologiche

ABI Lab
Tecnologia utile

Segmento Retail

II fattore di autenticazione*

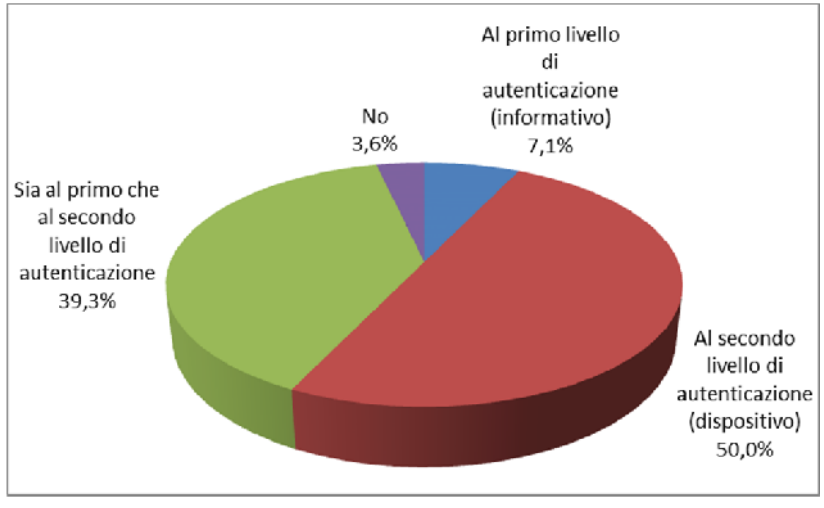


- **Tutte** le banche intervistate ricorrono a un **doppio livello di autenticazione**.
- **Tutte** le banche mettono a disposizione **almeno una tecnologia di II fattore:**
  - l'uso è **obbligatorio per tutti i clienti** nel **67,9%** delle banche
  - Tra le tecnologie più diffuse, vi sono l'**OTP via hardware disconnesso** (**57,1%**), la **tessera a combinazione** (**35,7%**) e **l'OTP via SMS** (**28,6%**)
- Il **64,3%** delle banche ha messo a disposizione della clientela un **II canale di comunicazione** per **notificare** le operazioni disposte via Internet Banking

Segmento Corporate

- **Tutte** le banche intervistate ricorrono a un **doppio livello di autenticazione**.
- Il **96,4%** delle banche mette a disposizione **almeno una tecnologia di II fattore:**
  - l'uso è **obbligatorio per tutti i clienti** nel **59,3%** delle banche
  - Tra le tecnologie più diffuse, vi sono l'**OTP via hardware disconnesso** (**55,6%**), il **certificato digitale** (**33,3%**) e la **tessera a combinazione** (**29,6%**)
- Il **50%** delle banche ha messo a disposizione della clientela un **II canale di comunicazione** per **notificare** le operazioni disposte via Internet Banking

II fattore di autenticazione*



* 28 rispondenti

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2013, 29 rispondenti

Nuove modalità di identificazione cliente
Il progetto STORK 2.0

- Tra le nuove opportunità di **identificazione** si inseriscono le potenzialità di innovazione che emergeranno dal **Progetto Europeo STORK 2.0,** cui partecipa anche **ABI Lab,** finalizzato a:
  - garantire l'**interoperabilità** a livello EU dei sistemi d'identità elettronica nazionali
  - permettere a imprese e cittadini di utilizzare la propria **eID nazionale** in qualsiasi Stato membro e in diversi contesti, tra cui l'ambito **bancario**.

PILOT BANCARIO

Use case 1: Apertura da remoto e cross-border di un nuovo conto corrente

- Obiettivo: consentire a **cittadini/imprese di una Nazione A** di **aprire** da **remoto online** un **conto corrente bancario** in una **Nazione B** differente.

Use case 2: Accesso da remoto e cross-border all'Internet Banking

- Obiettivo: consentire a **cittadini/imprese dei MS** partecipanti di utilizzare la propria identità elettronica per accedere alla piattaforma di **Internet Banking** di una **banca di un altro Paese,** a fini **informativi** e **dispositivi**. Tra le attività in programma nel pilota, è prevista la sperimentazione dell'autorizzazione del **pagamento delle fatture** (**e-invoicing**).

Si ritiene che gli **esiti dei pilota** definiti nel progetto **STORK 2.0** possano ulteriormente **sensibilizzare** le **Istituzioni** dei singoli stati membri nei riguardi dell'**uso integrato e cross settoriale dell'identità elettronica**

Ulteriori osservazioni BCE a seguito della consultazione

ABI Lab
Tecnologia utile

NEUTRALITÀ RISPETTO ALLE TECNOLOGIE

- Le raccomandazioni sono state formulate secondo principi di **neutralità rispetto a specifiche tecnologie**, in modo che siano indipendenti rispetto all'evoluzione tecnologica e al costante incremento dell'offerta di prodotti e servizi relativi ai pagamenti Internet.
- Rispetto alla versione in consultazione, sono state **eliminate le appendici con i riferimenti e i dettagli tecnologici**.

IL TRADE OFF TRA SICUREZZA E CONVENIENZA PER L'UTENTE

- Le raccomandazioni rappresentano dei **requisiti minimi** da seguire. Rimane valido il principio di ***comply or explain*** in fase di adozione da parte delle singole realtà.

RIFERIMENTO A STANDARD ESISTENTI

- Il Forum ha deliberatamente scelto di non **suggerire né richiamare specifici standard**, come invece era stato fatto nella versione in consultazione. Gli aspetti tecnici dovranno essere valutati e scelti da ogni PSP.

Raccomandazioni BCE sulla sicurezza dei servizi di accesso ai conti di pagamento (1/2)

La Banca Centrale Europea ha pubblicato il 31 gennaio u.s. in **consultazione** un documento di **raccomandazioni** relativo ai **servizi di accesso ai conti di pagamento**

OBIETTIVO GENERALE

- Definire i **requisiti minimi** principali che **soggetti terzi** (TP) **non regolamentati** devono rispettare quando utilizzano **servizi di accesso all'informazione sui conti di pagamento**, nell'ottica di contrastare e prevenire le frodi e aumentare la fiducia dei consumatori nell'utilizzo di tali servizi

FINALITÀ

- Far adottare a **TP misure di sicurezza** e di **controllo** simili a quelle richieste ai PSP nelle raccomandazioni sulla sicurezza dei pagamenti internet
- Aumentare la **trasparenza** e la **consapevolezza** dell'**utente** in fase di accesso ai servizi forniti da TP
- Assicurare la **tracciabilità** mediante opportuna **autenticazione** in tutte le comunicazioni tra le diverse entità coinvolte (TP, PSP, e-merchant e proprietario del conto)
- Favorire lo **scambio di informazioni** in caso di ripudio, incidenti di sicurezza e casi di frode
- Assicurare la **gestione** del **numero minimo di dati necessario** per l'erogazione del servizio
- Promuovere la **contrattualizzazione** dei rapporti tra TP ed e-merchants

TEMPI di IMPLEMENTAZIONE

- I tempi previsti per l'adeguamento **non** sono stati **ancora stabiliti** ma dipenderanno dalle problematiche e dalle esigenze emerse in fase di consultazione

Raccomandazioni BCE sulla sicurezza dei servizi di accesso ai conti di pagamento (2/2)

PRINCIPI GUIDA

- I 4 principi fondamentali delle raccomandazioni cui devono attenersi i destinatari prevedono:
  - Realizzazione di un **assessment** specifico dei **rischi**
  - Ricorso a strumenti di **strong authentication in fase di accesso** ai servizi
  - Implementazione di procedure efficaci in merito all'**autorizzazione e monitoraggio delle transazioni** per identificare comportamenti anomali e prevenire le frodi
  - Promozione di **iniziative di sensibilizzazione** della clientela

Si applica il principio di "comply or explain"

STRUTTURA DEL DOCUMENTO

- Il documento contiene **14 raccomandazioni**, distinte in 3 categorie
  - **General Control and Security Environment**
  - **Specific Control and Security Measures for Payment Account Access Services**
  - **Customer Awareness, Education and Communication**
- Ogni raccomandazione è specificata nel dettaglio attraverso Key Consideration (**KC**) e Best Practice (**BP**)
- La **struttura** e il **contenuto** delle raccomandazioni è simile al **documento di raccomandazioni** sulla sicurezza dei pagamenti internet