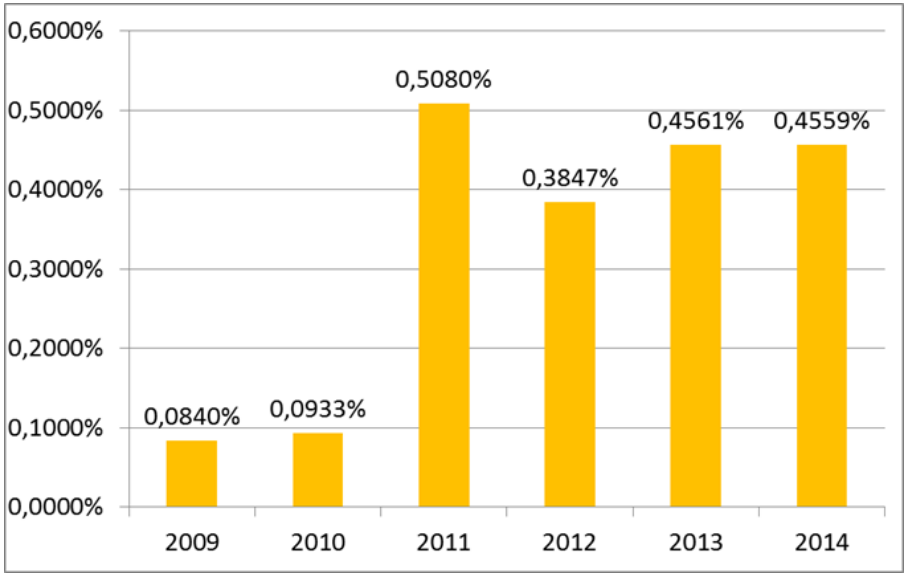
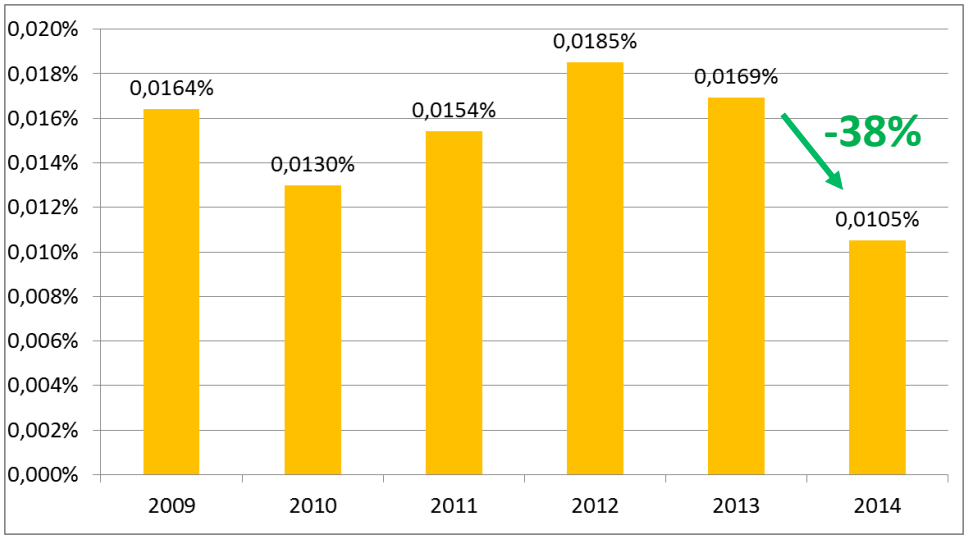
Il fenomeno delle frodi informatiche
Furto di credenziali e danno economico – ambito Corporate

- **Utilizzo diffuso dei servizi di Internet Banking: 1,2 miliardi** di **accessi** nel **2014** da parte di tutta la clientela.
- **Elevato indice di rischio** associato al segmento **Corporate** rispetto agli attacchi informatici: la **percentuale** di clienti vittima di **furto di credenziali** nel 2014 **in linea con il 2013.**

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



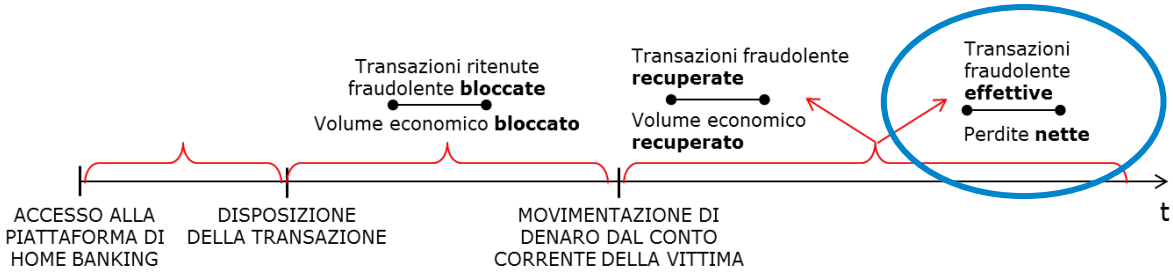
Percentuale di clienti attivi Corporate che hanno perso denaro - trend 2009-2014 (campione variabile)



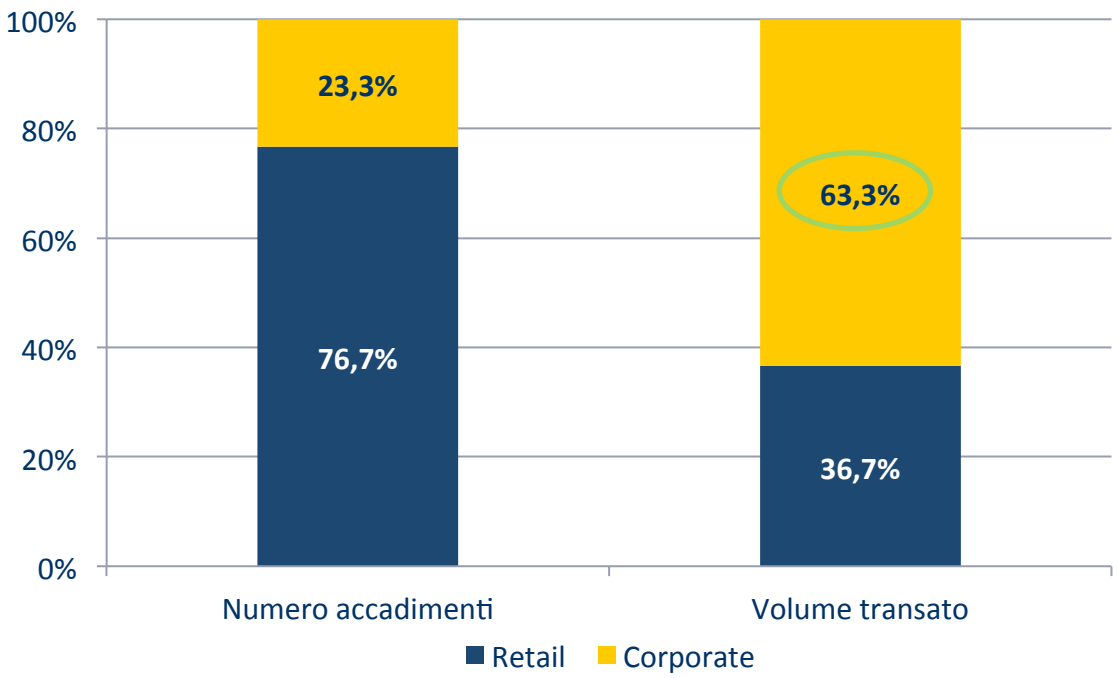
- **Diminuzione** quasi del **38%** rispetto al 2013 dei **clienti** che a fronte del furto di identità hanno subito un **danno economico**.
- In rapporto al **totale degli accessi** all'Internet Banking, la percentuale di **clienti che ha subito un danno economico** è pari allo **0,00009%.**

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

Scenario complessivo transazioni fraudolente
Confronto segmenti di clientela



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

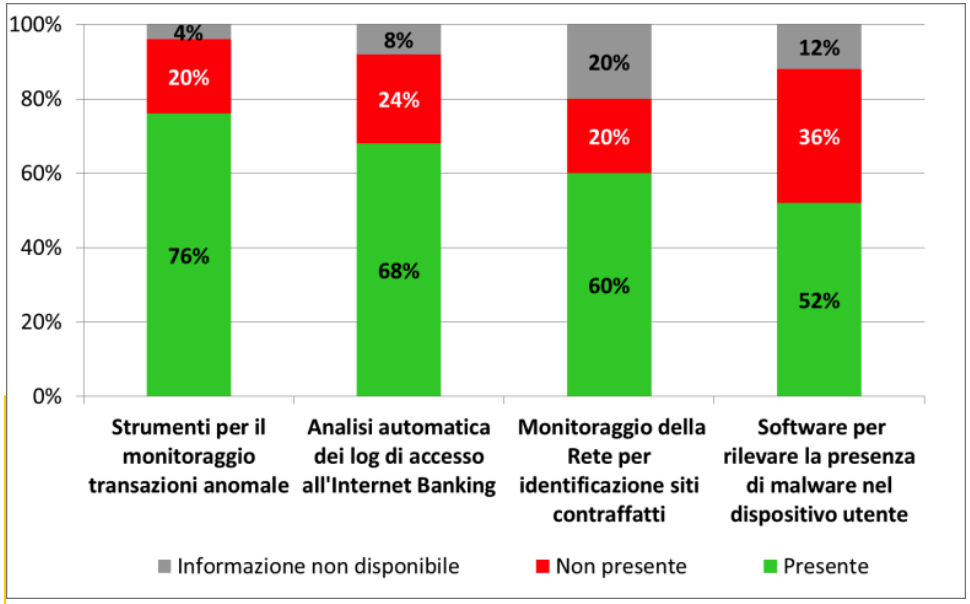


- La clientela **Retail** risulta maggiormente **colpita** (**76,7%**), rispetto al comparto imprese (23,3%).
- Il rapporto si inverte se si prende come riferimento il **volume economico** associato alle perdite, che è pari al **63,3%** per il segmento **Corporate.**
- In **media,** una **frode effettiva 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)

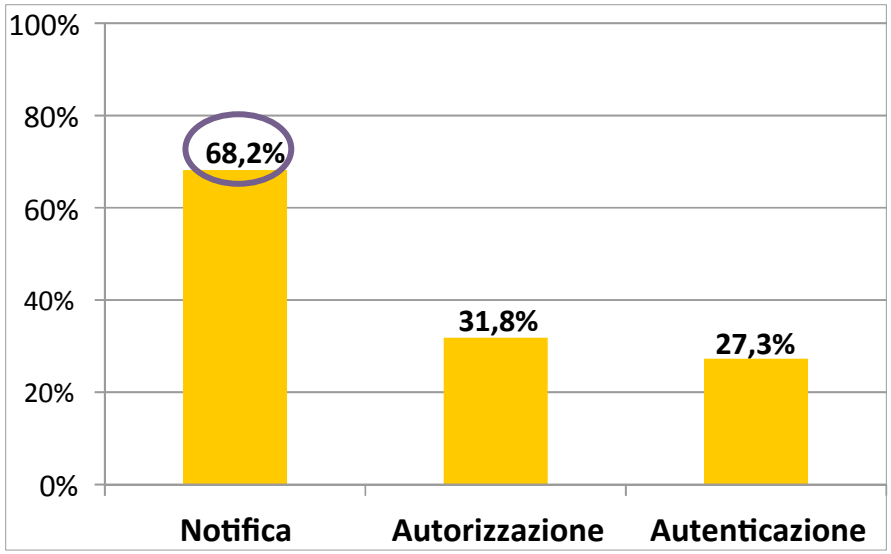
Strumenti di monitoraggio e secondo canale di comunicazione con la clientela

Attività di monitoraggio e dotazione tecnologica*



- Buona diffusione di **strumenti in grado individuare anomalie** nelle transazioni disposte dalla clientela (76%).
- L'**attenzione** del **settore bancario** sul contrasto al fenomeno delle **frodi informatiche** è **in linea** con le recenti previsioni **normative** a livello europeo (Raccomandazioni BCE e linee guida EBA).

Utilizzo di un canale alternativo di comunicazione – clientela Corporate**

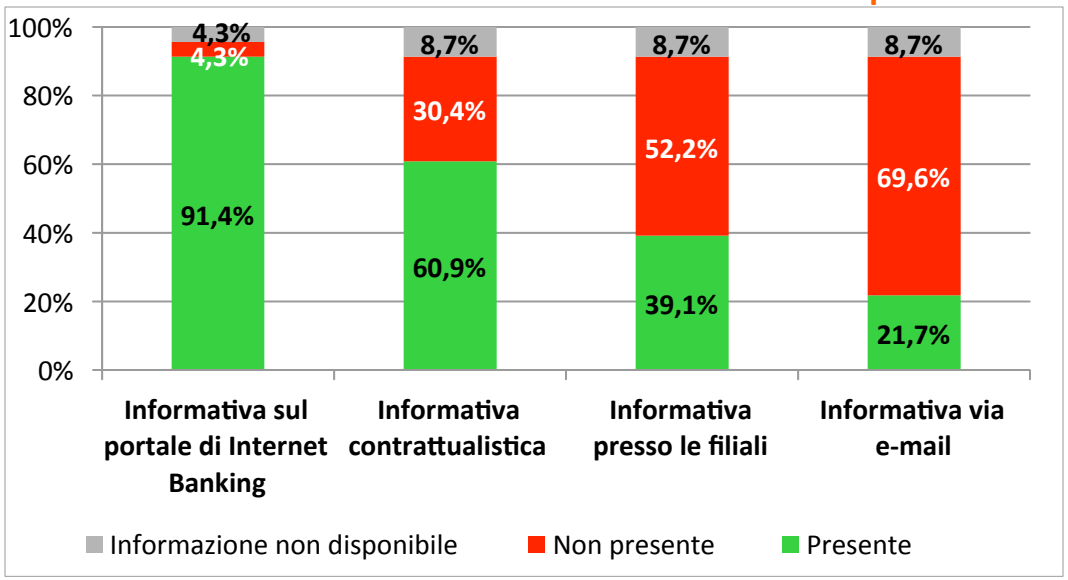


- Particolare **importanza** viene riconosciuta al **canale alternativo di comunicazione** in fase di **notifica** delle operazioni (68,2%).
- Le percentuali mediamente inferiori rispetto al comparto Retail sono dovute anche alla **maggiore complessità organizzativa** tipica delle aziende.

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2015
(Campione: 25 rispondenti; **Campione: 24 rispondenti)

Le azioni di sensibilizzazione verso la clientela Corporate

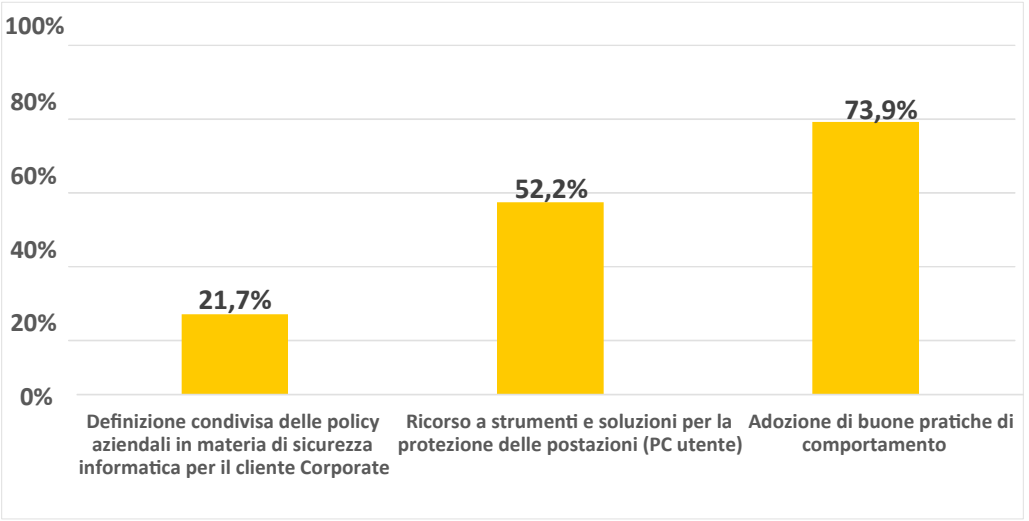
Attività informativa verso la clientela – clientela Corporate



- L'attività **informativa** è svolta in particolare attraverso il **portale** di Internet Banking (91,4%).
- Anche l'**importanza** delle azioni di **customer awareness** è confermata nelle **raccomandazioni BCE** sulla sicurezza dei pagamenti Internet.

- Il **73,9%** delle banche ha comunicato alle proprie imprese clienti le principali **buone pratiche di comportamento** per un utilizzo sicuro dei servizi di Internet Banking
- Necessità di **mantenere costante il dialogo** con tale segmento di clientela.

Azioni specifiche di sensibilizzazione clientela Corporate



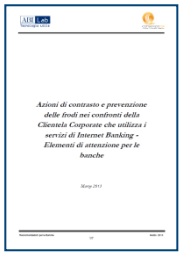
Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi identitarie 2015 (Campione: 23 rispondenti)

Azioni di sensibilizzazione
Documenti di raccomandazioni clientela Corporate

Il **Consorzio ABI Lab**, con il contributo del **Consorzio CBI,** ha realizzato nel 2013 due documenti di raccomandazioni per un **utilizzo sicuro dei servizi di Internet Banking**, da veicolare alle banche e alle imprese clienti.

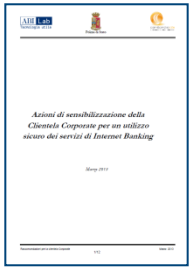
Nel dettaglio:

- *Azioni di contrasto e prevenzione delle frodi nei confronti della Clientela Corporate che utilizza i servizi di Internet Banking - Elementi di attenzione per le banche*



Documento contenente alcuni consigli che si ritiene possano essere di **ausilio alle banche** nel **rafforzamento delle attività di presidio**, **contrasto** e **prevenzione** delle **frodi**, da adottare, in particolare, nei rapporti con la clientela Corporate che utilizza i servizi di Internet Banking.

- *Azioni di sensibilizzazione della Clientela Corporate per un utilizzo sicuro dei servizi di Internet Banking*



Documento rivolto direttamente alle aziende Corporate, condiviso anche con la **Polizia Postale e delle Comunicazioni** e strutturato in tre sezioni:

- policy aziendali
- indicazioni per la protezione delle postazioni dalle quali viene svolta l'attività di Internet Banking (PC utente)
- buone pratiche di comportamento dell'utilizzatore dei servizi di Internet Banking

Azioni di sensibilizzazione
Documento di raccomandazioni verso la clientela Corporate

ABI Lab
Tecnologia utile

ELEMENTI DI ATTENZIONE PER LE BANCHE

Azioni di monitoraggio e di controllo

→ Introdurre e/o mantenere aggiornati **strumenti** e **tecnologie** a protezione di accessi, reti e operazioni

Tecnologie di protezione per la clientela

→ Mantenere elevata l'attenzione sull'utilizzo da parte della clientela di strumenti e tecnologie di **strong authentication** e di un **secondo canale** per la rilevazione di anomalie

Tecnologie e processi a protezione dei PC Cliente

→ Indirizzare la clientela Corporate verso la **corretta gestione** dei propri **sistemi informativi** e delle **password** di accesso

Info sharing

→ Rafforzare le iniziative di **dialogo** e di **collaborazione** intra e intersettoriali

Sensibilizzazione della clientela Corporate

→ Svolgere attività di «**education**» della clientela sui temi della sicurezza dei pagamenti on line

Vulnerability assessment e Penetration test

→ Eseguire **periodicamente** vulnerability assessment e Penetration test per evidenziare eventuali debolezze

Profilazione del portale di Internet Banking

→ Valutare l'opportunità di realizzare di **portali** di Internet Banking profilati sulla base delle **abilitazioni** degli utenti dell'azienda cliente

INDICAZIONI PER LE IMPRESE CLIENTI

I. Policy aziendali (1/2)

- ✓ Adottare una **policy in materia di sicurezza informatica** che dovrebbe:
  - Evidenziare **rischi correlati** allo svolgimento di un'operazione bancaria in via telematica
  - **Essere condivisa** all'interno di tutta l'azienda
  - **Specificare ruoli** e **responsabilità** all'interno dell'azienda, con compiti specifici e incarichi assunti relativamente alle attività di Internet Banking
  - Elencare **strumenti utilizzati** dall'azienda, i device e le postazioni da cui è possibile operare

- ✓ **Individuare** preventivamente i **dipendenti** e le **postazioni** dalle quali vengono svolte le operazioni di Internet Banking, con l'obiettivo di:
  - **Abilitare solo alcuni dipendenti** all'utilizzo dei canali e degli applicativi aziendali necessari per il corretto svolgimento delle attività
  - Effettuare **attività di controllo** ex-post sulle operazioni

- ✓ **Verificare** giornalmente le **movimentazioni bancarie effettuate.** Ciò consentirebbe di:
  - Avere sotto **controllo** le operazioni dispositive realizzate durante la **giornata**
  - **Controllare ex-post** la corrispondenza tra le operazioni

INDICAZIONI PER LE IMPRESE CLIENTI

I. Policy aziendali (2/2)

- ✓ Avviare **periodicamente iniziative di informazione e/o formazione interna** all'azienda in materia di sicurezza informatica per:
  - **Aggiornare i dipendenti** abilitati a compiere le operazioni telematiche circa gli aspetti di sicurezza
  - **Istruire** gli utilizzatori dei servizi di Internet Banking riguardo il tema della sicurezza on line
- ✓ Utilizzare il **canale alternativo di comunicazione** e gli **strumenti di II fattore** messi a disposizione dalla banca:
  - Rendendo **obbligatorio l'uso** a tutti gli utenti secondo le specifiche profilazioni
  - Attivare l'uso del **II canale di comunicazione** quando messo a disposizione della banca

  Ciò garantisce la ***massima sicurezza*** in fase di accesso e di autorizzazione delle operazioni via Internet
- ✓ **Aggiornare** periodicamente le **password** di **accesso** e le **postazioni utilizzate** nell'ottica di:
  - Ridurre il **rischio di** un **utilizzo** continuativo di eventuali **profili compromessi**
  - Ridurre il **rischio** che i dati vengano utilizzati per **scopi illeciti**
- ✓ Definire e divulgare **procedure** che identifichino le **modalità di comunicazione** tra l'utente, la banca e le **Autorità competenti** per consentire alle aziende di:
  - **Gestire** più rapidamente le **anomalie/inefficienze**
  - Avere **tempestivamente indicazioni** su come comportarsi e su come prendere provvedimenti

INDICAZIONI PER LE IMPRESE CLIENTI

II. Indicazioni per la protezione delle postazioni (1/2)

- ✓ **Installare e aggiornare** opportuni **antivirus** e impostare adeguati **firewall** per**:**
  - Garantire la **sicurezza dei dati** archiviati nelle diverse postazioni
  - **Limitare** la possibilità di **diffusione di virus** o trojan all'interno dell'azienda
  - Riconoscere virus e programmi infettati di recente creazione
  - **Vincolare la navigazione** e il libero flusso di dati verso la rete web

- ✓ **Aggiornare periodicamente i sistemi operativi** utilizzati sui PC utente mediante l'istallazione delle cosiddette patch

- ✓ **Limitare la navigazione** sul web e/o l'**installazione** di programmi non certificati. Si consiglia di:
  - **Permettere solo** agli **amministratori di sistema** di compiere azioni di **modifica** delle **configurazioni** impostate
  - **Vietare** agli utilizzatori abituali la possibilità di **scaricare e installare programmi** di cui non è possibile verificarne la provenienza
  - **Impedire** che **applicazioni scaricate** dalla rete possano essere **installate** nelle diverse postazioni

INDICAZIONI PER LE IMPRESE CLIENTI

II. Indicazioni per la protezione delle postazioni (2/2)

- ✓ **Differenziare i profili degli utenti** in base alle specifiche esigenze operative. È opportuno:
  - **Limitare/eliminare** i **diritti di «amministratore»** sulle singole postazioni per contrastare la possibilità di istallazione di codice malevolo
  - Creare **differenti profili di utilizzatori** di terminali dai quali è possibile accedere alla rete aziendale ed effettuare operazioni di Internet Banking, in modo da ridurre il rischio che vengano poste in essere transazioni non autorizzate

- ✓ **Se necessario**, per tutelare la sicurezza dell'azienda, svolgere le **operazioni di Internet Banking da una postazione dedicata**

  In tal modo si **riduce drasticamente il rischio** di compromissione dei terminali utilizzati e di sottrazione delle credenziali di accesso all'Internet Banking.

INDICAZIONI PER LE IMPRESE CLIENTI

III. Buone pratiche di comportamento rivolte all'utilizzatore dei servizi di IB

- ✓ **Assumere un comportamento diligente relativamente alla conservazione di dati** relativi a carte di pagamento, **chiavi di accesso** e **altre informazioni** associate al servizio di Internet Banking

Nessuna banca chiederà mai di fornire direttamente informazioni sensibili

- ✓ Collegarsi all'indirizzo internet della banca **digitando l'indirizzo sul browser** e non cliccando su link esterni. Bisogna quindi:
  - Prestare **attenzione** in caso di **anomalie** rispetto alle abituali modalità
  - **Segnalare tempestivamente** alla propria banca di riferimento e alle Autorità competenti la presenza di eventuali anomalie

- ✓ **Diffidare di qualsiasi messaggio** che rivolga l'invito a scaricare programmi o documenti di cui si ignora la provenienza

- ✓ **Conservare i codici e gli strumenti di accesso** al servizio di Internet Banking in maniera diligente

ABI Lab
Tecnologia utile

GRAZIE PER L'ATTENZIONE