# ABI – CIPA - CNIPA

## IL FURTO DI IDENTITA' ELETTRONICA TRAMITE INTERNET

## ANALISI DEL FENOMENO

**Aprile 2006**

ABI Lab Tecnologia utile

CIPA

CNIPA Centro Nazionale per l'Informatica nella Pubblica Amministrazione

e-committee

Il presente rapporto è stato predisposto dal gruppo di lavoro ABI-CIPA-CNIPA composto dai seguenti nominativi:

| | | |
|---|---|---|
| Massimiliano | MAGI SPINETTI | ABI |
| Alessandro | ZOLLO | ABI |
| Romano | STASI | ABI |
| Stefano | CONTI | ABI |
| Matteo | LUCCHETTI | ABI |
| Tommaso | GIACOMINO | Banca d'Italia – Segreteria CIPA |
| Beatrice | BERNARDINI | Banca d'Italia – Segreteria CIPA |
| Roberto | TRINCA | Banca d'Italia – Segreteria CIPA |
| Salvatore | FRATEJACCI | Banca d'Italia – Segreteria CIPA |
| Gino | GIAMBELLUCA | Banca d'Italia – Segreteria CIPA |
| Giancarlo | SPAGNA | CNIPA |

L'ABI, la CIPA e il CNIPA desiderano ringraziare i suddetti elementi per la collaborazione prestata e il contributo fornito nello svolgimento delle attività del gruppo di lavoro.

## Indice

**Sintesi**

Nel corso del 2005 ABI, CIPA e CNIPA hanno convenuto sull'opportunità di condurre uno studio sul "furto di identità elettronica", fenomeno che, incidendo sulla fiducia degli utenti, può costituire un fattore di freno allo sviluppo della domanda di servizi *on-line* offerti dal sistema bancario e dalla pubblica amministrazione.

È stato pertanto elaborato il presente rapporto nel quale sono prese in esame: le diverse tipologie di azioni fraudolente attraverso le quali si può realizzare il furto delle credenziali degli utenti per l'accesso ai servizi *on-line*; le iniziative di contrasto già avviate nel nostro Paese; le caratteristiche del fenomeno e le azioni di contrasto intraprese nei principali paesi industrializzati.

L'obiettivo che ci si è posti è quello di fornire agli operatori del settore una base di conoscenze comune sulla quale eventualmente innestare, ai vari livelli (aziendale, cooperativo e istituzionale), ulteriori iniziative per la prevenzione e il contrasto delle minacce emergenti.

Il **primo capitolo** del rapporto è dedicato a una sintetica descrizione del contesto di riferimento, cioè quello della domanda e dell'offerta dei servizi in rete in Italia, con particolare riferimento ai settori bancario e della pubblica amministrazione.

L'analisi dei dati sulla diffusione di Internet consente di evidenziare una crescente propensione delle famiglie e delle imprese italiane a servirsi dei canali telematici nell'interazione con le banche e con la PA.

Significative sono al riguardo le tendenze rilevate dall'Osservatorio e-Committee per il sistema bancario: per citarne solo alcune, nel 2004 il numero dei conti, accedibili mediante il canale Internet, "attivi" ha superato quello dei conti aperti sul medesimo canale ma non utilizzati; i conti con operatività dispositiva sono adesso in numero maggiore di quelli solamente informativi. All'evoluzione della domanda corrisponde una sempre più ampia e strutturata offerta di servizi bancari in rete, che costituisce ormai parte essenziale delle strategie distributive delle banche.

Anche presso la PA si registra un crescente ricorso a modalità di colloquio telematico con i cittadini. L'erogazione di servizi pubblici su rete rappresenta un passaggio chiave nella realizzazione del modello di *e-government* che la pubblica amministrazione ha adottato quale obiettivo prioritario nell'azione volta a innalzare qualità ed efficienza dei servizi resi ai cittadini.

La domanda di servizi *on-line* appare peraltro strettamente correlata alla percezione, da parte degli utenti, del grado di sicurezza delle transazioni effettuate su tale canale. Diverse ricerche segnalano come la fiducia degli utilizzatori rappresenti il principale fattore determinante il livello di espansione della richiesta dei servizi telematici; ne deriva quindi che il diffondersi di minacce, come quelle rappresentate dai furti di identità elettronica, possono sensibilmente condizionare le potenzialità di crescita del settore.

Nel **secondo capitolo** del rapporto sono esplorate le diverse forme di "furto di identità elettronica" a oggi conosciute. Traendo anche spunto da recenti analisi effettuate in ambito bancario, quali lo studio CIPA sul rischio informatico e la tassonomia elaborata da ABI Lab, sono analizzate principalmente due tipologie di frodi: quelle condotte attraverso attacchi diretti al sistema informativo del fornitore dei servizi o al computer dell'utente (es. tecniche di *sniffing*, di *connection hijacking*, varie tipologie di programmi "spia", quali ad esempio gli *spyware*) e quelle realizzate attraverso complesse forme di raggiro dell'utente. In quest'ultimo ambito l'attenzione è concentrata soprattutto sul *phishing*, fenomeno ormai ampiamente noto, consistente nella cattura dei dati personali attraverso l'invio di richieste apparentemente provenienti da una banca/istituzione operante *on-line*.

Per ciascuna tipologia di minaccia sono richiamate le possibili contromisure tecniche. Con riferimento al *phishing* si rimanda alle misure comportamentali contenute nei due "decaloghi" definiti da ABI Lab, uno rivolto alle banche, uno agli utenti dei servizi bancari *on-line*.

Nel **terzo capitolo** viene svolta una ricognizione dei casi di *phishing* fin qui registrati nel sistema creditizio nazionale.

Sono poi passate in rassegna le diverse iniziative di prevenzione già avviate in ambito associativo e presso la PA. Tra le prime rileva la costituzione, nel 2003, in seno ad ABI Lab, della "Centrale di allarme per attacchi informatici" operante su tre fronti: collaborazione con altre istituzioni operanti nel campo dei crimini informatici; analisi delle minacce emergenti; invio di segnalazioni su attacchi avvenuti.

Tra le iniziative della PA si segnala, tra l'altro, la costituzione del "GovCERT", struttura operante nell'ambito del CNIPA per favorire la prevenzione e fornire supporto alle pubbliche amministrazioni nella gestione delle problematiche connesse con gli attacchi e gli incidenti informatici.

Il **quarto capitolo** contiene infine una panoramica sulla diffusione dei fenomeni di furto di identità elettronica in alcuni dei principali paesi industrializzati, con particolare riferimento al settore bancario e finanziario, e sulle iniziative di contrasto adottate a livello istituzionale, associativo e di singoli operatori.

Emergono alcune linee di azione comune nei diversi paesi: gli organi legislativi si sono spesso posti il problema di rafforzare la legislazione punitiva in materia di reati informatici, ampliando le fattispecie criminose previste al fine di ricomprendervi il furto di identità elettronica; le autorità di vigilanza creditizia e finanziaria hanno evidenziato la pericolosità del fenomeno, stimolando gli operatori a dotarsi di sistemi di sicurezza adeguati e ad adottare coerenti *policy* in materia di sicurezza informatica; le associazioni bancarie hanno formulato specifiche raccomandazioni e *best practices* dirette agli operatori e hanno promosso la diffusione di informazioni tra gli associati, la collaborazione con organi di polizia, iniziative di sensibilizzazione e di educazione degli utenti; i singoli operatori hanno attivato forme di comunicazione e sensibilizzazione della clientela e hanno innalzato la sicurezza dei sistemi di accesso ai servizi *on-line*, spesso attraverso l'adozione di sistemi di "autenticazione forte".

**Premessa**

La diffusione di servizi *web-based* evoluti ha portato all'affermazione di Internet come canale per le transazioni di natura economica tra il cittadino e le imprese, le banche e la pubblica amministrazione. Nel loro processo di affermazione, l'*e-commerce*, l'*e-payment*, l'*e-banking* e l'*e-government* hanno reso necessario lo scambio *on-line* di quantità di sicurezza volte a garantire il riconoscimento dell'identità delle controparti.

In questo scenario si creano gli spazi per nuove forme di frodi informatiche finalizzate a sottrarre e utilizzare per scopi illeciti i dati che rappresentano l'identità elettronica del cittadino. Il tema della sicurezza assume quindi un ruolo strategico per consentire la sostenibilità del nuovo paradigma di relazione con l'utente. Le frodi informatiche, benché siano a oggi un fenomeno marginale, rischiano infatti di minare la fiducia degli utilizzatori della Rete, impedendo la diffusione dei servizi più evoluti.

Questo documento rappresenta il risultato di uno studio congiunto tra ABI, CIPA e CNIPA volto a condividere le rispettive conoscenze ed esperienze nell'ambito del furto di identità elettronica per tracciare un quadro completo degli impatti del fenomeno e delle possibili contromisure.

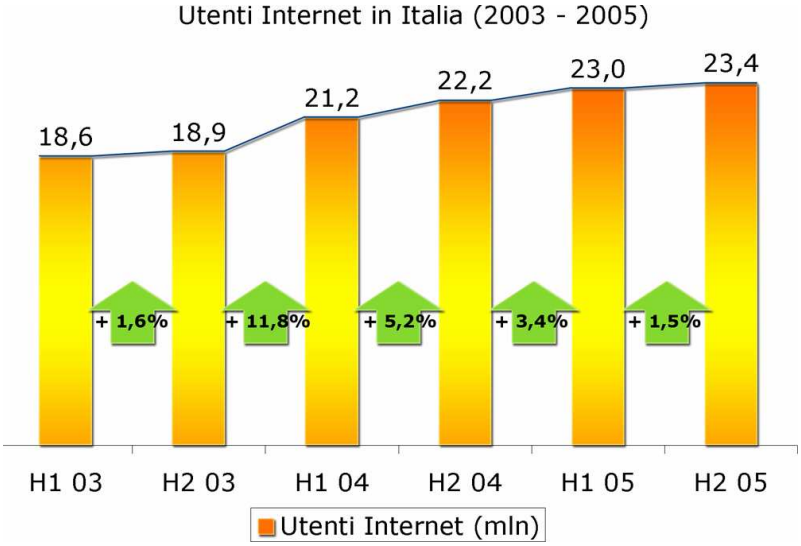
Lo studio – che comprende un'analisi del contesto dei servizi in Rete, una tassonomia dettagliata degli attacchi informatici, un rapporto sull'attuale esposizione del sistema italiano ai rischi di frode informatica e un'analisi del contesto internazionale – costituisce la base per l'avvio di un più ampio rapporto di collaborazione tra i tre organismi, con l'obiettivo di realizzare il costante monitoraggio del fenomeno nonché la condivisione di informazioni e di proposte operative per un'efficace azione di contrasto.

# 1. DESCRIZIONE DEL CONTESTO: EVOLUZIONE DEI SERVIZI IN RETE

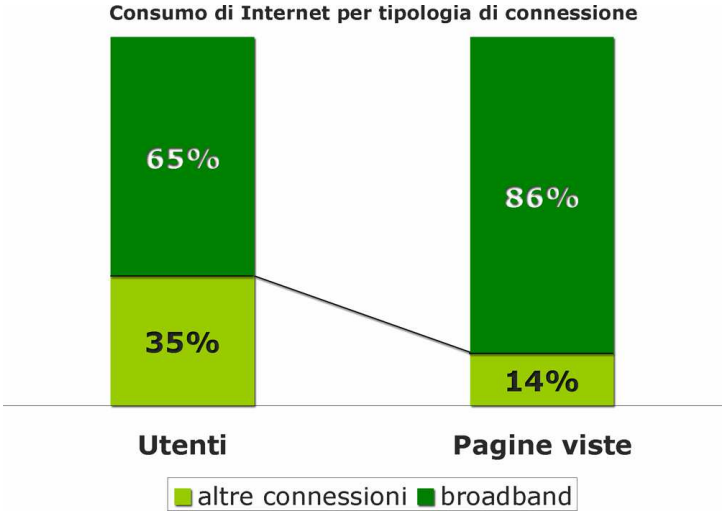
## 1.1. Diffusione di Internet in Italia

Il processo di alfabetizzazione informatica che ha caratterizzato gli ultimi anni ha portato ad una diffusa confidenza dei cittadini italiani con il web.

Da un'indagine dell'Osservatorio operante nell'ambito dell'e-Committee, associazione costituita in seno all'ABI, risulta che nel secondo semestre del 2005 sono stati 23,4 milioni gli italiani che si sono collegati almeno una volta al web. Continua il *trend* incrementale che ha caratterizzato gli ultimi anni: i navigatori Internet in Italia sono cresciuti dell'1,5% rispetto al primo trimestre e del 5% su base annua.




*Driver* di questa crescita si conferma la penetrazione delle connessioni a banda larga che presenta tassi incrementali ancora imponenti. Nel secondo semestre del 2005 sono stati 13,3 milioni i navigatori ad alta velocità (> 128K), il 19% in più rispetto al primo semestre e il 49% in più rispetto allo stesso periodo del 2004. Nella seconda parte dell'anno quasi due internauti su tre navigano in banda larga: i navigatori ad alta velocità rappresentano il 65% degli utenti Internet domestici e sono responsabili dell'86% di tutte le pagine web generate nel semestre.



L'utente *broadband* è infatti un grande consumatore della Rete: complessivamente, negli ultimi sei mesi del 2004 è rimasto connesso per 156 ore contro le 54 dell'utente collegato a banda stretta. Nel secondo semestre dell'anno la diffusione delle connessioni ad alta velocità registra un'incidenza significativa nel Sud: il 31% degli utenti *broadband* si trova in questa area, in linea con la distribuzione dell'utenza Internet generale.

## 1.2. Banche: sviluppo dell'*e-banking* e degli strumenti di pagamento innovativi

### *La presenza delle banche sulla Rete*

Lo scenario dell'offerta bancaria attraverso Internet è stato fotografato dal *Monitoraggio dell'attività on-line delle Banche - 2004*, indagine condotta per il secondo anno dall'Osservatorio e-Committee.

La rilevazione conferma un progressivo allineamento e consolidamento dell'offerta di servizi bancari diretti da parte degli operatori italiani. Nel corso degli ultimi 12 mesi si è infatti assistito a una crescita del numero complessivo di conti Internet, del grado di attivazione e impiego dispositivo dei servizi di *Phone Banking* e a uno sviluppo dei servizi di *Mobile Banking*.

L'offerta di servizi bancari diretti appare più matura e strutturata, in grado di soddisfare le più articolate esigenze della clientela e fornire una valida rappresentazione del livello progressivo di ammodernamento e innovazione del sistema bancario italiano.

Internet si conferma il cuore della strategia multicanale delle banche: con circa 6,5 milioni di conti correnti abilitati, arriva a coprire nel 2004 il 21% del mercato Famiglie. La crescita dei conti Internet *Banking* è stata del 65%, con una velocità di diffusione coerente con lo sviluppo nella società italiana di Internet. L'Osservatorio e-Committee stima che questi 6,5 milioni di conti siano rappresentativi di circa 8 milioni di clienti in grado di accedere *on-line* al proprio conto corrente.

Questa diffusione del servizio si accompagna a una corrispondente forte crescita dell'impiego del canale per compiere operazioni bancarie.

Si è verificato un duplice sorpasso. In primo luogo quello dei conti attivi sui conti dormienti: i conti su cui oggi si effettuano operazioni sono il 55% del totale (dato in parte penalizzato da vecchie contrattualizzazioni storicamente inattive), con una crescita su base annua pari al 10%.

Il secondo e più importante sorpasso è quello che porta il livello dei conti dispositivi a superare quello dei conti informativi: il 55% dei conti attivi risulta oggi dispositivo, con un numero di operazioni medio di un bonifico al mese, per un valore complessivo di circa € 15.000 all'anno.

Nel Rapporto 2004 la rilevazione è stata estesa al mercato Imprese. Su questo segmento la penetrazione netta dei canali diretti ha raggiunto nel 2004 il 18% del mercato complessivo dei conti correnti. Il Corporate *Banking* risulta il circuito dispositivo prevalente tra le imprese, con una quota di conti con banca proponente del 12%, pari a circa 650.000 unità, cui si affiancano i circa 550.000 conti correnti abilitati ai servizi di Internet *Banking* Imprese.

### *Lo sviluppo di servizi innovativi per i pagamenti elettronici*

L'avvento di Internet ha fortemente influenzato tutta l'attività bancaria, imponendo, da un lato, una ridefinizione dell'offerta e dei canali di distribuzione e, dall'altro lato, offrendo nuove possibilità di *business*. Le potenzialità dell'*e-banking* e dell'*e-business* in generale rappresentano un'importante sfida per il sistema bancario.

Da questa considerazione, nel dicembre del 2000 è nata una nuova associazione di banche, l'e-Committee - Comitato di Coordinamento delle Infrastrutture per l'*e-banking* – un motore per l'innovazione bancaria nell'ambito delle tecnologie dell'informazione.

L'e-Committee progetta e realizza prodotti, servizi e sistemi a supporto delle attività *on-line* delle banche definendone le caratteristiche tecniche, gli standard qualitativi e gli aspetti normativi; ne gestisce la diffusione e lo sviluppo, vigilando sull'operato dei soggetti coinvolti.

A oggi l'e-Committee conta circa 225 banche associate che rappresentano oltre il 90% del mercato dei sistemi di pagamento in Italia.

Le attività dell'e-Committee sono oggi rivolte alla realizzazione di servizi finalizzati a razionalizzare l'offerta bancaria nell'ambito dei sistemi di pagamento sui canali innovativi, presentati al mercato sotto il marchio Bankpass. In particolare sono stati a oggi lanciati sul mercato due servizi, Bankpass Web e Bankpass Bollette, che si pongono l'obiettivo di definire standard del sistema bancario per razionalizzare i pagamenti sulla Rete.

*Bankpass Web*

Bankpass Web, servizio attivo dall'ottobre del 2002, offre a consumatori ed esercenti una soluzione per effettuare transazioni sicure su Internet e, per la prima volta, apre le porte del commercio elettronico al PagoBANCOMAT.

Si tratta di un portafoglio virtuale nel quale il consumatore può inserire i propri strumenti di pagamento (Carte di credito e PagoBANCOMAT) per acquistare e pagare su qualsiasi sito di *e-commerce* senza dover digitare i dati delle proprie carte. Bankpass Web è anche una piattaforma con cui l'esercente può gestire tutti i pagamenti del proprio negozio *on-line* in maniera semplice ed efficiente. Per l'esercente significa garanzia dei pagamenti e una crescita del volume d'affari, perché grazie al PagoBANCOMAT può raggiungere un mercato più ampio. A oggi sono circa 6.000 gli esercenti che hanno aderito a Bankpass Web (su un mercato che conta circa 9.000 *players*).

*Bankpass Bollette*

Bankpass Bollette, servizio lanciato a gennaio 2005, è la soluzione per l'inoltro, la presentazione e il pagamento elettronico di bollette e fatture. Il servizio consente di gestire in forma elettronica le attività connesse alla riscossione dei crediti presso la propria clientela. Nel contempo il servizio offre ai debitori l'opportunità di ricevere e pagare le proprie bollette tramite il servizio di Internet *Banking* della propria banca.

## 1.3. Pubblica Amministrazione: strategie di sviluppo e di ammodernamento basate sui servizi in Rete

Nella strategia complessiva per lo sviluppo della Società dell'Informazione, l'utilizzo delle nuove tecnologie rappresenta uno dei punti qualificanti nel programma di Governo in cui si promuove una radicale riorganizzazione tramite l'informatizzazione della pubblica amministrazione.

Le linee guida di tale profonda trasformazione si articoleranno per:

- Pubblica Amministrazione Centrale
- Pubblica Amministrazione Locale
- Interventi sulle infrastrutture abilitanti della trasformazione

Inoltre verranno esaminati gli impatti del programma di cambiamento sulle risorse umane e i fabbisogni finanziari.

***Il modello di eGovernment***

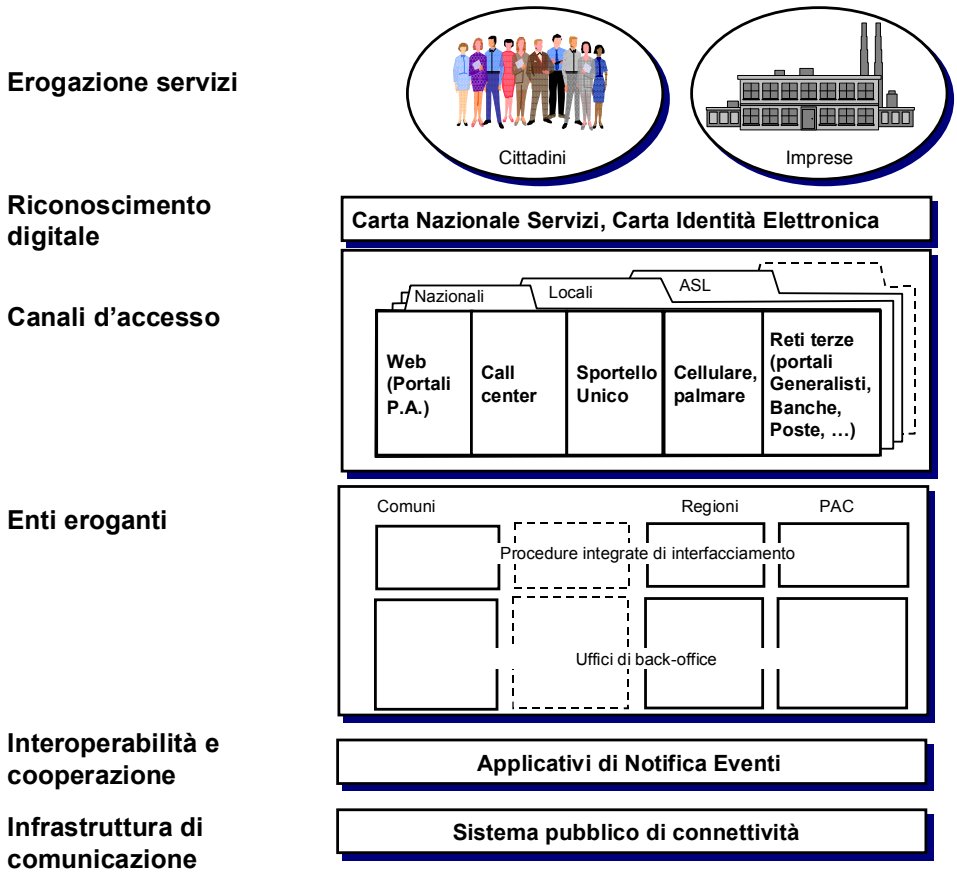
L'*eGovernment* rappresenta un passaggio innovativo fondamentale nell'evoluzione del rapporto cittadino/pubblica amministrazione, che si inserisce nel processo di profonda trasformazione che tutti gli enti pubblici stanno affrontando per servire i cittadini e le imprese come "clienti" da gestire con la massima attenzione. Il concetto di cliente non significa che le amministrazioni operano in un'ottica di profitto, ma più semplicemente che il loro obiettivo diventa quello di erogare servizi in linea con le esigenze di chi ne usufruisce e la soddisfazione del ricettore del servizio è strumento fondamentale di verifica della sua qualità. È opportuno sottolineare che tra i cittadini "clienti" debbono figurare a pieno titolo e con pari opportunità i cittadini italiani all'estero.

Per realizzare concretamente questo concetto il Dipartimento per l'Innovazione e le Tecnologie ha sviluppato il modello di riferimento strategico dell'eGovernment descritto di seguito.

Il modello è composto da sei elementi chiave:

- **Erogazione servizi** - Un insieme di servizi che dovranno essere resi disponibili attraverso modalità innovative e a un livello di qualità elevato a utenti-clienti (cittadini e imprese). Per focalizzare gli sforzi di sviluppo, sono stati individuati alcuni **servizi prioritari** dal punto di vista degli utenti-clienti, che saranno considerati nelle iniziative di digitalizzazione. Questi servizi saranno forniti con un unico punto di accesso anche se implicano l'intervento di più amministrazioni. Le complessità interne alla pubblica amministrazione verranno cioè mascherate all'utente/cliente.
- **Riconoscimento digitale** - Modalità di riconoscimento dell'utente e di firma sicure attraverso la Carta di Identità Elettronica, la Carta Nazionale dei Servizi e la firma digitale.
- **Canali di accesso** - Una pluralità di canali innovativi attraverso cui l'utente accede ai servizi offerti: Internet, *call-center*, cellulare, reti di terzi.
- **Enti eroganti** - Un *back-office* efficiente ed economicamente ottimizzato dei diversi enti eroganti.
- **Interoperabilità e cooperazione** - Standard di interfaccia tra le amministrazioni che consentano comunicazioni efficienti e trasparenza verso l'esterno.
- **Infrastruttura di comunicazione** - Un'infrastruttura di comunicazione che colleghi tutte le amministrazioni.

**Fig. 1– Il modello di eGovernment della Pubblica Amministrazione**




In aggiunta a queste componenti, le tecnologie oggi disponibili sono utilizzabili anche per migliorare l'efficienza dei processi interni dell' Amministrazione pubblica (es. acquisti di beni e servizi) e per valorizzare le risorse umane interne, aumentandone le competenze e il *know-how*.

### *I 10 obiettivi di legislatura per la Pubblica Amministrazione centrale*

Con specifico riferimento alle amministrazioni centrali, le iniziative prioritarie atte a realizzare il "modello di riferimento" e a sfruttare pienamente i vantaggi derivanti dalle nuove tecnologie sono state tradotte nei **10 obiettivi di legislatura** approvati il 13 febbraio 2002 dal Comitato dei Ministri per la Società dell'Informazione.

Le amministrazioni sono state inoltre chiamate a individuare ed elaborare **obiettivi specifici**, coerenti con la strategia di *eGovernment*, focalizzati sulle proprie aree di intervento e finalizzati a qualificare in modo innovativo l'azione dei singoli Ministeri.

| **Servizi *on-line* ai cittadini e alle imprese** |
|---|
| 1. Tutti i servizi 'prioritari' disponibili *on-line* |
| 2. 30 milioni di Carte di Identità Elettroniche e Carte Nazionali dei Servizi distribuite |
| 3. 1 milione di firme digitali diffuse entro il 2003 |
| **Efficienza interna della Pubblica Amministrazione** |
| 4. 50% della spesa per beni e servizi tramite *eProcurement* |
| 5. Tutta la posta interna alla Pubblica Amministrazione via *e-mail* |
| 6. Tutti gli impegni e mandati di pagamento gestiti *on-line* |
| **Valorizzazione delle Risorse Umane** |
| 7. Alfabetizzazione certificata di tutti i dipendenti pubblici eleggibili |
| 8. 1/3 della formazione erogata via *eLearning* |
| **Trasparenza** |
| 9. 2/3 degli uffici della Pubblica Amministrazione con accesso *on-line* all'iter delle pratiche da parte dei cittadini |
| **Qualità** |
| 10. Tutti gli uffici che erogano servizi dotati di un sistema di soddisfazione dell'utente |

Le attività svolte a fronte degli obiettivi di legislatura hanno portato ai risultati, aggiornati a febbraio 2006, sinteticamente riportati nella tabella seguente:

| Obiettivi legislatura | Risultati |
|---|---|
| **1. Tutti i servizi 'prioritari' disponibili *on-line*** | ▸ Il 61% dei servizi prioritari della Pubblica Amministrazione centrale è totalmente disponibile.<br>▸ Stato avanzamento dei 134 progetti sull'*e-government* (fase 1) focalizzati sui servizi prioritari attuato all'86% a fine 2005<br>▸ Entro la fine della legislatura questa percentuale sarà il 95% |
| **2. 30 milioni di Carte di Identità Elettroniche e Carte Nazionali dei Servizi distribuite** | ▸ 13 milioni di carte intelligenti (CIE, CNS, firma digitale) emesse a fine 2005<br>▸ Nel 2006, è prevista la distribuzione complessiva di 20 milioni di Carte Nazionali dei Servizi e Carte d'Identità Elettroniche<br>▸ Sono state distribuite o sono in corso di distribuzione nelle rimanenti Regioni le Tessere Sanitarie che consentono l'identificazione digitale del paziente |
| **3. 1 milione di firme digitali diffuse entro il 2003** | ▸ 2,1 milioni di firme digitali in circolazione al 2005<br>▸ 35.000 distribuite ai dipendenti nella PA centrale |
| **4. 50% della spesa per beni e servizi tramite *e-procurement*** | ▸ Circa il 60% delle pubbliche amministrazioni centrali usa l'*e-procurement* |
| **5. Tutta la posta interna alla Pubblica Amministrazione via *e-mail*** | ▸ Il 90% dei dipendenti della Pubblica Amministrazione ha la posta elettronica<br>▸ Introdotta la Posta Elettronica Certificata |
| **6. Tutti gli impegni e mandati di pagamento gestiti *on-line*** | ▸ 24 milioni tra mandati e impegni di pagamento *on-line* nelle amministrazioni centrali<br>▸ Nelle amministrazioni locali si sta introducendo l'ordinativo informatico |
| **7. Alfabetizzazione certificata di tutti i dipendenti pubblici eleggibili** | ▸ Il 90% dei dipendenti usa correntemente il PC<br>▸ Negli ultimi tre anni 1 dipendente su due ha ricevuto formazione, per complessive 800.000 giornate lavorative |

| | |
|---|---|
| **8. 1/3 della formazione erogata via *e-learning*** | ▸ Attivata scuola virtuale della PA<br>▸ Emessa una specifica Direttiva in materia<br>▸ Dati non disponibili |
| **9. 2/3 degli uffici della Pubblica Amministrazione con accesso *on-line* all'iter delle pratiche da parte dei cittadini** | ▸ Il 66% dei documenti (agosto 2005) è protocollato elettronicamente<br>▸ 20 amministrazioni centrali (tra cui agenzie fiscali ed enti di previdenza) hanno un *call center* attivo |
| **10. Tutti gli uffici che erogano servizi dotati di un sistema per la soddisfazione dell'utente** | ▸ Ad agosto 2005 il 52% degli uffici eroga servizi al pubblico misurando la *customer satisfaction*<br>▸ Introdotta la rilevazione anche per i servizi *on-line* |

### *Il Codice dell'Amministrazione Digitale (CDA)*

Il **Decreto legislativo del 7 marzo 2005, n. 82** recante il "**Codice dell'Amministrazione Digitale**" (pubblicato nella G.U. 16 maggio 2005, n.112 - S.O. n. 93) è il risultato di oltre due anni di lavoro, di continue interazioni con tutti i livelli istituzionali, con le Regioni e le Autonomie Locali. È stato redatto dal Ministero per l'innovazione e le tecnologie in collaborazione con tutte le amministrazioni statali e con il contributo di personalità del mondo dell'università, ricerca, imprenditoria, ordini professionali e associazioni di categoria. La diffusione delle tecnologie dell'informazione e della comunicazione è fortemente condizionata dalle regole che ne definiscono la cornice normativa. Innovazione e normativa sono legate da un rapporto di reciproca influenza molto articolato, reso ancor più complesso dall'accelerazione propria della dinamica tecnologica. Se i due aspetti non procedono di pari passo, la normativa rischia di diventare un ostacolo invece che una risorsa per promuovere e incoraggiare lo sviluppo.

Le pubbliche amministrazioni sono molto cambiate in questi ultimi anni: secondo i sondaggi i cittadini stessi le vedono mediamente più veloci e più attente ai bisogni dei loro utenti. I motori di questo cambiamento sono stati le reti telematiche, l'informatica, Internet. Eppure vi è ancora molto da fare: spesso infatti l'innovazione tecnologica si è solo affiancata ai vecchi sistemi e i computer hanno convissuto con i timbri e i raccoglitori d'archivio. Il Codice rende ora obbligatoria l'innovazione nella PA nel modo più naturale: da una parte offrendo ai cittadini il diritto di interagire sempre, dovunque e verso qualsiasi amministrazione attraverso Internet, posta elettronica, reti; dall'altra stabilendo che tutte le amministrazioni devono organizzarsi in modo da rendere sempre e comunque disponibili tutte le informazioni in modalità digitale. Il Codice, entrato in vigore il 1° gennaio 2006, è quindi una complessa riforma, una specie di "costituzione" del mondo digitale, che tiene conto di diritti e doveri e che contemporaneamente fornisce i principi operativi con cui tali diritti e doveri si possono concretizzare. In questo modo semplifica il sistema giuridico di riferimento e lo rende più efficace. In sostanza il Codice ha ordinato e riunito norme già esistenti e ne ha fatte di nuove per nuovi servizi e nuove opportunità, ha creato in sostanza il quadro legislativo necessario per dare validità giuridica alle innovazioni. Il Codice dà attuazione alla prima delle cinque missioni del Programma di Governo per la riorganizzazione della macchina pubblica e alla digitalizzazione della PA:

- introducendo nuovi diritti per i cittadini e le imprese e definendo il quadro giuridico che ne garantisce l'effettivo godimento;
- indicando nuovi strumenti e consolidando la loro validità giuridica;
- ponendo le basi per la costruzione di un federalismo efficiente;
- disegnando così una pubblica amministrazione che funzioni meglio e costi meno ai contribuenti.

*PA DIGITALE E NUOVI DIRITTI DEI CITTADINI*

Nella pubblica amministrazione digitale i cittadini e le imprese hanno nuovi diritti che il Codice precisa e definisce e che rende quindi effettivamente esercitabili:

**Diritto all'uso delle tecnologie (art. 3)** I cittadini e le imprese hanno diritto di usare le moderne tecnologie informatiche per tutti i rapporti con qualsiasi amministrazione dello Stato. Non sarà più possibile quindi per un'amministrazione o per un gestore di pubblico servizio obbligare i cittadini a recarsi agli sportelli per presentare documenti cartacei, per firmare fisicamente domande o istanze, per fornire chiarimenti: per tutto questo deve essere sempre e dovunque disponibile un canale digitale sicuro, certificato e con piena validità giuridica che permetta di dialogare con la PA dal proprio computer.

**Diritto all'accesso e all'invio di documenti digitali (art. 4)** In particolare i cittadini e le imprese hanno diritto di accedere agli atti che li riguardano e di partecipare ai procedimenti in cui sono coinvolti tramite le moderne tecnologie informatiche e telematiche. Tutte le amministrazioni devono quindi organizzarsi per rendere disponibili agli interessati documenti, atti e procedimenti, in modo sicuro e trasparente, in formato digitale.

**Diritto a effettuare qualsiasi pagamento in forma digitale (art. 5)** Dal 30 giugno 2007 i cittadini e le imprese avranno il diritto di effettuare in modo sicuro qualsiasi pagamento verso le pubbliche amministrazioni centrali attraverso le tecnologie informatiche e telematiche. Non sarà quindi più necessario alcun passaggio materiale di denaro né tanto meno fare file in banca o alla posta.

**Diritto a ricevere qualsiasi comunicazione pubblica per *e-mail* (art. 6)** I cittadini e le imprese che ne fanno richiesta hanno diritto a ricevere e inviare le comunicazioni dalle e verso le pubbliche amministrazioni via *e-mail* all'indirizzo che avranno dichiarato. La posta elettronica proveniente dalla PA sarà certificata, ossia saranno certe la data e l'ora della spedizione, della sua ricezione e provenienza. Le comunicazioni e i documenti ricevuti in questo modo avranno piena validità giuridica anche verso altre persone o aziende.

**Diritto alla qualità del servizio e alla misura della soddisfazione (art. 7)** I cittadini e le imprese hanno diritto a servizi pubblici di qualità e che rispondano alle loro reali esigenze. Le pubbliche amministrazioni devono organizzare i servizi in modo da controllarne periodicamente la qualità e la soddisfazione dell'utenza.

**Diritto alla partecipazione (art. 9)** I cittadini hanno diritto di partecipare al processo democratico e di esercitare i diritti politici usufruendo delle possibilità offerte dalle nuove tecnologie.

**Diritto a trovare *on-line* i moduli e i formulari validi e aggiornati (art. 57)** Entro due anni i cittadini e le imprese avranno diritto a trovare in rete i moduli, i formulari e l'elenco dei documenti rilevanti per qualsiasi pratica verso le pubbliche amministrazioni. I moduli e i formulari che non fossero disponibili in via telematica non saranno più giudicati validi, o almeno non saranno più necessari.

*GLI STRUMENTI DELLA PA DIGITALE*

Nella PA digitale questi diritti sono garantiti dalla disponibilità dei seguenti strumenti innovativi a cui il Codice dà piena validità giuridica:

**Posta elettronica certificata (art. 6 e art. 48)** Si tratta di una *e-mail* che garantisce ora e data di spedizione e di ricezione, provenienza (con una firma elettronica) e integrità del contenuto. D'ora in poi vale quanto una raccomandata con ricevuta di ritorno, costituisce una prova certa, costa molto meno e si può fare da casa.

**Firma digitale (art. 24)** È una firma elettronica che garantisce con sicurezza l'identificazione di chi firma e la sua volontà di firmare. Questa firma può sostituire per sempre sigilli, punzoni, timbri e dà validità giuridica a qualsiasi attestazione nei rapporti tra privati, tra privati e pubbliche amministrazioni e tra amministrazioni. Per rendere più sicura la firma elettronica questa deve essere certificata da un ente certificatore che risponda ai requisiti di legge e che si faccia garante dell'affidabilità della firma. Il codice regola tale certificazione in modo da conferire massima sicurezza alla firma elettronica, meglio di quanto ora avviene con la firma autografa.

**Documenti informatici (art. 20 e segg.; art. 40 e segg.)** Un documento informatico, sottoscritto con una firma elettronica certificata, ha sempre e dovunque la stessa identica validità del documento cartaceo ad ogni effetto di legge e deve essere accettato da qualsiasi soggetto pubblico o privato. È possibile quindi sostituire i documenti cartacei con documenti informatici, con considerevoli vantaggi in termini di tempo. Anche tutti i documenti contabili che la legge impone di conservare possono essere sostituiti da documenti informatici secondo le regole prescritte dal Codice e possono quindi essere conservati in forma digitale. Le pubbliche amministrazioni possono raccogliere tutti i documenti relativi a un procedimento in un fascicolo elettronico e devono comunicare ai cittadini interessati come accedervi, secondo quanto prescrive la legge sulla trasparenza (legge n. 241/90). Il Codice obbliga tutte le amministrazioni a gestire i documenti con sistemi informatici mediante il protocollo elettronico (certo e non modificabile, a garanzia di equità e di trasparenza, scoraggiando malcostumi e forme di corruzione) e l'archiviazione elettronica che consente enormi risparmi di spazio e soprattutto di rintracciare velocemente qualsiasi documento tra i miliardi di documenti conservati dalle pubbliche amministrazioni.

**Siti Internet delle PA (art. 53 e art. 54)** Quasi tutte le pubbliche amministrazioni hanno già i loro siti Internet, ma il Codice ne rende obbligatorie alcune caratteristiche fondamentali: i siti pubblici devono essere accessibili da tutti, anche dai disabili, reperibili, facilmente usabili, chiari nel linguaggio, affidabili, semplici, omogenei tra loro. I siti Internet diventano la "porta" privilegiata per entrare nelle pubbliche amministrazioni e sono tenuti quindi a riportare alcuni dati necessari per orientarsi: l'organigramma per sapere chi fa cosa; gli indirizzi *e-mail* a cui rivolgersi per ciascuna necessità; l'elenco dei servizi forniti in rete; l'elenco di tutti i bandi di gara; l'elenco dei procedimenti svolti da ciascun ufficio con la loro durata e il nome del responsabile. Dopo 15 anni la legge sulla trasparenza diventa quindi concreta. Non bisogna fare più domande per vedere lo stato di una pratica, sapere chi ne è il responsabile e quanto deve durare il procedimento: queste notizie devono essere a disposizione sul sito della PA interessata.

**Carte elettroniche (art. 66)** La carta di identità elettronica e la carta nazionale dei servizi diventano lo strumento chiave per razionalizzare e semplificare l'azione amministrativa e sono regolate dal Codice per essere uno strumento di autenticazione e di accesso ai servizi in rete della PA che sia universalmente valido in Italia, ma allo stesso tempo che contenga quei servizi che ciascuna amministrazione territoriale giudichi utili per i propri cittadini.

*La PA DIGITALE FUNZIONA MEGLIO*

Nella PA Digitale le amministrazioni cooperano tra loro e costituiscono una rete integrata di cui il Codice definisce principi e finalità:

**Federalismo efficiente (art. 14)** LA PA Digitale, integrata e interconnessa in rete, è il fattore chiave per costruire un federalismo efficiente. A tal fine il Sistema Pubblico di Connettività costituisce lo strumento che consente ai soggetti pubblici di dialogare, scambiare dati e documenti attraverso standard condivisi e canali sicuri: una rete fatta dalle reti delle pubbliche

amministrazioni, che mette in comunicazione PA centrale, PA locale, regioni e soggetti erogatori di servizi pubblici.

**Cooperazione (art. 12 e art. 63)** Le pubbliche amministrazioni utilizzano le tecnologie dell'informazione e della comunicazione garantendo l'accesso alla consultazione, la circolazione, lo scambio di dati e informazioni, l'interoperabilità, ossia la capacità dei sistemi informatici di scambiarsi e di usare mutuamente informazioni anche se diversi. Le pubbliche amministrazioni devono inoltre collaborare integrando i procedimenti di rispettiva competenza per rendere più efficienti i processi e agevolare i cittadini e le imprese nei loro adempimenti con la PA.

**Riorganizzazione gestionale e dei servizi (art. 15)** Il Codice lega strettamente l'utilizzo delle tecnologie al raggiungimento di obiettivi di efficacia, efficienza, economicità dell'attività amministrativa. Le pubbliche amministrazioni devono utilizzare le tecnologie in modo da razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, la modulistica, le modalità di accesso ai servizi. Non basta informatizzare: l'innovazione tecnologica deve essere chiaramente orientata a una maggiore efficienza interna ed efficacia dei servizi resi a cittadini e imprese.

**Gestione informatica dei procedimenti (art. 41)** Con il Codice nasce il fascicolo informatico. Le pubbliche amministrazioni devono gestire i procedimenti utilizzando le nuove tecnologie e possono raccogliere in un "fascicolo digitale" atti e documenti relativi a un procedimento anche se prodotti da amministrazioni diverse. In questo modo si accelerano tempi e procedure interne, con maggiore efficienza, minori costi per la pubblica amministrazione e maggiore trasparenza per i cittadini.

**Trasmissione informatica dei documenti (art. 45 e segg.)** Le amministrazioni possono comunicare e trasmettere documenti tra di loro in tempo reale. Il Codice dà piena validità giuridica all'utilizzo della posta elettronica nella comunicazione tra uffici pubblici. Anzi è lo strumento con cui di norma le amministrazioni devono comunicare. Comunicazioni, atti e documenti trasmessi per *e-mail* tra uffici pubblici sono validi ai fini del procedimento amministrativo in tutti i casi in cui è possibile accertare la provenienza e cioè se sono siglate con la firma digitale, oppure con protocollo informatico o trasmessi con posta certificata.

**Disponibilità dei dati (art. 50)** Le pubbliche amministrazioni devono rendere disponibili all'utilizzo da parte di altre amministrazioni i dati di cui sono in possesso, attraverso le tecnologie informatiche e telematiche. Ciascuna amministrazione titolare di dati è tenuta a renderli accessibili, nell'ambito del Sistema Pubblico di Connettività, ad altri soggetti pubblici che ne fanno richiesta per lo svolgimento dei propri compiti istituzionali.

**Basi di dati di interesse nazionale (art. 60)** Il Codice individua come basi di dati di interesse nazionale un insieme di informazioni, omogenee per tipologia e contenuto, come ad esempio gli archivi delle anagrafi, che, sebbene siano possedute da pubbliche amministrazioni diverse, sono necessarie ad altre pubbliche amministrazioni per lo svolgimento dei propri compiti. Le basi di dati di interesse nazionale costituiscono un sistema informativo unitario che deve essere gestito, nel rispetto delle competenze dell'amministrazione che possiede i dati, garantendo l'allineamento delle informazioni e l'accesso da parte delle amministrazioni interessate nell'ambito del Sistema Pubblico di Connettività. È questa novità introdotta dal Codice che renderà possibile, ad esempio, passare dall'autocertificazione alla de-certificazione: eliminare cioè la richiesta di un gran numero di certificazioni da parte delle pubbliche amministrazioni.

*LA PA DIGITALE COSTA MENO*

La pubblica amministrazione nel suo complesso già spende cifre considerevoli in nuove tecnologie (circa 1.300 milioni di € la PA locale e circa 1.800 milioni di € la PA centrale e gli Enti non economici) e ha dotato quasi tutti i dipendenti (91% dei posti "informatizzabili") di un posto di lavoro in rete, ma a tale sforzo spesso non si è accompagnato un incremento effettivo di efficienza e quindi un risparmio nei costi di funzionamento. Il Codice crea le condizioni per realizzare una PA che sia più efficiente, elimini gli sprechi e in definitiva costi meno.

**Azzeramento dei certificati (art. 42)** Sono 35 milioni i certificati prodotti annualmente dalle pubbliche amministrazioni con un costo per i cittadini di circa 13,50 € per ciascun certificato. La PA digitale potrà praticamente azzerare il numero dei certificati necessari attraverso la trasmissione dei documenti tra amministrazioni e la condivisione dei database. I cittadini e le imprese potrebbero risparmiare oltre 400 milioni di €.

**Uso della posta elettronica (art. 6 e art. 45 e segg.)** Si sono stimati in 31 milioni i messaggi di posta elettronica inviati tra pubbliche amministrazioni e nei contatti di queste con l'esterno e in 18 € il risparmio ottenuto per messaggio rispetto alla gestione di un messaggio di posta fisico. Il Codice, riconoscendo piena validità giuridica alle comunicazioni per via telematica, pone le basi per un incremento di tale numero e soprattutto per una sostituzione quasi totale della vecchia trasmissione cartacea.

**Archivi digitali (art. 43 e art. 44)** Con il Codice la pubblica amministrazione senza carta diventa realtà. Tutti gli atti, i dati, i documenti, le scritture contabili ed anche la corrispondenza prodotti o riprodotti in maniera digitale secondo le regole che garantiscono la conformità agli originali hanno la stessa validità giuridica di documenti cartacei e devono essere conservati in archivi informatici. Grazie alla conservazione digitale, si riducono tempi e costi di ricerca dei documenti, ma anche i costi di gestione e manutenzione degli archivi: processi più veloci, risparmi di spesa per le amministrazioni, enorme recupero di spazi prima occupati da ingombranti archivi cartacei.

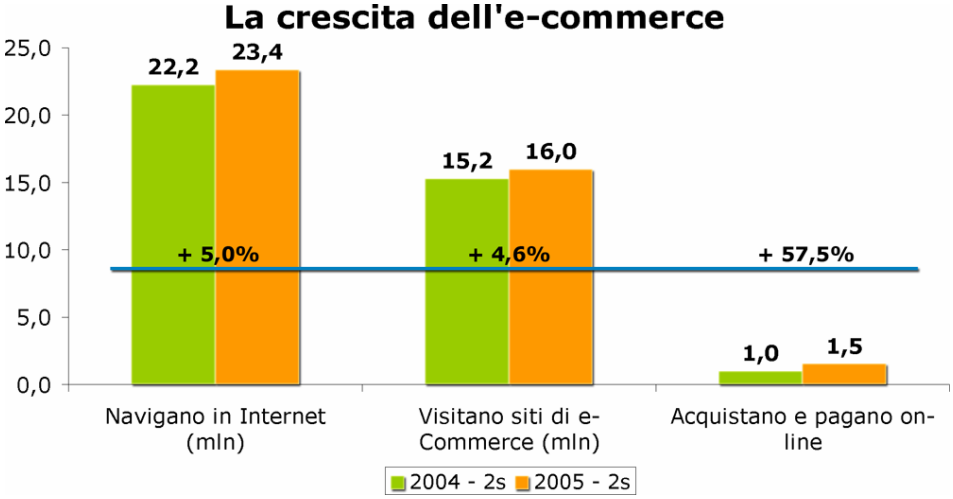
**Conferenze dei servizi *on-line* (art. 41)** Quando un qualsiasi procedimento pubblico (una licenza, una nuova opera pubblica, un evento, ecc.) coinvolge più amministrazioni, per semplificare il suo svolgimento viene indetta una "conferenza dei servizi" a cui partecipano responsabili di tutti gli enti interessati. Ora il Codice prevede la possibilità che queste conferenze si svolgano *on-line*, evitando viaggi, spese di trasferta, perdite di tempo e quindi con un notevole risparmio di denaro e una maggiore velocità.

**Riuso delle tecnologie (art. 69 e art. 70)** Il Codice istituisce la banca dati dei programmi informatici riutilizzabili, un elenco di programmi applicativi di proprietà pubblica. Prima di acquisire nuove applicazioni tecnologiche le pubbliche amministrazioni devono verificare se vi sono soluzioni riutilizzabili, che sono cedute in maniera gratuita dalle amministrazioni titolari. Il processo di riuso abbatte i costi degli investimenti in tecnologie e aiuta anche le amministrazioni con minore capacità di spesa ad acquisire tecnologie innovative. In questo modo tutte le amministrazioni, dalle più grandi alle più piccole, potranno erogare servizi avanzati a cittadini e imprese.

**Sportelli per le imprese (art. 10)** Gli sportelli unici per le attività produttive diventano telematici: devono riorganizzarsi per gestire i procedimenti e le attività interne in maniera informatica, acquisire istanze da parte delle imprese ed erogare i servizi attraverso Internet e posta elettronica. Per ottenere una maggiore efficienza e per risparmiare risorse il Codice prescrive forme di coordinamento tra le varie amministrazioni interessate che permetterà alle imprese di trovare ovunque una procedura omogenea. A livello centrale nasce il registro informatico degli adempimenti amministrativi di competenza delle amministrazioni centrali, nell'ambito però di una rete integrata di servizi gestiti dagli sportelli sul territorio (art. 11).

## 1.4. Altri operatori economici: sviluppo dell'*e-commerce*

Secondo un'indagine dell'Osservatorio e-Committee, nel secondo semestre 2005 oltre un milione e ottocentomila navigatori italiani hanno fatto acquisti *on-line*: essi rappresentano il 7,8% dei 23,4 milioni di navigatori italiani nel semestre e l'11,4% dei 16 milioni che hanno visitato siti di *e-commerce*.




L'84,6% degli acquirenti *on-line* (1.538 mila individui) ha pagato con carta di credito, il 40,7% ha pagato *off-line*, il 25,3% con entrambe le modalità. Gli acquirenti *on-line* che hanno pagato con carta di credito sono aumentati del 57,5% rispetto allo stesso periodo del 2004. Il *trend* di crescita dei "pagatori elettronici" registra quindi tassi molto superiori a quelli relativi alla crescita complessiva della Rete, benché i valori assoluti siano ancora contenuti: l'*e-commerce* cresce, anche se complessivamente non è ancora un comportamento diffuso.

Sempre leader dell'*e-payment* in Italia il settore dei viaggi *on-line*: il 35% degli acquirenti *on-line* ha acquistato un viaggio o un biglietto aereo o ferroviario. In valore assoluto gli acquirenti del settore sono oltre 750 mila, con un incremento del 23,7% rispetto al primo semestre. Accanto ai viaggi, gli acquirenti *on-line* comprano computer e apparecchiatura elettronica (22%), ricariche telefoniche (9%), libri (6%), oltre che contenuti digitali (5%) e stampe digitali.

Il "Sales Convertion Rate" (SCR), il tasso di conversione all'acquisto, è dell'11,4% sul totale dei siti di pagamento: ciò significa che, su 100 navigatori che accedono a un sito di *e-payment,* 11,4 concludono la transazione.

## 1.5. Il fattore abilitante: la fiducia degli utilizzatori

L'esperienza dell'*e-payment* mette in luce come esista una relazione diretta tra la fiducia nei confronti della sicurezza del canale e l'utilizzo evoluto/dispositivo dello stesso.

In particolare è possibile osservare come a un uso estremamente diffuso della Rete come strumento di raccolta di informazioni sugli acquisti non corrisponda un altrettanto esteso ricorso all'*e-commerce* e, soprattutto, ai pagamenti elettronici. Da un'indagine dell'Osservatorio emerge chiaramente che tale fenomeno è principalmente dovuto a una carenza di fiducia nella Rete ed in particolare nei livelli di sicurezza legati al processo di pagamento.

Benché i problemi e i disservizi riscontrati dagli *e-shopper* riguardino principalmente l'ambito logistico (36% "il pacco è arrivato in ritardo", 27% "il corriere non mi ha trovato e ho dovuto recuperare il pacco", 23% "il prodotto è arrivato un po' rovinato"), o comunque legato alla relazione con l'esercente (34% "annullata parte dell'ordine per indisponibilità del prodotto"; 18% "l'oggetto era diverso da come descritto"), due potenziali *e-shopper* su tre rinunciano all'acquisto *on-line* perché non si fidano a comunicare il numero della propria carta in Rete.

Inoltre, secondo un recente rapporto di Gartner relativo al mercato statunitense, oltre il 42% degli utilizzatori della Rete dichiara che i timori relativi agli attacchi informatici influenzano i loro comportamenti di acquisto. Tale studio sostiene che l'effetto negativo sulla fiducia dei consumatori dovuto alla diffusione di fenomeni di furto di identità elettronica contribuirà a ridurre la crescita dell'*e-commerce* di 1-3 punti percentuali entro il 2008.

Questo atteggiamento culturale può essere di fatto esteso a tutti gli altri ambiti di utilizzo dispositivo del web, dove il rischio percepito è ancora troppo elevato.

Una recente ricerca condotta da Forrester ha cercato di valutare la correlazione esistente tra il grado di fiducia dei consumatori europei nella sicurezza dell'Internet *banking* e la domanda dei servizi bancari *on-line*. È emerso innanzitutto che coloro che dichiarano di avere un grado più elevato di fiducia nella sicurezza dei sistemi di *banking on-line* sono in maggior misura titolari di conti *on-line*. Risulta inoltre che le motivazioni che portano alla scelta di non attivare un conto *on-line* sono riconducibili nel 40% dei casi ai timori connessi con la sicurezza, mentre risultano essere assai meno decisivi altri fattori apparentemente importanti, quali la scarsa conoscenza del canale (dichiarata dal 19% del campione), la sua complessità d'uso (7%) oppure la mancanza di assistenza di personale (11%).

Gli utenti hanno inoltre dichiarato quale più importante fattore incentivante per aprire un conto *on-line,* o per incrementare l'operatività a distanza, la garanzia da parte della banca della massima sicurezza del canale (34% del campione).

Le risposte raccolte confermano, infine, che la percezione della sicurezza dei servizi *on-line* è migliore nei paesi con un maggior grado di utilizzo degli stessi: così in Germania, Olanda e, soprattutto, Svezia, dove la quota di conti *on-line* è assai elevata, gli utenti mostrano preoccupazioni molto minori per la sicurezza dei dati immessi via Internet rispetto agli utenti dell'Italia, della Francia e della Spagna, dove è più bassa la propensione al *banking on-line*.

# 2. ANALISI DEL FENOMENO DEL FURTO DI IDENTITA' ELETTRONICA TRAMITE INTERNET

## 2.1. Il furto di identità elettronica

La diffusione crescente dei servizi disponibili in rete costituisce un fatto di rilevanza assoluta, con il quale un numero sempre maggiore di diverse realtà aziendali è chiamato oggi a confrontarsi. L'utilizzo di Internet per la fornitura di servizi moltiplica le opportunità di interazione tra il cittadino e l'ente che eroga tali servizi, sia esso pubblico o privato.

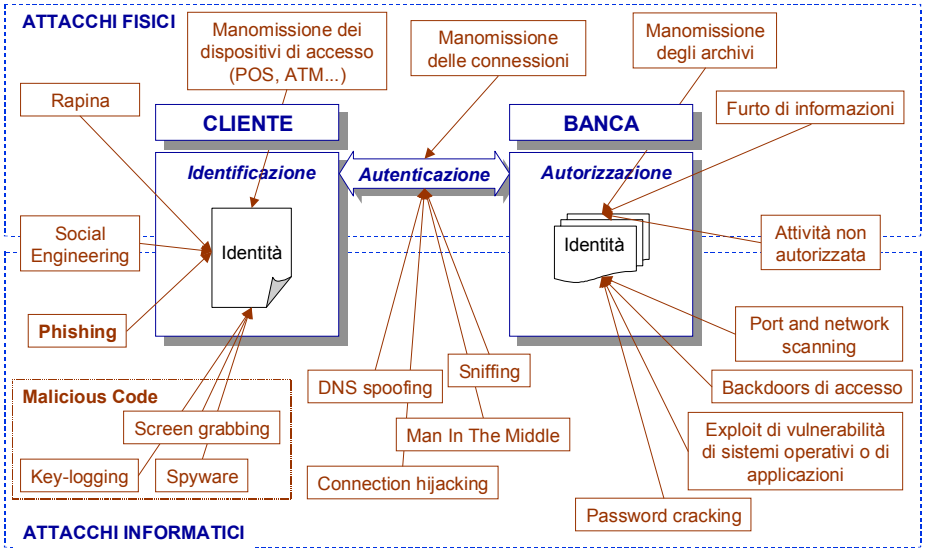
Il canale Internet pone, però, delle problematiche relative alla sicurezza delle operazioni che tramite esso avvengono che potrebbero essere percepite dall'utente finale come scarsa affidabilità dei servizi stessi.

In tale ottica, il furto dell'identità elettronica del cliente sul canale Internet costituisce una minaccia che può contribuire in larga misura a diminuire la percezione di affidabilità di un servizio che viene offerto in rete.

Nell'analisi dello scenario dei possibili attacchi mirati al furto dell'identità elettronica degli utenti dei servizi *on-line* di una banca, una prima distinzione va fatta tra attacchi fisici e attacchi informatici.

Gli attacchi fisici consistono principalmente in atti deliberati di manomissione delle strutture hardware che gestiscono la memorizzazione, il flusso e l'archiviazione delle credenziali digitali dell'utente, o in atti di furto e/o estorsione delle informazioni riservate. Una trattazione esaustiva di tali tipi di attacchi non rientra comunque negli scopi del presente documento.

Per attacchi informatici all'identità elettronica si intendono invece tutti quegli attacchi portati, tramite software eseguito da remoto, alle infrastrutture informatiche della banca, del cliente o della rete telematica che li connette, finalizzati a carpire le credenziali digitali dell'utente dei servizi *on-line*. A differenza dei precedenti non è necessaria la presenza fisica del frodatore nel luogo in cui la frode effettivamente avviene.




**Possibili scenari di furto di identità elettronica**

Le fasi durante le quali può essere lanciato un attacco, sia esso fisico o informatico, riguardano l'intero ciclo di utilizzo dell'identità elettronica dell'utente.

Sulla base di definizioni consolidate, si considerano tipicamente tre fasi, cui corrispondono tre differenti luoghi in cui le credenziali possono essere reperite: identificazione, autenticazione e autorizzazione.

La fase di identificazione corrisponde all'associazione delle credenziali digitali all'utente, che ne conserva la memoria; la fase di autenticazione corrisponde allo scambio di informazioni che avviene sulla rete telematica di connessione tra l'utente e la banca, circa l'identità di chi si sta accreditando; la fase di autorizzazione corrisponde alla verifica da parte della banca della correttezza dei dati di identificazione trasmessi dall'utente e alla successiva associazione a quest'ultimo dei privilegi di accesso alle operazioni *on-line*, sulla base di un archivio elettronico conservato dalla banca stessa.

Gli attacchi informatici che si rivolgono al cliente mirano quindi a reperire le informazioni di identificazione memorizzate dal singolo utente e sono pertanto portati in modalità molto massiva, nella speranza di estendere al massimo il numero dei possibili frodati.

Gli attacchi che mirano invece a intercettare le comunicazioni tra utente e banca fanno uso di appositi strumenti software in grado di frapporsi nel flusso di informazioni che viene scambiato, con la finalità di monitorarne i contenuti ed eventualmente dirottare o duplicare i dati di identificazione che transitano.

Da ultimo, gli attacchi che mirano agli archivi informatici delle banche sono tipicamente progettati per permettere all'*hacker* di penetrare all'interno dei data base degli istituti di credito, sfruttando vulnerabilità proprie o artatamente indotte nei sistemi informativi degli stessi.

L'ampia varietà delle azioni illecite attraverso le quali si può realizzare, con modalità sempre più insidiose e sofisticate, il furto dell'identità elettronica dovrebbe indurre coloro che offrono servizi e prodotti su rete a porre particolare attenzione ai processi operativi e tecnologici che presidiano le fasi della identificazione, autenticazione e autorizzazione dei propri utenti; la qualità e l'affidabilità dei servizi offerti su rete, infatti, tende sempre più a essere percepita e valutata dall'utente in relazione al grado di protezione assicurato alle proprie credenziali di autenticazione e quindi, in sostanza, alla tutela della sua identità elettronica.

## 2.2. Attacchi informatici mirati all'identità elettronica e possibili contromisure tecniche

In questo paragrafo si illustrano alcune tipologie di attacco attraverso le quali può realizzarsi il furto di identità elettronica a danno di utenti operanti *on-line*; si tratta di forme di attacco che vanno diffondendosi in connessione con lo sviluppo dell'offerta di nuovi servizi su rete e con l'utilizzo di tecnologie innovative.

Le definizioni di seguito riportate sono tratte dal rapporto CIPA "Il rischio informatico" (cfr. par. 3.3.) nonché dalla tassonomia elaborata in ambito ABI Lab.

### *Social engineering*

Tra le forme di attacco mirato all'identità elettronica dell'utente di servizi *on-line*, sta assumendo sempre maggiore rilevanza nel contesto informatico la c.d. *social engineering*. Con tale termine si intende una particolare tecnica psicologica che sfrutta l'inesperienza e, nella maggior parte dei casi, la buona fede degli utenti per carpire informazioni utili a portare successivi attacchi tecnologici ai sistemi.

Al di là dell'accezione apparentemente positiva della denominazione, la *social engineering* è una delle tecniche di attacco potenzialmente più dannose per la vittima.

Questo attacco ha di solito lo scopo di acquisire informazioni al fine di compiere azioni non consentite dai sistemi di controllo (quali avere accesso a locali o a dati riservati di pertinenza dell'azienda della vittima).

L'attacco è di solito condotto mediante un'impersonificazione, ovvero una sostituzione di identità o, nelle forme più sofisticate, con una pseudo-impersonificazione. In sostanza il soggetto che attacca si presenta, ad esempio mediante contatto telefonico, alla vittima prescelta - che ha accesso a informazioni utili all'attaccante o che svolge attività di controllo – e adotta, con finalità diverse, i seguenti comportamenti o atteggiamenti:

- assertivi: l'attaccante si finge un'altra persona in possesso dell'autorità necessaria a poter derogare alle regole[1] (impersonificazione) e porta il suo attacco usando come elemento di coercizione la minaccia implicita di danni che potrebbero derivare alla vittima o alla società se non viene soddisfatta la propria richiesta;
- empatici e spesso allusivi: l'attaccante induce la vittima ad attribuirgli un'identità o un'autorità che in realtà non è quella corretta (pseudo-impersonificazione);
- esplicitamente complici: l'attaccante induce la vittima a violare le regole di controllo nella convinzione che sia bene farlo (manipolazione);
- candidamente corruttivi: l'attaccante propone scambi tra quanto a lui interessa e benefici per la vittima.

Le prime tre modalità hanno in comune il fatto che l'attaccante costruisce situazioni nelle quali la vittima percepisce come lecita o conforme alle regole aziendali l'azione che è indotto a eseguire. Pertanto, questa tipologia di attacco ha buone probabilità di avere successo, considerata anche la frequente presenza di ulteriori circostanze favorevoli all'attaccante:

- scarsa conoscenza da parte della vittima delle responsabilità e dei ruoli aziendali, delle regole e delle prassi operative soprattutto in condizioni non ordinarie o di emergenza;

[1] Ad esempio si qualifica come una persona che ha una posizione notevolmente più elevata dell'interlocutore in un'altra azienda che ha rapporti con l'azienda cui appartiene la vittima.

- scarsa preparazione della vittima in tema di gestione della comunicazione (in modo particolare delle fasi conflittuali e delle interviste);
- sottovalutazione da parte della vittima delle conseguenze delle violazioni.

*Contromisure*

La possibile difesa da questa tipologia di attacco consiste nell'adozione di sistemi di formalizzazione delle richieste secondo gli standard aziendali e di controllo dell'autenticità dell'interlocutore.

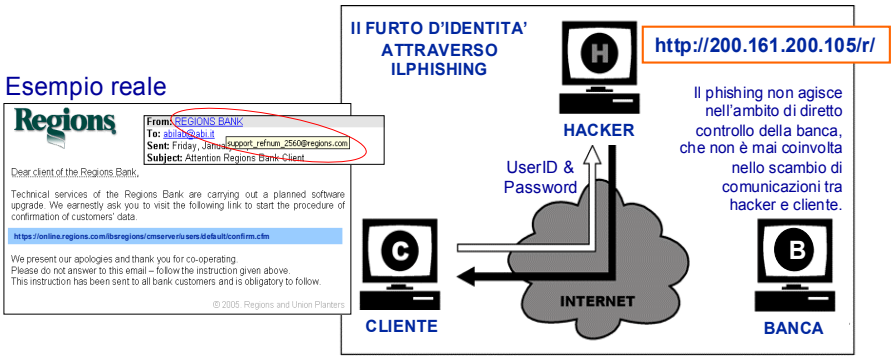
Considerato, inoltre, che gran parte dei danni è spesso causata dalla superficialità e da comportamenti non accorti all'interno dell'azienda, al fine di contenere i rischi di questo tipo di attacco può essere utile effettuare alcuni interventi, quali:

- stabilire norme volte a prevenire l'indebita pubblicizzazione, comunicazione o diffusione di dati e informazioni inerenti all'azienda, sia sul posto di lavoro, sia al di fuori dello stesso, anche in contesti non lavorativi[2];
- prevedere l'obbligo di segnalare qualsiasi contatto dall'esterno di natura sospetta;
- attuare un piano di formazione nei confronti di tutti i dipendenti e dei collaboratori esterni in merito a questo tipo di attacco, alle sue possibili conseguenze e alle relative contromisure;
- svolgere una specifica attività di formazione nei confronti della struttura di *help-desk/customer–care*.

### *Phishing*

Il *phishing* si può considerare una forma particolare di *social engineering*. Consiste nella creazione e nell'uso di *e-mail* e siti web ideati per apparire come *e-mail* e siti web istituzionali di organizzazioni finanziarie o governative, con lo scopo di raggirare gli utenti Internet di tali enti e carpire loro informazioni personali riguardanti il proprio account, quali le proprie *password* per accedere a servizi di *home banking* o il proprio numero di carta di credito. Tali informazioni vengono catturate dai *phishers* e vengono successivamente riutilizzate per scopi criminali, come frodi finanziarie o furti di identità.

Le *e-mail* apparentemente provengono da una banca o da una società emittente carte di credito e vengono composte utilizzando il logo, il nome e il *layout* tipico dell'azienda imitata. Tali *e-mail* invitano il destinatario a collegarsi tramite un *link* a un sito Internet del tutto simile a quello della banca e a inserirvi, generalmente attraverso una finestra *pop up* che si apre dallo stesso *link*, le informazioni riservate.




[2] Predisporre regole da adottare per il comportamento da tenere in viaggio di lavoro, in riunioni con esterni, in conferenze e convegni, nella vita privata circa il lavoro svolto.

Tipicamente, le *e-mail* di *phishing* contengono false dichiarazioni finalizzate a creare l'impressione che ci sia una minaccia immediata o un rischio di disabilitazione per l'account della persona cui sono destinate. Esempi in tal senso possono essere rappresentati da falsi annunci circa transazioni non andate a buon fine o false comunicazioni circa l'utilizzo da parte di un terzo della propria carta di credito o ancora circa un aggiornamento del data base aziendale da effettuare a opera degli utenti, pena l'annullamento del privilegio di accesso. Di più basso livello allarmistico, ma comunque molto diffuse, sono le *e-mail* che riguardano false attività promozionali, alle quali sarebbe possibile accedere solo comunicando i propri dati personali. Sono noti inoltre casi in cui le *e-mail* di *phishing* fanno riferimento a promesse di remunerazione immediata a seguito della trasmissione delle proprie credenziali.

Da un punto di vista tecnico le *e-mail* sono in formato HTML e contengono un collegamento nascosto al sito web contraffatto, che si presenta come se si riferisse al reale sito istituzionale (offuscamento dell'URL).

Lo strumento della posta elettronica è usualmente utilizzato dai truffatori con la logica dello *spamming*, secondo la quale migliaia di persone vengono inserite tra i destinatari, non curandosi dell'effettiva affiliazione dell'utente. La conseguenza di tale modalità di invio, però, è quella di dover utilizzare un testo del messaggio piuttosto generico, non specificato sul particolare profilo dell'utente che si sta tentando di adescare, fatto che costituisce un punto di debolezza di questo tipo di trappola.

*Contromisure*

L'Associazione Bancaria Italiana, tramite ABI Lab, ha evidenziato due decaloghi comportamentali, riportati nell'Allegato 1, da valutare al fine di contrastare l'espansione del fenomeno del *phishing*, uno rivolto alle banche e uno ai rispettivi clienti.

Il decalogo per le banche include provvedimenti che possono essere valutati dagli istituti al fine di ridurre per quanto possibile l'incidenza del *phishing* tra i propri clienti, potenziando il livello di comprensione del fenomeno. A tal fine potrebbe risultare opportuno:

- definire e divulgare *policy* per il contatto del cliente via *e-mail*, con particolare attenzione a comunicare se e in quali occasioni verranno richiesti via posta elettronica i codici personali di accesso ai servizi *on-line*;
- predisporre l'*help desk* clienti e i *call centre* per fornire informazioni circa eventuali attacchi subiti o in corso.

Da un punto di vista tecnico gli istituti di credito potrebbero valutare l'opportunità di:

- individuare meccanismi di monitoraggio delle transazioni per evidenziare eventuali comportamenti anomali;
- fornire strumenti di autenticazione maggiormente sicuri rispetto all'utilizzo di una singola *password* per l'accesso alle operazioni dispositive *on-line*.

Per quanto riguarda i clienti, nel relativo decalogo si sottolinea la necessità di:

- individuare l'autenticità di *e-mail* e siti che sembrano provenire da banche;
- mantenere aggiornati i software di protezione dei sistemi dai quali si effettuano le transazioni *on-line*;
- monitorare costantemente le operazioni dispositive effettuate.

Si evidenzia infine l'opportunità che l'utente acquisisca piena consapevolezza dell'importanza dei dati di accesso ai servizi *on-line*.

***Malicious code***

Questo termine, che ha come sinonimi "*malware"* e "*MMC (Malicious Mobile Code*)", si riferisce a quella famiglia di software che ha come obiettivo il danneggiamento, totale o parziale, o l'alterazione del funzionamento di un sistema informatico/telematico.

Alcune forme di codice malevolo, quali virus, *worm*, *trojan horse*, *mass mailing* e *mixed mmc*, sono in grado di autoinstallarsi, di autoriprodursi, di diffondersi, di determinare alterazioni del corretto funzionamento del sistema e anche di esportare i dati o di prendere il controllo del sistema stesso, spesso sfruttando vulnerabilità presenti nei software di sistema e/o applicativi.

Ai fini di perpetrare il furto di identità elettronica si possono evidenziare principalmente quattro classi di *malicious code*:

- ***Spyware***: programmi spia, in grado di raccogliere informazioni sul computer infettato e di inviarle anche tramite un proprio motore SMTP al destinatario fraudolento;
- ***Key-logging***: programmi in grado di attivarsi quando l'utente si connette a un sito di una banca o instaura una connessione protetta (https), scritti in modo che registrino i tasti contestualmente digitati dall'utente e che successivamente li rispediscano a un ignoto destinatario;
- ***Redirector***: codice malevolo scritto per reindirizzare il traffico Internet del computer infetto verso indirizzi IP differenti da quelli che si intendevano raggiungere;
- ***Screeen grabbing***: programmi che si attivano con modalità simili a quelle descritte per i *key-logger*, in grado di effettuare istantanee dello schermo dell'utente quando questo scrive informazioni sensibili sui siti di *home-banking* e di inviarle successivamente a ignoti tramite un motore SMTP interno.

<u>*Contromisure*</u>

Si richiamano di seguito le principali cautele da adottare per contrastare eventuali infezioni da *malicious code*:

- utilizzare solo software "certificato";
- assegnare al software solo i privilegi minimi necessari;
- innalzare e mantenere elevato il livello di sicurezza delle stazioni di lavoro;
- aggiornare tempestivamente i software anti-virus;
- applicare tempestivamente al software le correzioni (*patch)* rilasciate dai produttori;
- utilizzare specifici software antivirus in grado di rilevare i *malicious code* analizzando i flussi informativi in transito o sui sistemi;
- installare e mantenere aggiornato un *firewall* in grado di verificare il traffico in ingresso e in uscita dal proprio computer;
- sensibilizzare tutto il personale con riferimento ai rischi inerenti all'introduzione di software estraneo sulle postazioni di lavoro.

***Spoofing***

Lo *spoofing* non rappresenta un attacco nel senso stretto del termine, ma piuttosto una tecnica complementare a vari tipi di attacco. Consiste nel falsificare l'origine della connessione in modo tale da far credere di essere un soggetto/sistema diverso da quello reale.

Le principali tipologie di *spoofing* sono:

- ***User account spoofing***: consiste nell'utilizzo della *userid* e della *password* di un altro utente senza averne il diritto. Può essere attuato sfruttando comportamenti non corretti degli utenti o utilizzando strumenti quali *sniffing* e *password crackers*.
- ***DNS spoofing***: consiste nel sostituirsi a un *server* DNS[3] lecito nei confronti di un *client* che ha effettuato una richiesta a un *Name Server*. In particolare questa tecnica può essere utilizzata per reindirizzare il traffico indirizzato a un sito web istituzionale verso siti contraffatti, predisposti per carpire le credenziali digitali dell'ignaro navigatore.
- ***IP Address spoofing***: è l'attacco più diffuso. Si basa sul fatto che la maggior parte dei *routers* all'interno di una rete utilizzano solo l'indirizzo IP di destinazione e non quello di origine. Questo fa sì che un attaccante possa inviare dei pacchetti a un sistema bersaglio utilizzando *source* IP fittizi in maniera che le risposte siano inviate al falso IP indicato dall'attaccante.

*Contromisure*

La principale contromisura è costituita dall'utilizzo di tecniche crittografiche finalizzate all'autenticazione forte dei soggetti/sistemi coinvolti.

L'*IP Address spoofing* può essere limitato inserendo dei filtri sull'indirizzo IP sorgente a livello di *routers* e *firewall*.

### *Connection hijacking*

È un metodo di attacco che riguarda principalmente le transazioni o, comunque, i flussi di dati che transitano da un computer all'altro. Con tale violazione l'intrusore, dopo averne analizzato il flusso, si inserisce materialmente nella transazione alterandone il contenuto e riuscendo a operare con le credenziali di chi legittimamente ha iniziato la sessione.

*Contromisure*

Si basano generalmente sull'adozione di tecniche crittografiche, utilizzate sia per gestire la cifratura delle informazioni in transito sia per l'autenticazione dei poli terminali della transazione.

### *Man in the middle*

È un attacco che consiste nel dirottare il traffico generato durante la comunicazione tra due *host* connessi alla stessa rete verso un terzo *host*. Durante l'attacco il terzo *host* si frappone alla comunicazione tra i due *end-point* e intercetta il flusso di dati che si scambiano, riuscendo a far credere loro di essere il rispettivo legittimo interlocutore.

*Contromisure*

Come nel caso precedente, le possibili contromisure si basano generalmente sulla crittografia delle informazioni in transito e sulla mutua autenticazione dei poli terminali della transazione.

[3] Domain Name *Server*, ovvero *server* che traduce un nome di dominio nel relativo indirizzo IP.

### *Sniffing*

Consiste in un' operazione di intercettazione passiva delle comunicazioni per la cattura di dati; l'attaccante può riuscire a intercettare informazioni e dati di varia natura (*password*, messaggi di posta elettronica, ecc.). Normalmente questa attività di intercettazione illecita viene effettuata con l'ausilio di strumenti informatici denominati *sniffer* – talora posizionati illecitamente su un sistema di proprietà di un utente inconsapevole – che catturano le informazioni in transito nel punto in cui sono stati installati: si tratta in sostanza di hardware o software - legali e reperibili normalmente in commercio - analizzatori, in grado di intercettare, selezionare per protocollo, tradurre, visualizzare e memorizzare tutti i tipi di pacchetti in transito sulla rete.

*Contromisure*

Riconoscere la presenza di tali tipologie di strumenti non è sempre facile. Un rilevamento specifico può essere effettuato mediante:

- il controllo locale dello stato dell'interfaccia di rete dei singoli sistemi o la verifica della presenza di schede di rete configurate in modalità promiscua;
- l'utilizzo di software specializzati;
- l'analisi delle segnalazioni delle eventuali "sonde" utilizzate.

Per impedire un attacco della specie, si hanno a disposizione diverse possibilità:

- realizzazione di una topologia di rete sicura adottando tecniche di segmentazione;
- applicazione di funzioni crittografiche per rendere i dati intelligibili al solo legittimo destinatario;
- adozione di sistemi di autenticazione forte;
- preclusione della possibilità di configurare le interfacce di rete in modalità promiscua.

### *Password cracking*

Trattasi di programmi che effettuano a ripetizione tentativi di accesso ad aree riservate, provando ad accedere con *password* generate secondo algoritmi interni predefiniti.

*Contromisure*

Una possibile azione per rendere meno nocivo tale tipo di attacco consiste in una corretta gestione delle *password* di accesso a informazioni riservate. Risulta quindi opportuno:

- scegliere *password* che non siano facilmente individuabili (utilizzo di almeno otto caratteri, che includano maiuscole, minuscole, numeri e caratteri speciali);
- predisporre *policy* di aggiornamento periodico delle *password*.

### *Exploit di vulnerabilità di sistema o di applicazioni*

Si tratta dello sfruttamento di vulnerabilità note dei sistemi operativi delle banche o delle piattaforme software che esse utilizzano. Le vulnerabilità maggiormente critiche possono essere utilizzate dall'*hacker* per elevare i propri privilegi di accesso fino ad assumere in alcuni casi anche il controllo completo del sistema attaccato. In tali casi il furto delle identità elettroniche avviene garantendosi l'autorizzazione all'accesso all'archivio del sistema. Spesso

presuppongono la conoscenza della struttura dei sistemi informativi dell'azienda che si intende attaccare.

*Contromisure*

Una continua azione di *patching* delle applicazioni e dei sistemi utilizzati per gestire le informazioni riservate risulta necessaria per mantenere costantemente monitorato e protetto il perimetro delle vulnerabilità delle proprie infrastrutture informatiche.

### *Information gathering (network and port scanning)*

È il tentativo di rilevare indirizzi IP o porte TCP al fine di individuare quali servizi o sistemi siano presenti e attivi, per poter successivamente procedere a un tentativo di intrusione.

*Contromisure*

Adottare *firewall* di rete, *personal firewall* sulle stazioni di lavoro e strumenti di *intrusion detection* che consentano l'attivazione delle forme di reazione più appropriate.

### *Tecniche miste*

Per quanto riguarda il furto di identità elettronica, si sta affermando di recente la tendenza a utilizzare tecniche composte sulla base della combinazione di diverse tipologie di attacco, che sfruttano come base comune lo schema di *phishing* della falsa *e-mail* e/o del sito civetta, al fine di compromettere le funzionalità di connessione della postazione dell'utente finale.

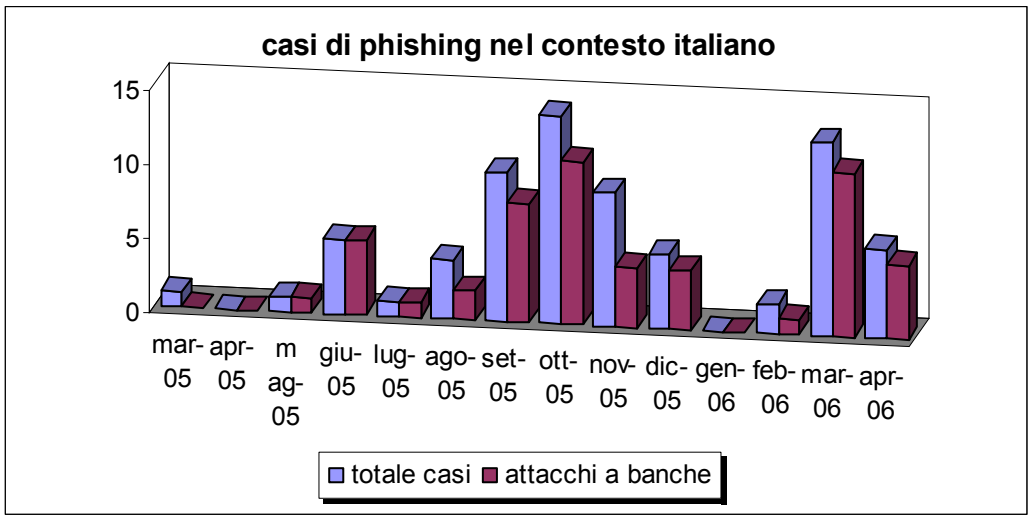
Esistono casi in cui il collegamento inserito nella *e-mail* fa riferimento a un sito "maligno" che funge da *man in the middle*, reindirizzando in *real-time* al sito istituzionale le informazioni che dal cliente gli vengono inviate e viceversa. In tali casi è anche possibile che il sito "maligno" controlli le finestre *pop up* del sito istituzionale, alterandole e carpendone il contenuto.

Infine si segnala la presenza di tecniche di compromissione dei *server* DNS, che vengono forzati ad attribuire al nome reale di un sito affidabile un indirizzo IP che si riferisce ad un sito "maligno", dirottando su quest'ultimo il traffico diretto al primo (fenomeno cui è stato dato il nome di *pharming*).

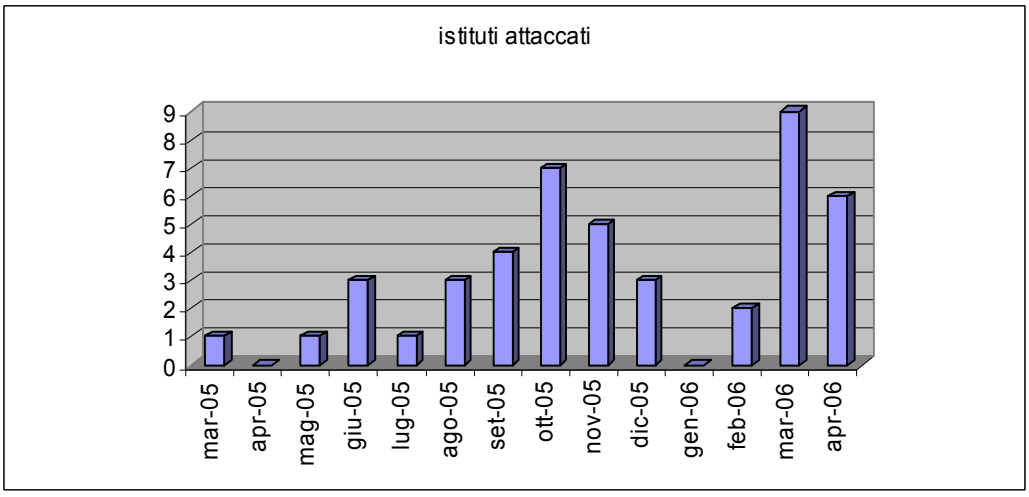
# 3. IL FURTO DI IDENTITA' ELETTRONICA IN ITALIA: LE INIZIATIVE GIA' AVVIATE

## 3.1. I primi casi di *phishing* nel contesto nazionale

Nel corso del 2005 grande attenzione è stata dedicata dal settore bancario al fenomeno delle frodi connesse al furto di identità elettronica. La relativa semplicità che è stata riscontrata nell'architettura di tali frodi, l'elevato numero di clienti attaccabili e il conseguente danno potenzialmente arrecabile alle imprese bancarie, sia sotto il profilo economico che di immagine, hanno fatto sì che venisse effettuato un approfondito monitoraggio dell'evoluzione dello scenario, per supportare l'ampia risonanza mediatica data al fenomeno con dati contestualizzati rispetto alla reale incidenza nel panorama italiano.




A seguito dei numerosi casi riscontrati nel contesto extra-nazionale, nel mese di marzo è stato riscontrato il primo attacco di *phishing* rivolto ai clienti di un ente italiano, Banco Posta.

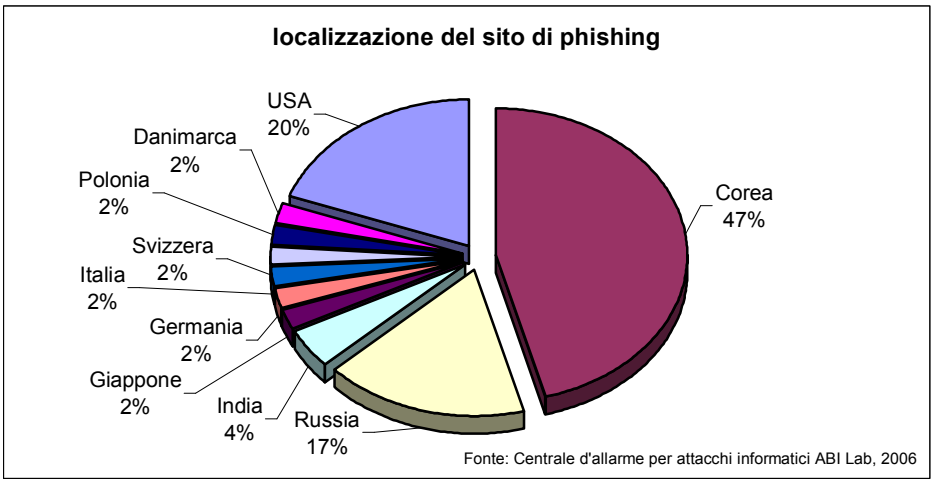



Sono seguiti nei mesi successivi diversi attacchi anche alle banche, culminati in un picco registrato nel mese di ottobre, al quale è poi seguito un progressivo decremento della numerosità dei casi, che ha portato a registrare nel mese di dicembre tre soli casi. La

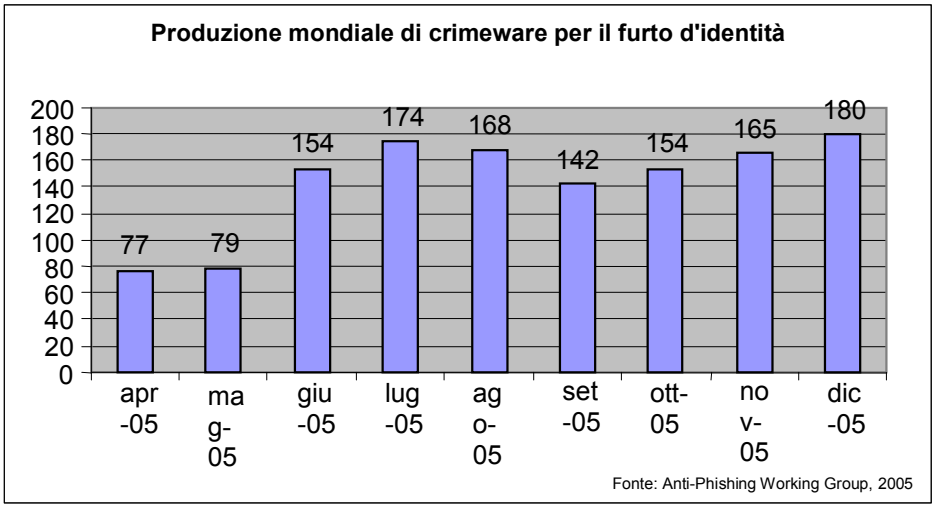
diffusione di modalità di attacco multiplo, che coinvolgessero in un solo invio di *e-mail* fraudolente più istituti di credito, ha fatto sì che, a partire dal mese di marzo 2006, si registrasse un nuovo incremento del numero di casi di *phishing* rivolti alla clientela di banche italiane, come è evidenziabile dai dati raccolti dalla Centrale d'allarme per attacchi informatici di ABI Lab.

Un andamento simile è stato registrato di conseguenza anche nel numero dei differenti istituti attaccati.

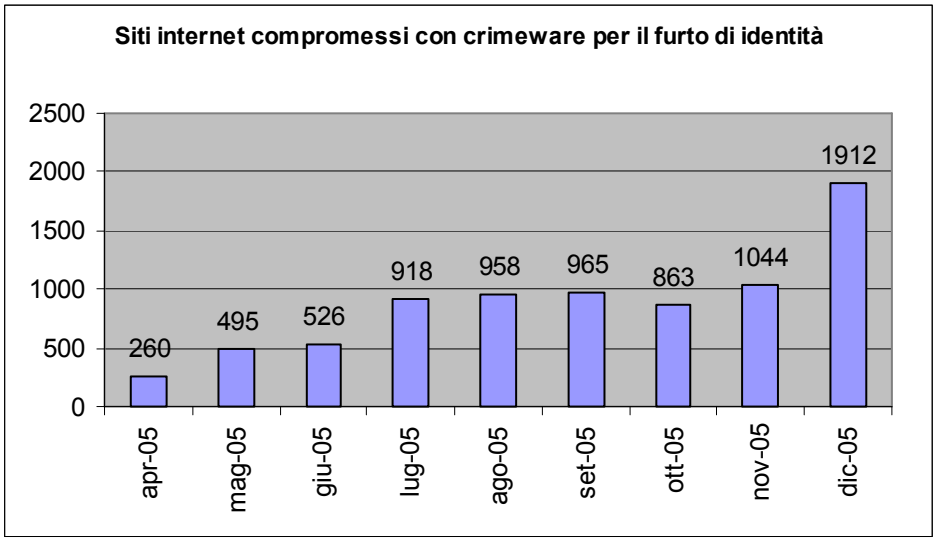
È stato rilevato come i *server* presso i quali sono installati i siti di *phishing*, inizialmente collocati in Italia, siano stati posizionati con sempre maggior frequenza in paesi esteri con cui la collaborazione delle Forze dell'Ordine potesse risultare maggiormente difficoltosa (es. Corea e Russia), fatto che ha inizialmente comportato un incremento del tempo di attività del sito fraudolento prima del suo oscuramento. Ciò nonostante, man mano che si sono resi disponibili strumenti di prevenzione e monitoraggio più affidabili e che si sono rafforzati i presidi di collaborazione tra le banche e le forze dell'ordine preposte alla repressione del reato, il tempo medio di attività dei siti di *phishing* è diminuito sensibilmente e al mese di dicembre si è attestato ben al di sotto delle 12 ore.




Si segnala, inoltre, come sia in aumento la diffusione di codice malevolo atto a perpetrare il furto di identità elettronica (*spyware*, key-logger,…) e con esso la produzione di appositi siti Internet per il *download* fraudolento del suddetto *malware*.



In particolare, sono stati segnalati nel contesto italiano *redirector* che, alterando il file *host* del computer infetto e altre informazioni a livello di DNS, reindirizzano il traffico Internet in uscita verso un DNS fasullo che, una volta interpellato, associa l'indirizzo IP del sito contraffatto alla richiesta che gli viene inoltrata.



## 3.2. Utilizzo delle credenziali digitali illecitamente sottratte

A seguito della raccolta delle credenziali digitali, fraudolentemente carpite ai clienti delle banche anche tramite phishing e/o key-logging, sono state rilevate a oggi due modalità di utilizzo delle identità elettroniche rubate.

La prima consiste nell'effettuare bonifici dai conti dei clienti che hanno ceduto le credenziali su un conto corrente aperto da poco tempo presso la stessa banca e nel tentare di ritirare quasi immediatamente le somme ivi pervenute, recandosi di persona in filiale. In alcuni casi, inoltre, il conto corrente che ha ricevuto detti bonifici è risultato essere un conto estero.

La seconda modalità, più insidiosa e meno tracciabile, consiste nel coinvolgere nel giro di denaro clienti da tempo affiliati a una struttura bancaria. Tali clienti vengono contattati telefonicamente o via e-mail e a essi viene proposto di rendere disponibile il proprio conto corrente per un'operazione di tramitazione di denaro a favore di persone o organizzazioni impossibilitate a ricevere denaro mediante semplice bonifico. Se accettano, essi ricevono un bonifico sul proprio conto e sono tenuti a ritirare l'importo ricevuto e a effettuare un successivo versamento in contanti (tramite agenzie internazionali di trasferimento di denaro) a favore di non meglio precisate compagnie estere, che celano la reale identità del frodatore. In cambio della loro disponibilità viene offerta la possibilità di trattenere sul proprio conto una percentuale dell'importo (es. 10%), fatto che può implicare anche la possibilità di complicità volontaria nelle azioni fraudolente da parte del cliente che fa da tramite.

## 3.3. Le iniziative del sistema bancario

***Iniziative ABI***

Il danno maggiore che le banche rischiano di dover fronteggiare, di fatto, risiede in una diminuzione della fiducia da parte degli utenti dei servizi *on-line*, che va a incidere direttamente sull'immagine aziendale. In considerazione di ciò, sono state attivate numerose iniziative di prevenzione, anche a livello di sistema bancario italiano.

L'Associazione Bancaria Italiana presidia la tematica del furto di identità elettronica (e in particolare del *phishing*) mediante le attività della Centrale d'allarme per attacchi informatici, costituitasi in seno ad ABI Lab nel 2003.

Le iniziative avviate rispondono all'esigenza espressa dal sistema bancario nazionale di un monitoraggio continuativo dell'evoluzione delle diverse tipologie di minacce, al fine di poter offrire la miglior risposta, in termini sia di efficacia della soluzione sia di prontezza.

Le modalità operative della Centrale si articolano principalmente su tre canali.

*Rapporti con le Istituzioni*

- mantenimento di un rapporto agevolato di comunicazione e di reciproca collaborazione con la Polizia Postale e delle Comunicazioni[4], a seguito della firma della 'Convenzione per la prevenzione dei crimini informatici nel sistema bancario', sottoscritta da ABI e Ministero dell'Interno a febbraio 2004;
- partecipazione all'*EU Fraud Prevention Expert Group*, relativamente al sottogruppo *Identity Theft, E-Fraud and Phishing*, che ha lo scopo di valutare l'opportunità di disporre di strumenti legislativi comuni per combattere le attività della criminalità organizzata legate al furto di identità;
- partecipazione al gruppo di lavoro 'Gestione delle Emergenze e degli Incidenti', attivato presso il Ministero delle Comunicazioni e rivolto alle infrastrutture critiche nazionali, con lo scopo di condividere le principali modalità di collaborazione e coordinamento tra gli IRT e i CERT che ciascun soggetto ha singolarmente predisposto.

*Approfondimento e Analisi*

- convocazione periodica di un tavolo tecnico formato da banche e aziende ICT, che periodicamente analizza i *trend* degli attacchi informatici subiti dalle banche, focalizzando l'attenzione sulle tematiche di maggior rilievo;
- attivazione di un'Unità di Crisi Attacchi Informatici, composta dalle principali banche, in stretto contatto e frequentemente convocate, finalizzato a monitorare l'evoluzione di particolari minacce e a definire rapidamente azioni congiunte di risposta;

[4] Il Servizio di Polizia Postale e delle Comunicazioni costituisce l'organo centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni. Il Servizio opera a livello periferico attraverso i Compartimenti di Polizia Postale e le Sezioni provinciali, avvalendosi di risorse distribuite sul territorio, sia investigative sia tecniche. Al Servizio sono affidate le seguenti competenze:

- prevenzione e repressione dei reati postali;
- studio, analisi e contrasto dei crimini informatici ovvero dei reati commessi attraverso l'uso di mezzi di comunicazione ad alta tecnologia quali, ad esempio, le violazioni del diritto d'autore, le frodi e pedofilia on-line;
- formazione specialistica del personale;
- instaurazione di relazioni internazionali finalizzate allo studio dei fenomeni criminali e alla collaborazione investigativa.

- attività di ricerca tramite un monitoraggio continuativo dello scenario della sicurezza informatica e delle frodi su Internet, con l'ausilio dei partner tecnologici di ABI Lab, allo scopo di evidenziare criticità o approfondimenti da sottoporre al tavolo tecnico.

*Comunicazione*

- invio di allarmi e segnalazioni su frodi informatiche, epidemie di virus e vulnerabilità dei sistemi a una lista di contatto costituita da più di 160 diversi destinatari, tra banche e intermediari finanziari;
- pubblicazione del materiale di ricerca e dei documenti prodotti dal tavolo tecnico nella *knowledge base* del portale www.abilab.it, accessibile a tutti i consorziati;
- aggregazione delle segnalazioni prodotte internamente e delle segnalazioni riportate dalle aziende partner di ABI Lab tramite la costituzione di un portale web sulla sicurezza informatica, raggiungibile a partire dal sito di ABI Lab.

Le analisi svolte dal tavolo tecnico in collaborazione con la Polizia Postale e delle Comunicazioni hanno permesso di inviare una prima comunicazione sul *phishing* alla lista di contatto già a dicembre 2004, che poi è stata diffusa all'intero sistema bancario nazionale tramite una circolare tecnica ABI nel mese di gennaio 2005. Nella comunicazione sono stati allegati i due citati decaloghi comportamentali (cfr. par. 2.2), uno rivolto alle banche e uno ai rispettivi clienti, da seguire al fine di ridurre l'espansione e contenere i danni arrecati dal fenomeno del *phishing*.

È stata inoltre realizzata una *survey* esplorativa su un campione di banche, rappresentative del 51% del totale attivo nazionale, per verificare lo stato di evoluzione e di diffusione del *phishing* in Italia. I risultati hanno messo in evidenza come tale fenomeno fraudolento sia a uno stato primordiale di evoluzione rispetto al livello di sensibilizzazione sul tema ormai raggiunto dagli istituti di credito.

La prima segnalazione e i relativi decaloghi sono stati integrati e rafforzati con una nuova comunicazione diffusa alla lista di contatto in data 23 maggio 2005, riguardante il verificarsi dei primi episodi di *phishing* rivolti alla clientela di banche italiane.

La collaborazione con la Polizia Postale e delle Comunicazioni ha permesso inoltre di definire in questo contesto un processo per la richiesta di primo intervento delle forze dell'ordine in caso di sospetta attività illecita, da attivare prescindendo dalla procedibilità del crimine per il quale si richiede l'intervento stesso. È stata diffusa ai partecipanti del gruppo di lavoro una lista di contatti corrispondenti ai referenti regionali della Polizia Postale e delle Comunicazioni che garantiscono un presidio operativo per le banche in tema di criminalità informatica.

Nell'ambito dell'Unità di Crisi Attacchi Informatici è stato poi possibile condividere le caratteristiche comuni delle operazioni dispositive effettuate mediante le credenziali illecitamente sottratte e definirne le peculiarità fraudolente. Ciò ha portato alla realizzazione di una ulteriore segnalazione che è stata diffusa alla lista di contatto in data 22 giugno 2005, relativa all'esecuzione di bonifici anomali a seguito di furto di identità elettronica.

Sempre nel contesto dell'Unità di Crisi Attacchi Informatici, sono stati inoltre comunicati gli indirizzi IP dai quali sono state riscontrate attività illecite o dai quali sono stati effettuati bonifici disconosciuti ed è stata costituita una *black-list* aggregata di indirizzi IP da monitorare ed eventualmente bloccare. Tale lista è stata diffusa al momento alle sole banche che hanno contribuito a comporla.

Il presidio offerto dalla Centrale d'allarme per attacchi informatici sulla tematica del furto di identità elettronica ha a oggi permesso alle banche di allestire le difese necessarie con tempestività ed efficienza ben prima che il fenomeno fraudolento si verificasse e che quindi giungessero le segnalazioni di allerta da parte delle forze dell'ordine.

Al proprio interno, le azioni di risposta delle banche si sono concretizzate nella realizzazione di *policy* aziendali per la gestione delle emergenze e nell'implementazione di opportune contromisure tecnologiche per il monitoraggio, la prevenzione e il contenimento degli attacchi di *phishing* rivolti alla propria clientela.

In considerazione però del fatto che il fenomeno del *phishing* agisce all'esterno della struttura della banca, gran parte delle iniziative predisposte dagli istituti di credito è andata nella direzione di aumentare il livello di sensibilizzazione della propria clientela sulle caratteristiche della frode, tramite opportuni piani di comunicazione, arrivando anche a estendere, tramite il proprio sito, alcune misure minimali di sicurezza sulla postazione dalla quale l'utente effettua operazioni di *home-banking*.

In proposito, nell'ambito del tavolo tecnico della Centrale d'allarme per attacchi informatici è stata ribadita l'importanza che potrebbe avere la realizzazione da parte dell'utente stesso di misure minime di sicurezza per la postazione che utilizza per le operazioni *on-line*. Il gruppo di lavoro ha dato la disponibilità a condividere le iniziative già singolarmente attivate nei confronti delle rispettive clientele, in modo che sia possibile aggregare una base di esperienze comuni di cui pianificare tempi e modalità di divulgazione.

### *Il rapporto CIPA sul rischio informatico*

Utili elementi ai fini dell'analisi delle possibili contromisure da adottare per prevenire "furti" di credenziali di autenticazione a danno dei clienti delle banche sono contenuti in diverse parti del rapporto CIPA "Il rischio informatico" (novembre 2004), elaborato da un apposito gruppo di lavoro formato da esponenti della Banca d'Italia, dell'ABI, di alcune banche, della SIA e dei Centri Applicativi (il rapporto è disponibile sul sito della CIPA, www.cipa.it).

In particolare, il rapporto, dopo aver analizzato il processo di gestione del rischio informatico all'interno delle banche e gli aspetti organizzativi della sicurezza informatica, fornisce indicazioni sulle cautele da adottare nello sviluppo delle applicazioni e nella gestione dei sistemi e delle reti. Si tratta di aspetti molto importanti poiché errori o omissioni commessi in queste attività possono determinare vulnerabilità dei sistemi informativi aziendali, ivi inclusi quelli operanti per il *banking on-line*, suscettibili di generare minacce alla riservatezza, all'integrità e alla disponibilità delle informazioni generate e raccolte nell'operatività aziendale. Viene quindi effettuata una ricognizione delle contromisure da adottare nella fase di acquisizione e/o sviluppo dei programmi, nonché delle attività di monitoraggio e di controllo degli accessi, finalizzate alla sicurezza, da prevedere nella gestione dei sistemi operativi e delle reti (cap. 6).

Il rapporto dedica poi specifica attenzione agli aspetti di sicurezza connessi con l'utilizzo di Internet e delle tecnologie innovative, soffermandosi su talune delle più insidiose modalità di attacco che si vanno diffondendo di pari passo con lo sviluppo dell'offerta di nuovi servizi informatici e con l'utilizzo delle tecnologie innovative (cfr. sopra, par. 2.2). Per ognuna di tali tipologie di attacco vengono indicate le possibili contromisure; vengono anche fornite alcune raccomandazioni per la gestione degli incidenti di sicurezza (cap. 7).

## 3.4. Le iniziative della Pubblica Amministrazione

I fattori di crescita ed evoluzione dell'ICT, con particolare riguardo allo sviluppo di reti di interconnessione tra i sistemi informativi, e la sua diffusione in uno spettro di applicazione sempre più vasto impongono una rigorosa attenzione agli aspetti legati alla sicurezza. Questo fattore vale per tutto lo scenario delle applicazioni informatiche e di telecomunicazioni, in particolare per le pubbliche amministrazioni. La diffusione dell'utilizzo delle reti presenta ormai fattori di crescita esponenziali e le applicazioni su reti aperte sono diventate una realtà non più esclusiva del mondo imprenditoriale, bensì una necessità gestionale e di colloquio delle PA, tra loro, con le imprese, con i cittadini. Internet sta divenendo sempre più il sistema di scambio di informazioni, di accesso alle grandi banche dati, di esecuzione di transazioni e disposizioni finanziarie, di sviluppo di attività professionali. Parallelamente si sta evidenziando anche la sua fragilità. In questo scenario la sicurezza informatica deve essere un elemento fondamentale nel processo di avvicinamento, tramite la tecnologia, del cittadino e delle istituzioni private alla pubblica amministrazione.

### *Il Comitato Tecnico Nazionale*

Il Decreto interministeriale, siglato il 24 luglio 2002 fra il Ministro per l'Innovazione e le Tecnologie e il Ministro delle Comunicazioni, ha istituito il "Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni". I compiti di questo Comitato sono molteplici. Essi vanno dalla predisposizione di un piano nazionale alla definizione dell'apposito modello organizzativo; dalla formulazione di proposte in materia di certificazione e valutazione all'elaborazione di linee guida riguardanti la formazione dei dipendenti; dalla riduzione delle vulnerabilità dei sistemi informatici alla garanzia di integrità e affidabilità dell'informazione pubblica. La Direttiva emessa il 16 gennaio 2002 dal titolo "Sicurezza informatica e delle Telecomunicazioni nelle PA statali" (G.U. 22 marzo 2002, n. 69) raccomanda a tutti gli organi pubblici l'adozione di misure minime di sicurezza, tali da garantire la tutela del loro patrimonio informativo. La distribuzione delle prime carte di identità elettronica ha reso necessario affrontare i problemi di sicurezza connessi all'erogazione in rete dei servizi al cittadino; mentre all'interno del circuito della RUPA la garanzia del rispetto di adeguati livelli di sicurezza è delegata al fornitore del contratto dell'interoperabilità, il circuito cittadino - pubblica amministrazione necessita della definizione di linee guida, ovvero di regolamentazione, per i processi di identificazione e di autenticazione in rete.
Il Comitato, presieduto da un componente del CNIPA, ha concluso la stesura del primo documento di riferimento per la sicurezza ICT nella PA, "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni (ICT) per la Pubblica Amministrazione". Il documento contiene le indicazioni atte a permettere alla PA la redazione del Piano nazionale della sicurezza e la predisposizione del modello organizzativo nazionale di sicurezza ICT.

### *Il GovCERT.IT e il Centro di Formazione*

La sicurezza rappresenta un elemento essenziale nell'organizzazione e gestione dell'infrastruttura ICT di ciascuna amministrazione, sia al suo interno sia in relazione ai servizi resi a cittadini e imprese e, più in generale, nel piano di attuazione dell'e-gov. Nel corso del 2004 il CNIPA ha costituito al proprio interno - in attuazione del progetto "Sicurezza ICT nella PA" proposto dal Comitato nazionale - l'unità di prevenzione e supporto alla PA per le problematiche connesse alla gestione degli attacchi e incidenti informatici,

denominato "GovCERT", in analogia con i CERT governativi di altri paesi europei. GovCERT.IT è inoltre il nome del dominio Internet dell'infrastruttura tecnologica dell'unità. L'obiettivo prioritario del GovCERT.IT è di supportare le PA ai fini della prevenzione attraverso un servizio di carattere informativo che sarà successivamente arricchito da un servizio di sorveglianza e di raccolta dati: CERT-PA (*Computer Emergency Readiness Team*) e il Centro di formazione e sensibilizzazione sulla sicurezza ICT nella PA. Quest'ultimo avrà sede presso l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI) e si avvarrà per il suo funzionamento anche della collaborazione della Fondazione Ugo Bordoni. Il GovCERT.IT e il Centro di formazione collaboreranno su una serie di temi di reciproco interesse.

A queste proposte va aggiunto l'impegno del Comitato Tecnico Nazionale di promuovere incontri periodici con le istituzioni, *Internet provider* e rappresentanti del mondo bancario, assicurativo, finanziario per individuare linee comuni nel campo della sicurezza informatica.

## 3.5. IL QUADRO NORMATIVO

Il *phishing* si presenta come un fenomeno decisamente complesso da un punto di vista legale.

Nell'ordinamento giuridico italiano non esiste alcuna legge che preveda una definizione del *phishing* né che prescriva una qualche sanzione a carico dei *phisher*.

In prima approssimazione l'azione del *phishing*, volta a carpire i dati personali degli utenti titolari di conti correnti bancari o postali *on-line* in modo da potersi introdurre telematicamente all'interno degli stessi conti al fine di sottrarne denaro, costituisce un illecito di natura sia civile che penale.

Con riferimento alla natura penale, di maggiore rilevanza, vengono immediatamente in rilievo:

- l'illecito trattamento di dati personali in violazione del D.Lgs. n. 196/2003 (Codice privacy);
- il reato di truffa (art. 640 del codice penale) nei confronti dei soggetti colpiti, titolari dei conti correnti;
- la frode informatica, di cui all'art. 640 ter del codice penale, introdotto dalla legge n. 547/93 (legge istitutiva dei cosiddetti reati informatici o *computer crimes*) nei confronti dell'istituto di credito per l'intervento senza diritto all'interno del sistema informatico successivo al furto delle credenziali di identità.

In taluni casi potrebbe essere contestato anche l'ulteriore reato di accesso abusivo a un sistema informatico, previsto dall'art. 615 ter del codice penale (anch'esso introdotto dalla legge n. 547/93)

L'applicazione di una o più delle diverse ipotesi di reato, nonché delle eventuali aggravanti, ha particolare rilevanza, non solo in funzione, come è ovvio, del differente regime sanzionatorio, ma anche della diversa procedibilità: d'ufficio o su querela del soggetto offeso.

Molti procedimenti penali, che recentemente hanno visto interessate diverse unità operative della Guardia di Finanza e della Polizia Postale, sono in corso. Indubbiamente le sentenze della Magistratura che concluderanno tutte le operazioni investigative legate al *phishing* svolte negli ultimi tempi contribuiranno a delineare con la dovuta autorevolezza i contorni del fenomeno.

Solo allora si potrà esprimere un giudizio sull'efficacia dell'attuale quadro normativo e valutare, quindi, l'eventuale necessità di un intervento legislativo più specifico.

# 4. IL FURTO DI IDENTITA' ELETTRONICA IN ALCUNI DEI PRINCIPALI PAESI INDUSTRIALIZZATI

Il presente capitolo contiene una panoramica sulla diffusione dei fenomeni di furto di identità elettronica in alcuni dei principali paesi industrializzati [5], con particolare riferimento al settore bancario e finanziario, nonché sulle iniziative di contrasto adottate a livello istituzionale, associativo e di singoli operatori [6].

Al fine di inquadrare correttamente tali fenomeni nei rispettivi contesti di operatività, vengono anche fornite sintetiche informazioni sullo stadio di sviluppo, in ciascun paese, dei servizi di *e-commerce*, Internet *banking* ed *e-government*.

Sullo specifico tema delle iniziative di contrasto avviate, nel rinviare al paragrafo 4.3 per una descrizione di dettaglio, si evidenziano le seguenti linee di azione riscontrabili, in linea di massima, nei diversi paesi:

- le iniziative adottate a livello istituzionale si sostanziano nel rafforzamento della legislazione punitiva in materia di reati informatici e nell'ampliamento delle fattispecie criminose previste, al fine di ricomprendervi il furto di identità elettronica; in diversi paesi sono state costituite, nell'ambito delle autorità di polizia, unità specializzate nella lotta alla criminalità informatica;
- le autorità di vigilanza creditizia e finanziaria svolgono, in genere, attività volte a stimolare gli operatori a dotarsi di sistemi di sicurezza adeguati e aggiornati, a sviluppare un'azione preventiva nella protezione dei dati, ad adottare coerenti *policy* in materia di sicurezza informatica; di particolare interesse è l'iniziativa dell'organo di vigilanza bancaria francese che ha affidato a un comitato tecnico interbancario il compito di definire requisiti minimali dei siti Internet bancari dedicati all'*home banking*, da utilizzare quale punto di riferimento per un'eventuale certificazione dei siti stessi;
- le associazioni bancarie indirizzano le loro attività prevalentemente verso la formulazione di raccomandazioni e *best practices* dirette agli operatori, la raccolta di informazioni sui casi rilevati e la loro successiva diffusione agli associati e agli organi di polizia, la promozione di iniziative di sensibilizzazione e di educazione degli utenti;
- gli interventi intrapresi dai singoli operatori riguardano, da un lato, la sensibilizzazione della clientela attraverso messaggi di posta elettronica, avvisi sui siti, opuscoli distribuiti allo sportello o inviati via posta, dall'altro lato, l'adozione di contromisure tecnologiche e operative, quali i sistemi di accesso ai servizi *on-line* basati sulla "autenticazione forte", tramite l'utilizzo di *smart card* o di *token*, e su un doppio livello di autenticazione.

[5] Trattandosi di fattispecie nuove nell'ambito del cybercrime, non esistono nei paesi analizzati rilevazioni statistiche sistematiche e omogenee sulla loro diffusione e sull'entità delle connesse frodi subìte dagli operatori e dalla clientela.

[6] Per la redazione del presente capitolo, ci si è avvalsi della collaborazione delle Delegazioni estere della Banca d'Italia.

## 4.1. Dati di contesto

### *Dati su e-commerce ed e-banking*

*Stati Uniti*

Negli Stati Uniti l'*e-commerce* è in continuo sviluppo, in termini di volumi di affari, qualità dei servizi offerti, integrazione con gli altri canali distributivi. Recenti stime[7] valutano i ricavi dell'*e-commerce* nel 2004 in circa 118 miliardi di dollari, con una crescita del 25% rispetto all'anno precedente. Le previsioni per gli anni a venire continuano a evidenziare tassi di crescita a due cifre, tra il 15 e il 20 per cento l'anno.

Secondo la stessa fonte, nel 2004 le vendite *on-line* negli USA sarebbero state pari a circa il 2% del totale delle vendite al dettaglio[8] (contro l'1% circa nel 2000), percentuale che si prevede in ulteriore crescita nei prossimi anni.

Nel 2004 circa 31 milioni di famiglie americane avrebbero utilizzato servizi di banking *on-line* (erano 12,5 nel 2000), numero che si stima possa crescere fino a 45 milioni nel 2007.

Un ultimo dato può rendere l'idea delle potenzialità dei mercati *on-line* in un paese come gli USA: nel 2004 il numero di utenti statunitensi di servizi di telecomunicazione a banda larga era pari a circa 37 milioni (circa 12,8 ogni 100 abitanti), su un totale di 118 milioni nei paesi OCSE; circa il 30% degli utenti mondiali di servizi del genere risiede pertanto negli Stati Uniti[9].

*Regno Unito*

Secondo un'indagine dell'APACS[10] (*Association for Payment Clearing Services*) sull'*e-commerce* e sull'Internet *banking*, quasi la metà della popolazione adulta del Regno Unito, pari a circa il 70% del totale degli utenti Internet, ha effettuato nella seconda metà del 2004 acquisti *on-line*. Nello stesso periodo del 2002 tale percentuale era pari al 51%.

Nel 2004 la spesa con carte di credito su Internet si è ragguagliata a 12 miliardi di sterline, pari all'11% delle spese personali effettuate tramite carte di credito. La spesa *on-line* tramite carte di debito è stata pari a 5 miliardi di sterline nel 2004, raggiungendo il 3% del totale della spesa con tale strumento.

Secondo la stessa indagine, 14,8 milioni di adulti hanno utilizzato servizi di Internet *banking* nella seconda metà del 2004, quasi un adulto su tre. Rispetto allo stesso periodo del 2001 il numero di utenti è più che raddoppiato. La metà di tali utenti usa servizi *on-line* almeno una volta alla settimana e uno su dieci se ne avvale quotidianamente. I correntisti che utilizzano servizi di Internet *banking* hanno una media di 1,7 conti correnti su banche diverse, paragonata a 1,5 conti correnti di coloro che non usano l'Internet *banking*.

*Germania*

L'*e-commerce* in Germania appare in crescita: nel 2004 il suo fatturato ha raggiunto i 202,6 miliardi di euro (per il 90% riguardanti il segmento B2B) con un aumento del 76% rispetto al

[7] Fonte: eMarketer

[8] Dato che non tiene conto del settore viaggi; si stima che, includendo quest'ultimo settore, fortemente presente sul web, si avrebbe un incremento di uno/due punti percentuali del rapporto in esame.

[9] Fonte: OECD Broadband Statistic 2004.

[10] L'APACS è un'associazione di categoria che riunisce le istituzioni che forniscono servizi di pagamento; oltre alla materia dei mezzi di pagamento, essa segue le problematiche connesse con le frodi su carte di credito.

2003. Si prevede un'ulteriore forte espansione: per il 2008 si stima un fatturato pari a circa 670 miliardi di euro, di cui circa 89 miliardi verso clientela privata.

Secondo un sondaggio condotto dall'associazione delle banche private tedesche (*BdB*) nel maggio 2004, il 34% dei tedeschi (28% nel 2003) ha già effettuato acquisiti via Internet, mentre il 41% (31% nel 2003) accede a Internet per effettuare confronti di prezzo.

L'utilizzo della carta di credito per il pagamento degli acquisti eseguiti via Internet è ancora limitato (20% degli utenti), a causa soprattutto delle perplessità riguardo alla sicurezza (un utente su tre non ritiene sicuro l'utilizzo della carta di credito via Internet).

L'*e-banking* ha trovato ampia diffusione in Germania: le associazioni bancarie hanno stimato che nel 2003 i conti *on-line* erano circa 40 milioni. I dati pubblicati dall'Ente federale di statistica (*Destatis*)[11] evidenziano che il 33% degli utenti privati di Internet e il 70% delle imprese accede ai servizi di *e-banking*. Tuttavia solamente un terzo dei conti *on-line* dei privati è usato con regolarità. Tra i motivi di un tale ridotto utilizzo riveste un ruolo rilevante quello della sicurezza: secondo un sondaggio condotto dal BdB, più del 40% degli intervistati è dell'avviso che l'*e-banking* non sia molto sicuro.

*Francia*

In Francia il volume d'affari realizzato dall'*e-commerce*, attestatosi secondo alcuni studi a 5,5 miliardi di euro nel 2004 (senza tener conto delle transazioni *business to business* e dei servizi bancari e finanziari), costituirebbe circa il 3% del commercio al dettaglio non alimentare del paese.

La percentuale di utenti di Internet che hanno effettuato acquisti *on-line* è passata dal 10% del 1999 al 52% del giugno 2004; in valore assoluto, la popolazione degli acquirenti tramite Internet si attesterebbe a circa 9,5 milioni di individui. Sul lato dell'offerta, peraltro, sarebbe ancora prevalente la funzione di semplice "vetrina" dei siti aziendali, con conseguente scarso peso della funzione commerciale: quest'ultima in Francia è "attivata", con o senza pagamento *on-line*, dal 14% dei siti (a fronte di un 20% per i siti tedeschi e italiani)[12].

Quanto ai servizi bancari *on-line*, per i quali non esiste una raccolta sistematica di dati, secondo alcuni studi di società di consulenza circa 7 milioni di utenti Internet francesi hanno visitato almeno una volta un sito di una banca nel mese di dicembre 2003 (il dato alla fine del 2002 era di 5 milioni)[13].

*Paesi Bassi e Belgio*

Nei Paesi Bassi e in Belgio le dimensioni del mercato dell'*e-commerce* e dell'*e-banking* riflettono il diverso grado di diffusione di Internet nei due paesi. Oltre la metà della popolazione olandese utilizza Internet, a fronte di una quota pari al 40% in Belgio. Anche il numero di persone che hanno effettuato, nel 2004 , almeno un acquisto *on-line* è più elevato in Olanda che in Belgio (rispettivamente il 28,8% e il 21,6% della popolazione). In entrambi i paesi il valore degli acquisti su Internet è fortemente cresciuto negli ultimi anni. Nei Paesi Bassi esso è aumentato di oltre cinque volte tra il 2000 e il 2004, raggiungendo 1,68 miliardi di euro. In rapporto al fatturato complessivo degli esercizi di commercio al dettaglio, il valore

[11] I dati *Destatis* sono tutti tratti dalla pubblicazione: Destatis (2005), *Informationstechnologie in Unternehmen und Haushalten 2004*.

[12] Fonte BNP Paribas, citata dal Rapporto 'La société de l'information en France en 2004'.

[13] Dati elaborati da Mediamétrie/Net ratings.

degli acquisti *on-line* rimane tuttavia modesto, attestandosi nel 2004 al 2,1% (0,5% nel 2000). In Belgio, l'incidenza è meno della metà.

Secondo la banca centrale olandese (*De Nederlandsche Bank*, DNB), la diffusione dei servizi di Internet *banking* nei Paesi Bassi è tra le più elevate in Europa: nel 2004 il numero di utenti ha raggiunto i 6 milioni di persone, pari a oltre un terzo degli abitanti[14]. Per il Belgio stime effettuate sulla base dei dati relativi alle principali banche indicano l'esistenza di 1,5 milioni di abbonati ai servizi di *banking on-line* (meno del 15% della popolazione), di cui 1,2 milioni utenti regolarmente attivi[15].

*Giappone*

La diffusione di Internet in Giappone è in continua espansione; il numero di utenti viene attualmente stimato attorno agli 80 milioni (pari al 60,6 per cento della popolazione); circa il 60 per cento dei collegamenti a Internet avverrebbe tramite telefonia mobile.

L'*e-commerce* rappresenta una importante realtà. Sulla base delle informazioni più recenti diffuse dal Ministero dell'Economia, la dimensione del segmento *business to consumer* (B2C) era valutabile, a fine 2003, in una cifra corrispondente (al tasso di cambio attuale) a circa 33 miliardi di euro. Le prospettive future sono legate alla continua espansione e al perfezionamento dei sistemi di pagamento *on-line*, ma soprattutto dei sistemi di pagamento attivabili tramite telefoni cellulari.

Con riferimento all'*e-banking* – sebbene esso susciti una notevole attenzione nell'Organo di Vigilanza con riferimento ai profili della costituzione di Internet banks, della sicurezza informatica e dell'adeguamento tecnologico – non esistono al momento rilevazioni ad hoc sull'utilizzo del canale telematico da parte della clientela.

In Giappone coesistono due tipologie di intermediari bancari per i quali l'*e-banking* assume particolare rilevanza: le cosiddette *Net Banks*[16] (aziende di credito che forniscono i propri servizi prevalentemente attraverso il collegamento telematico) e le banche tradizionali (sia giapponesi sia straniere) che hanno affiancato portali di accesso via Internet ai consueti canali di distribuzione dei propri servizi.

La clientela delle banche ordinarie predilige comunque ancora il contatto diretto con la banca; l'utilizzo dell'Internet *banking* è maggiore da parte delle imprese. I privati – anche attraverso il collegamento via cellulare – effettuano principalmente accessi di tipo informativo e/o dispositivo, questi ultimi soprattutto con riferimento alle operazioni di compravendita di attività finanziarie.

### *Dati sulle amministrazioni pubbliche on-line*

Un recente studio condotto dalle Nazioni Unite sull'*e-government* in 191 paesi (*Global E-government Readiness Report 2004: Towards Access for Opportunity*) evidenzia come l'amministrazione pubblica statunitense sia la prima nel mondo per i servizi, di tipo sia informativo sia operativo, offerti *on-line*. Al secondo posto figura il Regno Unito, mentre tra gli altri paesi europei spiccano il 10° posto della Germania, il 12° del Belgio, il 16° dei Paesi Bassi.

[14] L'*e-banking* riveste notevole importanza per le banche olandesi anche come mezzo di penetrazione nei mercati esteri. L'esempio più noto è ING Direct, con oltre undici milioni di clienti in numerosi paesi avanzati, tra cui l'Italia.

[15] La stima è stata effettuata a partire dai dati forniti da quattro banche (Dexia, Fortis Banque, ING Belgium e KBC/CBC), che rappresentano circa l'82% del mercato bancario belga.

[16] Attualmente sono cinque: Ito-Yokado Bank, eBank Corp., The Japan Net Bank, Nippon Shinko Bank e Sony Bank.

Italia e Francia si collocano rispettivamente al 33° e al 36° posto (appena dopo il Giappone, 25°).

*Regno Unito*

La pubblica amministrazione nel Regno Unito può contare su circa 6.000 centri che forniscono servizi pubblici *on-line*. Questo risultato è frutto dell'azione svolta dal governo, a partire dal 1999, nel promuovere i servizi *on-line*, azione basata su tre pilastri: la "comprensibilità" del valore di tali servizi; l'"accessibilità" alle amministrazioni da parte dei cittadini; l'"affidabilità" dei servizi stessi, che ingeneri fiducia tra i consumatori e assicuri che questi ultimi siano in grado sia di fruirne pienamente sia di reagire a eventuali attacchi.

Le autorità di governo sono attente all'evolversi di questo settore: la *Prime Minister's Strategy Unit*, di concerto con il *Department of Trade and Industry*, ha recentemente pubblicato un rapporto dal titolo "*Connecting the UK: the Digital Strategy*". Tra le iniziative previste per aumentare la diffusione dei servizi pubblici *on-line* figura il c.d. *Digital Challenge*, un riconoscimento agli enti locali e ai loro partners, del settore pubblico o del settore privato, mirato a promuovere l'utilizzo "globale" della tecnologia informatica. Questa strategia aspira ad attrarre quel 49% degli utenti che ancora non utilizza servizi pubblici *on-line*. Secondo il rapporto citato, il 75% dei servizi della pubblica amministrazione è ormai disponibile elettronicamente[17].

*Germania*

Lo sviluppo dell'*e-government* appare essere in Germania non ancora particolarmente pronunciato, atteso che la disponibilità *on-line* copre il 40% dei venti più importanti servizi amministrativi.

Nel 2003 è stato definito un piano strategico per l'*e-government* (*Deutschland-On-line*), che prevede una serie di progetti volti all'individuazione di servizi amministrativi ad alta priorità, allo sviluppo delle infrastrutture e alla definizione di standard. È fissata inoltre una precisa tempistica, in base alla quale entro il 2008 tutte le amministrazioni pubbliche dovranno essere tra loro interconnesse e tutte le procedure amministrative adatte a essere offerte *on-line* dovranno essere disponibili via Internet.

Lo sviluppo dell'*e-government* dipenderà anche dal grado di diffusione e di accettazione della firma digitale, che allo stato attuale appare essere ridotto: secondo alcuni studi solamente il 14% delle amministrazioni pubbliche ha adottato la firma digitale, mentre pochi utenti, soprattutto imprese e professionisti, sfruttano tale modalità per il colloquio con la pubblica amministrazione. La limitata diffusione della firma digitale, non solo a livello di *e-government*, è dovuta soprattutto alla sua mancata standardizzazione, per cui per ogni singola applicazione è necessaria una diversa firma digitale. Per ovviare a tale problematica, gli enti pubblici stanno cooperando con imprese private per la definizione di uno standard comune (c.d. *Signaturbündnis*)[18].

[17] L'*On-line Center Network* della funzione pubblica inglese, costituito nel 2000, ha predisposto presidi su tutto il territorio nazionale per la formazione di base degli utenti. Attualmente l'affluenza presso questi centri è pari a circa 50.000 utenti a settimana.

[18] Un significativo impulso alla diffusione della firma digitale potrebbe provenire dalla realizzazione della carta di identità elettronica, che dovrà essere introdotta a partire dal 2007. Il progetto prevede di dotare tale carta, su richiesta, anche della funzione di firma digitale. Vi sono inoltre progetti per l'introduzione di una c.d. carta del cittadino (*Bürgerkarte*), che dovrà contenere non solo i dati relativi alla carta d'identità, alla patente e all'assicurazione malattia, ma anche i codici segreti per applicazioni *on-line*, tra cui l'*e-banking*.

*Francia*

Lo Stato francese ha destinato allo sviluppo dell'attività *on-line* della pubblica amministrazione circa 1,8 miliardi di euro per il quadriennio 2004-2007. Ad oggi, l'*administration electronique* riguarda più di 200 servizi, forniti attraverso circa 7.000 siti (+ 27% dal 2002). Il 90% dei formulari amministrativi è disponibile *on-line*. Gli incrementi di produttività legati all'introduzione dell'interfaccia elettronica sono stimati nell'ordine di 5-7 miliardi di euro nel 2007.

*Paesi Bassi e Belgio*

Un rapporto relativo alla situazione dei siti *on-line* della pubblica amministrazione nei Paesi Bassi indica che nel 2004 circa la metà dei servizi ai cittadini e alle imprese erano offerti anche su Internet, in netto aumento rispetto all'anno precedente; il governo si è posto l'obiettivo di raggiungere la quota del 65% entro il 2006.

Per quanto riguarda il Belgio, un'indagine campionaria svolta da una società di consulenza evidenzia che nel 2004 quattro quinti dei "navigatori" su Internet avrebbero consultato almeno un sito della pubblica amministrazione e un quinto avrebbe anche contattato l'amministrazione tramite *e-mail*. Tra i servizi che suscitano maggiore interesse vi è quello fiscale (*Tax-on-Web*), cui hanno fatto ricorso circa 125 mila cittadini belgi.

*Giappone*

La qualità e la tempestività dei servizi della pubblica amministrazione giapponese offerti sui canali tradizionali sono particolarmente elevate. Numerosi adempimenti, anziché essere compiuti presso gli sportelli, possono essere richiesti o effettuati anche via telefono; le relative risposte vengono fornite in tempi brevissimi.

Ciò contribuisce a spiegare l'esistenza di un'offerta di servizi *on-line* non particolarmente sviluppata; nella maggior parte dei casi, i portali web degli enti pubblici si limitano a riportare informazioni relative ai recapiti e all'organizzazione interna degli uffici.

Le principali istituzioni (es. Ministeri, Governo, sistema giudiziario) dispongono di un secondo sito in lingua inglese.

## 4.2. Diffusione dei casi di "furto di identità elettronica"

***Stati Uniti***

Negli Stati Uniti la *Federal Trade Commission* (FTC) ha calcolato che nel 2003 quasi dieci milioni di americani siano stati vittime del furto di identità elettronica, con un costo massimo stimato per le imprese e per i consumatori di 2,4 miliardi di dollari[19]. La FTC ha anche evidenziato che i reclami connessi con il furto di identità elettronica riguardano essenzialmente le carte di credito (26%), la telefonia e altre utenze (19%), le banche (18%), i servizi all'impiego (13%).

Dal 2003 il *Financial Crimes Enforcement Network* ha sottoposto a monitoraggio il fenomeno con riferimento al settore bancario e finanziario: un recente rapporto (giugno 2005) evidenzia come nel 2004 si siano registrati negli USA 15.491 casi di furto di identità contro i 3.165 rilevati nell'anno precedente.

***Regno Unito***

Dati statistici sulle frodi sono disponibili soltanto relativamente alle operazioni con carte. L'APACS ha recentemente condotto un'analisi[20] sulle frodi nel settore delle carte di credito e di debito e sulle relative perdite. Dall'indagine è emerso che tali perdite hanno registrato, tra il 2003 e il 2004, un aumento di circa il 20%, passando da 420 a 504 milioni di sterline. Nell'ambito di tali frodi quelle perpetrate tramite Internet sarebbero state pari a 117 milioni di sterline (23% circa del totale), di cui circa 12 milioni realizzate tramite tecniche di *phishing*.

Secondo l'APACS la crescita delle frodi sarebbe da imputare principalmente al fatto che le più avanzate misure di sicurezza ideate, essenzialmente basate sull'utilizzo della tecnologia del microchip e del PIN, non sono state ancora pienamente applicate.

***Germania***

Nel 2003 i casi di criminalità informatica denunciati agli organi di polizia sono stati circa 60.000, la maggior parte dei quali riguardanti la fattispecie di truffa mediante l'utilizzo illecito di carte di debito e relativo PIN (circa 36.000); in un centinaio di casi si è trattato di attacchi informatici volti a "spiare" dati.

Per quanto concerne l'*e-government*, non risulta che vi siano stati attacchi volti al furto di identità elettronica[21].

Il fenomeno del *phishing*, per il quale non vi sono dati statistici disponibili, ha avuto una certa diffusione in Germania a partire dal 2004 e avrebbe assunto dimensioni rilevanti nel 2005[22]. Da ultimo vengono resi noti anche casi di *pharming*.

Tuttavia i danni arrecati da tali attacchi, provenienti soprattutto dalla criminalità organizzata russa, sarebbero stati relativamente contenuti, atteso che è stato possibile revocare in tempo gran parte dei bonifici effettuati mediante l'utilizzo delle informazioni fraudolentemente acquisite. Nei casi in cui ciò non sia stato possibile, le banche hanno rimborsato le somme ai

[19] Studio effettuato dalle società di consulenza Truste e Gartner.

[20] APACS, *Card Frauds. The Facts*, 2005.

[21] Le autorità pubbliche pongono una grande attenzione alla sicurezza dei propri servizi di *e-government*. Ad esempio, con riferimento alla dichiarazione dei redditi *on-line*, è stato realizzato un programma che verifica l'autenticità dell'apposito software messo a disposizione dal Ministero delle Finanze per evitare alterazioni nel processo di *download*.

[22] Si registrerebbero circa due o tre attacchi di *phishing* a settimana. Finora tali casi si sono concentrati quasi esclusivamente sulle banche, tra cui soprattutto la Deutsche Bank e la Postbank.

propri clienti al fine di minimizzare i rischi di immagine connessi con un calo di fiducia nei confronti della sicurezza dell'*e-banking*.

Nei primi casi verificatisi, il trasferimento dei fondi avveniva su conti bancari extracomunitari, per cui era più facile revocare l'operazione per via dei tempi di regolamento relativamente lunghi. Successivamente sono stati posti in essere tentativi di *phishing* con l'utilizzo di conti bancari d'appoggio nazionali[23].

Secondo un sondaggio di opinione condotto nel 2005, l'89% degli intervistati è a conoscenza del rischio connesso con l'utilizzo illecito dei dati personali tra cui il *phishing*, mentre solamente il 46% lo considera un rischio elevato. Solo il 2% ha dichiarato di aver avuto esperienze con tale rischio[24].

***Francia***

L'*Office Centrale de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication* (OCLCTIC) costituito presso il Ministero degli Interni, che coordina gli sforzi di repressione contro questo tipo di fenomeni delittuosi, ha censito, per il 2004, circa 60.000 casi di cybercriminalità, tra i quali sono ricompresi quelli relativi alla falsificazione e all'uso illecito di carte di credito. Ad oggi non esistono statistiche specifiche sugli attacchi che utilizzano i brand delle banche per carpire la fiducia dei clienti. Da indagini condotte è risultato che nel giugno 2004 il 32% dei francesi non era convinto della sicurezza dei pagamenti *on-line* (48% nel 2001).

Il furto di identità elettronico é diventato, di recente, un argomento di grande attualità. Il 27 maggio 2005, infatti, migliaia di utenti di Internet avrebbero ricevuto una *e-mail* che simulava la provenienza da quattro delle principali banche francesi[25]. Il testo, redatto in lingua inglese, chiedeva ai destinatari di avviare un processo di identificazione con il pretesto di problemi incontrati nell'attivazione delle rispettive caselle postali. Il *link* presente nella mail avrebbe condotto l'utente alla *home* page di un falso sito bancario.

Non si tratta, in realtà, del primo caso di *phishing* registrato in Francia. Secondo notizie di stampa, l'organismo di polizia competente per questo genere di reati, la *Brigade d'enquêtes sur les fraudes aux tecnologies d'information* (BEFTI), ne aveva già registrati, per la sola area metropolitana di Parigi, quattro nel 2003 e altrettanti nella prima metà del 2004[26].

In ogni caso, al di là del clamore con cui i recenti casi sono stati riportati dagli organi di stampa, il fenomeno del *phishing* non sembra debba essere considerato una vera emergenza per la Francia. Tale opinione è confortata da due ordini di considerazioni: innanzi tutto, gli attacchi sembrano provenire da siti di paesi con scarsa familiarità con la lingua francese (es. Russia); in secondo luogo, gli utenti Internet francesi, a differenza di quanto si rileva per quelli dei paesi anglosassoni, mostrano una tendenza a non "aprire" le mail indesiderate e, quindi, a non rispondere.

[23] Ad esempio, in un caso, per il quale le forze di polizia tedesche sono potute intervenire effettuando una serie di arresti, gli inquirenti avrebbero accertato che una ditta russa si era dotata di una pluralità di conti d'appoggio nazionali sfruttando i conti bancari di residenti contattati mediante un'offerta di lavoro. Le persone contattate avrebbero dovuto mettere a disposizione i loro conti bancari, prelevando immediatamente le somme ricevute e trasferendole in Russia tramite bonifico per contanti, generalmente tramite operatori specializzati nei servizi di trasferimento di denaro all'estero, ricevendo un corrispettivo pari al 5-10% dell'importo delle operazioni effettuate.

[24] Cfr. TNS-Emnid (2005), *Sicherheit im Internet*, 18 maggio 2005.

[25] Si trattava di BNP Paribas, Société Générale, CCF e CIC

[26] La prima condanna per furto di identità perpetrato attraverso un falso sito web è stata pronunciata il 2 settembre 2004 dal Tribunale di Strasburgo, che ha inflitto un anno di prigione e 8.500 euro di multa a uno studente che aveva riprodotto il sito del Crédit Lyonnais, riuscendo a recuperare circa 20.000 euro da una dozzina di clienti della banca. Nel 2004 si erano inoltre verificati tentativi di frode ai danni di clienti della Société Générale e della BRED (gruppo Banques Populaires), attraverso "cavalli di troia" installati sui computer delle vittime, in grado di attivarsi al momento delle connessioni ai siti delle banche.

***Paesi Bassi e Belgio***

Anche nei Paesi Bassi e in Belgio non esistono dati puntuali sulle frodi informatiche a danno delle banche e dei loro clienti[27].

Alcune informazioni possono essere ricavate dalle comunicazioni effettuate dalle associazioni bancarie dei due paesi. Secondo quella olandese (*Nederlandse Vereniging van Banken*, NVB), non sarebbero finora emersi significativi problemi per la sicurezza dell'*e-banking*. Vi sarebbe stato finora soltanto un caso di rilievo, che non avrebbe peraltro determinato alcuna perdita presso i clienti .

In Belgio, l'associazione bancaria (*Association belge des banques*, ABB) ha segnalato un solo caso di *phishing* nel 2004[28]. Anche secondo l'autorità belga di vigilanza sugli intermediari finanziari (*Commission bancaire, financière et des assurances*, CBFA) il fenomeno del *phishing* è stato finora marginale.

Non sono invece disponibili informazioni quantitative sugli attacchi subiti dalla pubblica amministrazione. L'evento più importante è accaduto nell'ottobre del 2004, quando diversi siti web dell'amministrazione olandese sono rimasti bloccati, per ben cinque giorni, a seguito dell'attacco da parte di un gruppo di *hackers*. L'azione è stata intrapresa non per realizzare guadagni illeciti, ma in segno di protesta nei confronti delle politiche del governo[29].

***Giappone***

Le banche giapponesi denunciano un numero significativo di utilizzi fraudolenti di carte di credito, soprattutto di carte per il prelievo presso ATM, che vengono clonate con frequenza o sottratte con sotterfugi al titolare[30].

L'esposizione al rischio di furto di identità dei consumatori giapponesi può ritenersi in termini potenziali abbastanza elevato. Infatti, sebbene esistano taluni fattori che contribuiscono in parte a mitigarlo rispetto ad attacchi dall'estero (es. complessità della lingua[31]), si ritiene che i consumatori giapponesi abbiano una "soglia di attenzione individuale bassa" rispetto alla possibilità di venire in qualche modo tratti in inganno o di subíre il furto di identità. Non fa parte della cultura giapponese, infatti, prestare eccessiva attenzione alla tutela di dati e informazioni personali. Ciò va ascritto, almeno in parte, al forte senso di "onore e rispettabilità" che pervade la società giapponese.

Con specifico riferimento al *phishing*, esso sarebbe in crescita, ma si tratterebbe di un fenomeno relativamente recente sul quale non sono sinora state raccolte sufficienti evidenze. Il primo tentativo di *phishing* in Giappone è stato rilevato nel dicembre 2003, mentre nel novembre 2004 è stata rilevata la prima frode informatica che ha determinato danni di natura economica per la vittima.

---

[27] È stato contraffatto il sito di Postbank, una banca detenuta dal gruppo ING con oltre un milione di clienti *on-line*.

[28] L'attacco è stato condotto ai danni del gruppo Fortis. Di recente è stato reso noto anche un tentativo di frode ai danni della filiale belga di Citibank. Alcuni clienti avrebbero perso somme comprese tra i tre e i cinque mila euro; secondo la stampa il numero di casi si aggirerebbe intorno alla decina, mentre la banca coinvolta ne indica soltanto quattro. Un cliente avrebbe già ottenuto da Citibank il rimborso della perdita subita, il che costituisce il primo caso di risarcimento per danni a seguito di *phishing* in Belgio. All'inizio dell'anno, tre clienti di Citibank Belgium erano stati vittime di *spyware*, perdendo somme di importo limitato (non superiori a 1.500 euro secondo quanto riferito dalla banca).

[29] Al termine delle indagini, cinque *hackers* sono stati giudicati colpevoli; si tratterebbe della prima sentenza per il reato di *hacking* nei Paesi Bassi.

[30] Secondo le informazioni diffuse dall'Associazione bancaria giapponese nel 2004, nel periodo 2000 - 2003 si sono registrati, oltre che frodi tramite l'utilizzo di carte clonate o sottratte per un valore superiore a 300 milioni di euro, 3.872 casi in cui il prelievo in danno della clientela è stato effettuato in data posteriore alla notifica, da parte del titolare, dello smarrimento della carta. Tale ultima notazione evidenzia l'esistenza di consistenti margini di miglioramento delle procedure di controllo e prevenzione delle banche.

[31] La configurazione di "falsi" siti web in lingua giapponese non è facile da realizzare all'estero.

Inoltre, si sono registrati diversi episodi di sottrazione di dati personali. Il portale Internet maggiormente colpito risulterebbe *Yahoo Japan*[32]. Sono stati già chiusi quattro siti "esca" (non in lingua giapponese) configurati in modo da trarre in inganno i consumatori.

Alcuni eventi hanno interessato il sistema finanziario: nel novembre 2003, a uno dei maggiori intermediari mobiliari (*UFJ Securities*) sono stati sottratti i dati personali di 11.000 clienti. Nel febbraio 2005 il gruppo bancario UFJ ha dichiarato che otto clienti hanno subìto un danno economico complessivamente pari a 1,5 milioni di yen (circa 11.300 euro) per aver comunicato *on-line* i propri dati personali.

Il 14 giugno 2005 è stato effettuato a Osaka il primo arresto di un individuo che gestiva un falso sito web (configurato come *Yahoo Japan's Internet Auction*)[33].

[32] Nel gennaio 2004 i dati personali di 6,6 milioni di clienti di Yahoo Japan sono stati sottratti da una persona che ha ottenuto i codici di accesso da un ignaro dipendente della società. Tale dipendente svolgeva mansioni di tipo "temporaneo", ma disponeva, a causa di evidenti carenze nella configurazione delle procedure di sicurezza, dei codici di accesso agli archivi della clientela.

[33] Sono stati confiscati dodici computer e al soggetto in questione è stato contestato anche il reato di infrazione di copyright, avendo utilizzato una riproduzione del sito web sopracitato. L'autorità di polizia ha dichiarato che erano stati ottenuti dati personali di circa trenta clienti, ma che questi non avevano ancora subìto danni economici.

## 4.3. Contromisure

***Stati Uniti***

Negli USA si è cercato di fronteggiare il fenomeno del furto di identità innanzi tutto attraverso un rafforzamento della legge in vigore in materia di criminalità informatica che, sebbene già consideri sia il *phishing* sia lo *spyware*, non risulta idonea da sola a frenarli[34]. È così in corso di approvazione *l'Internet Spyware Prevention Act of 2005* (I-SPY) che, oltre a fornire nuove risorse per la lotta al fenomeno, amplia le fattispecie criminose attualmente previste, considerando consumato l'atto criminoso con il semplice invio di *phishing e-mail* o con la creazione di *phishing web sites*, indipendentemente dalla prova di un danno subìto dalle eventuali vittime. In tal modo si intende accelerare e facilitare l'incriminazione degli utilizzatori fraudolenti del web, assai difficoltosa anche per la breve permanenza *on-line* dei siti fasulli o per la loro localizzazione in stati esteri.

Tra le iniziative delle autorità di controllo in materia di *phishing* si segnala l'emanazione di una circolare alle banche da parte dell'*Office of the Comptroller of the Currency* (OCC), organismo che svolge la vigilanza sulle banche a statuto federale, con la quale vengono fornite alcune linee guida che le banche devono seguire nella predisposizione di contromisure per gli attacchi di *phishing*[35].

La *Federal Deposit Insurance Corporation* (FDIC), che vigila sulle banche a statuto statale non aderenti al *Federal System*, ha condotto un approfondito studio sul fenomeno36, soffermandosi sul quadro normativo, sulle iniziative di contrasto in atto a livello cooperativo e, soprattutto, sulle contromisure tecnologiche adottabili dalle banche per ridurre il rischio di attacchi (cfr. allegato 2). Vengono formulate alcune raccomandazioni, quali: adozione di sistemi di autenticazione a due fattori (parole chiave+supporto fisico); utilizzo di sistemi di scansione del web per conoscere tempestivamente eventuali attacchi in corso; rafforzamento delle iniziative di comunicazione e formazione della clientela, assumendo al contempo iniziative per limitare la responsabilità della banca per eventuali frodi; sviluppo di continui scambi informativi tra le istituzioni finanziarie, la pubblica amministrazione e i fornitori di ICT.

Da segnalare inoltre che sul sito del *Federal Reserve System* è disponibile una brochure "*Internet Pirates Are Trying to Steal Your Information*", che ciascuna banca è invitata a diffondere presso i propri clienti, con l'obiettivo di sensibilizzarli sui pericoli del *phishing*[37].

A livello associativo, un importante organismo che opera nel campo della lotta alle varie forme di minacce alla sicurezza delle transazioni finanziarie è la *Financial Services Information Sharing and Analysis Center* (FS/ISAC). Si tratta di una partnership tra le principali banche e società del campo finanziario e assicurativo per lo scambio di informazioni e la condivisione di analisi sulle minacce alla sicurezza fisica e informatica; gli enti partecipanti mettono a disposizione di tale organismo i propri migliori esperti sulla materia. Le informazioni sugli incidenti di sicurezza sono comunicate alle autorità federali, con le quali è instaurato un rapporto di collaborazione continuativa. Nel 2003 il Dipartimento del Tesoro ha stanziato un contributo di due milioni di dollari per il finanziamento dei programmi del FS/ISAC finalizzati ad

[34] Con l'*Identity Theft ACT* del 1998 è stata attribuita al furto di identità rilevanza autonoma di reato federale. In particolare, può essere punito con la reclusione fino a 15 anni e con una multa fino a $250.000 chiunque possegga, trasferisca o usi, senza autorizzazione, uno strumento di identificazione di un altro soggetto, con l'intento di commettere o favorire altro reato federale o statale.

[35] OCC Bullettin n. 2005-24, July 1, 2005. In particolare, si fa riferimento a: l'opportunità di azioni di sensibilizzazione nei confronti della clientela; la necessità di predisporre idonee procedure interne, presidiate da personale appositamente addestrato, per la rapida attivazione delle contromisure in caso di attacco; l'attivazione di azioni per consentire la tempestiva scoperta (strumenti di scansione del web, software di verifica dei *log* del *server*) e il conseguente blocco di eventuali attacchi, con il coinvolgimento dell'*Internet service provider*; le comunicazioni da effettuare, al verificarsi di attacchi, agli organi investigativi e di vigilanza.

[36] FDIC, *Putting an End to Account-Hijacking Identity Theft*, December 2004, pubblicato su www.fdic.gov.

[37] www.federalreserve.gov/consumers.htm

accrescere la cultura della sicurezza, le capacità analitiche e la gestione degli incidenti presso il sistema finanziario.

Altra iniziativa recente è la costituzione dell'*Identity Theft Assistance Corporation* (ITAC)[38], organismo cooperativo che funge da centrale informativa per i casi di furto di identità a danno di clienti di società finanziarie.

Per lo scambio di informazioni e di analisi in materia di *cybercrime* opera anche *Infragard*, struttura facente capo all'FBI e organizzata in diverse sedi territoriali, cui partecipano esponenti del mondo delle imprese, dell'università e di altre istituzioni pubbliche.

Va citato infine l'*Anti-Phishing Working Group* (APWG), associazione che annovera oltre 600 membri tra istituzioni finanziarie (vi partecipano otto delle principali dieci banche USA), operatori dell'*e-commerce*, *Internet Service Providers* e fornitori di software. L'APWG effettua approfondimenti sulla diffusione e sulle caratteristiche dei casi di *phishing*, nonché sulle possibili soluzioni tecnologiche per contrastare il fenomeno. In quest'ambito sono state formulate alcune raccomandazioni volte a favorire l'introduzione nei servizi di *banking on-line* di sistemi di *Strong Website Authentication*, ovvero delle *smartcard* e dei *token*.

Un'altra raccomandazione ha per oggetto l'adozione di un sistema di *Mail Server Authentication*: le *e-mail*, prima di essere ricevute, devono transitare per un *server* di controllo che ne verifichi la fonte. Inoltre, si consiglia alle società vulnerabili al *phishing* di allegare la firma digitale a tutte le proprie *e-mail* in modo che i clienti possano facilmente verificare l'origine dell'*e-mail* ricevuta (*Digitally Signed Email With Desktop Verification*). In alternativa, si prevede che la verifica dell'origine dell'*e-mail* sia demandata a un *server* (*Digitally Signed Email With Gateway Verification*)[39].

Con riferimento infine alle iniziative individuali, va evidenziato come tutte le principali istituzioni finanziarie abbiano attivato forme mirate di comunicazione alla clientela sul fenomeno del *phishing*. In particolare sui maggiori siti di *on-line banking* sono presenti informazioni quali: esempi di *phishing e-mail*; consigli su come comportarsi per prevenire la sottrazione di dati personali; numeri verdi e indirizzi *e-mail* cui comunicare i tentativi di *phishing*; collegamenti ai siti istituzionali per avere maggiori informazioni sulla materia; avvisi aggiornati sull'evoluzione delle forme di attacco.

### ***Regno Unito***

Il 25 maggio 2005 il Ministero degli Interni britannico ha presentato presso la *House of Lords* un disegno di legge volto a modificare e ampliare la definizione del reato di frode, in termini tali da farvi rientrare il *phishing*, in modo da colmare le lacune della normativa in vigore e rafforzare l'efficacia della repressione penale del fenomeno[40].

---

[38] L'iniziativa è stata promossa dal *Banking Information Technology Secretariat* (BITS), organismo cui partecipano un centinaio tra le più importanti imprese finanziarie statunitensi. L'attività del BITS è rivolta alle iniziative di sostegno della fiducia dei consumatori, attraverso il miglioramento della sicurezza, riservatezza e integrità delle transazioni finanziarie.

[39] Importanti società che svolgono attività on-line hanno iniziato a porre in essere alcune di tali contromisure al fine di limitare il rischio di furti di dati sensibili dei propri clienti. In particolare, American Express ha sviluppato una serie di requisiti essenziali di sicurezza, di agevole attuazione, che riducono notevolmente le capacità degli *hacker* di accedere ai dati sensibili attraverso internet. In proposito si segnalano: l'adozione di *firewall network* e di software antivirus; l'aggiornamento sistematico delle connessioni di sicurezza (*security patch*); l'assegnazione di un unico numero di identificazione per ciascun soggetto abilitato a inserire i dati; l'utilizzo di codici per il trasferimento dei dati attraverso il *network*. Un altro metodo, attualmente utilizzato da Visa, consiste nella "profilatura" dei titolari delle carte, che consente di rilevare prontamente comportamenti anomali di acquisto.

[40] La proposta di legge ha destato perplessità in quanto essa non fa espresso richiamo al furto elettronico di identità. Infatti, sebbene un inasprimento della pena rispetto al passato e una definizione più ampia del reato di frode costituiscano un notevole deterrente, è diffusa l'opinione che il contrasto al fenomeno del *phishing* vada affrontato attraverso soluzioni, anche normative, che tengano conto della sua specifica natura tecnologica. Il disegno di legge prevede anche le fattispecie criminose dell'accesso illegale ai servizi finanziari (l'esecuzione di operazioni fraudolente on-line su carta di credito) e della partecipazione in attività finanziaria fraudolenta che, sebbene non immediatamente riconducibile al *phishing*, può essere a esso strumentale (anziché configurare un sito fittizio di un istituto di credito, al fine di derubare il cliente inconsapevole di dati identificativi, si sfrutta il sito in questione per creare una istituzione finanziaria inesistente, attraverso la quale esercitare, pur non avendone titolo, attività finanziaria. In quest'ultimo caso il

Altre significative attività di prevenzione a livello istituzionale sono state svolte dalla *Financial Services Authority* (FSA), che, coerentemente con il suo compito primario di mantenere la fiducia nel mercato finanziario, promuoverne la conoscenza da parte degli investitori e garantirne la protezione anche attraverso il contrasto alla criminalità finanziaria, ha provveduto, attraverso il dipartimento per la valutazione del rischio, a ispezionare diciotto aziende tra istituti di credito, società di investimento e assicurazioni al fine di verificare la sicurezza dei loro sistemi informatici. In tale contesto è stata rilevata una sostanziale debolezza rispetto ai crescenti attacchi informatici, soprattutto nelle società più piccole. Il rapporto su "*Countering Financial Crime Risks in Information Security*" del novembre 2004, che contiene i risultati dell'indagine, individua le vulnerabilità del settore principalmente nella mancanza, negli anni passati, di investimenti per l'adozione di adeguati sistemi di sicurezza da parte delle istituzioni finanziarie. Le stesse sono risultate carenti sotto il profilo della scarsa regolamentazione delle modalità di accesso dei dipendenti ai dati della clientela, così come nella predisposizione di software sicuro per il monitoraggio privilegiato e autonomo del proprio conto bancario da parte del singolo correntista.

La critica principale rivolta alle banche dalla FSA consiste nell'avere sottovalutato l'importanza di un'azione preventiva nella gestione dei sistemi di sicurezza informatica, orientata a proteggere le informazioni della clientela da attacchi esterni e interni al sistema, e di essersi invece concentrate sulla reazione all'atto fraudolento una volta verificatosi.

A livello associativo, l'APACS ha emanato una serie di *best practices*[41] dirette agli operatori maggiormente interessati dal *phishing*. Punti cardine di tali istruzioni operative, oltre alla sensibilizzazione della clientela al problema - già condotta dai singoli operatori - sono sia lo sviluppo di sistemi di prevenzione dell'attacco o di pronta reazione all'attacco subìto, sia l'individuazione di canali e contatti attraverso i quali la clientela possa immediatamente denunciare eventuali casi di *phishing*.

Secondo l'APACS, è necessario l'aggiornamento continuo delle procedure atte all'individuazione di *e-mail* provenienti dalla clientela in risposta a messaggi inviati attraverso siti falsi e la realizzazione di una rete di contatti con associazioni e autorità di vigilanza estere, affinché eventuali *phishing web sites* possano essere prontamente disattivati. Infine, si ritiene utile per le banche ricorrere a società esterne per il controllo della posta elettronica e della propria *home* page.

Recentemente è stato creato un sito web ad hoc[42] volto a consentire alla clientela di conoscere i rischi collegati al *phishing* e di operare in modo sicuro *on-line*. In una pagina del sito viene riportato un *Phishing IQ Test*, che consente al cliente di accertare se il sito su cui sta operando è realmente quello della propria banca.

La modalità di contrasto al fenomeno del *phishing* che nel Regno Unito appare essere più efficace è la sensibilizzazione degli utenti effettuata a livello di singolo operatore, sia attraverso messaggi di posta elettronica e informazioni contenute nel sito della banca, sia attraverso opuscoli distribuiti allo sportello o per posta ordinaria. Già in occasione del primo accesso al servizio, l'istituto di credito assicura al cliente che determinate informazioni non verranno mai richieste attraverso messaggi di posta elettronica e invita lo stesso a prestare particolare attenzione alle *e-mail* che dovessero contenere richieste di informazioni relative a suoi dati sensibili (quali dati identificativi, *password*, codice PIN e numero di conto corrente). Tuttavia, viene considerato un problema il fatto che, mentre si raccomanda ai clienti di non inviare i

---

cliente inconsapevole non solo verrà truffato nel ricevere un servizio da parte di un intermediario finanziario abusivo, ma verrà derubato dei propri dati).

[41] *E-banking* Fraud Liaison Group: *Phishing-Guidance, Best Practice & Lessons Learnt*

[42] www.banksafeon-line.org.uk

propri dati via *e-mail*, si richiedono poi, agli stessi clienti, adempimenti che possono essere effettuati esclusivamente per via telematica e che implicano l'indicazione *on-line* di dati riservati.

Alcuni istituti di credito includono, nella propria *home* page, *link*s tramite i quali i clienti possono segnalare eventuali messaggi sospetti, provenienti all'apparenza dalla banca. Sulla base di queste segnalazioni, la banca può agire legalmente affinché il sito "simulato" venga soppresso.

***Germania***

Le linee di azione del Governo tedesco in risposta al diffondersi del *phishing* sono indirizzate a promuovere: una più precisa informazione degli utenti da parte delle banche sui rischi insiti nell'*e-banking* e sulle misure di sicurezza da adottare; un maggiore ricorso alla firma elettronica a fini di autenticazione; un maggiore utilizzo dello standard per l'*e-banking* elaborato dal sistema bancario tedesco (*HBCI - Home Banking Computer Interface*, v. oltre), pur non intendendo imporre normativamente l'adozione di determinati standard tecnici.

Sul fronte della legislazione penale vi è disaccordo sul fatto se il *phishing* integri o meno fattispecie di reato. Secondo l'opinione prevalente si avrebbe un reato solamente nel caso in cui i dati di accesso venissero effettivamente utilizzati per movimentare somme di denaro. È stata pertanto avanzata la richiesta di introdurre nel diritto penale tedesco la fattispecie del *phishing*. Tale proposta non sarebbe sostenuta dalle associazioni bancarie che temono un danno per l'immagine delle banche tedesche, in quanto ciò potrebbe essere interpretato come segno dell'incapacità del sistema bancario tedesco di tenere sotto controllo il fenomeno.

L'Autorità di vigilanza sul settore finanziario (*BaFin*) ha iniziato nel 2001 a sottoporre a controllo le piattaforme di *e-banking* dal punto di vista della sicurezza, costituendo un gruppo di lavoro composto anche da rappresentanti della Bundesbank e del BSI[43], l'ente pubblico che in Germania si occupa delle problematiche inerenti alla sicurezza informatica. Sulla base dei risultati della verifica, il BaFin sta predisponendo una raccomandazione rivolta a tutti gli istituti che offrono servizi di *e-banking* che, tra l'altro, potrebbe contenere indicazioni in materia di sicurezza nei rapporti con la clientela, anche con riferimento all'utilizzo dei sistemi di autenticazione.

Le misure adottate dagli istituti di credito e dalle associazioni bancarie si sono concentrate prevalentemente sul fronte dell'informativa alla clientela riguardante sia i rischi connessi con l'*e-banking* e le relative misure di sicurezza sia i problemi attinenti al *phishing*. Tale informativa viene fornita in maniera ampia attraverso i siti Internet delle banche, delle federazioni bancarie e di altre istituzioni. L'Associazione delle banche private tedesche di recente ha pubblicato un opuscolo informativo sull'argomento.

L'azione svolta dalle banche sotto il profilo della protezione del sistema non è invece considerata particolarmente adeguata; oggetto di critica è la procedura diffusamente adottata dalle banche per l'accesso ai servizi di *e-banking*, basata sulla digitazione del PIN e del c.d. TAN, che rappresenta il codice identificativo di una transazione. La comunicazione del TAN avviene generalmente mediante l'invio per posta di un elenco di codici, tra i quali il cliente può sceglierne uno qualsiasi che perde di efficacia dopo l'utilizzo.

[43] Il BSI (*Bundesamt für Sicherheit in der Informationstechnik*), che fa capo al Ministero degli Interni, oltre a svolgere una funzione di informazione sui vantaggi e i rischi connessi con l'ICT, sviluppa metodi per proteggersi da tali rischi, mettendo a punto, in cooperazione con l'industria privata, nuove tecniche e fornendo consulenze alle imprese e alle amministrazioni pubbliche. Inoltre collabora allo sviluppo di tecnologie connesse con la biometria e con la firma digitale. Il *BSI* ha messo a punto una serie di manuali, tra cui quello per l'*e-government* e quello di sicurezza di base per l'IT. Quest'ultimo costituisce una raccolta di *best practices*, riconosciuta anche dal *BaFin*, in tema di misure di sicurezza per i sistemi IT e relative applicazioni.

Lo standard HBCI[44] (*Home Banking Computer Interface*), messo a punto dal sistema bancario tedesco a partire dal 1995 e continuamente aggiornato, non ha ancora avuto un'ampia diffusione. Esso definisce i protocolli di trasmissione, il formato dei dati e le procedure di sicurezza e prevede l'autenticazione del cliente tramite un PIN e, alternativamente, una *smart-card* o un dischetto. La scarsa diffusione dell'HBCI è dovuta a una serie di motivi riconducibili sia alla offerta limitata da parte delle banche sia alla preferenza della clientela per la procedura PIN/TAN, che permette di effettuare le operazioni bancarie da qualsiasi personal computer e non necessita di hardware aggiuntivo.

L'introduzione su ampia scala di procedure di autenticazione mediante firma digitale, anche se già offerte da alcune banche, oltre a scontrarsi con la ritrosia dei clienti, troverebbe anche resistenze da parte delle banche che, per motivi economici, non sarebbero disposte a svolgere la funzione di "apripista" (secondo alcuni, le banche starebbero aspettando l'introduzione della citata "carta del cittadino").

Negli ultimi tempi, peraltro, si registrano diverse iniziative volte a migliorare il livello di protezione del sistema. Esse riguardano:

<u>contromisure percepite dalla clientela:</u>

- modifiche alla procedura PIN/TAN: ad esempio, introduzione del c.d. *mobileTan* (il TAN viene trasmesso su richiesta dell'utente via sms sul telefonino ed é valido solamente per un periodo limitato di tempo), utilizzo di *token* per la generazione dei TAN, previsione di domande di sicurezza basate su dati personali. Gli istituti maggiormente colpiti dal *phishing* hanno annunciato di voler introdurre la procedura del c.d. TAN indicizzato, che prevede l'inserimento da parte del cliente di un determinato TAN riportato nel proprio elenco e individuato su base *random* dalla banca[45];
- adozione di ulteriori misure di sicurezza: ad esempio, invio di un sms a un numero indicato dall'utente ogniqualvolta si accede al conto *on-line* o definizione da parte dell'utente di orari nei quali poter effettuare operazioni *on-line*;
- introduzione di limitazioni all'operatività dell'*e-banking*: ad esempio, previsione di un importo massimo per i bonifici effettuati[46];
- maggiore diffusione dell'HBCI: soprattutto le casse di risparmio e le banche cooperative, che avrebbero effettuato maggiori investimenti nella firma digitale, spingono verso un utilizzo dell'HBCI da parte della clientela;

<u>contromisure non percepite dalla clientela:</u>

- ristrutturazione dei siti Internet delle banche (rinunciando, ad esempio, a utilizzare *frames* non sicuri contro manipolazioni[47]);
- monitoraggio delle operazioni di bonifico, soprattutto se transfrontaliere;
- modifiche al software (introducendo, ad esempio, l'utilizzo di espressioni in codice per il TAN al fine di evitare che *trojan horses* possano individuarli);
- adozione di software che permetta di individuare le *e-mail* truffaldine mediante un sistema di *early warning*, mettendo gli istituti nelle condizioni di reagire in maniera tempestiva e di bloccare i siti contraffatti.

[44] Nel 2002 lo *standard* HBCI è stato ridenominato FinTS.

[45] La Dresdner Bank ha recentemente introdotto la procedura di autenticazione "e-P@d-PIN" con la quale i clienti inseriscono i loro PIN e TAN non più tramite la tastiera ma cliccando con il mouse sulle cifre indicate sullo schermo; in tal modo si vogliono evitare i rischi di furti di dati attraverso *trojans* in grado di registrare i dati digitati sulla tastiera.

[46] La Postbank ha introdotto la possibilità per ciascun cliente di stabilire un limite massimo di importo dei bonifici effettuabili *on-line*.

[47] La Postbank ha annunciato tale misura, essendo stata oggetto di un attacco di *framespoofing*.

Infine, atteso l'ampio risalto dato dai mass-media al fenomeno del *phishing*, un istituto di ricerca ha analizzato le modalità con le quali un campione di quindici banche aiuta la propria clientela a individuare tali attacchi[48]. Tale analisi ha preso in considerazione una pluralità di criteri che possono essere anche interpretati come una guida fornita alle banche per contrastare il *phishing*[49]. Sulla base dell'aderenza o meno a tali criteri è stato attribuito un punteggio a ciascuna banca del campione; è stato confermato che, in diversi casi, vi sarebbero margini di miglioramento dell'azione di prevenzione.

***Francia***

Riconoscendo il rischio reputazionale ed economico legato a disfunzioni dei servizi di *banking on-line*, le autorità pubbliche francesi hanno cercato di orientare le imprese verso l'utilizzo di standard comuni e congrui. In questo senso la definizione di requisiti minimali dei siti Internet degli operatori bancari (*profil de protection*) è stata affidata dal Segretariato Generale della *Commission Bancaire* (l'autorità di vigilanza bancaria nazionale) a un comitato interbancario, il *Comité français d'organisation et de normalisation bancaire* (CFONB)[50]. Il processo di definizione del profilo di protezione dovrebbe sfociare in una certificazione dei siti dedicati all'*home banking*.

Con riferimento ai più recenti attacchi fondati sui furti di identità, le contromisure adottate dalle istituzioni e dalle associazioni di imprese sono centrate, innanzi tutto, sulla promozione di iniziative di sensibilizzazione di clienti e utenti.

La *Fédération Bancaire Française* (FBF) ha pubblicato una guida all'utilizzo sicuro di Internet per i pagamenti; essa si inserisce nell'ambito di una campagna di educazione, condivisa con diverse autorità pubbliche, volta a migliorare l'utilizzo di Internet, segnatamente attraverso l'aggiornamento continuo dei sistemi operativi e l'installazione e l'aggiornamento di *antivirus* e *firewall*.

La FBF, inoltre, ha attivato un sistema di allerta che consente, in presenza di un evento rischioso segnalato da una banca, la diffusione tempestiva delle informazioni relative alle caratteristiche del rischio all'intero sistema bancario e la segnalazione della fattispecie agli organi di polizia competenti.

Per quanto concerne le misure poste in essere dalle banche per contrastare le frodi in parola, la FBF ha dato atto di un impegno continuo da parte delle banche per il miglioramento dei sistemi di individuazione e verifica delle operazioni atipiche, per l'ammodernamento progressivo delle modalità di accesso *on-line* ai servizi bancari[51], per la moltiplicazione delle chiavi di accesso in funzioni delle diverse possibilità operative offerte.

Alcune delle banche coinvolte di recente in episodi di *phishing* hanno pubblicato sui propri siti, attivabili con *link* bene evidenziati nella *home* page, delle pagine di *warning* volte a sensibilizzare la propria clientela, anche attraverso la riproduzione del testo delle mail fraudolente, e a indicare il comportamento corretto da porre in essere.

---

[48] Cfr. Fraunhofer Institut Sichere Informations-Technologie (2004), *Phishing-Schutz im On-line-banking. Hilfe zum Selbstschutz für Nutzer*.

[49] Sono stati presi in considerazione: requisiti di struttura tecnica (coincidenza tra la *2nd-level domain* del sito internet pubblico della banca e del sito dell'*e-banking*; visibilità dell'URL; certificato SSL: validità ed emissione a favore della banca stessa; connessione sicura con il *server* almeno a partire dalla pagina di *login*); l'offerta dello standard HBCI e la fornitura delle informazioni necessarie per l'installazione del software; le informazioni fornite alla clientela sulla sicurezza dell'*e-banking* in genere e sul *phishing* in particolare, con le indicazioni su come verificare che il sito sia vero e su chi contattare in caso di necessità.

[50] Si tratta dell'organizzazione di categoria che si occupa prevalentemente delle problematiche di natura tecnica concernenti i sistemi di pagamento bancari. È l'organismo nazionale di collegamento all'European Committee for Banking Standards.

[51] In particolare, due banche francesi (BNP Paribas e CCF) avrebbero adottato un sistema di autenticazione "non ripetibile", fornendo all'utente possibilità di accesso "oneshot".

***Paesi Bassi e Belgio***

Nei Paesi Bassi e in Belgio sono state costituite unità specializzate nella lotta alla criminalità informatica: il *National High Tech Crime Center* (NHTCC) nei Paesi Bassi, composto da membri della polizia e di tre ministeri (Interno, Giustizia, Economia); la *Federal Computer Crime Unit* (FCCU) in Belgio, all'interno della polizia federale, cui si aggiungono le *Computer Crime Unit* decentrate sul territorio.

Per quanto concerne le istituzioni finanziarie, le autorità di vigilanza di entrambi i paesi hanno scelto, per il momento, di non emanare istruzioni dettagliate in materia di sicurezza informatica, limitandosi a richiedere che l'ente vigilato adotti adeguati provvedimenti, adattandoli agli sviluppi delle tecnologie. Tale posizione riflette la consapevolezza della continua evoluzione dei rischi informatici e, di conseguenza, della necessità di aggiornare le contromisure. Un regolamento della banca centrale olandese (DNB) prevede che l'ente vigilato si attenga alle *sound practices* comunemente adottate nel settore per il controllo dei rischi informatici. In una circolare emanata nel 2000 dall'autorità di vigilanza belga (CBFA) si dispone che le banche predispongano un sistema che garantisca una sicurezza adeguata del sito web, dell'infrastruttura e delle operazioni *on-line*. Presso la CBFA è attualmente in corso una revisione della citata circolare. Non è stato ancora deciso se rendere obbligatoria l'adozione di un doppio livello di autenticazione.

Nel 2004 le banche olandesi hanno costituito il *Financial Institutions – Information Sharing and Analysis Centre* (FI-ISAC.NL) nell'intento di favorire lo scambio e la diffusione delle informazioni sugli attacchi informatici subiti dalle istituzioni finanziarie e, più in generale, sui principali fattori di vulnerabilità del settore bancario alla criminalità su Internet. Inoltre, *ABN Amro*, primario istituto olandese, partecipa al *Trusted Electronic Communications Forum* (TECF), che persegue analoghe finalità in un contesto internazionale e intersettoriale[52]. Non si rilevano invece, né nei Paesi Bassi né in Belgio, iniziative a livello di sistema miranti a elaborare contromisure tecnologiche ovvero a sensibilizzare la clientela; le associazioni bancarie non hanno svolto finora attività specifiche al riguardo.

Per quanto riguarda le iniziative intraprese a livello di singoli operatori, nei Paesi Bassi tutte le principali banche hanno adottato un sistema di accesso ai servizi *on-line* basato su un doppio livello di autenticazione. In particolare, molto diffuso è un apparecchio elettronico da cui l'utente, digitando il proprio PIN, effettua la generazione di un codice segreto da inserire su Internet valido soltanto per una transazione bancaria (*one time password*)[53]. Meno frequente, ma dal forte potenziale di crescita, è un sistema molto simile in cui il codice segreto necessario per l'operazione è generato da una tessera contenente un microchip; esso è più costoso, in quanto richiede che l'utente si doti anche di un apposito lettore da collegare al computer. Infine, nei Paesi Bassi sono utilizzate due ulteriori modalità di protezione: l'invio tramite SMS al telefono cellulare dell'utente del codice segreto per la transazione; l'invio di un documento cartaceo contenente un elenco di codici segreti, da inserire volta per volta per ogni operazione.

In Belgio solamente due banche[54] si affidano a un sistema con un doppio livello di autenticazione, basato sul sistema della *one time password*. Gli altri operatori dispongono di un minor grado di protezione, limitandosi a richiedere il PIN per l'accesso ai servizi *on-line*. Tra le altre contromisure adottate dalle banche, figurano gli avvisi, esposti sui siti web, miranti a sensibilizzare gli utenti di fronte ai rischi di frodi informatiche; essi precisano, inoltre, che le

[52] Al TECF partecipano 17 gruppi internazionali, tra cui AT&T Wireless, E*Trade, IBM, HSBC.

[53] L'apparecchio più utilizzato è il Digipass, prodotto dalla società belgo-statunitense Vasco.

[54] Fortis, che è leader del mercato, e ING, limitatamente ad alcuni clienti; l'introduzione, nel 2006, di un Digipass è prevista soltanto da Dexia

banche non richiedono dati riservati con semplici *e-mail*. Infine, un importante gruppo bancario ha ridotto, da un centinaio a una decina, il numero dei siti ufficiali del gruppo.

Nell'ambito della pubblica amministrazione rileva l'introduzione della carta di identità elettronica, ancora a uno stadio progettuale nei Paesi Bassi, mentre il Belgio, tra i primi paesi al mondo, ne ha già iniziato la distribuzione. Il numero di cittadini belgi in possesso del documento elettronico era pari, all'inizio di aprile 2005, a 350.000 e dovrebbe superare il milione entro la fine dell'anno. La carta di identità elettronica belga contiene un microchip in cui sono conservati i dati personali nonché un certificato digitale che consente, tramite l'utilizzo di un apposito lettore collegato al computer, di effettuare una serie di operazioni su Internet (firma digitale, accesso a servizi della pubblica amministrazione, *banking on-line*, ecc.)[55]. Solo ultimamente nei Paesi Bassi è stata avviata l'elaborazione di una carta di identità elettronica, che dovrebbe includere, oltre a un certificato digitale, anche dati biometrici. Nell'agosto del 2004 è stato condotto un test pilota, che ha coinvolto 15.000 persone. Secondo il governo olandese la carta di identità elettronica dovrebbe essere introdotta a partire dal 2007.

***Giappone***

Il vigente quadro normativo è composto dalla *Unauthorized Computer Access Law* (emanata nel 1999), dalle previsioni del Codice Penale (recentemente emendato per tener conto dell'evoluzione della tecnologia) e dalla legge per i reati connessi alla pornografia diffusa *on-line* (emanata, anch'essa, nel 1999).

La struttura della normativa vigente prevede sanzioni penali per le infrazioni concernenti la riproduzione illegale di *records* elettromagnetici, interferenze con il normale svolgimento degli affari attraverso l'utilizzo di sistemi computerizzati, le *computer frauds* in generale, la distruzione di *records* elettromagnetici. Con la *Unauthorized Computer Access Law* si è inteso proibire l'accesso non autorizzato ai sistemi computerizzati (ad es. da parte di *hackers*), prevedendo sanzioni penali per i trasgressori.

Nel 2003 è stata emanata la *Protection of Personal Data Law*, per le rilevanti esigenze di disciplinare il trattamento e la tutela dei dati personali nel settore privato. Inoltre, sono stati emanati numerosi provvedimenti normativi con riferimento alla tutela della proprietà intellettuale nel contesto del *cybercrime*, in materia di commercio elettronico e di firma elettronica, di telecomunicazioni, di responsabilità dei *providers* dei servizi telematici[56].

La lotta al *cybercrime* è condotta principalmente dall'autorità di Polizia. La *Cybercrime Division*[57] coordina l'attività degli uffici decentrati in materia di indagine e di repressione del crimine, oltre ad avere la responsabilità di approntare proposte in materia normativa con riferimento all'esigenza di repressione del fenomeno. La *National Police Agency* ha anche istituito una *High Tech Crime Technology Division*, che studia le modalità con le quali il fenomeno evolve e ha rapporti con autorità o strutture di controllo di altri paesi.

Va detto che il *phishing*, essendo una tipologia di *cybercrime* relativamente nuova, non trova ancora una collocazione propria nelle statistiche sulle attività di tali organismi. Da dicembre 2004 la Polizia conduce una campagna di informazione e di prevenzione. È stato istituito un "numero verde" per la denuncia anonima di tentativi di frode e, una volta accertata, la frode

[55] Per informazioni più dettagliate, si rinvia al sito ufficiale: http://eid.belgium.be/.

[56] Tra questi, assumono particolare rilevanza, con riferimento al fenomeno del furto di identità, le guidelines del Ministero dell'Economia che, tra l'altro, prendono in considerazione esplicitamente il settore dell'*e-commerce*. Esse introducono il divieto di utilizzo dei cookies a fini commerciali se non autorizzato esplicitamente, l'obbligo per le aziende che operano anche attraverso il canale on-line di dotarsi di procedure trasparenti per l'acquisizione e il trattamento di dati personali, l'obbligo di predisporre procedure per informare tempestivamente la clientela in caso di perdita o sottrazione di tali dati.

[57] La Divisione è stata costituita nel 2004 e conta un organico di venti persone.

viene perseguita anche obbligando il *provider* Internet a "scollegare" il sito web utilizzato dai *phishers*.

È attualmente allo studio l'ipotesi di introdurre l'obbligo di rimborso ai clienti delle banche che hanno subìto danni conseguenti dall'improprio utilizzo dei dati delle carte usate presso gli sportelli automatici. La bozza di provvedimento è stata accolta con molte critiche dalle banche[58].

La tradizionale ritrosia del sistema bancario nel confrontarsi con media e opinione pubblica è in parte riconducibile a fattori di natura culturale (tra i quali l'estrema riservatezza tipica delle imprese giapponesi, che continuano a essere considerate tipicamente poco trasparenti), ma soprattutto alla mancanza di previsioni normative che favoriscano un più elevato livello di *disclosure*.

Lo stesso Organo di Vigilanza, tra l'altro, preferisce adottare nei confronti dei soggetti vigilati un approccio incentrato sulla risoluzione dei problemi via via rilevati prima che questi diventino di dominio pubblico. Dal 2005, comunque, esso ha iniziato a indirizzare alle banche richieste formali di procedere a un rapido miglioramento delle strutture organizzative al fine di rafforzare i presidi per la tutela dei dati personali.

[58] Le banche sono contrarie all'introduzione di un obbligo di rimborso sia perché ritengono che la corretta custodia di carte magnetiche e *password* sia responsabilità esclusiva della clientela, sia perché, una volta introdotto tale obbligo, temono di assistere a un aumento di denunce di smarrimento fraudolente.

*ALLEGATO 1*

## Come proteggersi dal *PHISHING*

### – Decalogo ABI Lab per i clienti

1. Diffidate di qualunque mail che vi richieda l'inserimento di dati riservati riguardanti codici di carte di pagamento, chiavi di accesso al servizio di *home banking* o altre informazioni personali. **La vostra banca non richiederà tali informazioni via *e-mail***.

2. **È possibile riconoscere le truffe via *e-mail*** con qualche piccola attenzione; generalmente queste *e-mail*:
   - non sono personalizzate e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (es. scadenza, smarrimento, problemi tecnici);
   - fanno uso di toni "intimidatori", ad esempio minacciando la sospensione dell'account in caso di mancata risposta da parte dell'utente;
   - promettono remunerazione immediata a seguito della verifica delle proprie credenziali di identificazione;
   - non riportano una data di scadenza per l'invio delle informazioni.

3. Nel caso in cui riceviate un'*e-mail* contenente richieste di questo tipo, **non rispondete all'*e-mail*** stessa, ma informate subito la vostra banca tramite il *call centre* o recandovi in filiale.

4. **Non cliccate su *link* presenti in *e-mail* sospette**, in quanto questi collegamenti potrebbero condurvi a un sito contraffatto, difficilmente distinguibile dall'originale. Anche se sulla barra degli indirizzi del browser viene visualizzato l'indirizzo corretto, non vi fidate: è possibile infatti per un *hacker* visualizzare nella barra degli indirizzi del vostro browser un indirizzo diverso da quello nel quale realmente vi trovate. Diffidate inoltre di *e-mail* con indirizzi web molto lunghi, contenenti caratteri inusuali, quali in particolare @.

5. Quando inserite dati riservati in una pagina web, **assicuratevi che si tratti di una pagina protetta**: queste pagine sono riconoscibili in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con "https://" e non con "http://" e nella parte in basso a destra della pagina è presente un lucchetto. In proposito si sottolinea la necessità di stabilire l'autenticità della connessione sicura facendo doppio click sul lucchetto in basso a destra e verificando la correttezza delle informazioni di rilascio e validità che compaiono per il relativo certificato digitale.

6. **Diffidate se improvvisamente cambia la modalità con la quale vi viene chiesto di inserire i vostri codici di accesso all'*home banking***: ad esempio, se questi vengono chiesti non tramite una pagina del sito, ma tramite *pop up* (una finestra aggiuntiva di dimensioni ridotte). In questo caso, contattate la vostra banca tramite il *call centre* o recandovi in filiale.

7. **Controllate regolarmente gli estratti conto** del vostro conto corrente e delle carte di credito per assicurarvi che le transazioni riportate siano quelle realmente effettuate. In caso contrario, contattate la banca e/o l'emittente della carta di credito.

8. Le aziende produttrici dei browser rendono periodicamente disponibili *on-line* e scaricabili gratuitamente degli aggiornamenti (cosiddette patch) che incrementano la sicurezza di questi programmi. Sui siti di queste aziende è anche possibile verificare che il vostro browser sia aggiornato; in caso contrario, **è consigliabile scaricare e installare le patch**.

9. Sia le *e-mail* che i siti di *phishing* tentano spesso di installare sul computer della vittima codice malevolo atto a carpire le informazioni personali in un secondo momento, attivandosi nel momento in cui vengono digitate. Si può impedire tale operazione tenendo sempre **aggiornato il software anti-virus presente sul proprio computer**.

**10.** Internet è un po' come il mondo reale: come non dareste a uno sconosciuto il codice PIN del vostro bancomat, allo stesso modo occorre essere estremamente diffidenti nel consegnare i vostri dati riservati senza essere sicuri dell'identità di chi li sta chiedendo. **In caso di dubbio, rivolgetevi alla vostra banca!**

## – Decalogo ABI Lab per le banche

Sebbene il fenomeno del *phishing* sia un tipo di frode che agisce all'esterno del sistema bancario, alcuni accorgimenti possono essere ravvisati, in modo da ridurne per quanto possibile l'incidenza tra i propri clienti. In particolare può risultare opportuno quanto segue.

1. **Definire *policy* aziendali stringenti per il contatto del cliente via *e-mail***; ad esempio, stabilire i processi autorizzativi e gli indirizzi di posta elettronica abilitati per l'invio di *e-mail* ai clienti, non utilizzare mai un indirizzo *e-mail* che non appartiene al dominio web della banca.

2. **Pubblicizzare ai dipendenti e ai clienti della banca le *policy* di utilizzo dell'*e-mail***; in particolare, evidenziare che in nessun caso la banca chiederà ai clienti informazioni quali chiavi di accesso al servizio di *home banking*, codici di carte di pagamento o altre informazioni personali via *e-mail*. È opportuno inoltre diffondere le *policy* di utilizzo del contatto via *e-mail* della banca attraverso canali diversificati; ad esempio tramite spazi sul sito istituzionale, comunicazioni cartacee, messaggi in filiale,...

3. In caso di *e-mail* inviate ai clienti, **non inserire *link* a pagine interne del sito istituzionale o a siti esterni**, ma rimandare a comunicazioni che si trovano nella *home* page del sito, in modo che il cliente possa verificare l'autenticità della comunicazione, digitando manualmente l'indirizzo web della banca nella barra degli indirizzi del proprio browser.

4. **Aggiungere un ulteriore livello di autenticazione** (con *password* differenziata) per l'esecuzione di operazioni dispositive tramite il servizio di *home banking*. Si tratta di un ulteriore accorgimento in grado di limitare i danni prodotti da questo tipo di frode.

5. **Prevedere un processo di modifica / aggiornamento delle chiavi di accesso** al servizio di *home banking* su richiesta o necessità legata alla perdita della riservatezza di tali dati. Se non è possibile un'immediata modifica delle chiavi di accesso, è opportuno predisporre un servizio di blocco immediato delle chiavi stesse.

6. **Non utilizzare *pop up* per operazioni che richiedano interazione con l'utente**, in particolar modo per l'autenticazione e l'inserimento di dati. Il *pop up* di navigazione è la modalità principale con cui vengono condotte queste frodi e quindi può essere utilizzato come elemento di riconoscimento della frode da parte dell'utente.

7. Predisporre **strumenti di monitoraggio delle transazioni** dei propri conti *on-line*, in modo da evidenziare eventuali comportamenti anomali.

8. Predisporre un apposito **indirizzo *e-mail* ed eventualmente un numero telefonico cui i clienti possano rivolgersi in caso di sospetta frode**. Può inoltre essere utile costituire una raccolta delle segnalazioni pervenute.

9. Dare **informazione all'help desk clienti e al *call centre*** della banca affinché possa supportare la clientela su eventuali richieste di informazioni riguardanti questa tipologia di frode.

10. In caso di rilevazione di un attacco di *phishing*, informare la Polizia Postale e delle Comunicazioni.

*ALLEGATO 2*

## Estratto dal rapporto FDIC "Putting an End to Account Hijacking Identity Theft"

*(dicembre 2004 e supplemento giugno 2005, pubblicato su www.fdic.gov)*

MISURE TECNICHE PER CONTRASTARE I FURTI DI IDENTITA'A DANNO DEI TITOLARI DI CONTI CORRENTI BANCARI

Nello studio del *Federal Deposit Insurance Corporation (FDIC*), sono analizzate le tecnologie che possono essere usate per attenuare il rischio dei furti di identità in generale e il *phishing* sui conti correnti in particolare.

SOFTWARE DI SCANSIONE

I software di scansione esaminano continuamente Internet alla ricerca di indizi che possano far ritenere che una determinata istituzione sia oggetto di un attacco di *phishing*. A tal fine vengono ricercati sul *web* con cadenza giornaliera: a) ricorrenze del nome dell'azienda, della marca, dei marchi di fabbrica, degli slogan, ecc…b) nomi dei domini (DNS) che somigliano al nome dell'azienda, secondo predeterminati criteri. I software di scansione aiutano le istituzioni finanziarie a individuare siti che potrebbero simulare l'appartenenza all'azienda stessa, ovvero che dichiarano illegalmente di avere un legame con l'istituzione finanziaria. Un'istituzione finanziaria può acquistare e attivare software di scansione per conto proprio, oppure può esternalizzare il servizio; quest'ultimo è il caso più frequente per le piccole istituzioni finanziarie.

STRUMENTI DI ANALISI DEI LOG DEL *SERVER*

Simili ai software di scansione, tali strumenti analizzano il *server* dell'istituzione finanziaria, fornendo informazioni sull'attivitità quotidiana dell'infrastruttura telematica aziendale e aiutando così a scoprire attività sospette indicative di attacchi di *phishing* in corso. I log sono voluminosi e costosi da consultare; i software in questione sono in grado di analizzarli ed estrarre informazioni utili per il "*Network administrator*" nel giro di qualche minuto. In tal modo, è possibile monitorare l'evoluzione di eventuali tentativi di frode ed è facilitata l'identificazione dei "pirati". Tale attività può essere esternalizzata, anche se il software non richiede una complessa implementazione.

AUTENTICAZIONE DELLE *E-MAIL*

Le *e-mail* ingannevoli, apparentemente provenienti da un'istituzione finanziaria, sono il primo passo di un attacco di *phishing* che può portare a indebiti prelievi sui conti correnti. L'inganno è agevolato dal fatto che l'*e-mail* non è autenticata dal mittente. L'autenticazione delle *e-mail* consente di eliminare il *domain spoofing* verificando, attraverso l'IP address (IPA) del *server* mittente, che le *e-mail* provengano da dove dichiarano di venire. Questo standard può anche consentire di riconoscere i tentativi fraudolenti di registrare domini con un nome simile a quello dell'istituzione finanziaria presa di mira. Il processo di autenticazione è il seguente:

- il mittente invia una *e-mail* al destinatario;
- il servizio di posta riceve la *e-mail* e il *server* ricevente controlla, sulla base di una lista pubblica di DNS , il nome del dominio del mittente verificando che l'indirizzo IP del *server* del mittente coincide con quello pubblicato nella lista;
- se il controllo dà esito positivo, la *e-mail* viene recapitata, altrimenti viene scartata.

L'autenticazione richiede la cooperazione di più soggetti con diverse responsabilità: gli *Internet Server Providers* (ISP), l'*Internet Engineering Task Force* (IETF)[59] e le società fornitrici di software.

[59] Lo IETF è un organismo indipendente costituito da sistemisti, operatori, vendors e ricercatori, che si occupa del buon funzionamento di Internet e della sua evoluzione.

AUTENTICAZIONE DELL'UTENTE

L'utente viene autenticato attraverso la presentazione di credenziali. Generalmente si intende per "credenziale" una o più dei seguenti elementi: qualcosa che l'utente "sa" (es. la *password*); qualcosa che l'utente "ha" (es. il *token,* che può contenere un certificato digitale); qualcosa che l'utente "è" (in questo caso si parla di caratteristiche biometriche, es. le impronte digitali). Quando l'autenticazione dell'utente utilizza congiuntamente due di questi sistemi, si parla di autenticazione "a due fattori". L'autenticazione attraverso certificati digitali è considerata generalmente come una tra le più sicure tecnologie di autenticazione. Si ha inoltre una mutua autenticazione quando anche la pagina web del sito dell'istituzione è protetta da un certificato SSL (*Secure Socket Layer*): in questo caso il *browser* dell'utente verifica che la *Certification Authority* che ha emesso il certificato sia accreditata e se il certificato sia ancora valido o meno.

Si descrivono di seguito alcune modalità tecniche che consentono, in associazione all'utilizzo di *userid* e *password*, di effettuare una autenticazione a due fattori:

*Segreti condivisi* Si tratta di domande personali poste al momento dell'autenticazione e delle quali il "pirata informatico" verosimilmente non conosce le risposte. Una forma più recente di questa tecnica riguarda l'aver concordato all'inizio un segreto, rappresentato da una parola o da un'immagine, in modo che l'utente possa riconoscere l'autenticità della comunicazione ricevuta dalla presenza della parola/immagine inizialmente concordata. Va posta particolare attenzione, in questo caso, alla frode cosiddetta *man in the middle* che potrebbe consentire al "pirata", spacciandosi per l'utente, di acquisire in modo fraudolento il segreto condiviso.

*Token* Possono essere raggruppati principalmente in tre tipologie: l'*USB token*, la *smart card* e il generatore di *password*.

1. *USB token*: è grande quanto la chiave di una serratura a cilindro; contiene normalmente un microprocessore e usa un sistema forte di crittazione; si introduce nella porta USB del computer e non richiede nessuna installazione aggiuntiva; è costituito da un unico pezzo e l'eventuale tentativo di forzatura lo renderebbe inutilizzabile; è in grado di memorizzare certificati digitali da usare in ambiente PKI.
2. *Smart card*: concettualmente simile all'*USB token*, la *smart card* ha le dimensioni di una carta di credito e richiede, per il suo riconoscimento, un hardware specifico e l'installazione del software associato.
3. *Generatori di password*: si tratta di dispositivi che producono un codice di accesso utilizzabile una sola volta – *one time password* - (OTP); l'OTP viene visualizzato sul piccolo schermo del *token.* Esiste una versione a più bassa tecnologia, consistente in una scheda con più parole chiave da scoprire e usare in sequenza negli accessi; questa soluzione presenta lo svantaggio della complessità di gestione a carico dell'azienda finanziaria, costretta a tenere traccia e a verificare le *password* fornite ai clienti; essa è comunque più economica dell'*USB token*, non richiedendo apparecchiature aggiuntive.

*Tecnologie biometriche* L'autenticazione avviene in questo caso per mezzo di caratteristiche fisiche o fisiologiche (p.es. impronte digitali, riconoscimento facciale, caratteristiche vocali, tipicità della scrittura sulla tastiera). Durante il processo di registrazione le caratteristiche fisiche e/o fisiologiche concordate vengono valutate e convertite in un modello matematico; questo viene registrato in un database per le successive elaborazioni. A tale proposito, il *National Institute of Standards and Technology (*NIST*)* ha sviluppato uno standard, denominato *Common Biometric Exchange File Format (*CBEFF) – per descrivere i dati a sostegno delle tecnologie biometriche. Normalmente vengono aggiunti controlli per evitare l'uso fraudolento di fotografie o registrazioni. Esistono due tipologie di problemi in cui la presente tecnologia può incorrere: accettare una credenziale falsa e scartare una credenziale valida. Infatti, a differenza della *password* che può solo essere corretta o errata, i sistemi a tecnologia biometrica si basano su una probabilità di riconoscimento: se il valore viene fissato troppo in basso si rischia di accettare utenti non accreditati, mentre se viene fissato troppo in alto si rischia di rifiutare l'accesso al legittimo proprietario.

Si riportano di seguito alcuni esempi di impiego di tecnologie biometriche:
*1. Riconoscimento delle impronte digitali*
Questa tecnologia è considerata tra le più mature e accurate per l'identificazione biometrica. L'apparecchiatura per la scansione va installata presso ogni utente (è quindi una soluzione "non portabile") ed è generalmente considerata tra le più facili da installare e da usare tra le tecnologie biometriche.
*2. Riconoscimento facciale*
La bontà del sistema di riconoscimento attraverso il riconoscimento facciale dipende molto dell'ambiente in cui viene usato. È facile da usare (basta disporre di una *web-cam* e del software di riconoscimento), non è intrusivo ed è perciò ben accettato dell'utente.
*3. Riconoscimento dello stile di battitura sulla tastiera*
Esistono software che consentono il riconoscimento dell'utente attraverso le caratteristiche del movimento delle mani sulla tastiera. Non è necessaria nessuna installazione aggiuntiva di hardware. Alcuni sistemi si limitano a riconoscere l'utente all'atto del *logon*, altri continuano il monitoraggio durante l'intera sessione.

AUTENTICAZIONE DEL DISPOSITIVO FISICO
È una tecnologia relativamente nuova che prevede l'utilizzo di un software residente che riconosce l'impronta univoca del PC. Lo svantaggio consiste nel fatto che il cliente proprietario del conto non può comunque accedere ai propri dati se non ha fatto prima autorizzare l'hardware da cui accede. Anche se non è necessario né hardware né software aggiuntivo, l'azienda finanziaria dovrà prevedere procedure di recovery che consentano di utilizzare il sistema da parte del legittimo utente nel caso di problemi di accesso.

TRUSTED PLATFORM MODULE (TPM)
Si tratta di un dispositivo, inserito direttamente nell'hardware del computer, che usa un chip per memorizzare *password*, certificati digitali e chiavi di crittografia. La TPM agisce come un *caveau* virtuale e usa lo standard PKI. Il chip è a prova di scasso e l'integrità viene verificata al momento dello start-up. I due svantaggi tipici di questa tecnologia sono: a) incapacità di riconoscere software non autorizzato o non collegato con il sistema operativo in uso; b) alti costi di conversione, una volta che il prodotto sia stato usato. Nonostante questi chip vengano installati su molti PC distribuiti dalle maggiori aziende, essi sono in realtà, ad oggi, disinseriti. L'idea è promettente, ma i sistemi operativi e il supporto applicativo non sono ancora diffusi.

INTERNET PROTOCOL ADDRESS (IPA) & LOCALIZZAZIONE GEOGRAFICA
L'idea alla base è di utilizzare l'IPA assegnato nella sessione all'utente per filtrare eventuali richieste fraudolente, tenendo conto che l'IPA può cambiare nel tempo e che a volte non è possibile associare all'IPA il suo attuale proprietario. Sono in commercio prodotti software in grado di setacciare Internet alla ricerca di informazioni sulle IPA. Il software effettua dei controlli in tempo reale confrontando i dati attuali con i profili degli accessi per individuare eventuali accessi non autorizzati. Oltre a questi controlli sono anche disponibili alcune tecnologie in grado di stabilire dove l'utente è localizzato geograficamente ovvero dove non può trovarsi al momento della transazione.

AUTENTICAZIONE FUORI BANDA
Con questo termine si indicano tutte quelle tecniche finalizzate ad autenticare l'utente attraverso un canale diverso da quello su cui l'utente sta facendo transitare i suoi dati. Oltre a ridurre il rischio di frodi, queste tecniche consentono anche di prevenire errori sui dati significativi. Ad esempio, all'inizio della transazione viene generata una chiamata telefonica, una *e-mail* o un SMS, e solo dopo che è arrivata la conferma, la transazione può procedere.

* * *

**Il rapporto della FDIC pone l'enfasi sui sistemi di autenticazione a due fattori quale strumento per ridurre drasticamente il rischio di frodi a danno dei clienti di istituzioni**

**finanziarie.** Viene quindi fornita una elencazione, non esaustiva, di istituzioni finanziarie che adottano, o stanno per adottare, sistemi della specie.

| Esempi di adozione di sistemi di autenticazione a due fattori negli USA | | | |
|---|---|---|---|
| AZIENDA | TECNOLOGIA | APPLICAZIONE | STATO |
| E-Trade Bank | OTP hardware token | Internet Banking | Progetto pilota |
| Bank of America | Tecnologie a 2 fattori | Accesso a internet per impiegati e clienti (aziende) | Funzioni per interni (estate '05) funzioni per l'esterno (aut/inv 2005) |
| Sovereign Bank | OTP hardware token | Business banking: clienti aziendali e istituzionali | In produzione |
| ABN AMRO | OTP hardware token | Gestione *on-line* della tesoreria | In produzione |
| ING Direct | Segreti condivisi a rotazione | Internet Banking | In produzione |
| Standford Federal Credit Union | Autenticazione del dispositivo fisico | Internet Banking | In produzione |
| Purdue Employees Federal Credit Union | Biometrica: Impronte digitali | Centri servizi automatizzati | In produzione |
| San Antonio City Employess Federal Credit Union | Biometrica: geometria della mano e tipicità della scrittura con la tastiera | Accesso alla cassetta di sicurezza; accesso degli impiegati alla rete | In produzione |
| Commerce Bank | OTP hardware token | Internet Banking per clienti aziendali | In produzione |
| Wachovia | OTP hardware token | Internet Banking | Allo studio |
| Dollar Bank | OTP hardware token | Internet Banking per clienti aziendali | In produzione |

| Esempi di adozione di sistemi di autenticazione a due fattori a livello internazionale | | | |
|---|---|---|---|
| AZIENDA | TECNOLOGIA | APPLICAZIONE | STATO |
| Australian Bankers Association | Tecnologie varie a due fattori | Internet Banking | Progetto pilota |
| Bank of Valletta | OTP hardware token | Internet Banking, telephone banking, centro servizi per i clienti, mobile banking | In produzione |
| Rabobank | OTP hardware token | Internet Banking | In produzione |
| SEB Bank | OTP hardware token | Internet Banking | In produzione |
| SwedBank | OTP hardware token | Internet Banking | In produzione |
| Banca di Tokyo – Mitsubishi | Biometrica: geometria della mano | ATM | Marzo 2006 |
| Surugo Bank Shizuoka Prefecture | Biometrica: geometria della mano | ATM | In produzione |
| Mizuho Bank | Biometrica: geometria della mano | ATM | In produzione |
| Sumitomo Mitsui Bank | Biometrica: geometria della mano | ATM | Marzo 2006 |
| Citibank, UK Division | Tastiera virtuale sullo schermo | ATM | Allo studio |
| First National Bank del Sudafrica | OTP hardware token | Internet Banking | In produzione |
| Royal Bank of Scotland | OTP hardware token | Internet Banking | In produzione |
| Loyal Bank | OTP hardware token | Internet Banking | In produzione |
| Fortis, NV | OTP hardware token | Internet Banking | In produzione |
| Gruppo Aval | Autenticazione del dispositivo fisico | Internet Banking | Luglio 2005 |
| Barclays | Tastiera virtuale sullo schermo<br><br>Autenticazione fuori banda | Internet Banking<br><br>Internet Banking | In produzione<br><br>Allo studio |