Home Banking
storia, opportunità, sicurezza e futuro

Calambrone, 22 Maggio 2015

Claudio Telmon

claudio@telmon.org

Partiamo un po' prima...

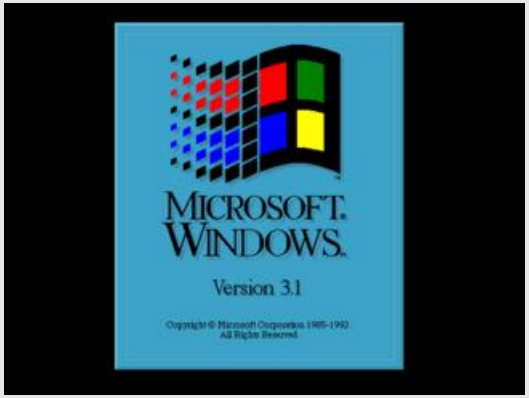
IBM
Fonte: Wikimedia

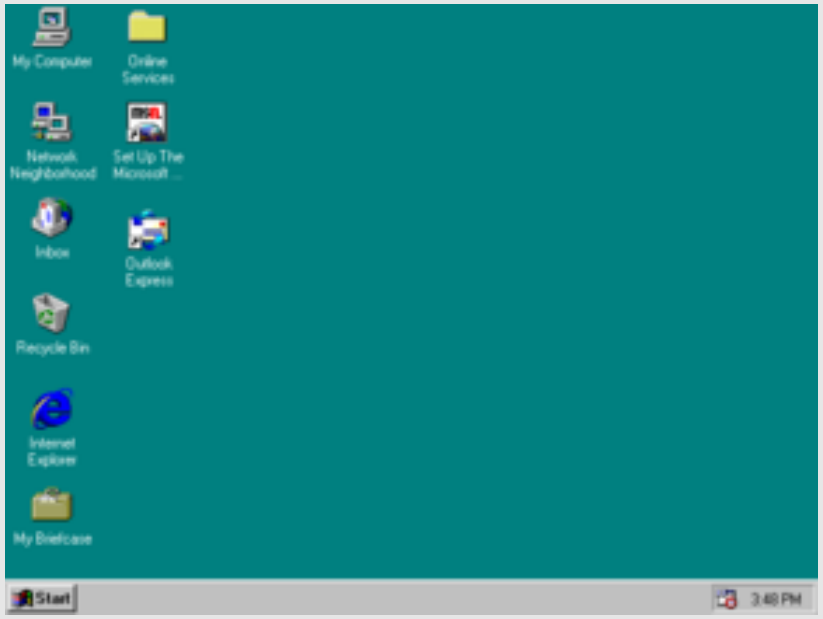
Fino agli anni ‘90 il sistema informativo della banca era chiuso su sé stesso:

- Sicurezza fisica
- Accesso da terminali principalmente nelle filiali
- Poca connettività, con sistemi bancari e «linee dedicate»

Poi iniziano i cambiamenti…

Tcpman





"Analogue modem - acoustic coupler" by secretlondon123 CC BY-SA 2.0 via Wikimedia

IBM
Fonte: Wikimedia

Home Banking

Costringe le banche ad «aprire» i loro sistemi ad una rete pubblica mondiale incontrollata, Internet
le grandi aziende avevano già canali diversi dallo «sportello»

Posizioni inizialmente negative, i rischi sono alti ed i vantaggi (per la banca) limitati
i primi esperimenti negli USA non avevano avuto un grande successo

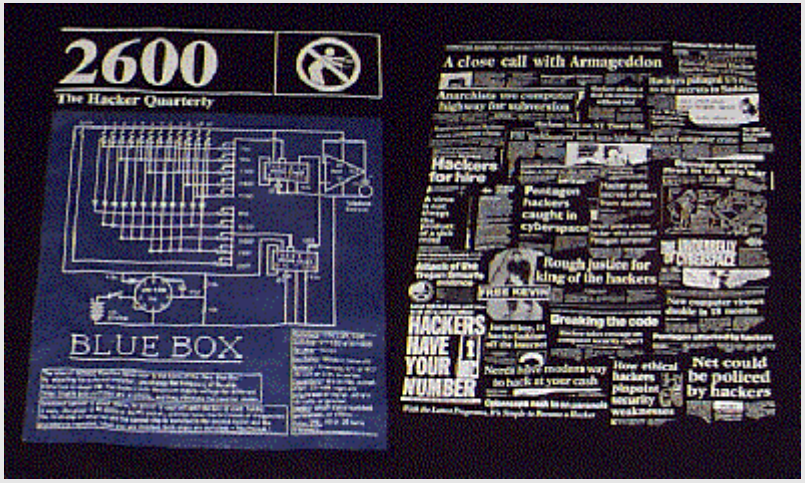
In Italia si arriva a metà degli anni ‘90, ma quando una banca ha cominciato, le altre hanno dovuto seguire
il rischio più alto diventava quello di perdere clienti

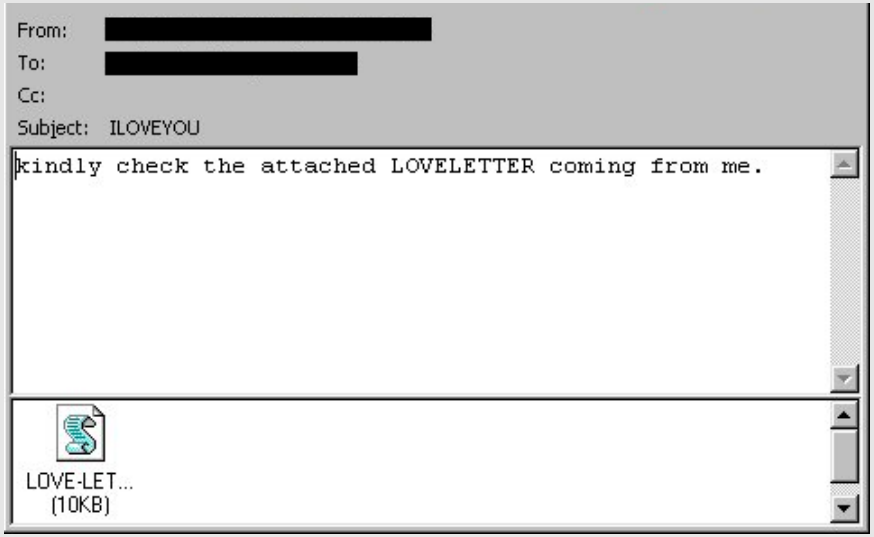
Comunque un servizio da far pagare, non un risparmio per la banca
negli anni successivi nascono però banche che offrono principalmente servizi online più per il trading (fine anni ‘90) che per il banking

I rischi?

La scena «hacker» di quegli anni era molto diversa

I «virus» avevano un effetto dimostrativo o dannoso sul PC («Cascade», «I Love You»…)
Il furto (di soldi) era un'eccezione, a volte osteggiata, e comunque era concentrato sui numeri di carta di credito (poco usate in Italia)





Gli attacchi richiedevano una competenza tecnica ed erano praticati di individui o piccoli gruppi

Per le banche erano più critiche le frodi interne e la clonazione di carte di debito e credito

Le tendenze attuali

I delinquenti vanno dove ci sono i soldi

- la tendenza alla smaterializzazione del contante è inarrestabile

L'hacker «romantico» non esiste più

- gli attacchi sono praticati da gruppi riconducibili alla criminalità organizzata, spesso russa
- gli strumenti sono professionali, sviluppati e venduti a prezzo considerevole
- il malware cerca di farsi notare il meno possibile, e di raccogliere informazioni spendibili o rivendibili

Le banche si sono dotate di uffici con personale e strumenti per mettere in evidenza le operazioni sospette, bloccarle (verificando con il cliente) o stornarle

Tuttora i problemi maggiori sono con le carte di debito e credito

Malware e phishing

Malware bancario: programmi («virus») che si installano sul pc/smartphone del cliente e usano le credenziali e gli accessi del cliente per effettuare operazioni fraudolente

molto efficaci: in realtà non esiste una vera «protezione», arrivano anche a modificare le risposte della banca; ci sono molti palliativi, che in generale sono più che sufficienti; attualmente, lo strumento più efficace «lato cliente» è l'SMS di notifica delle attività

Phishing: convince il cliente a connettersi ad una pagina «fasulla» e a inserire le proprie credenziali

meno efficace, specialmente se il cliente segue la buona pratica di non seguire i link (e la banca segue la buona pratica di non mandarne)

NON VI INSEGNO COME RICONOSCERLO!!!
NON SEGUITE I LINK!!!

E le banche?

Gli uffici delle banche che si occupano di contrasto alle frodfi riescono a riconoscere e a bloccare una percentuale molto alta delle transazioni fraduolente importanti (bonifici, non ricariche)

Spesso hanno delle offerte di strumenti di protezione dal malware («antivirus») a prezzo agevolato

Sistemi di «strong authentication»: sistemi più robusti della password (SMS, token, ecc.) resi obbligatori dalle ultime disposizioni di BCE/Banca d'Italia, limitano il danno degli attacchi

USATELI!

Il pc/smarphone è sempre più il nostro collegamento con soldi, amici, istituzioni… proteggerlo è proteggere la nostra vita (sociale)

In caso di problemi

Il cliente è contrattualmente obbligato a:

1. Custodire bene le credenziali
2. Segnalare tempestivamente eventuali problemi

Se ha fatto questo, al netto di eventuali franchigie, il cliente di solito è tutelato

Molte banche seguono una politica di rimborso per evitare il danno di immagine, salvo quando il comportamento del cliente sia sospetto

Ombudsman Bancario (Conciliatore Bancario Finanziario) presso Banca d'Italia
La conciliazione è uno strumento obbligatorio dal 2011

www.conciliatorebancario.it

I ricorsi al conciliatore di BdI, pubblicati sul sito (quindi si può capire la giurisprudenza) riguardano per la maggior parte le carte di debito e credito, molto meno l'home banking

La banca multicanale… e non solo

Smartphone, tablet, smart TV…

Le banche seguono il cliente

Strumenti con nuovi rischi, nuovi attacchi e nuove tecnologie di protezione

Anche in questo caso, la strada non è stabilita dalle banche (ma neanche dal cliente?)

Le banche e la regolamentazione cercano di seguire i fenomeni…

"IPhone 5S home button" by Kelvinsong - CC BY 3.0 via Wikimedia

"LG smart TV" by LG CC BY 2.0 via Wikimedia

E la sicurezza?

È tutto meno sicuro? La risposta è...

Sì

…almeno dal punto di vista tecnologico. È una conseguenza della consumerizzazione degli strumenti

Ma al cliente è richiesto solo di seguire le solite precauzioni
Le banche si stanno attrezzando con strumenti più sofisticati

adaptive authentication: autenticazione semplice per operazioni «tranquille», avanzata per quelle più a rischio

«**semplice, economico, sicuro: scegline due**»
…ma nessuno sceglie la sicurezza

DOMANDE?