CERTFin

LE SFIDE DEI PAGAMENTI DIGITALI: SICURI ED INTELLIGENTI IN UN CLICK

24 novembre 2023

Romano Stasi

Chief Operating Officer

TLP GREEN

I pagamenti digitali in Italia

- **Le App guidano il Digital Banking**: l'operatività dispositiva gioca un ruolo determinante nella crescita complessiva dei clienti attivi, in particolare per il canale Mobile Banking da App, nel quale i clienti dispositivi crescono del **14,5%**.*
- **I bonifici istantanei aumentano significativamente tra il 2021 e il 2022**, soprattutto tramite App (**+43,9%**), mentre l'Internet Banking registra volumi più contenuti, sebbene in crescita (**+18%**).*
- Il **48%** dei **Mobile Banking users** hanno **aumentato l'utilizzo anche dell'Internet Banking**; il **66%** indica un **ricorso alla filiale in diminuzione**.**
- **Fra le diverse app utilizzate quelle bancarie continuano ad essere percepite come le più sicure** (**45%**), tuttavia il primato è meno brillante che in passato (-11 punti percentuali vs. il 2022);**
- **Resta maggioritaria e stabile (85%) la quota di quanti giudicano complessivamente sicuro l'utilizzo della app bancaria**, e, all'interno di questo bacino, **cresce in modo significativo chi si sente addirittura molto sicuro**, ormai ben un quarto della clientela (un terzo fra chi ha rapporti con tre banche o più). **
- **Oltre un intervistato su due non percepisce un differenziale di sicurezza in base al device utilizzato**: smartphone e pc sono ugualmente sicuri.**
- **Investimenti in sicurezza sui servizi alla clientela da parte delle banche in forte crescita** per il **91%** dei rispondenti

**Fonte: ABI Lab-Rapporto Osservatorio Digital Banking, House of Digital – ed. 2023.*
*** Fonte: Report "Che cliente (digitale) sei?", ABI Lab in collaborazione con Doxa - Survey su un campione di 1.000 clienti bancari che utilizzano i canali digitali, luglio 2023.*

Il rafforzamento delle normative sulla sicurezza

- La **Direttiva NIS2**, entrata in vigore il 17/1/23, introduce **nuovi obblighi di sicurezza informatica,** attribuendo maggiori responsabilità agli OSE e oneri di segnalazione più ampi.

- Il **DORA** (Digital Operational Resilience Act), entrato in vigore il 16/1/23:
  - ❑ rafforza il framework di **governance e risk management;**
  - ❑ introduce nuove **modalità di verifica delle contromisure di sicurezza**, attraverso un approccio di "*effective testing*" che include l'esecuzione di TLTP;
  - ❑ prevede un **nuovo framework regolamentare per le terze parti** che prestano servizi critici in ambito ICT, con un regime di sorveglianza a livello europeo condotta dalle ESA.

- Il **PSR (**Payments Service Regulation), parte del cd «Payments Package» proposto dalla CE il 28 giugno scorso, si propone di rendere **più uniforme e dettagliato** il quadro normativo per il settore dei pagamenti, con norme dedicate ai psp e ai consumatori.
- Il **contrasto alle frodi** costituisce uno dei principali obiettivi del PSR. Tra le misure introdotte, si segnalano la condivisione delle informazioni relative alle frodi, la sensibilizzazione dei consumatori e la collaborazione tra psp e operatori di telecomunicazione (rif. art 59).

Lo scenario delle frodi nel panorama italiano

- Il **65%** delle **transazioni fraudolente effettive**, considerando il solo segmento Retail, **sono state avviate dall'utente in seguito alla manipolazione da parte del frodatore**.***
- Con riferimento alla clientela Retail, oltre il **67,5% delle frodi effettive** è stato realizzato sfruttando come **punto di contatto iniziale** le **chiamate telefoniche** e gli **SMS**.
- Nella maggioranza dei casi di **frodi effettive**, sia negli SMS che nelle chiamate telefoniche, il mittente/originatore della comunicazione è stato falsificato (**spoofing**).***
- La distribuzione **dell'età delle vittime** in relazione alle frodi effettive ha una prevalenza (30% del totale) nella fascia di età compresa tra i **45 e i 60 anni**.***
- Per finalizzare le frodi verso i money mules vengono effettuati per il **42% *bonifico istantanei*** per il **30 % *bonifico ordinario*** ***
- Tutte i pagamenti vengono monitorati con strumenti di Transaction monitoring e il **94% delle operazioni fraudolente sono bloccate o recuperate**
- **Si intensificano le azioni istituzionali e operative a supporto dell'infosharing intersettoriale, grazie alla collaborazione con l'ACN, e nel settore finanziario anche a livello internazionale.**

****Fonte: CERTFin - SICUREZZA E FRODI INFORMATICHE IN BANCA – Rapporto Osservatorio Cyber Security and Knowledge – ed. 2023.*

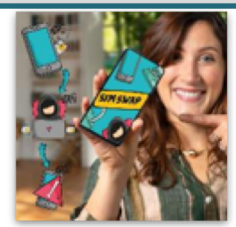
i Navigati: campagna di awareness retail (1/2)

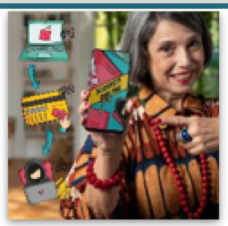
- La campagna di cybersecurity awareness retail “I Navigati” ha l’obiettivo di incoraggiare **l’uso sicuro e consapevole dei canali e degli strumenti digitali** e sensibilizzare i clienti sui rischi di attacchi e frodi online nella fruizione di servizi finanziari. Il payoff **Informati e Sicuri**, spiega l’importanza dell’informazione per acquisire le conoscenze adatte a navigare il web in sicurezza.
- Promossa dal CERTFin, la campagna ha visto la partecipazione di Banca d’Italia, IVASS, ABI e 16 gruppi bancari.

- **COLLABORAZIONI ISTITUZIONALI**

Agenzia Cybersicurezza Nazionale nel 2021 e Autorità Garante per la protezione dei dati personali nel 2022.

i Navigati: campagna di awareness retail (2/2)





Smishing **Social network** **Social engineering** **Money Muling**

Downloading pericolosi **Sim Swap** **Acquisti online** **Ghost Broking**

MATERIALI

- TV spot, formati 6" 10" 15" 30" 45"
- Spot radio
- Web series, 8 episodi sulle principali truffe
- Video Interviste ad esperti di settore

CONCEPT

Per parlare al target in maniera diretta e coinvolgente e attraverso un approccio positivo è stato scelto di rappresentare luoghi e personaggi in cui tutti si possano immedesimare.

CANALI

- TV
- Radio
- Stampa
- Canali digitali
- Media relations

inavigati.it

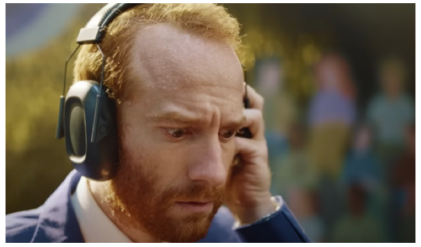
CYBERSICURI: campagna di awareness corporate (1/3)

- La campagna di sensibilizzazione sulla cybersecurity rivolta alle aziende ha l'obiettivo di aumentare la **consapevolezza sull'importanza di investire nella sicurezza dei sistemi ed educare i dipendenti**. Comprendere la minaccia rappresentata dagli attacchi informatici contribuisce ad aumentare il livello di responsabilità e consapevolezza sia tra le aziende che tra i loro dipendenti.
- Promossa dal CERTFin, la campagna è partecipata da Banca d'Italia, IVASS, ABI, Polizia di Stato e 12 gruppi bancari.

- **COLLABORAZIONI ISTITUZIONALI**

Agenzia Cybersicurezza Nazionale e Autorità Garante per la protezione dei dati personali.

CYBERSICURI: campagna di awareness corporate (2/3)



MATERIALI

- Main video 30" e 15"
- Spot radio 15"
- 3 infografiche (ceo fraud, invoice fraud, tech support scam)
- Web banner
- Stories, pp link e carousel
- DEM

CONCEPT

La vita aziendale si trasforma metaforicamente in un "quiz", dove in pochi secondi bisogna rispondere alle domande e adottare quei comportamenti virtuosi che consentono di riconoscere le minacce e di districarsi tra le possibili insidie informatiche.

CANALI

- Youtube
- Online video
- Digital Radio – Radio24
- Display Banner
- Social adv (FB, IG, LinkedIn)
- Media

cybersicuri.it

CYBERSICURI: campagna di awareness corporate (3/3)

Sono state create **tre video pillole** di approfondimento per descrivere le **truffe più comuni** in cui può restare vittima un'impresa.

Il truffatore chiama o invia una e-mail a un dipendente fingendosi un Top Manager chiedendo di fare un pagamento urgente

Il truffatore contatta l'azienda via telefono o e-mail. Chiede di modificare le coordinate bancarie per il pagamento di fatture o fornisce direttamente una fattura con nuove coordinate

Il truffatore contatta la vittima fingendosi un tecnico IT pronto a risolvere un problema su un dispositivo aziendale

Thank You!

CERTFin

Defend. Inform. Evolve.

For more info visit www.certfin.it or write to ricerca@certfin.it