

Tracce digitali e tecniche di *social engineering* Consapevolezza come difesa

Sessione: «Denaro e sicurezza nell'era digitale»
Incontri per le scuole secondarie di II grado

Salone dei Pagamenti - Milano, 24 novembre 2023

Silvia Cambi
Divisione *Fintech Milano*

Tracce digitali: quanto la «rete» ci conosce?

«Frequentando» il web lasciamo «**tracce**» di noi:

- **volontarie** (es. social -> foto, post, ...)
- **involontarie** (es. dati navigazione -> IP, e-mail, device; lingua; tempo e orario di utilizzo; sistema operativo, ...)

sistemi di tracciamento



ATTIVI >> COOKIES

(file di testo memorizzati sul device dell'utente con possibilità di cancellazione in autonomia delle info acquisite)

PASSIVI >> FINGERPRINTING

(acquisizione diretta delle info sul dispositivo utilizzato con impossibilità di cancellazione in autonomia delle info acquisite)

«**Finalità**», fra le altre: velocizzare l'accesso (performance); semplificare la fruizione (v. carrello o form); misurare il traffico per elaborazioni statistiche; **profilare l'utente** (pubblicità, personalizzazione offerta, anti-frode, ...).
... i dati possono essere condivisi con terze parti.



Tracce digitali: quanto la «rete» ci conosce?



L'evoluzione tecnologica e i comportamenti degli utenti sul web moltiplicano la possibilità di raccolta e incrocio di dati anche personali.

Linee guida Garante Privacy 2021

(operative dal 09.01.2022):

- equiparazione tra «tracciati» attivi e passivi
- indicazioni per rafforzare la trasparenza dell'informatica e il **consenso**:
specifico - libero - informato - inequivocabile
- alcune modalità illegittime

Un esempio:

sanzione di 3 milioni di euro a una società di videogiochi per l'uso senza consenso di un tracciante su **app** per finalità pubblicitarie (CNIL 29.12.2022)



Social engineering

Strategia di **attacco informatico** che si basa sull'**analisi** della vittima per **manipolarla**. Sfrutta la **psicologia**, la **fiducia**, la **mancanza di conoscenze** e le **vulnerabilità** della persona per acquisire **dati confidenziali** (password, codici dinamici, dettagli su conti correnti e informazioni finanziarie).



Pagamenti on-line PSD2 - SCA



Le trappole più comuni

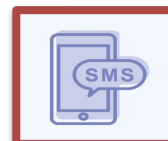
Quello che i truffatori cercano sono i tuoi dati, le tue password, le tue credenziali dinamiche e per ottenerli lanciano delle **esche**.

Phishing deriva da fishing che vuol dire andare a pesca... e i truffatori vanno a pesca con **e-mail** - **siti truffa su cui tentano di dirottarti** - **SMS** - **telefonate**.

NON ABBOCCARE!!



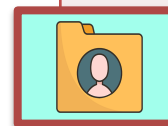
Phishing



Smshing



Vhising



Spoofing




Esche ... alcuni esempi




Non aprire mai link ricevuti via sms/whatsapp o via e-mail!

Verifica sempre l'indirizzo email del mittente prima di scaricare allegati.

Non fornire mai a nessuno i tuoi dati personali/le tue credenziali bancarie!!!

 Ciao, sono l'operatore

 Metto io al sicuro il tuo denaro, dimmi il codice che ti è arrivato.

NO GRAZIE!



Esche ... alcuni esempi



80 [redacted]	sconosciuto	11:20	(i)
+39 345 [redacted]	cellulare	11:18	(i)
+39 011 [redacted]	Torino, Piemonte	11:05	(i)
+39 011 [redacted]	Torino, Piemonte	11:04	(i)
Numero sconosciuto	sconosciuto	10:37	(i)
+39 80 [redacted]	Italia	10:29	(i)
+39 345 [redacted]	cellulare	08:40	(i)
+39 345 [redacted]	cellulare	08:38	(i)
[redacted]	WhatsApp audio	ieri	(i)

Chiamata dall'apparente **numero verde** della banca

- Il numero corrisponde al numero verde ufficiale della banca **ma...è preceduto da +39**



- I numeri verdi sono abilitati alle sole chiamate in entrata

La banca non ti chiede mai le credenziali, non comunicarle mai!



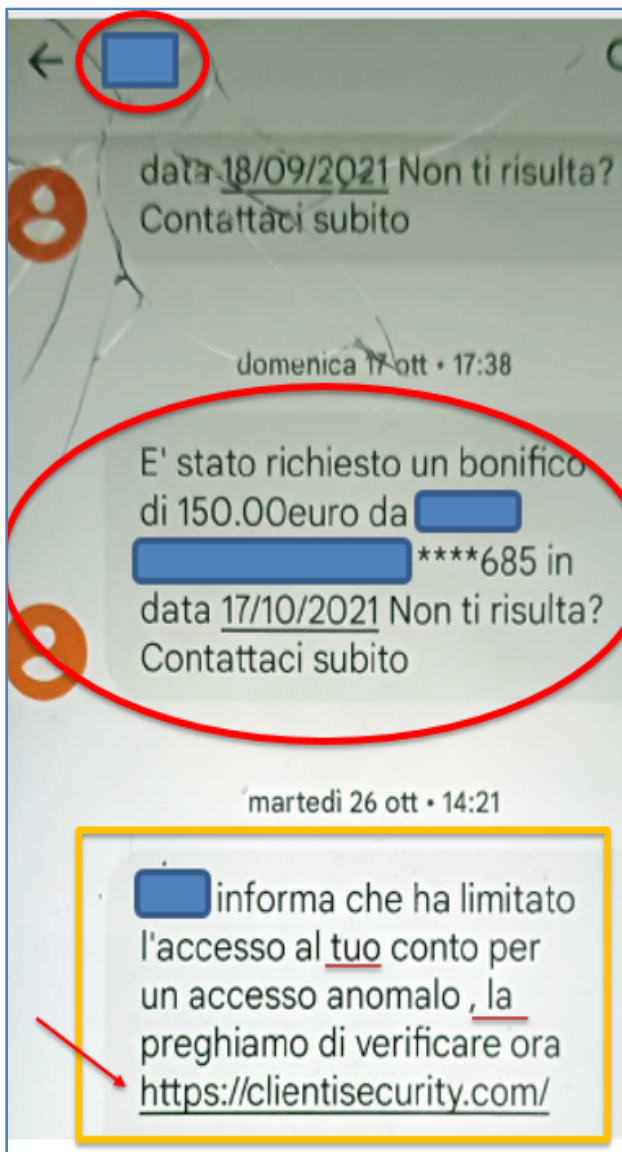
Esche ... alcuni esempi



SMS relativo ad un presunto accesso anomalo

- Chat autentica con la banca
- Presenza di sms autentici
- **Sintassi, punteggiatura, link non riconducibile alla banca**

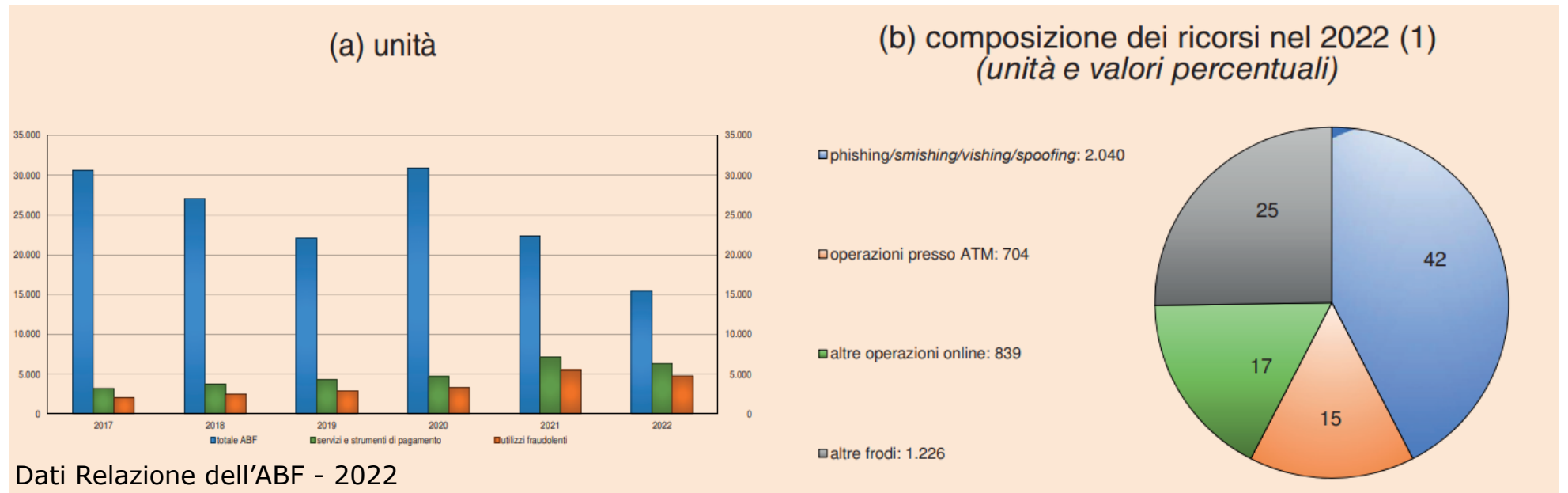
Ricorda: la banca non ti invia link!



Evidenze contenzioso Arbitro Bancario Finanziario



Nel 2022 nella materia degli utilizzi fraudolenti di strumenti e servizi di pagamento **2040 ricorsi** all'ABF (**42%**) hanno riguardato casi associati a tecniche di **social engineering** (*phishing, smishing, vishing, spoofing*).



Nel 71% dei casi la decisione è stata sostanzialmente favorevole al ricorrente (accoglimento/cmc)



Comportamenti utili

per proteggere i dispositivi
(computer, tablet, smartphone)



1 Installa e mantieni aggiornati i **SOFTWARE DI PROTEZIONE**



2 **INSTALLA LE PATCH** ("toppe" di protezione). Scarica solo gli aggiornamenti ufficiali



3 **INSTALLA I FIREWALL** (programmi di filtraggio del flusso di dati)



4 **INSTALLA** dal web solo **PROGRAMMI SICURI** di cui puoi verificare la provenienza



Verifica l'**AUTENTICITÀ** della **CONNESSIONE** con la tua banca mediante il controllo accurato del nome del sito nella barra di navigazione



per evitare errori

DIFFIDA di qualunque **RICHIESTA DI DATI** relativi a carte di pagamento, chiavi di accesso all'home banking o altre informazioni personali



NON CLICCARE SU LINK PRESENTI IN E-MAIL SOSPETTE potresti essere indirizzato a un sito malevolo



CONTROLLA regolarmente **L'ESTRATTO CONTO**



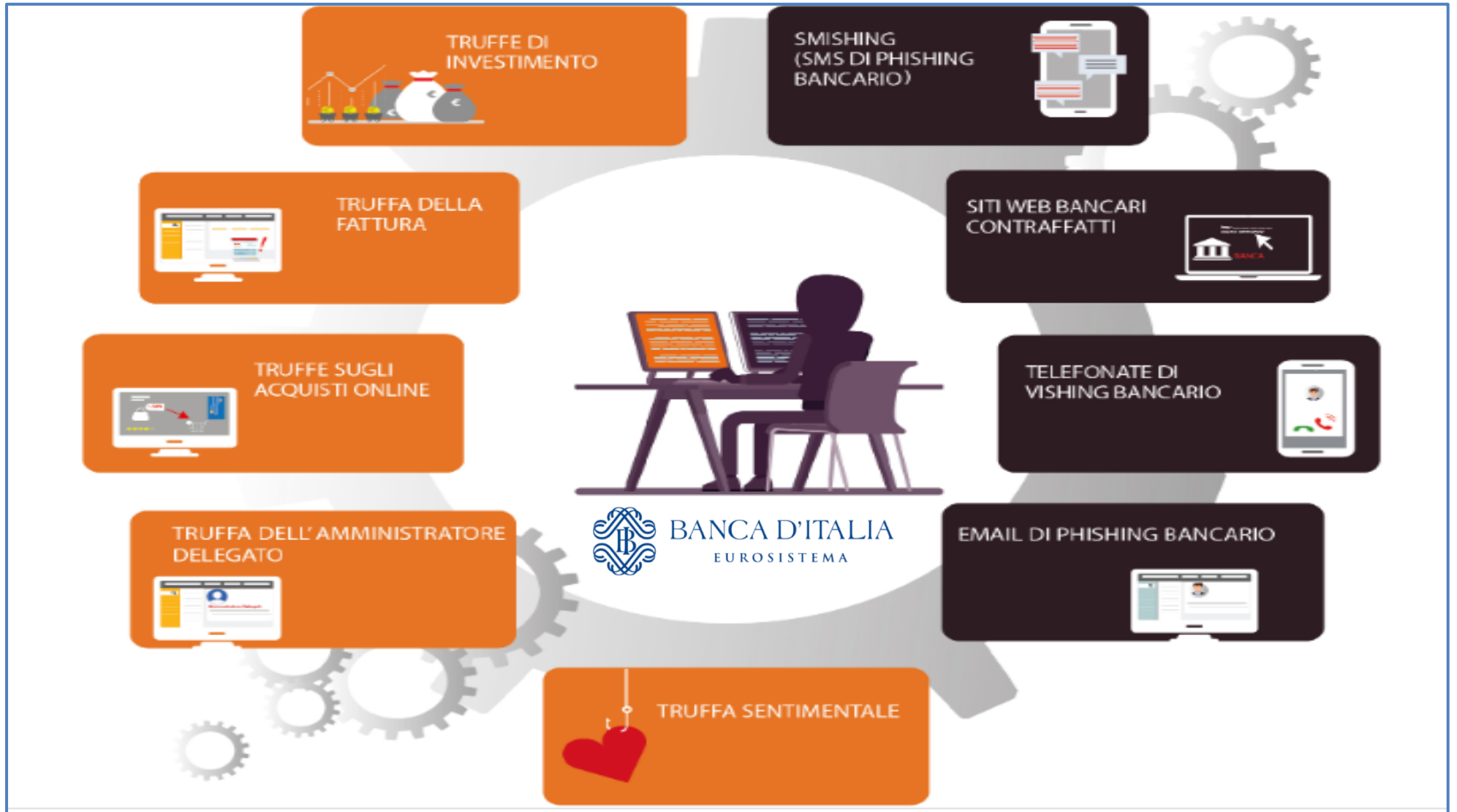
DIFFIDA DI MESSAGGI online di cui **IGNORI LA PROVENIENZA**



NON CONSEGNARE I TUOI DATI senza essere **SICURO** dell'**IDENTITÀ DI CHI LI STA CHIEDENDO**



Stay Tuned!!!



<https://economieapertutti.bancaditalia.it/infografiche/pericoli-online/>



Grazie per l'attenzione.

silvia.cambi@bancaditalia.it