CERTFin

Evoluzione delle minacce cyber e dei pattern di frode nel settore finanziario

Mario Trinchera
Technical Coordinator

Salone dei Pagamenti
3 novembre 2021

CERTFin

Agenda

1. LO SCENARIO ATTUALE DELLE FRODI NEL SETTORE BANCARIO ITALIANO

2. LA GESTIONE DELLA SICUREZZA E LE FRODI NEL SETTORE ASSICURATIVO ITALIANO

3. EVOLUZIONE DEI PATTERN DI ATTACCO

4. INIZIATIVE DI SETTORE PER LA MITIGAZIONE DEI RISCHI

Report Sicurezza e Frodi nel settore bancario
…in Sintesi

Maggiori investimenti dedicati alla sicurezza dei servizi erogati

+20% *del budget*

La clientela retail si conferma la più colpita

80% *del totale*

Enorme aumento del numero di transazioni anomale

+8x *Rispetto allo scorso anno*

Le tecniche miste sono diventate dominanti

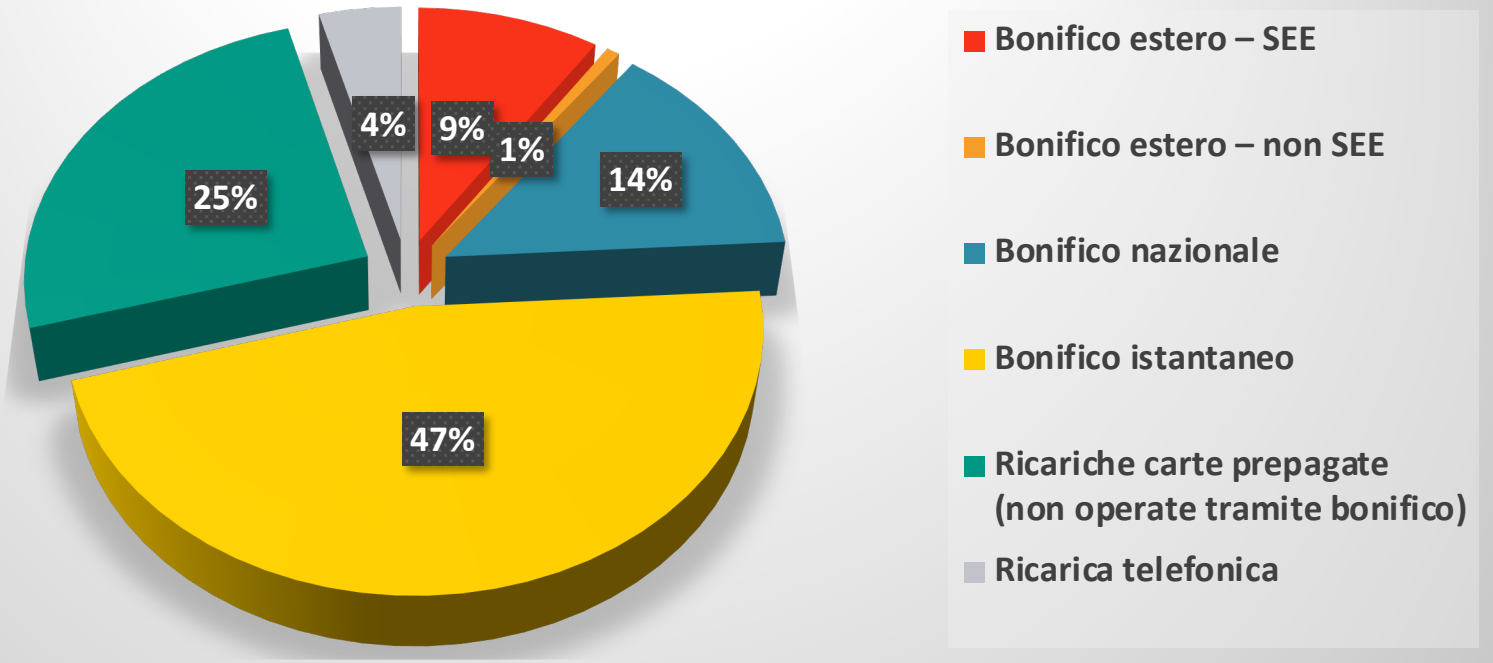
65% *del totale*

La gestione delle transazioni fraudolente resta efficace

83% *Transazioni bloccate o recuperate sul totale delle anomale*

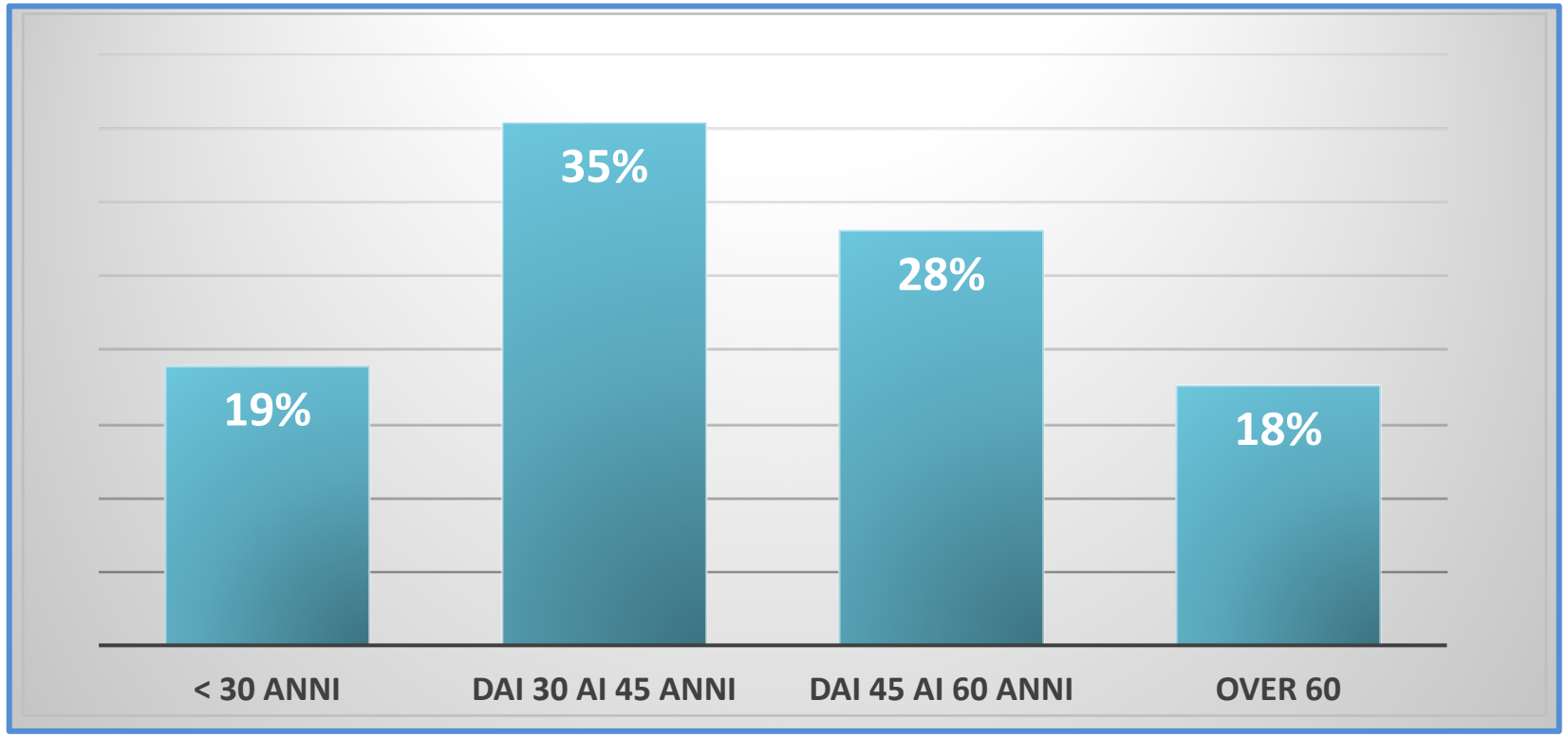
Transazioni Fraudolente Effettive

Clientela Retail - Ripartizione per strumento utilizzato (analisi sul numero di accadimenti)



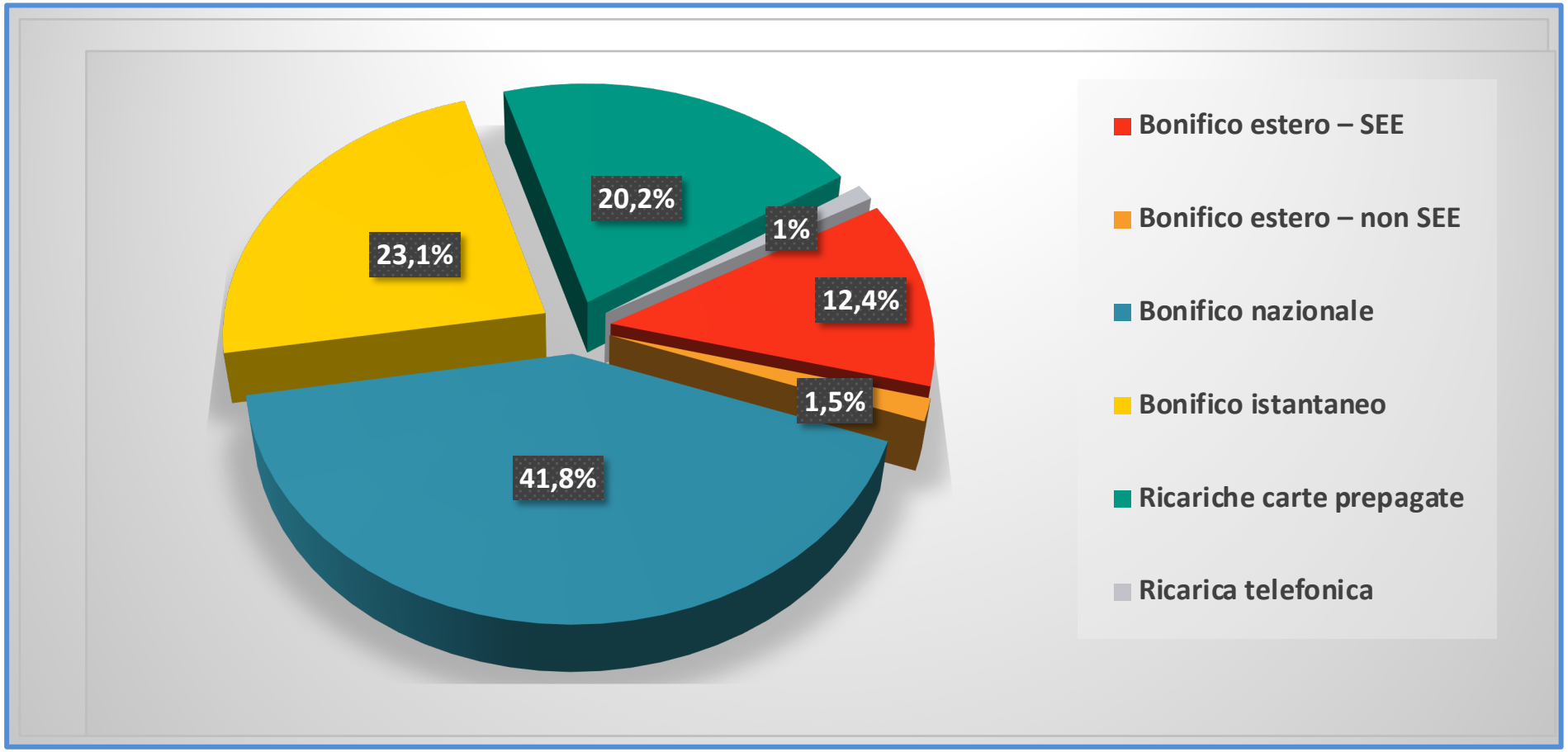
Età delle vittime

Età delle vittime di frodi effettive (solo clientela Retail)



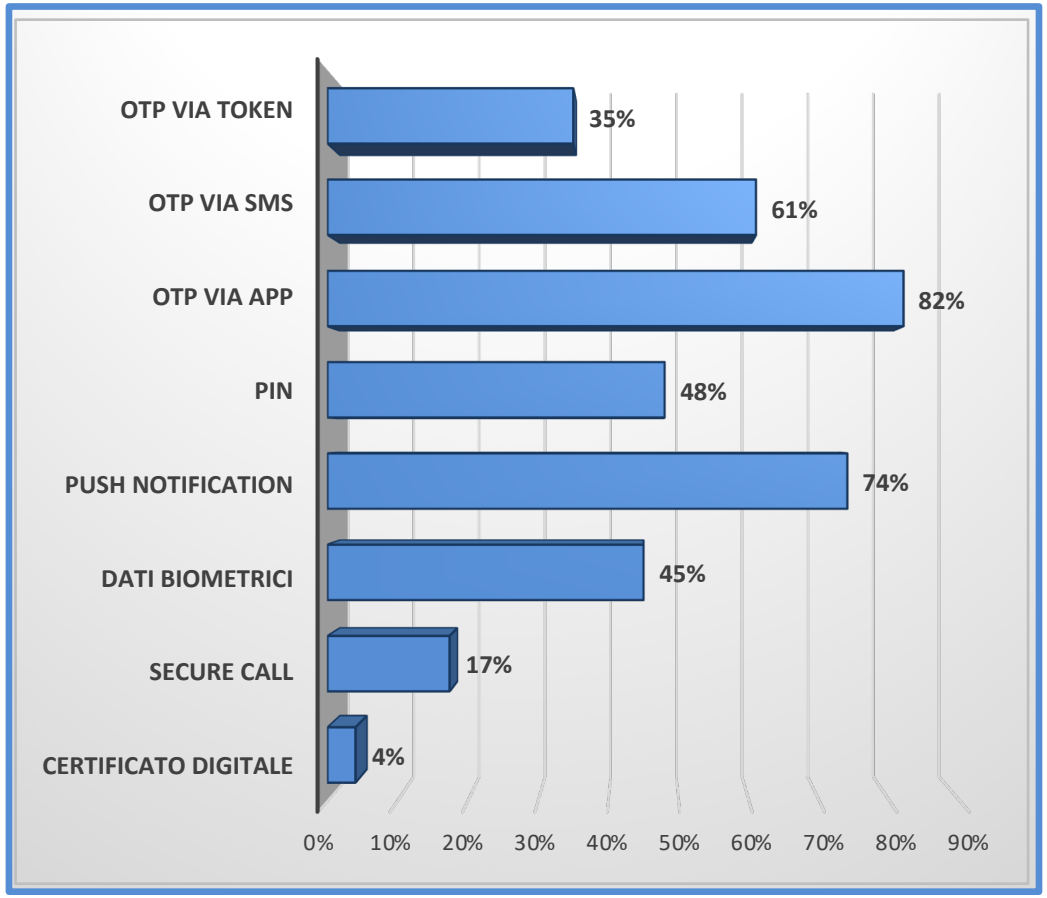
Transazioni Fraudolente Effettive

Clientela Corporate - Ripartizione per strumento utilizzato (analisi sul numero di accadimenti)

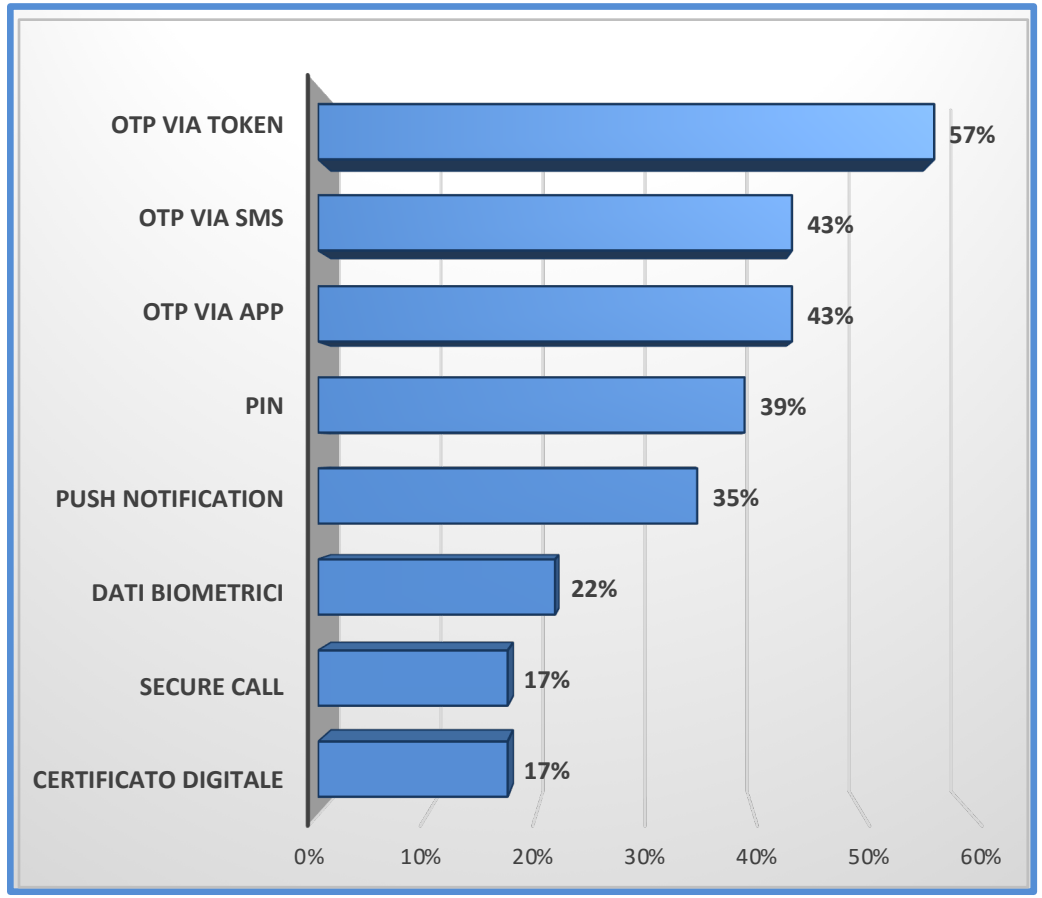


Tecnologie 2FA utilizzate in fase dispositiva

Retail

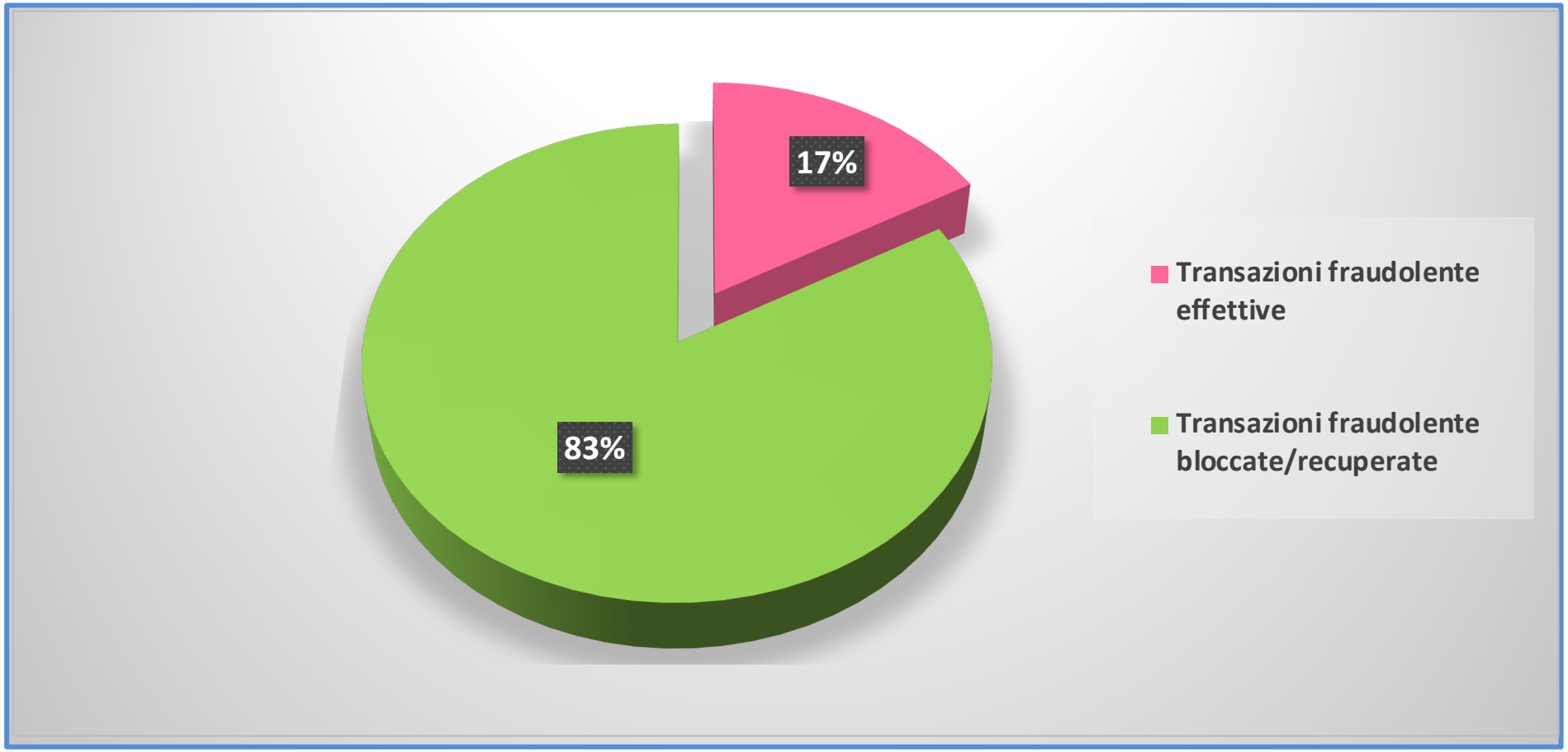


Corporate



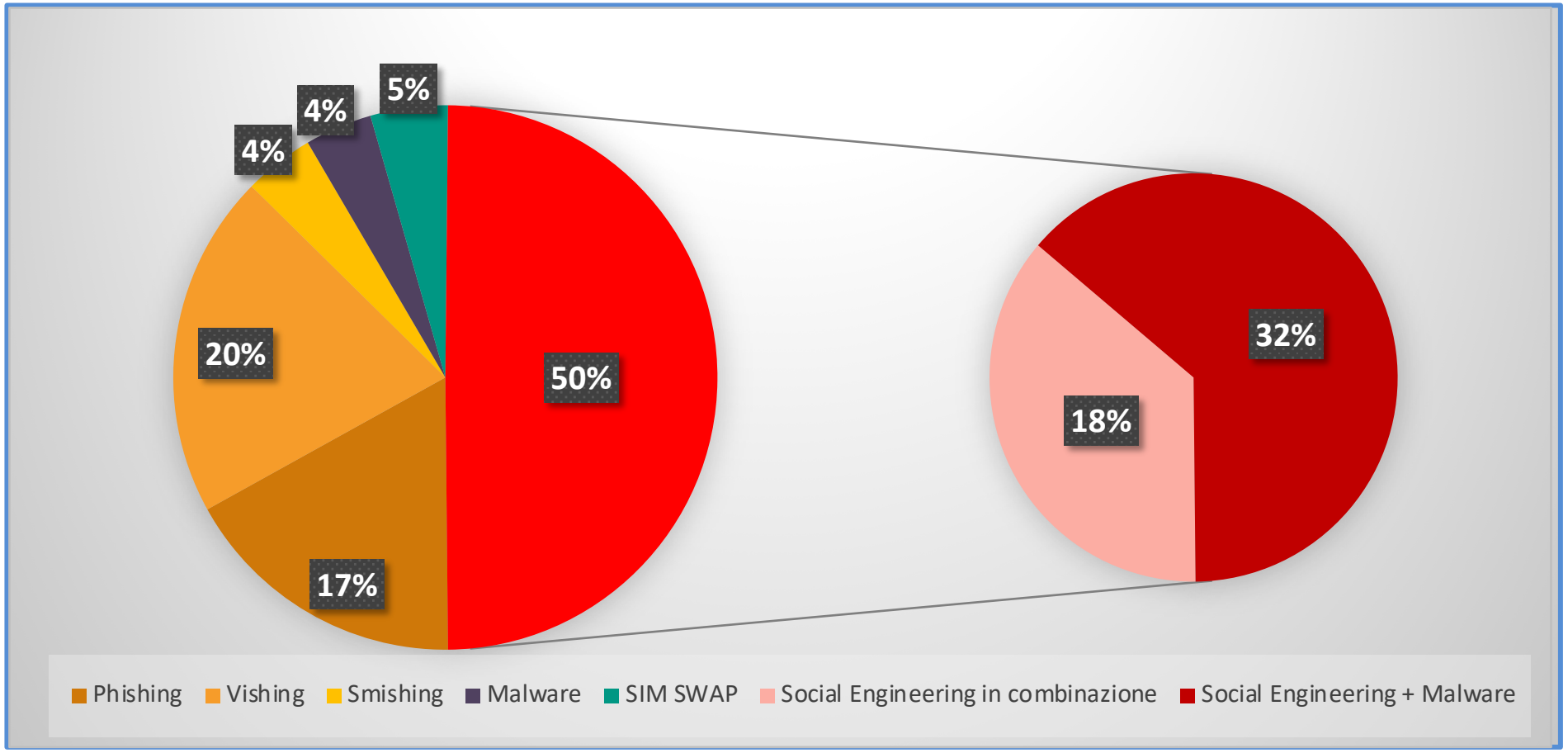
Transazioni Anomale

Ripartizione percentuale sul numero di accadimenti (complessivo Retail e Corporate)



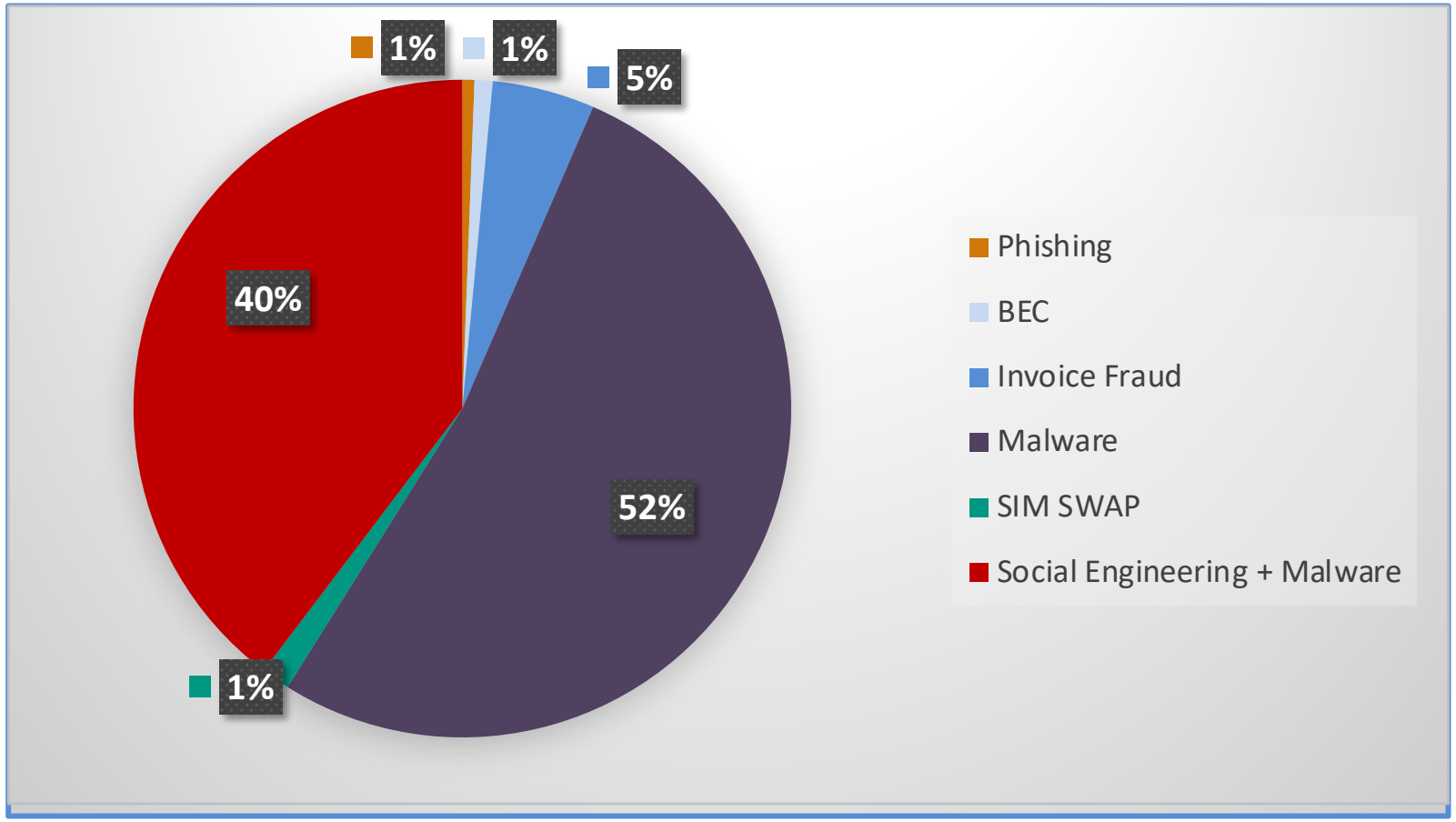
Tipologie di Frode

Clientela Retail - Tipologie di frode rilevate su canale Internet



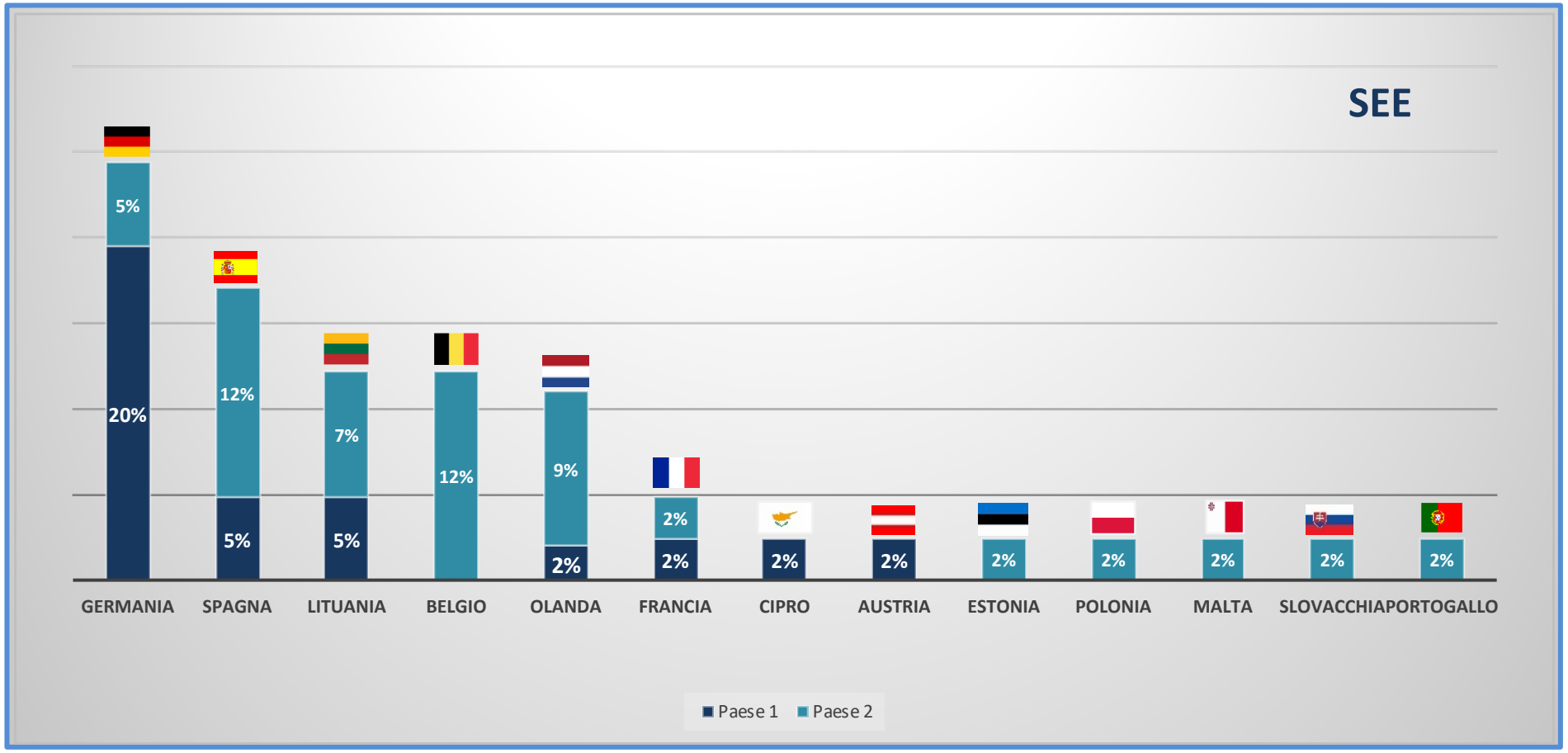
Tipologie di Frode

Clientela Corporate - Tipologie di frode rilevate su canale Internet



Distribuzione geografica

Elenco, in ordine percentuale, dei Paesi destinatari di bonifici fraudolenti



CERTFin

Agenda

1. LO SCENARIO ATTUALE DELLE FRODI NEL SETTORE BANCARIO ITALIANO

2. LA GESTIONE DELLA SICUREZZA E LE FRODI NEL SETTORE ASSICURATIVO ITALIANO

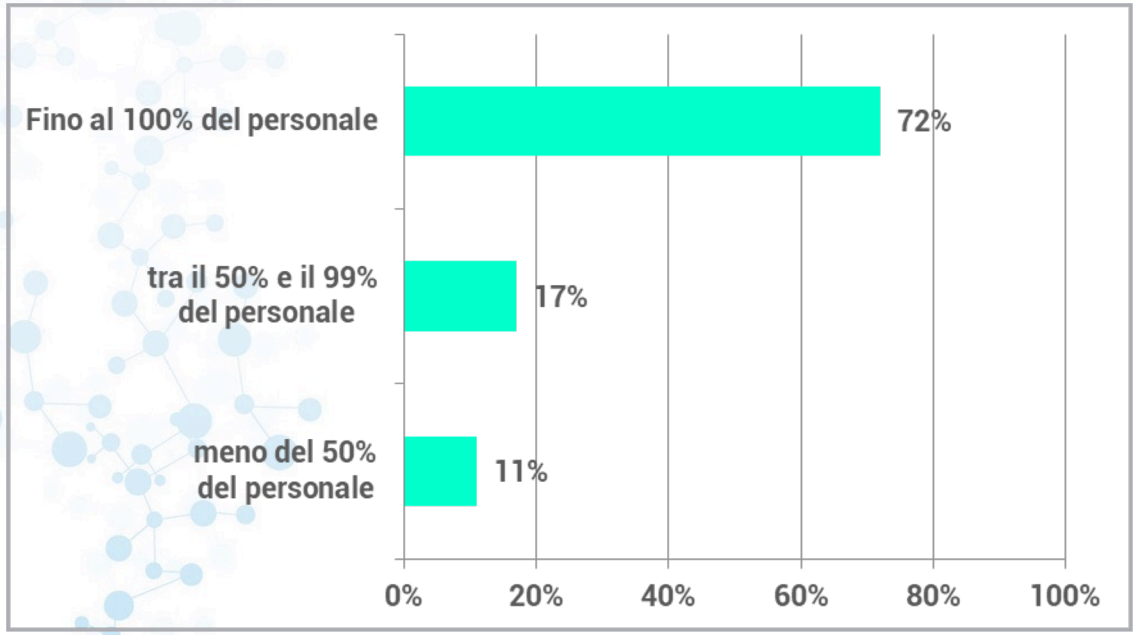
3. EVOLUZIONE DEI PATTERN DI ATTACCO

4. INIZIATIVE DI SETTORE PER LA MITIGAZIONE DEI RISCHI

Le Strutture di Cybersecurity
Ricorso al lavoro agile

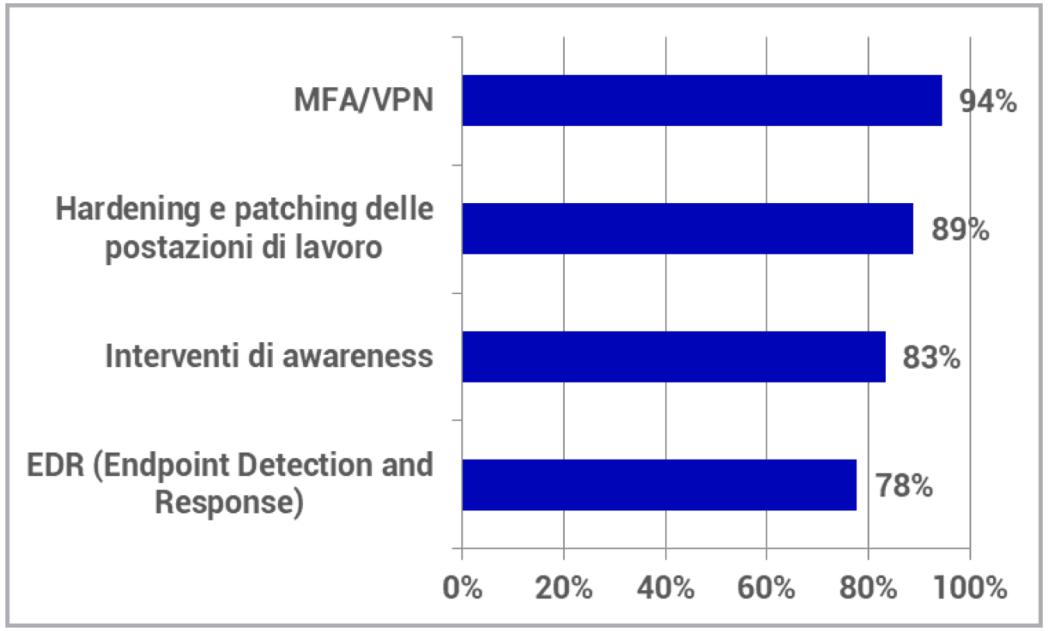
Il **100%** delle imprese rispondenti ha dichiarato di avere utilizzato il **«lavoro agile»,** seppur con quote di personale differenziate.

PERCENTUALE DI PERSONALE INDIRIZZATO VERSO IL LAVORO AGILE



La cybersecurity nel settore assicurativo 2021 – Percentuale di dipendenti indirizzati verso il lavoro agile nell'arco del 2020 (18 rispondenti)

STRUMENTI TECNLOGICI ADOTTATI PER PREVENIRE EVENTI CYBER

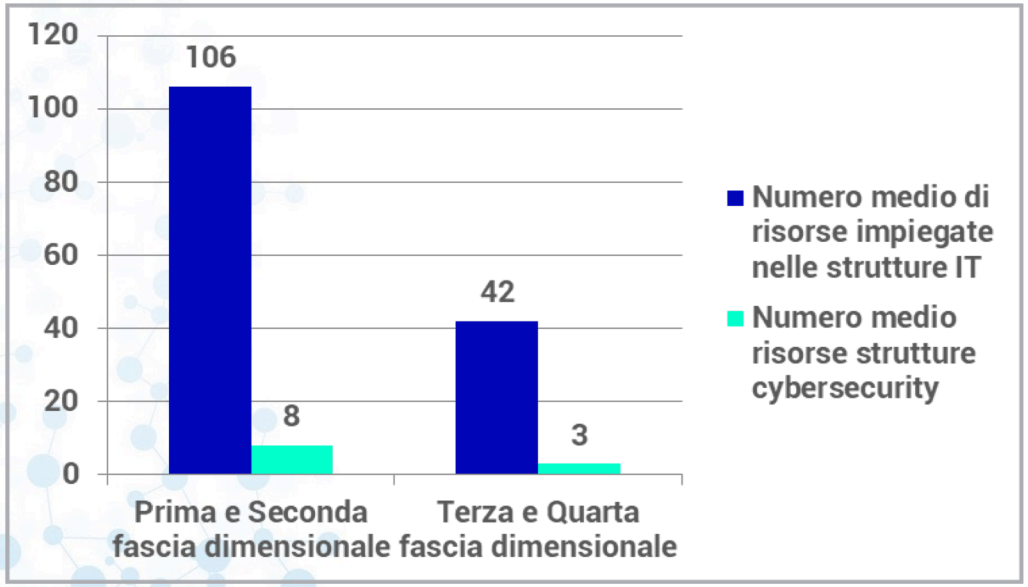


La cybersecurity nel settore assicurativo 2021 – Dotazione di strumenti tecnologici per prevenire eventuali eventi di sicurezza verso dipendenti/agenti che operano da remoto (18 rispondenti)

Il 94% delle imprese rispondenti, prevede di mantenere il «lavoro agile» tra le possibili modalità di lavoro per il personale dipendente anche a conclusione della crisi pandemica.

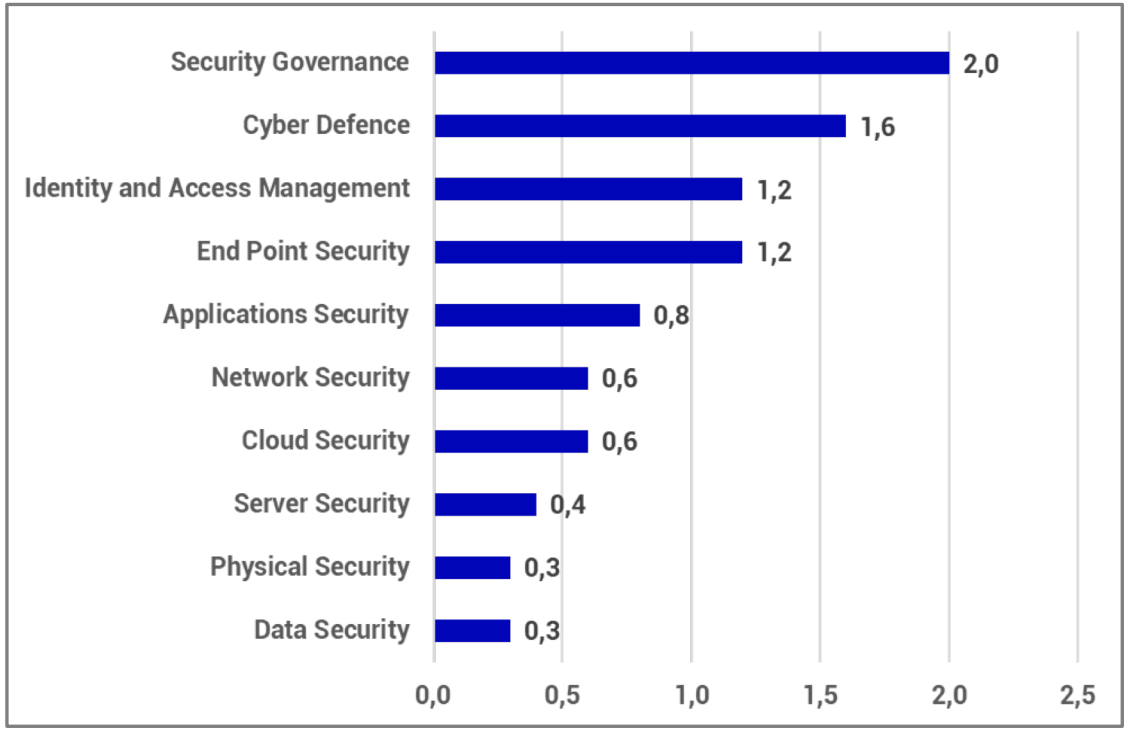
Le Strutture di Cybersecurity
Le Risorse umane dedicate

NUMERO DI RISORSE IMPIEGATE NELL'IT E NELLA CYBESECURITY



La cybersecurity nel settore assicurativo 2021 – Numero medio di risorse impiegate nelle strutture IT e numero medio di risorse impiegate per le attività di cybersecurity (15 rispondenti)

NUMERO DI RISORSE IMPIEGATE NEI DIVERSI AMBITI DI CYBERSECURITY

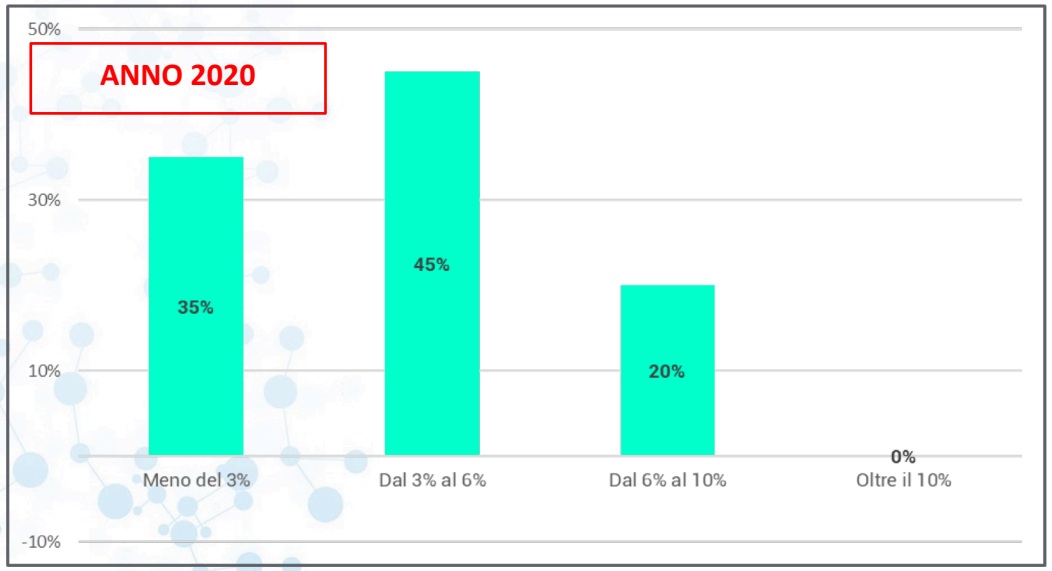


La cybersecurity nel settore assicurativo 2021 – Numero di risorse dedicate ai diversi ambiti della cybersecurity in FTE (15 rispondenti)

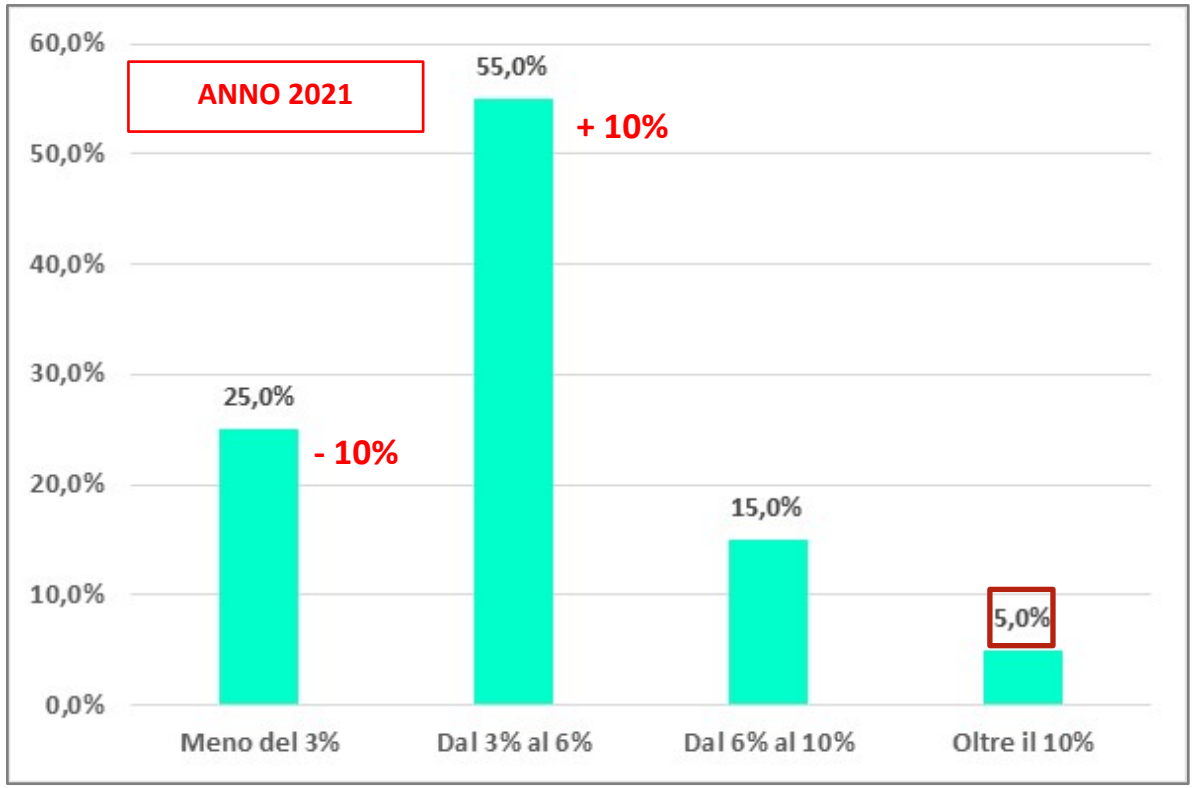
In entrambi i cluster di analisi, **il rapporto tra il numero medio di risorse impiegato all'interno delle strutture IT e il numero medio di risorse dedicato alle attività di cybersecurity si aggira intorno al 7%.**

Investimenti

Per il 2021 i volumi di budget previsti dalle imprese assicurative italiane, destinati alle attività di cybersecurity, continuano ad essere significativi, in linea con il trend registrato lo scorso anno:



La cybersecurity nel settore assicurativo 2021 – Previsioni di budget destinati alla sicurezza informatica, rispetto al totale del budget ICT stanziato dall'azienda.per l'anno 2020 (18 rispondenti)

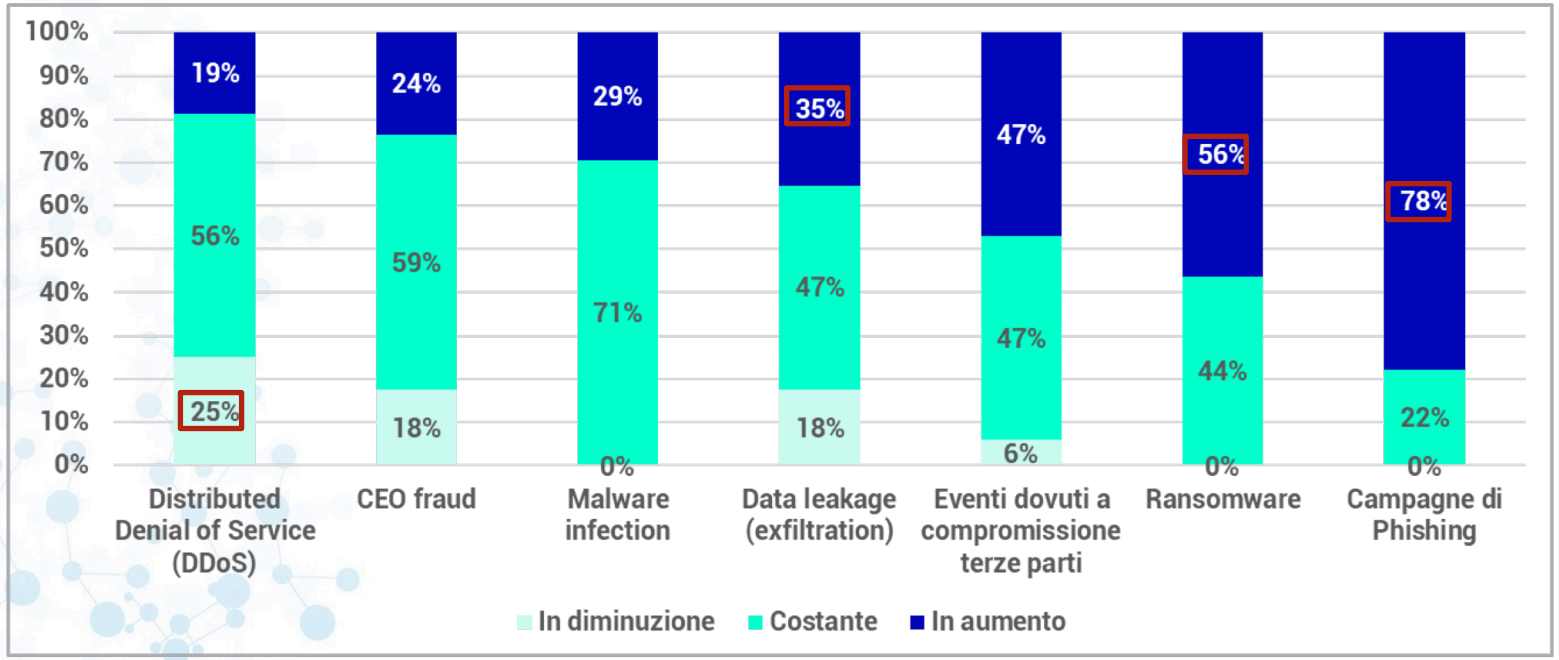


La cybersecurity nel settore assicurativo 2021 – Previsioni di budget destinati alla sicurezza informatica, rispetto al totale del budget ICT stanziato dall'azienda.per l'anno 2021 (189rispondenti)

Per il breve/medio periodo **il 73% delle imprese prevede un ulteriore aumento delle spese dedicate alla «security posture»** dell'azienda.

Trend degli eventi cyber

TENDENZA EVOLUTIVA DEGLI EVENTI CYBER



La cybersecurity nel settore assicurativo 2021 – Tendenza evolutiva degli attacchi cyber rilevati (16 rispondenti)

Il fenomeno del «furto di credenziali» ai danni della clientela resta molto circoscritto ma comunque segnalato da diverse organizzazioni.

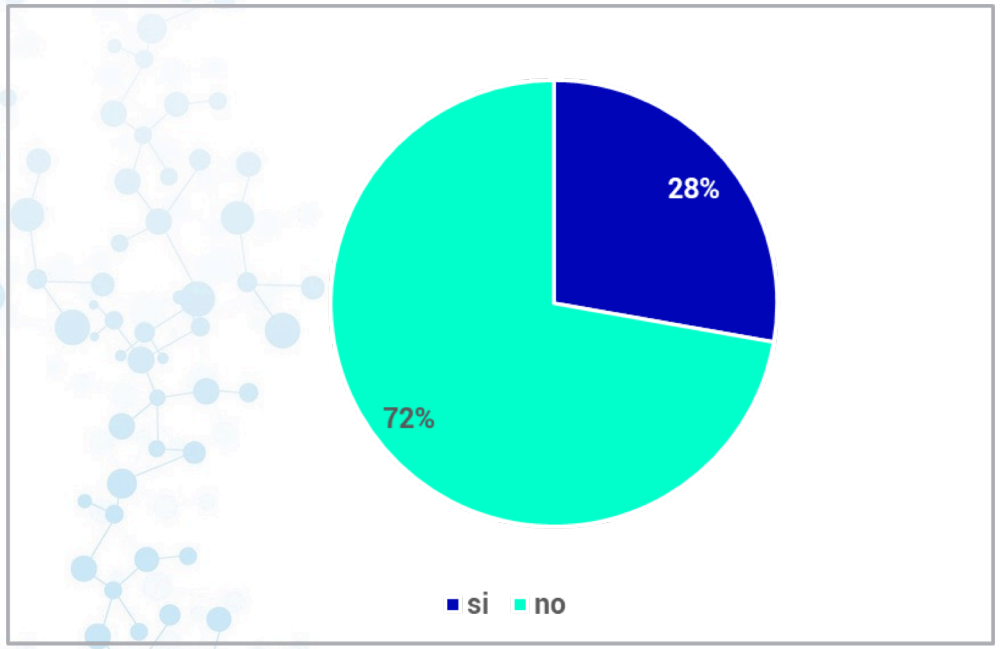
Alcune evidenze…..

- Il 25% dei rispondenti dichiara una diminuzione degli attacchi DDoS;
- Aumento delle campagne di Phishing;
- Aumento degli attacchi Ransomware;
- Aumento dei casi di Data Leakage.

Clonazione di siti web

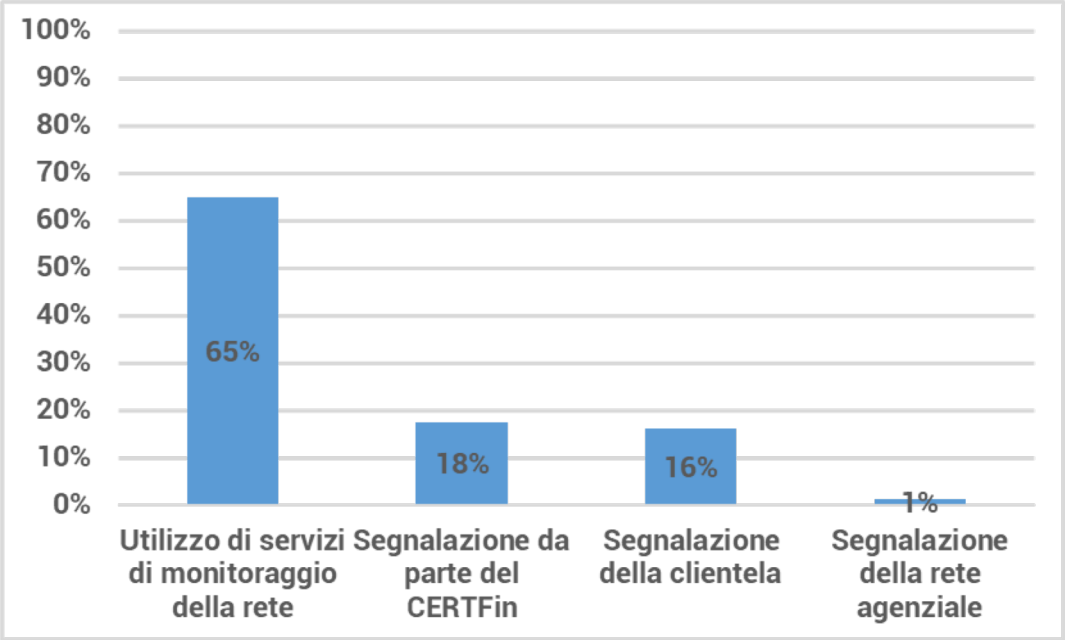
La clonazione a scopo fraudolento dei siti web delle imprese è un fenomeno di specifico interesse per il settore assicurativo. La maggior parte delle imprese presenti sul mercato italiano si è dotata di strumenti utili per la «*detection*» di questo tipo di minaccia.

IMPRESE CHE HANNO RISCONTRATO FENOMENI DI CLONAZIONE DI SITI UFFICIALI DELL'AZIENDA



La cybersecurity nel settore assicurativo 2021 – Percentuale di imprese che hanno rilevato casi di clonazione di siti web ufficiali di proprietà dell'azienda. (17 rispondenti)

MODALITA' TRAMITE LE QUALI LE IMPRESE SONO VENUTE A CONOSCENZA DI CASI DI CLONAZIONE DA SITI WEB.

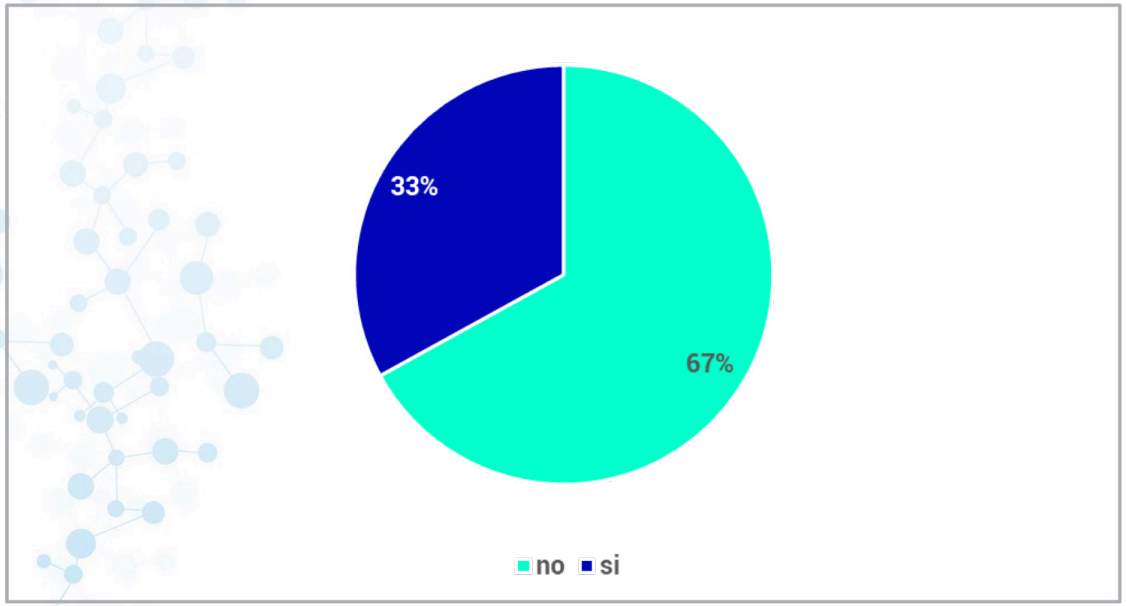


La cybersecurity nel settore assicurativo 2021 – Modalità con le quali l'impresa è venuta a conoscenza dei «siti clone». (5 rispondenti)

Ghost Broking

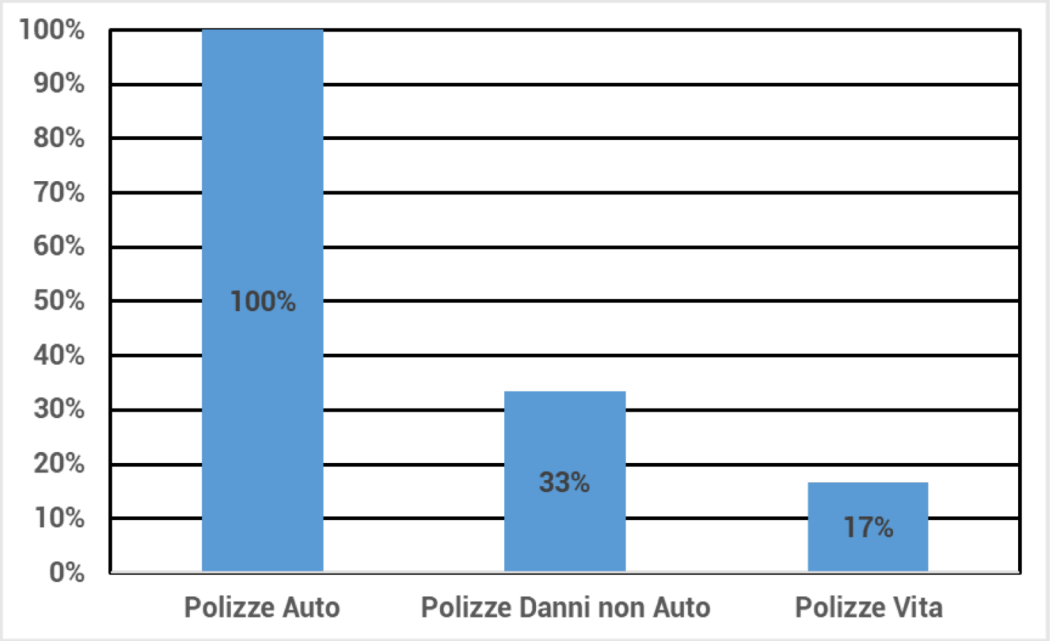
Con il termine ***«Ghost Broking»*** si intende quel fenomeno nel quale il frodatore, spacciandosi per agente di una impresa assicurativa, a seguito del pagamento di una somma di denaro rilascia una «polizza» assicurativa falsa.

IMPRESE CHE HANNO GHOST BROKING ATTRAVERSO IL CANALE INTERNET



La cybersecurity nel settore assicurativo 2021 – Percentuale di imprese che hanno rilevato casi di clonazione di siti web ufficiali di proprietà dell'azienda. (17 rispondenti)

IMPRESE CHE HANNO RISCONTRATO FENOMENI DI CLONAZIONE DI SITI UFFICIALI DELL'AZIENDA



La cybersecurity nel settore assicurativo 2021 – Ambiti all'interno dei quali si sono verificati casi di «ghost broking» nell'anno 2020 (6 rispondenti)

Per questo particolare fenomeno di frode si prevede, per il futuro, un trend in crescita

CERTFin

Agenda

1. LO SCENARIO ATTUALE DELLE FRODI NEL SETTORE BANCARIO ITALIANO

2. LA GESTIONE DELLA SICUREZZA E LE FRODI NEL SETTORE ASSICURATIVO ITALIANO

3. EVOLUZIONE DEI PATTERN DI ATTACCO

4. INIZIATIVE DI SETTORE PER LA MITIGAZIONE DEI RISCHI

Debolezze del canale di comunicazione

Negli ultimi anni gli attaccanti hanno imparato a sfruttare abilmente alcuni *vulnus* propri delle comunicazioni elettroniche, contattando i clienti con finalità malevole fingendo di essere la banca.

Social Engineering: nell'ambito bancario, un attacco di ingegneria sociale, condotto ai danni della clientela, prevede l'interazione del cybercriminale con l'utente al fine di indurlo a cedere i suoi dati riservati (es. dati bancari, codici OTP, etc.).

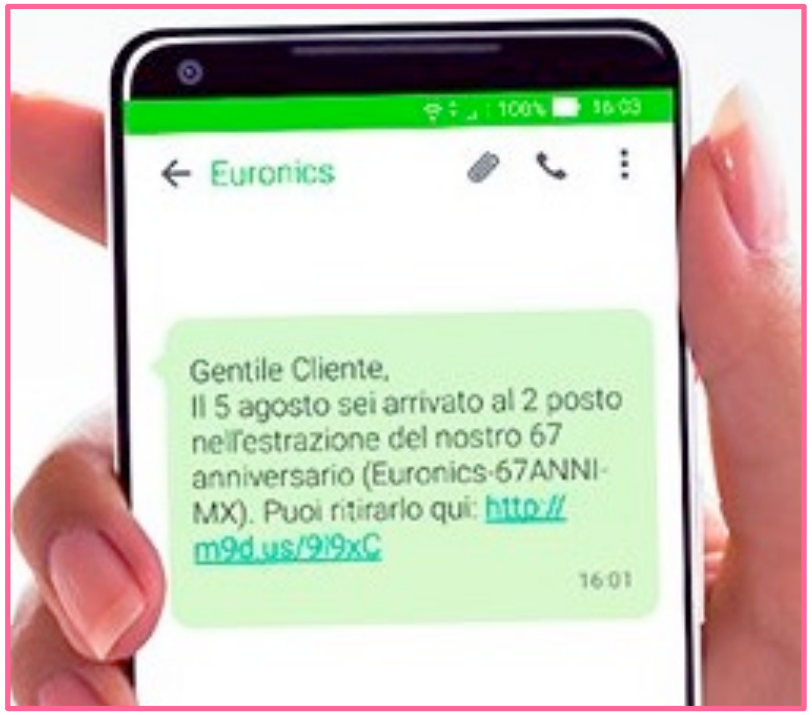
Tali attacchi sono stati resi sempre più sofisticati e spesso l'attaccante perfeziona il suo mascheramento utilizzando diverse tecniche, a volte anche in combinazione tra loro:

Smishing: descrive i tentativi dei truffatori di ottenere informazioni personali, finanziarie o di sicurezza tramite SMS. Spesso la vittima viene invitata a cliccare su un link malevolo.

Vishing: la vittima riceve una telefonata in cui i truffatori, sempre mascherandosi da qualcun altro, cercano di indurre la vittima a rivelare informazioni personali, finanziarie o di sicurezza o anche a trasferire denaro.

Alcune tecniche sfruttate dai frodatori

SMS con Alias Illegittimi: Negli schemi fraudolenti più comuni gli attaccanti utilizzano un alias illegittimo che evoca il nome della banca o di un altro mittente attendibile.



Alcune tecniche sfruttate dai frodatori

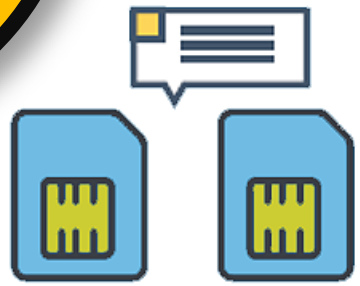
CLI Spoofing: La tecnica che permette di mascherare il numero originatore di una chiamata (su canale fonia) con una numerazione fittizia.

CERTFin

SIM SWAP Fraud

A fraudster obtains the **victim's personal data** through phishing, malicious app, data breaches, malware.

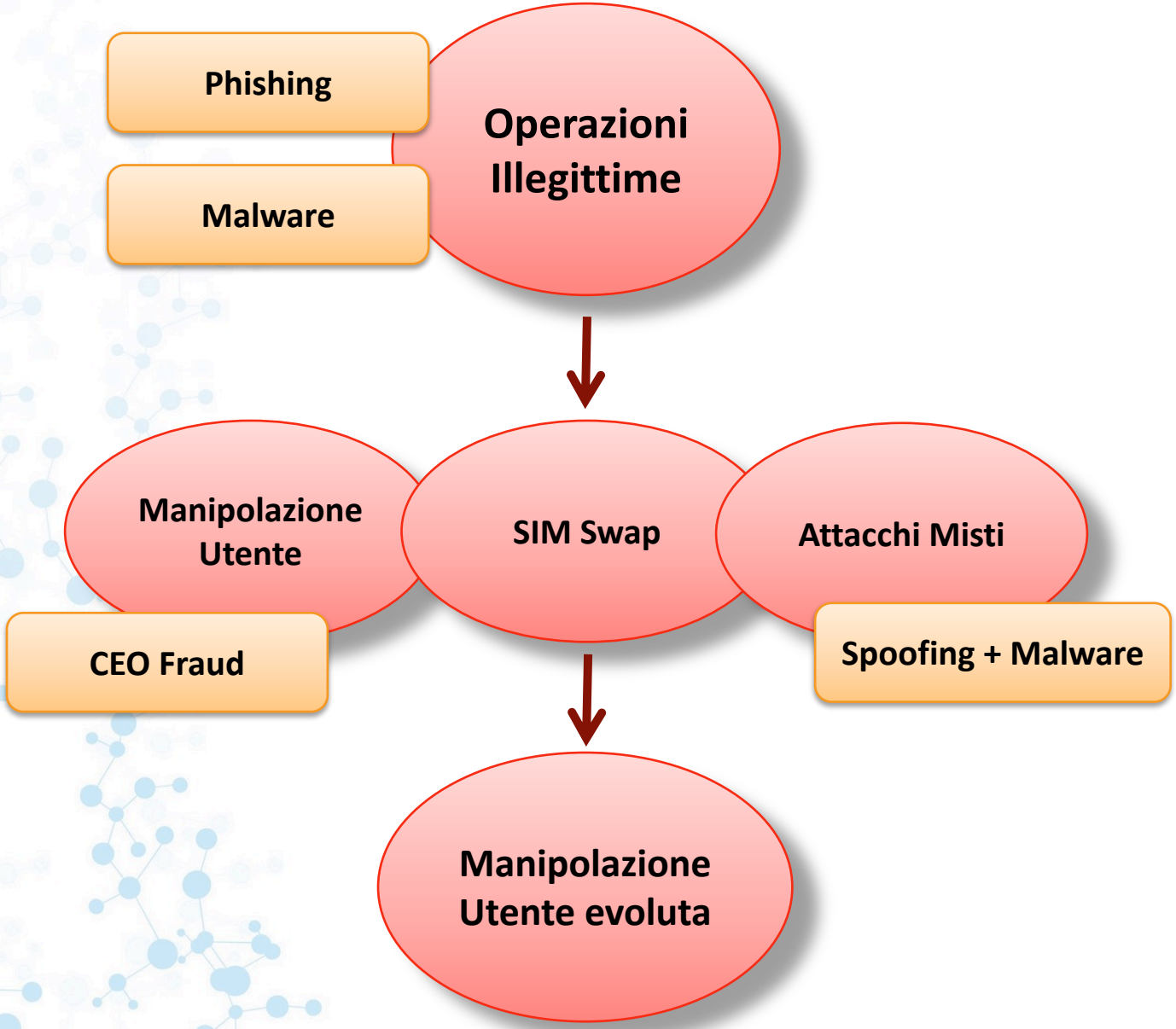
With this information the fraudster convinces the mobile operator to move the victim's number in a **SIM in his possession**

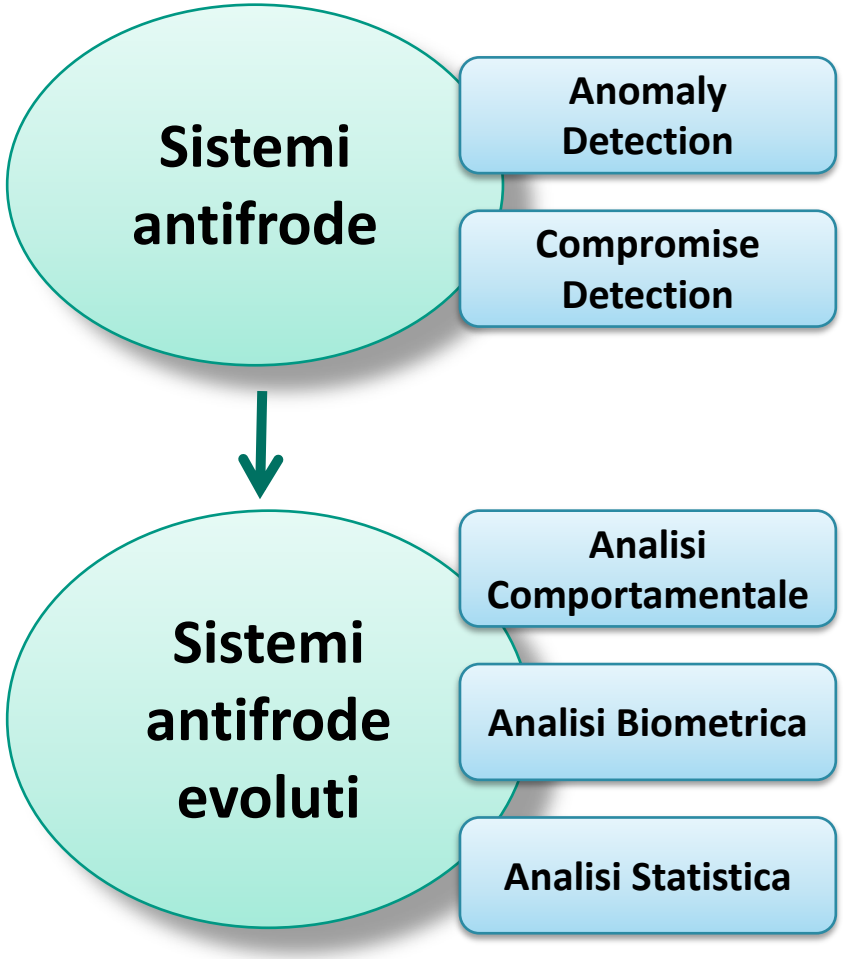


Now the fraudster can receive incoming calls and SMS, and **access to victim's bank account**

The victim will notice **the phone lost service** and eventually he discovers he cannot login in his bank account

Evoluzione dei Fraud Patterns





Caso 1:
Smishing + Spoofing + Social Engineering

#1

La vittima riceve un SMS inviato apparentemente dalla propria banca (SMS Alias). Tipicamente il messaggio annuncia che è stato rilevato un accesso non autorizzato al conto e che a breve sarà contattato dal reparto sicurezza

15:22

15:25

#2

La vittima riceve una chiamata apparentemente proveniente dalla sua banca in cui un finto operatore di banca convince il cliente che alcuni hackers hanno ottenuto l'accesso al suo conto e che i suoi soldi sono in pericolo

#3

Il falso operatore trasmette alla vittima ansia e un senso di urgenza ad intervenire, le fornisce un IBAN di appoggio nel quale depositare temporaneamente i suoi soldi finché la situazione non sarà ripristinata. **La vittima, di suo pugno, procede a trasferire i soldi sul conto del frodatore**

15:48

***Totale**: 24 minuti*

Un bonifico bancario fraudolento realizzato tramite questa modalità di attacco è molto complesso da identificate da parte dei sistemi antifrode: non c'è compromissione ed è l'utente stesso ad effettuare la transazione utilizzando credenziali e device corretti.

Caso 2:
Smishing + Vishing + Malware

11:46

#1

La vittima riceve un SMS sospetto con un link alla pagina di phishing inviato apparentemente dalla propria banca (SMS Alias). Tipicamente nel messaggio si invita la vittima a cliccare su un link con la scusa di aver rilevato un accesso non autorizzato al conto

11:50

#2

Un finto operatore di banca chiama la vittima sfruttando le informazioni che la vittima stessa ha consegnato al frodatore tramite la pagina di phishing

11:52

#3

Il falso operatore di banca invita la vittima a scaricare un aggiornamento dell'app bancaria. **Invio del link per scaricare il malware via SMS alla vittima.**

12:24

#4

Il frodatore ha il pieno controllo del dispositivo della vittima, può quindi interagire con l'applicazione bancaria e disporre 2 bonifici bancari.

La Vittima riceve quindi 2 SMS legittimi dalla propria banca che confermano l'autorizzazione di 2 bonifici bancari

12:30

#5

La vittima riceve un SMS falso inviato apparentemente dalla propria banca che **conferma lo storno (falso) dei 2 bonifici**

***Totale**: 44 minuti*

Anche in questo caso l'attaccante inganna la vittima e utilizza il suo stesso device per effettuare transazioni non autorizzate, pur supportato dalla presenza di un software malevolo.

Caso 3:
Vishing + Social Engineering + Malware

#1
La vittima riceve una telefonata durante la quale viene convinta ad **effettuare un investimento di prova su una piattaforma di trading online.** La vittima effettua un bonifico di 1000 euro e le viene aperto un conto *ibanizzato*.

GIORNO 1

GIORNO 7

#2
Si susseguono telefonate tra il frodatore e la vittima, quest'ultima investendo seguendo le indicazioni ricevute, **arriva a totalizzare sulla piattaforma un importo di 5000 euro**

GIORNO 8

#3
Dopo la presunta prova che la piattaforma funziona, il frodatore convince la vittima ad incrementare il suo investimento.
La vittima effettua un secondo bonifico di altri 1000 euro.

GIORNO 28

#4
Dopo altre tre settimane di continue interazioni, in cui il frodatore continua a guidare la vittima nei suoi (finti) investimenti, questa si ritrova un (flaso) credito di 41.000 euro. A questo punto il frodatore convince la vittima a scaricare una suite sw in grado di automatizzare le operazioni e incrementare ulteriormente i profitti.

GIORNO 30

#5
Attraverso la suite (di malware) il frodatore ruba ogni tipo di credenziale alla vittima ed acquisisce il controllo dei suoi devices.
Successivamente finalizza il prosciugamento del suo conto bancario

***Totale**: un mese!*

Il frodatore instaura una relazione duratura con la vittima, attraverso la quale guadagna la sua fiducia. La finezza tecnica, in questo caso, è l'aver trasferito i soldi dal conto della vittima non solo utilizzando le sue credenziali e il suo device, ma usando un IBAN verso il quale la vittima aveva già trasferito fondi senza disconosce le operazioni.

CERTFin

Agenda

1. LO SCENARIO ATTUALE DELLE FRODI NEL SETTORE BANCARIO ITALIANO

2. LA GESTIONE DELLA SICUREZZA E LE FRODI NEL SETTORE ASSICURATIVO ITALIANO

3. EVOLUZIONE DEI PATTERN DI ATTACCO

4. INIZIATIVE DI SETTORE PER LA MITIGAZIONE DEI RISCHI

Alcune considerazioni….

Le istituzioni finanziarie aumentano il budget dedicato alla sicurezza, **affinano costantemente i propri sistemi di monitoraggio** e provvedono ad una identificazione continua di nuovi pattern di frode attraverso acquisizione di Indicators of Compromise.

L'evoluzione delle soluzioni di sicurezza (es. SCA) ormai è continua e adattiva per la necessità di cambiare appena si rilevano nuove modalità /vulnerabilità utilizzate dai frodatori.

La sofisticazione delle frodi ormai passa da tecniche miste, ma ogni tecnica non prescinde dalla **manipolazione, diretta o indiretta, dell'utente**

Tuttavia, l'attaccante non compromette i sistemi informativi ma agisce prevalentemente con azioni di social engineering, che la banca può prevenire **solo con campagne di awareness**

Iniziative di settore per gli operatori: Esercitazioni presso il CERTFin

2018 Pubblicazione di TIBER_EU da parte della BCE (sulla base delle esperienze in Olanda e Belgio) e sviluppo di un progetto nazionale (REDFin)

2018 Analisi sullo stato dell'arte in Italia ed Europa delle esercitazioni Cyber Table-top e (Threat Intelligent Based) Red Teaming

2019 Definizione di metodologie di Cyber Threat Intelligence per la definizione di scenari di rischio e per la gestione ed esecuzione di Cyber Table-top e Red Teaming basati su tali scenari

2020 Applicazione sul campo di tali metodologie e conduzione di 2 sessioni di Table-top (circa 90 risorse coinvolte) e 5 RED Teaming insingole aziende

2021 1 esercitazione Table-top

2021
2022 In ragione delle esigenze della Constituency:

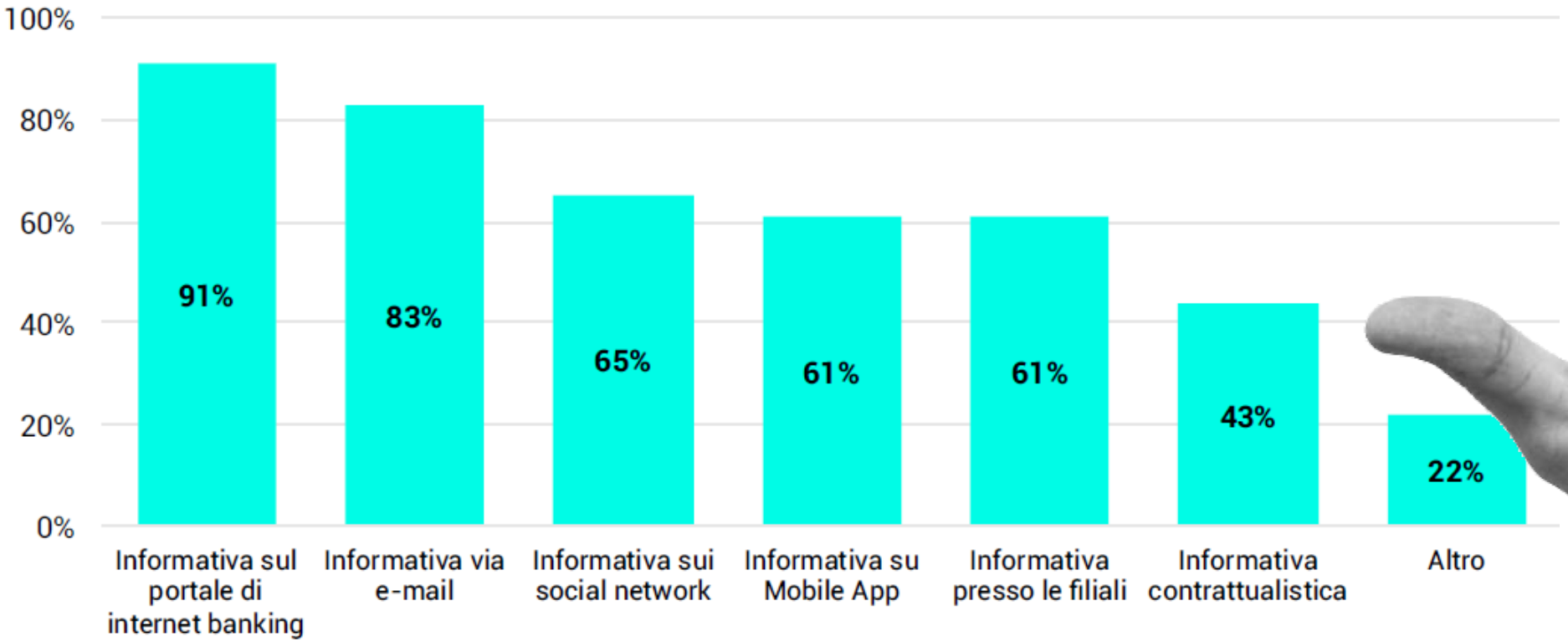
- 2 esercitazioni Table Top
- 2 esercitazioni Capture the Flag
- supporto per sessioni di RED Teaming

Iniziative di settore per la clientela: Campagna di awareness

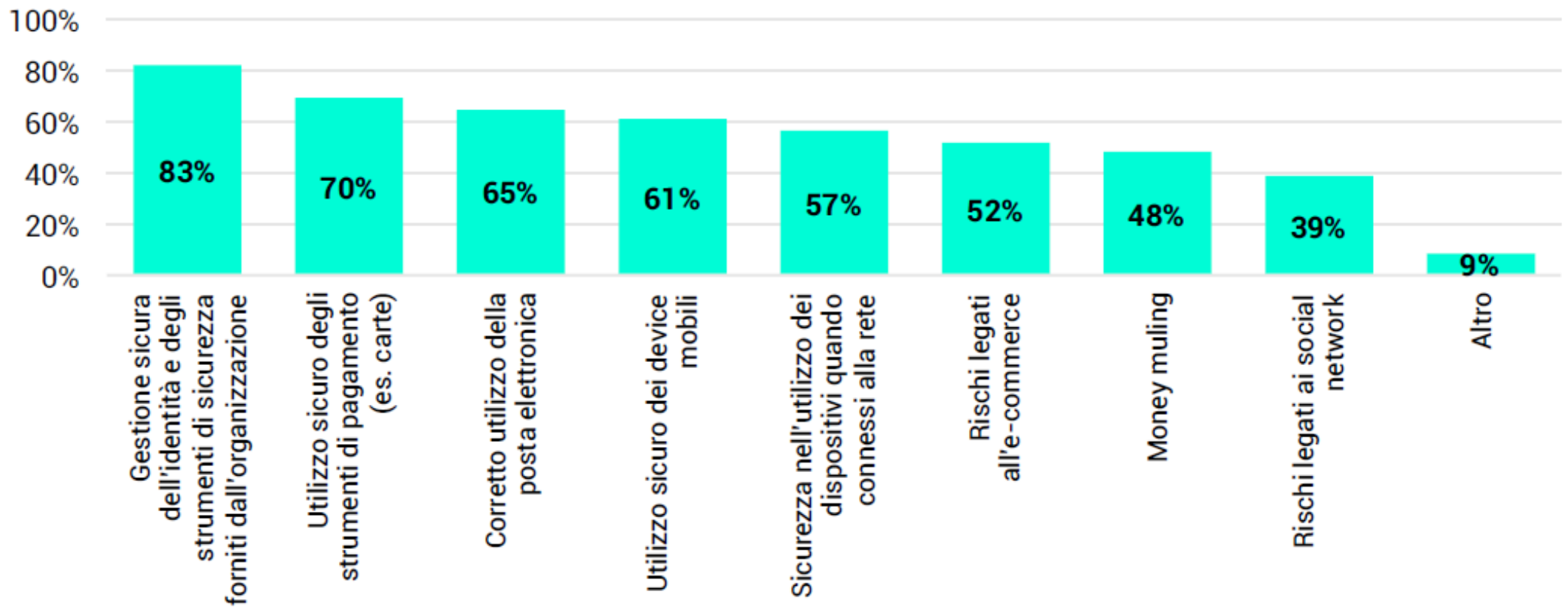
Campagna awareness

Cybersecurity awareness per la clientela
i canali

Le banche sfruttano tutti i diversi canali disponibili per comunicare con i propri clienti e condividere aggiornamenti e raccomandazioni su un corretto uso dei device e su buone pratiche di comportamento nella gestione di credenziali e strumenti di pagamento.



Cyber awareness per la clientela
i temi



I clienti sono periodicamente informati in merito a diverse tematiche che vanno da un uso corretto dei dispositivi per realizzare operazioni bancarie a distanza a buone pratiche nella gestione di credenziali e password.

Iniziative di settore per la clientela
Campagna di awareness

Il CERTFin, insieme a ABI, Banca d'Italia e Ivass, sta per lanciare una **campagna di comunicazione integrata** volta ad evidenziare l'attenzione e l'impegno del settore finanziario sui temi legati alla cybersecurity, con lo scopo di informare e proteggere la propria clientela.

OBIETTIVI:

- innalzare il livello di attenzione sulla cybersecurity
- motivare l'utenza finale ad un uso sicuro dei canali e strumenti digitali
- aumentare la consapevolezza dei clienti e sensibilizzarli sui comportamenti virtuosi da adottare per ridurre i rischi di attacchi informatici e frodi online e sull'uso sicuro degli strumenti digitali, mantenendo alta la fiducia verso i canali remoti
- valorizzare l'azione congiunta di settore e rendere consapevole la clientela del ruolo di presidio/protezione svolto dal sistema finanziario e dalla propria banca
- moltiplicare il messaggio attraverso azioni di partnership con le realtà aderenti al progetto

Campagna di cybersecurity awareness
Dettagli

QUANDO?

La campagna sarà on air dal 23 novembre alla fine dell'anno.

INCLUSIVITÀ

Nella nostra famiglia ci sarà spazio per diverse declinazioni di diversity.

Tone of voice

La cybersecurity e il mondo delle minacce informatiche saranno affrontate attraverso un **tono di voce leggero, ironico, chiaro** e **diretto**.

CANALI

TV, stampa, digital, social

La campagna sarà veicolata attraverso canali complementari rispetto a quelli usati abitualmente dalle banche.

OUTPUT

spot TV, web serie, banner, carousel e quiz per piattaforme social, materiali btl per rete fisica

8 video pillole dedicate a 8 tipologie di truffe informatiche

Thank You!

CERTFin

Defend. Inform. Evolve.

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

CERTFin

BACK UP

I Principali Steps

Furto di credenziali e/o dati riservati della vittima

Accesso non autorizzato all'home banking e/o Account Takeover

Realizzazione operazioni non autorizzate

Transaction Monitoring → Blocco Operazione

Spostamento del denaro verso uno o più conti di appoggio e successivo riciclaggio

Procedure di collaborazione → Blocco C/C