24 NOVEMBRE 2021

ATTENTI A QUEL LINK!

Come proteggere i tuoi dati bancari e non cadere nelle trappole delle frodi online

Relatore: Anna Gardumi (Servizio Information Security – Cassa Centrale Banca)

La Cassa Rurale
Adamello Giudicarie Valsabbia Paganella
CREDITO COOPERATIVO ITALIANO

CASSA CENTRALE BANCA
CREDITO COOPERATIVO ITALIANO

INDICE DEI CONTENUTI

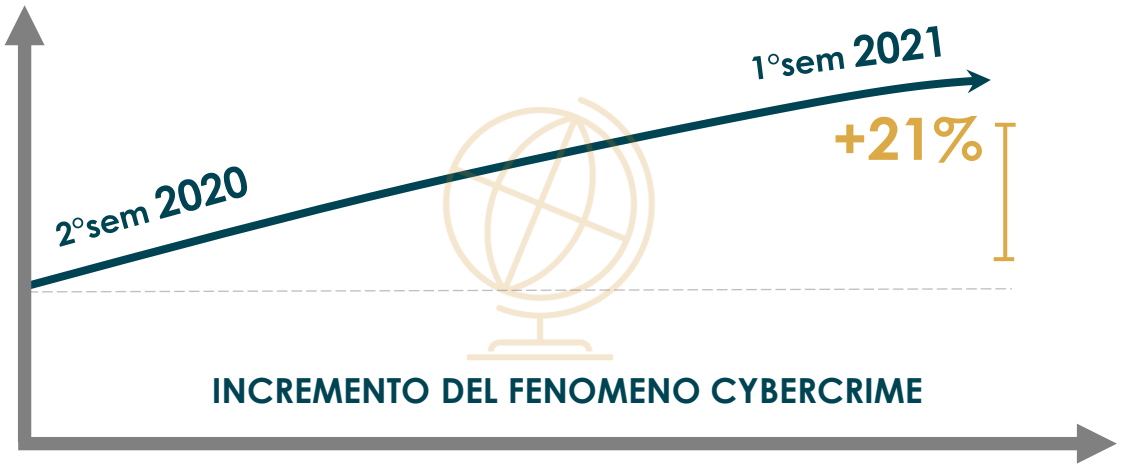
INTRODUZIONE E CONTESTO

INTRODUZIONE E CONTESTO

Cybercrime

Per «cybercrime» si intendono quei reati perpetrati attraverso l'uso di Internet da soggetti, singoli o organizzazioni, spinti da motivazioni criminose e, generalmente, per trarne profitto.

Rapporto Clusit Nov. 2021: «se ad oggi il 2020 è stato l'anno *peggiore di sempre* in termini di evoluzione delle minacce "cyber" e dei relativi impatti, evidenziando un trend persistente di crescita degli attacchi, della loro gravità e dei danni conseguenti, tale tendenza negativa si conferma ampiamente anche nel primo semestre 2021»



Truffe on-line

Per «truffe on-line» si intendono tutte le **varie tipologie di truffe che si riscontrato in rete**: e-commerce, immobiliari, finanziarie, falso trading on-line, "sentimentali", etc.

Rapporto Clusit Nov. 2021 (Polizia Postale): «Attraverso sofisticate metodologie di **social engineering** e facendo leva sui "bisogni" delle persone i cyber-criminali, proponendo facili guadagni, investimenti miracolosi o illusorie relazioni sentimentali, individuano il loro target che, con artifici e raggiri, viene invogliato ad investire ingenti somme di denaro, acquistare "prodotti" a prezzi sensibilmente più bassi di quelli proposti dal mercato o su siti web abilmente contraffatti»

Le truffe on-line nel 2020 sono state **agevolate dall'emergenza sanitaria** che ha determinato un aumento inimmaginabile dello smart working, degli acquisti on-line e, in generale, dell'utilizzo di internet nella vita professionale e privata ed ha reso più appetibili e credibili email di spam basate attorno a finte comunicazioni apparentemente provenienti dell'Agenzia dell'Entrate, INPS o altri enti che erogavano contributi economici.

CYBERCRIME FINANZIARIO

Il settore finanziario, che include le industrie bancarie e assicurative, è stato il settore più attaccato per il quinto anno consecutivo nel corso del 2020 (23% di tutti gli attacchi)[1].

La **frode bancaria** passa quasi sempre attraverso il **furto delle credenziali d'accesso** ai sistemi bancari o di pagamento, **dei fattori di autenticazione forte, dei dati delle carte di pagamento** ed il loro riutilizzo per transazioni fraudolente all'insaputa del titolare.

Invece di attaccare direttamente la banca, è preferito l'obiettivo più facile di attaccare i suoi clienti.

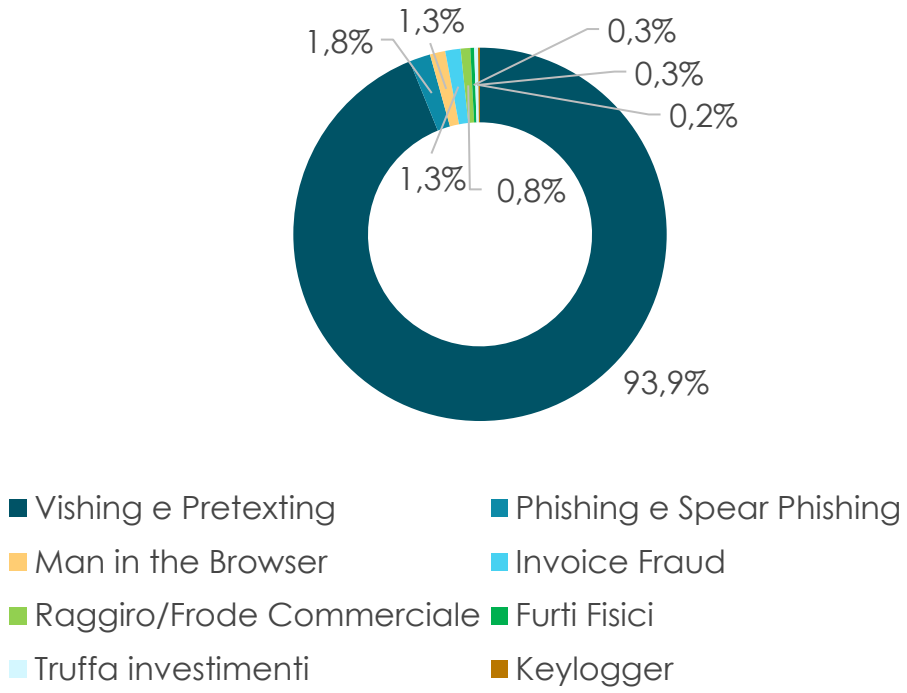
L'analisi delle principali campagne del 2021 mostra che la frode avviene prevalentemente attraverso il **Social Engineering** (ingegneria sociale).

Di seguito i principali vettori di attacco:

- **Phishing, vishing e smishing:** truffa che sfrutta la buona fede dell'utente utilizzando i canali di comunicazione digitali (email, chiamate e sms) per ottenere dati di accesso e/o informazioni personali;
- **Malware:** software malevolo in grado di infettare il dispositivo dell'utente ed esfiltrare informazioni sensibili o manipolare transazioni;
- **hacking del dispositivo** mobile: ad esempio tramite SIM Swap.

La tecnica, o la **combinazione di tecniche**, varia in base alla vittima, con differenze tra il cliente finale (*retail*) oppure aziendale (*corporate*).

Tecniche di frode più utilizzate[2]



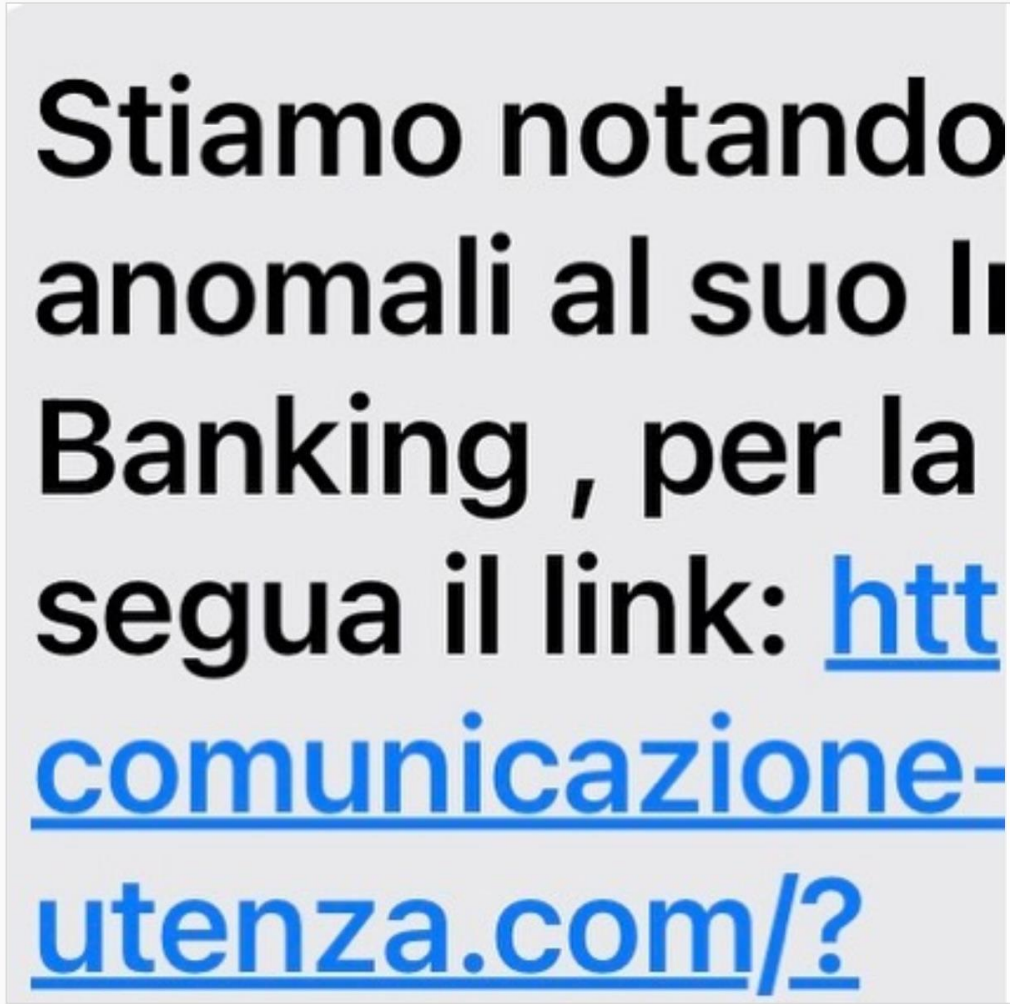
[1]Rapporto Clusit 2021 – Edizione di Novembre 2021
[2]Dati del Gruppo Cassa Centrale

CASI «NOTI»: LINUS E IL PHISHING BANCARIO

https://www.deejay.it/articoli/linus-sono-rimasto-vittima-di-una-truffa-digitale-il-racconto-a-deejay-chiama-italia/

CASI «NOTI»: LINUS E IL PHISHING BANCARIO

Linus: “Sono rimasto vittima di una truffa digitale”. Il racconto a Deejay Chiama Italia



linus_dj L’avevo detto stamattina che la giornata prometteva male.
Ma può sempre andare peggio.
È stata una progressione inesorabile, fino al capolavoro di poco fa. Mi arriva un sms dalla banca che mi dice che sono stati notati movimenti anomali. Controllo il mio account e non c’è nulla, per fortuna. Poi mi chiama un gentilissimo funzionario che mi chiede se ho fatto qualcosa con riferimento Lugano. Mi viene in mente Roberto Ferrari ma per una volta non c’entra nulla, quindi no.
Allora il tipo al telefono con grande pazienza mi spiega che sono stati fatti quattro bonifici dal mio conto è che bisogna bloccarli.
Parte tutto un giro di sms con codici da inserire che dura almeno 45 minuti.
Dopodiché sparisce.
Apro l’home banking e ci sono due prelievi da 2500 euro l’uno.
Fottuto!
Questa volta finalmente chiamo io la banca e con imbarazzo mi dicono una cosa che è la vera morale della favola: la Banca non chiama mai.
Al massimo vi può chiamare la vostra persona di riferimento.
Non rispondete mai ad sms e mail, soprattutto non aprite gli allegati.

https://www.deejay.it/articoli/linus-sono-rimasto-vittima-di-una-truffa-digitale-il-racconto-a-deejay-chiama-italia/

PHISHING E SITI CLONE

PHISHING E SITI CLONE

Di seguito si descrivono le fasi principali della tipologia di frodi più comune nel caso di phishing:

1 SMS

Sul cellulare del Cliente arriva un SMS a nome Inbank che segnala la sospensione temporanea dell'utenza dell'Internet Banking e che invita ad aggiornare le informazioni legate all'utenza stessa.

2 Siti di phishing

Il link presente nel messaggio porta ad un sito clone di Inbank, in cui il Cliente inserisce non solo le **credenziali personali** (**username** e **password**), ma anche il numero di **telefono**, il numero della **carta di credito**, la scadenza e il CVV2 della stessa.

3 Contatto telefonico

Il Cliente riceve una telefonata dal finto numero di assistenza di Inbank (o dal numero ufficiale della Banca) da parte del truffatore che impersona un impiegato e gli comunica la necessità di bloccare alcune disposizioni fraudolente. Tale azione ha l'obiettivo di carpire i codici di autorizzazione.

4 Azioni pre-frode

Il Frodatore con le informazioni ottenute è in grado agire in autonomia al fine di occultare la propria operatività e preparare quanto necessario per commettere la frode vera e propria

5 Disposizioni fraudolente

Il frodatore è ora in grado di operare in autonomia mediante le credenziali e accedere al conto per effettuare le disposizioni fraudolente es. bonifici, ricariche di carte prepagate, acquisto di beni immateriali quali Bitcoin o altre criptovalute.

NUOVE PAGINE DI PHISHING AL GIORNO[1]

3,2 pagine/gg
2° sem. 2020

10,5 pagine/gg
Feb. 2021

COME SIMULANO IL NUMERO DELLA BANCA?

Molti sistemi VOIP consentono la configurazione del numero chiamante in uscita.

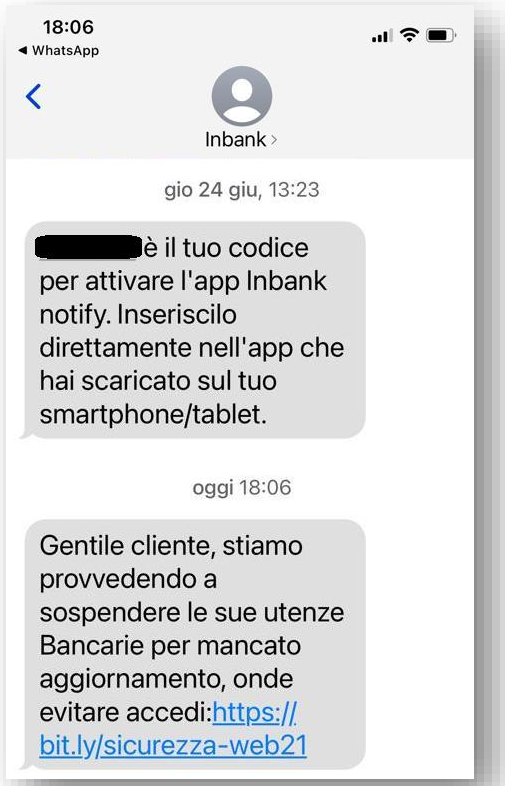
ABBATTIMENTO DELLE PAGINE DI PHISHING[1]

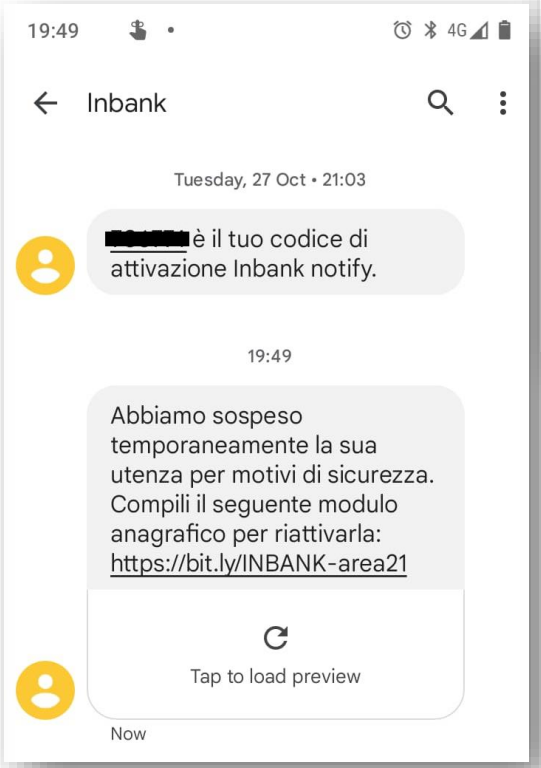
Nel 72% dei casi una pagina di phishing dura meno di 48 ore (grazie alle azioni di contrasto «takedown»), ma il ricambio è tale da mantenere il numero di pagine attive sempre sostenuto

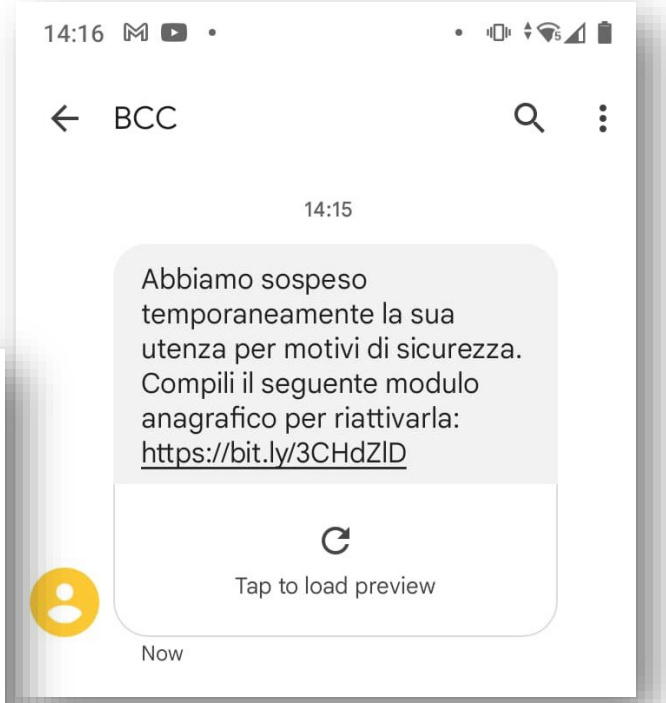
[1]Rapporto Clusit 2021 – Edizione di Novembre 2021

PHISHING E SITI CLONE

Esempi di SMISHING reali

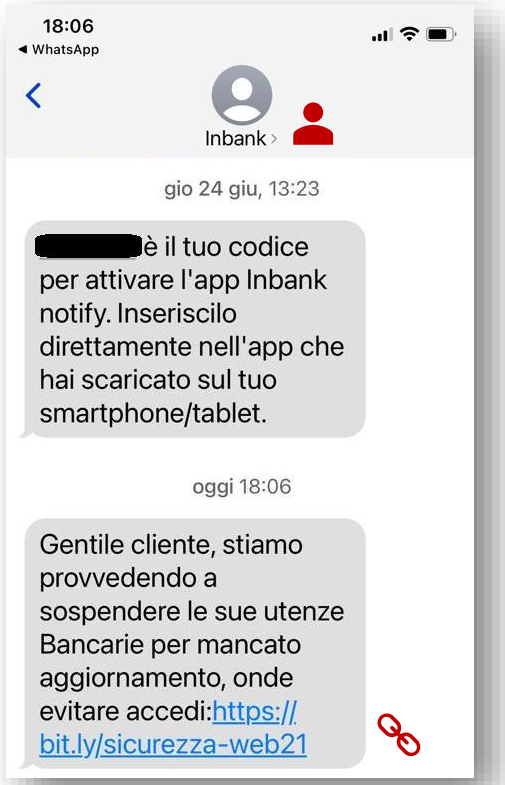


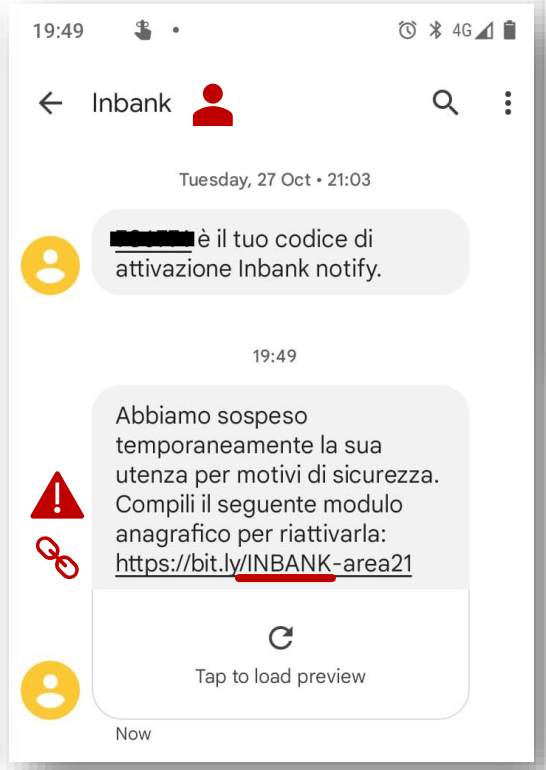


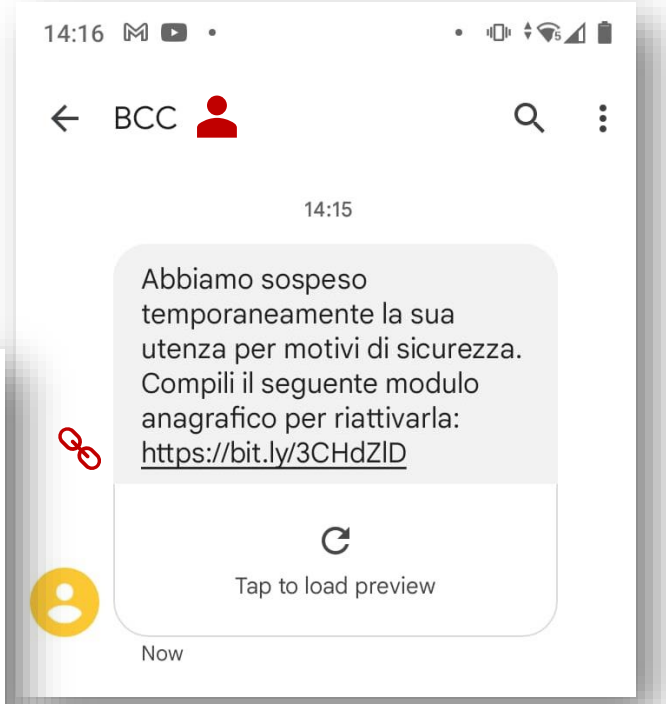


PHISHING E SITI CLONE

Esempi di SMISHING reali







Punti di attenzione:

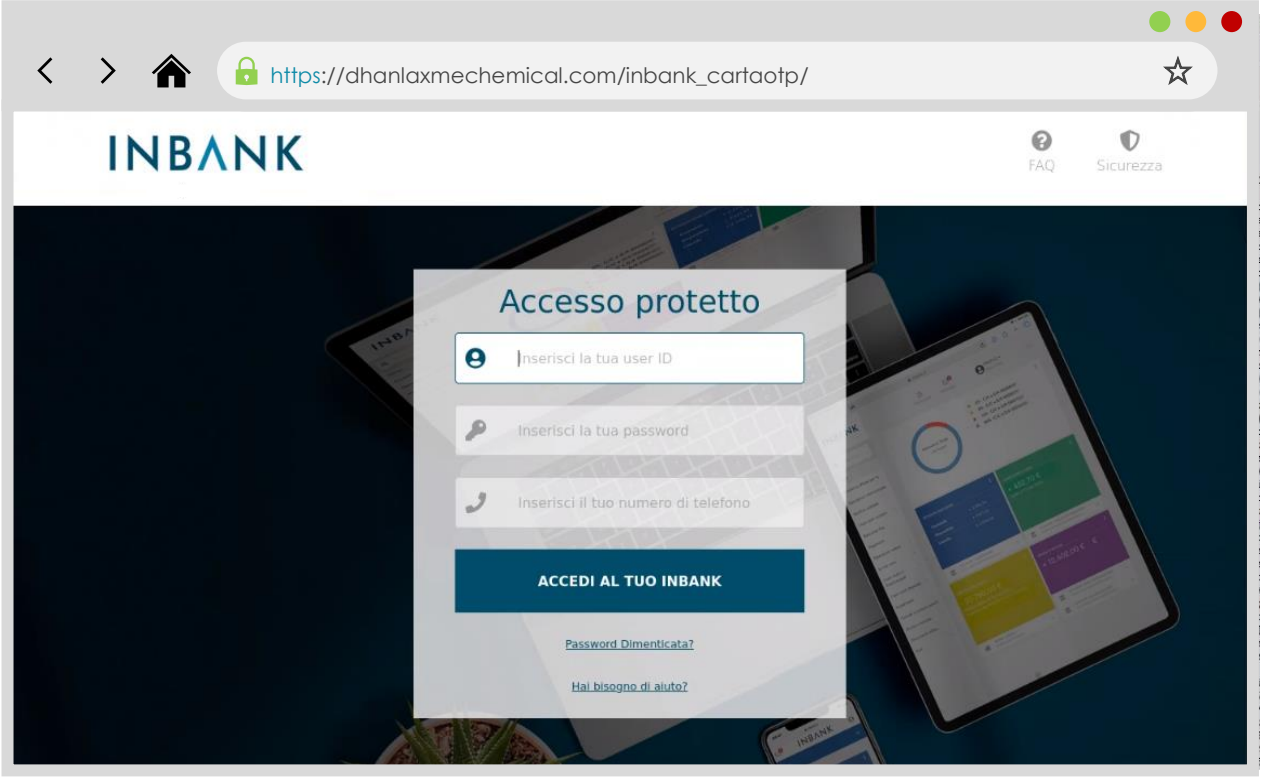
- Sospettare sempre della presenza di un link
- Il mittente può essere falsificato
- La presenza del nome «inbank» all'interno del link non è sufficiente

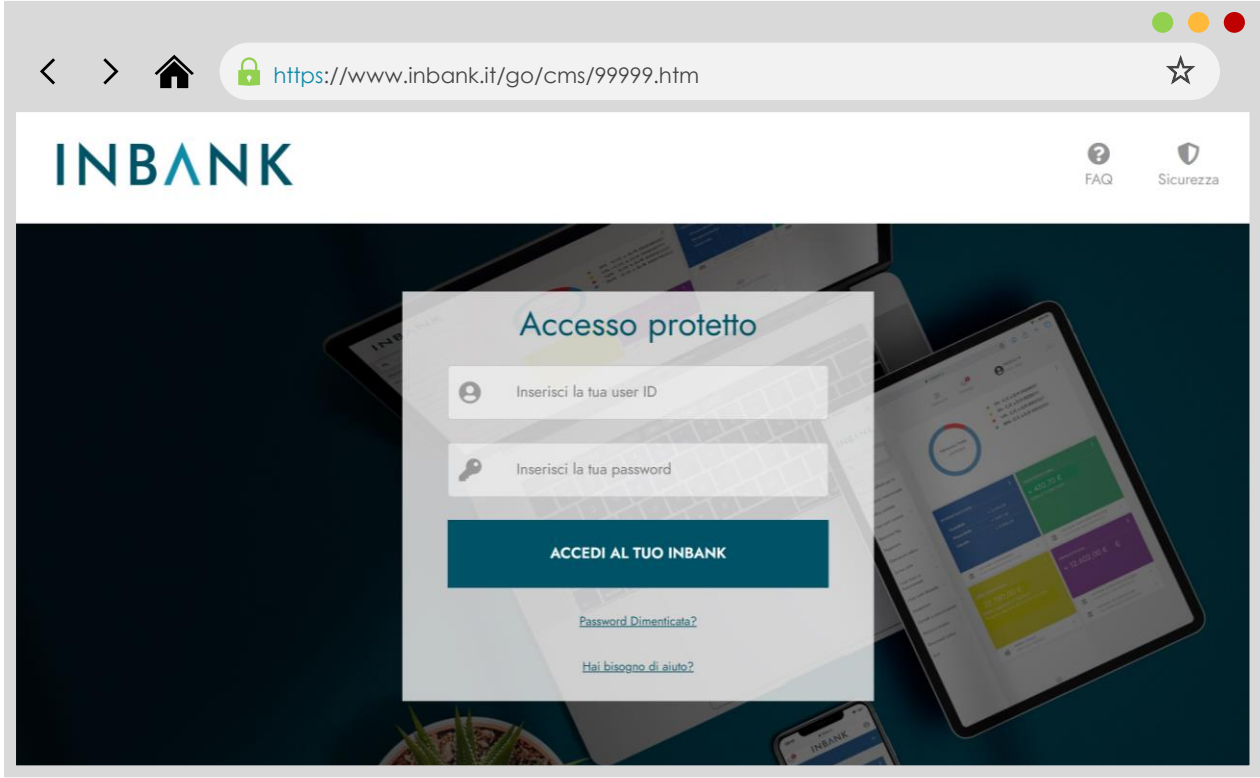
PHISHING E SITI CLONE

sito autentico o **sito clone**?

PHISHING E SITI CLONE

sito autentico o **sito clone**?

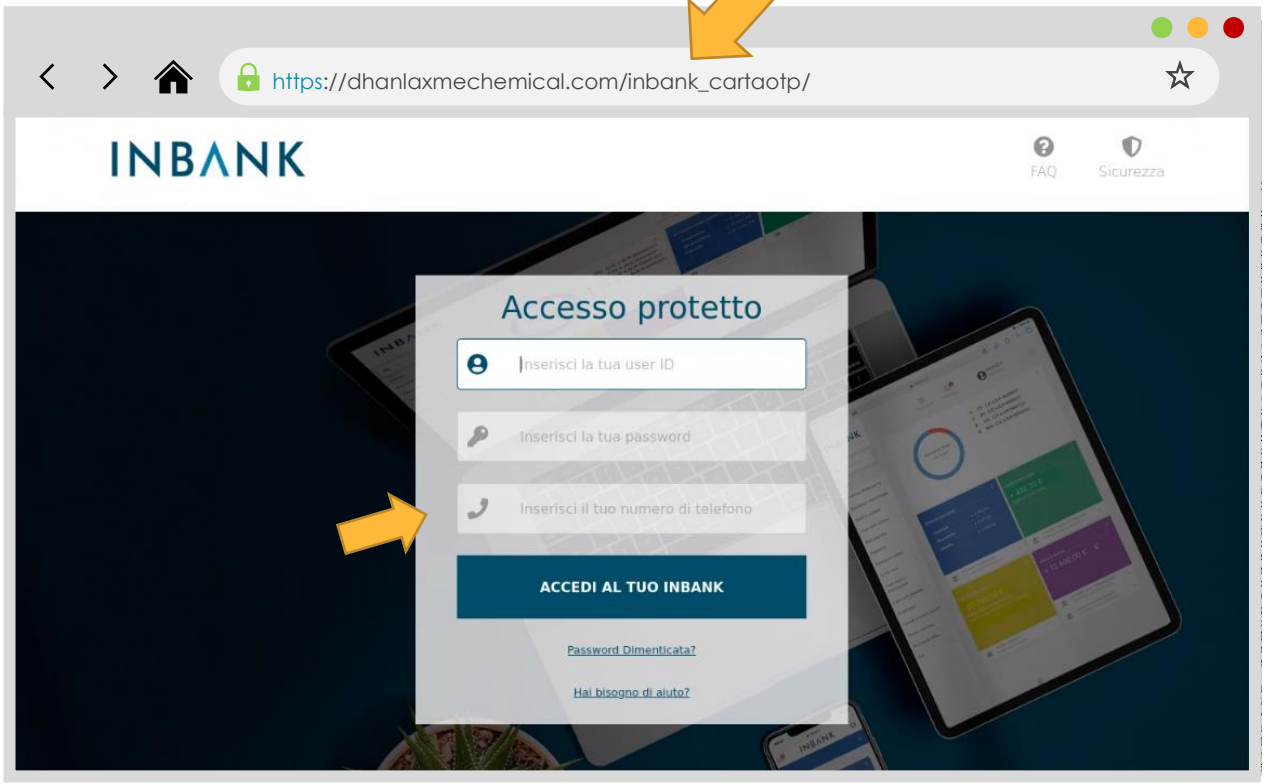




PHISHING E SITI CLONE

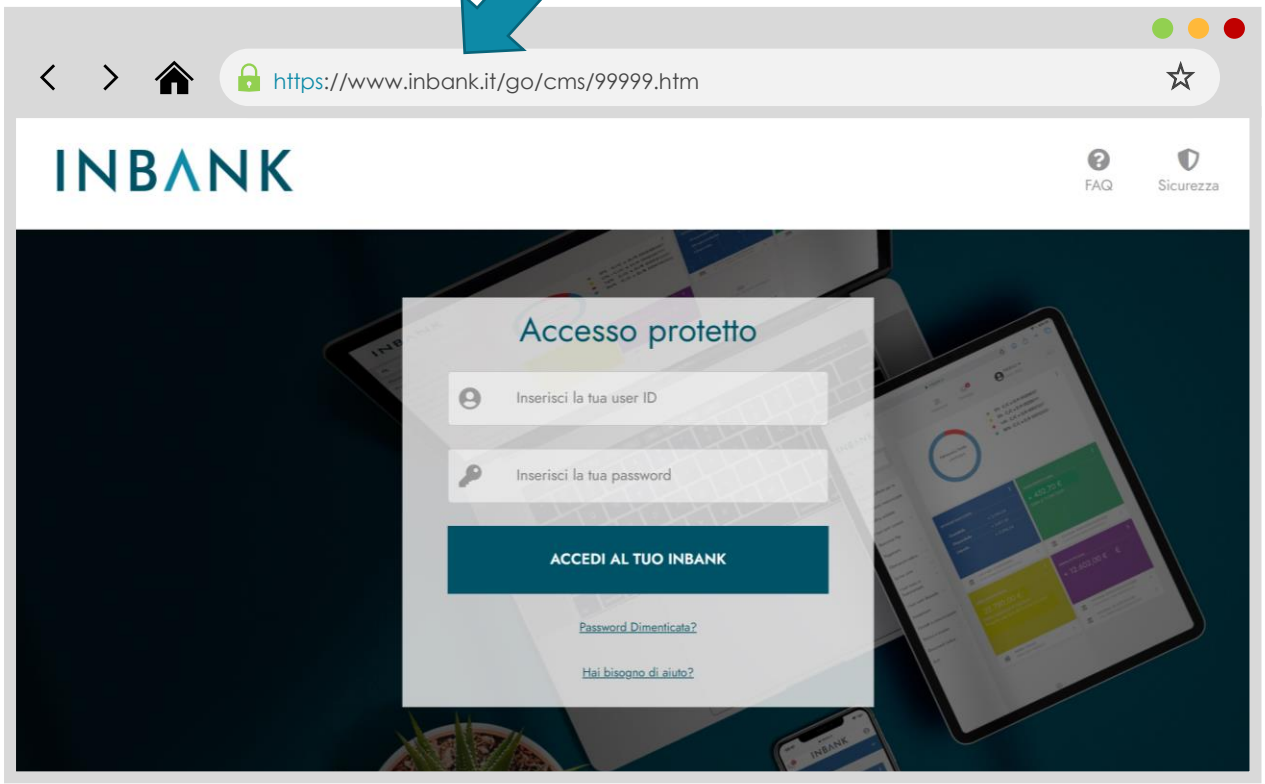
L'URL contiene la parola «inbank», ma NON corrisponde all'indirizzo corretto

Sito clone realmente usato!



Corrisponde all'URL corretto e in particolare al dominio **inbank.it**

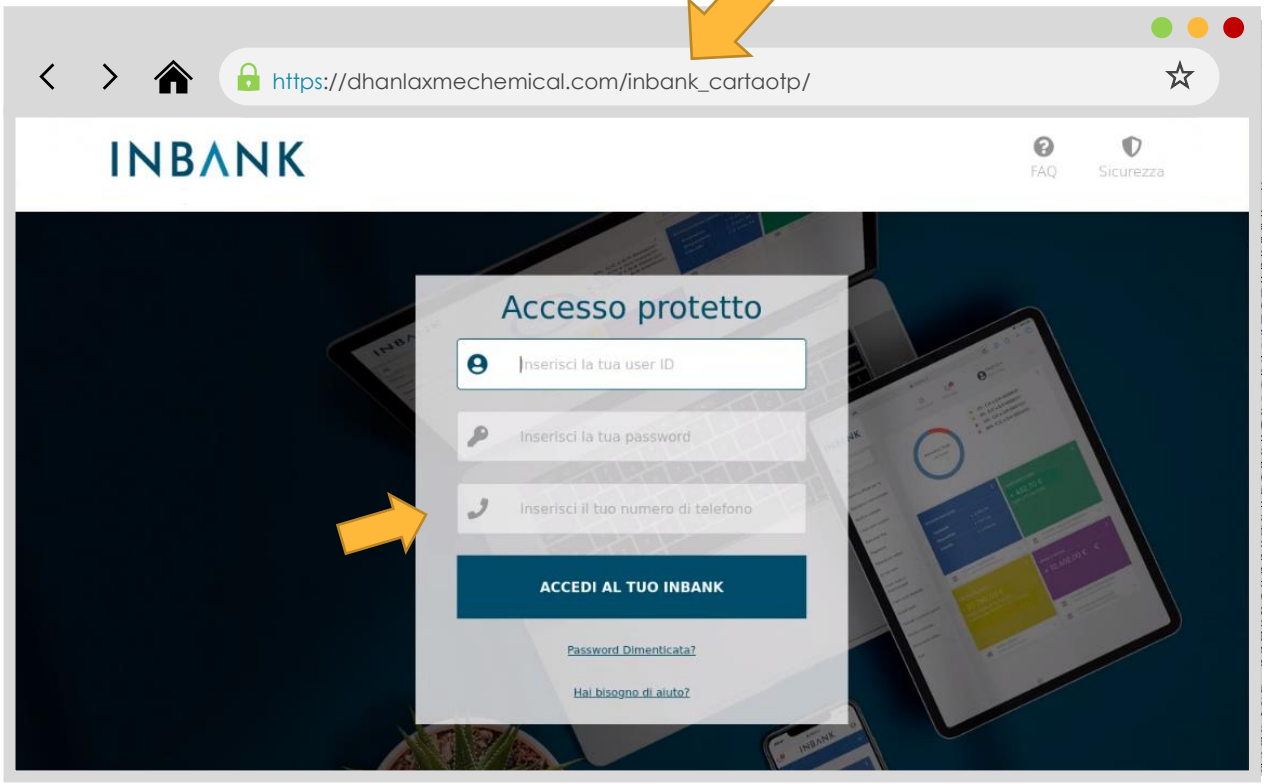
Sito autentico!



PHISHING E SITI CLONE

L'URL contiene la parola «inbank», ma NON corrisponde all'indirizzo corretto

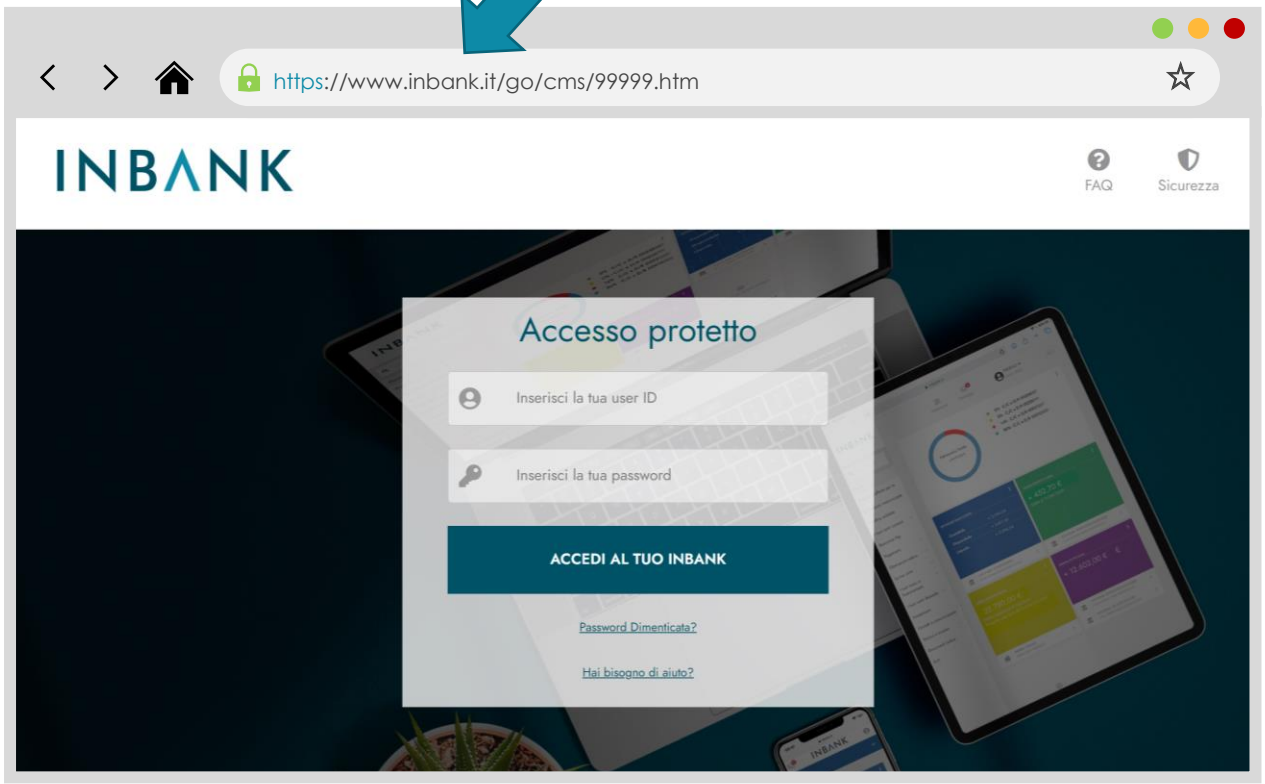
Sito clone realmente usato!



La migliore pratica è non cliccare mai sui link ricevuti, ma **digitare l'indirizzo direttamente nel browser!**

Corrisponde all'URL corretto e in particolare al dominio **inbank.it**

Sito autentico!



L'indirizzo del sito web di Inbank è sempre: **https://www.inbank.it**

MALWARE

MALWARE

I *malware* sono dei software malevoli in grado di infettare il dispositivo dell'utente a sua insaputa ed esfiltrare informazioni sensibili o manipolare transazioni. Di seguito i veicoli più comunemente utilizzati per diffonderli e le fasi della truffa:

A ALLEGATI e LINK

I frodatori inviano email con **allegati** e **link**.
Gli allegati, anche se in formato apparentemente innocuo, contengono direttamente i malware, mentre i link rinviano a siti web poco affidabili visitando i quali si viene infettati.

B DOWNLOAD

I malware possono essere contenuti in file scaricati da internet da **fonti non affidabili**, come ad esempio programmi, **giochi** e **app**

C PUBBLICITA'

Anche le **pubblicità** ed i **pop-up** che rimandano ad altri url possono essere veicolo di malware

D DISPOSITIVI USB

Spesso i malware sono in grado di diffondersi tra dispositivi collegati alla stessa rete, oppure ad esempio da dispositivi USB a PC e server.

1

2 Dispositivo del Cliente infettato

Una volta che il dispositivo del Cliente è stato infettato dal malware, ecco può, a seconda del caso, **esfiltrare dati sensibili** (credenziali), oppure permettere la **manipolazione delle transazioni disposte** (es. IBAN swap)

3 Disposizioni fraudolente

Il frodatore è ora in grado o di operare in autonomia mediante le credenziali sottratte oppure è in grado di modificare le transazioni disposte dal Cliente sostituendo ad esempio l'IBAN di destinazione.

Malware contenuti in allegati, siti, download, pubblicità e dispositivi USB nella maggior parte dei casi **sfruttano software e dispositivi <u>non</u> aggiornati**

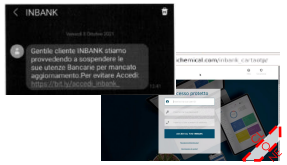
*Rapporto Clusit 2021 – Edizione di Novembre 2021

SIM SWAP

SIM SWAP

Il *SIM swap* (scambio di SIM) è così chiamato perché perpetrato attraverso una nuova SIM con stesso numero telefonico della vittima, ma emessa a sua insaputa. Di seguito le fasi di attuazione della frode:

1 PHISHING +

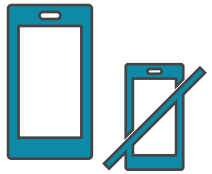


Il frodatore sfrutta tecniche di phishing per impossessarsi delle **credenziali** del Cliente (UserId e password)

2 Duplicazione SIM o portabilità del numero

Il frodatore richiede l'emissione di **una nuova SIM con stesso numero telefonico** della vittima, usando un suo documento rubato o contraffatto, e in taluni casi anche in assenza del documento sfruttando la compiacenza del rivenditore.

3 Attivazione della nuova SIM



Nel momento in cui viene attivata la nuova SIM, il frodatore è in grado di ricevere gli SMS o gli altri codici autorizzativi inviati dalla banca alla vittima.
In contemporanea, la SIM del Cliente cessa di funzionare (non riceve quindi nemmeno messaggi di alert della Banca)

4 Disposizioni fraudolente

Il frodatore è ora in grado di operare in autonomia e accedere al conto per effettuare le disposizioni fraudolente es. bonifici, ricariche di carte prepagate, acquisto di beni immateriali come Bitcoin o altre criptovalute.

Nel corso degli ultimi anni si è assistito ad una diminuzione del fenomeno di SIM swap (solo il 5% per retail) anche grazie allo sforzo prodotto dal tavolo di lavoro congiunto tra settore bancario, rappresentato dal CERTFin, e gli operatori telefonici, attivo già dalla fine del 2019.

COME PROTEGGERSI

COME PROTEGGERSI DALLE TRUFFE BANCARIE?

I due pezzi di puzzle, simboleggianti **Inbank** e l'**utente**, si incastrano tra loro come la sicurezza informatica è frutto della complementarità e dell'unione tra i **presidi di sicurezza tecnologici** di Inbank e **l'uso prudente e consapevole** di Inbank da parte dell'utente.

Ciascuna delle due parti è essenziale per comporre il puzzle: come dice lo slogan, "La sicurezza informatica è un gioco di squadra"!

COME PROTEGGERSI DALLE TRUFFE BANCARIE?

Inbank, a tutela dei clienti, prevede i più avanzati **sistemi di protezione**:

- la **cifratura per le pagine web** tutela gli utenti di Inbank inibendo la possibilità di leggere o alterare i dati in transito tra il dispositivo del cliente e i sistemi bancari;
- l'autenticazione a più fattori è la cosiddetta "**autenticazione forte**" e protegge l'accesso a Inbank richiedendo – oltre a username e password – l'inserimento di un codice di conferma ricevuto tramite Inbank notify o SMS. Questo tipo di autenticazione è richiesto e previsto dalla normativa, per aumentare la sicurezza delle operazioni (es. per effettuare disposizioni o modificare dati personali);
- il sistema di **notifiche automatiche di operazioni** ad alto rischio (modifica delle anagrafiche e disposizioni effettuate) è molto efficace a protezione dalle frodi digitali. L'utente riceve infatti tempestivamente una notifica via e-mail, via SMS o tramite Inbank notify, con una sintesi dell'attività in atto sul suo conto corrente o sulle sue carte di pagamento, avendo quindi la possibilità di intervenire con velocità qualora si trattasse di operazioni e/o di modifiche non disposte direttamente, ma frutto di frodi;
- il **sistema di fraud management evoluto**, rileva comportamenti sospetti e blocca in automatico le transazioni anomale.
- Come ulteriore garanzia, vi è un **presidio H24/365** dedicato al monitoraggio tutti gli eventi di sicurezza.

A dimostrazione dell'efficacia di tali presidi tecnologici e della tempestività di intervento degli operatori di banca, circa l'82% delle disposizioni fraudolente viene identificata e bloccata con successo[1].

[1]Rapporto Clusit 2021 – Edizione di Novembre 2021

COME PROTEGGERSI DALLE TRUFFE BANCARIE?

Il modo migliore per proteggersi dalle frodi digitali è:

- tenersi sempre aggiornati sulle strategie della criminalità digitale
- adottare alcune semplici precauzioni:

Non fornire mai credenziali, PIN o codici di conferma

Credenziali (nome utente e password), PIN e codici di conferma (token e OTP) sono informazioni **strettamente confidenziali** che **solo tu** devi conoscere.

Nemmeno la tua Banca o l'assistenza te li chiederà mai né via email né al telefono. Sospetta di chi ti chiede di fornire informazioni riservate, interrompi la comunicazione e contatta la tua filiale di fiducia.

Non cliccare mai su link arrivati via e-mail, SMS, chat o social

Le comunicazioni della tua Banca non avranno mai link a pagine o applicazioni esterne in cui sia richiesto l'inserimento di informazioni riservate.

Qualora dovessi accidentalmente aprire un link, non inserire mai dati o credenziali: si tratta di una ricostruzione fraudolenta, spesso molto fedele, del sito di internet banking che ha il solo scopo di sottrarre i dati d'accesso.

Proteggi i dispositivi e utilizza siti e store ufficiali

Utilizza le versioni più recenti dei programmi, esegui costantemente gli aggiornamenti di sicurezza. Sfrutta le opzioni e i software di protezione spesso già integrati in computer e dispositivi (antivirus, antispam e firewall) che garantiscono la protezione dei dati ed evitano la trasmissione di malware.

Non scaricare né aprire documenti o programmi su richiesta o da fonti delle quali non si è certi della identità.

COME PROTEGGERSI DALLE TRUFFE BANCARIE?

Buone pratiche da mettere in atto e tenere sempre a mente:

Nel caso ricevessi comunicazioni (email/sms/telefonate) inattese e/o differenti dal solito la cosa migliore da fare è **prendersi un attimo per riflettere**:

- Vengono chieste informazioni personali, o relative a codici di accesso?
- Sono mai stato contattato in questo modo?
- Il tono è il solito? (inteso come colloquiale/ formale, mette urgenza o meno).
- Ci si aspettava una comunicazione di questo tipo?
- Vengono richieste le solite informazioni?

In caso di dubbi, non procedere, contatta la tua filiale di fiducia.

Per accedere a Inbank, non cliccare mai sui link ricevuti, ma **digita l'indirizzo https://www.inbank.it direttamente nel browser**.

Per **verificare i link**, basta passare sopra (senza cliccare) il puntatore del mouse per visualizzare la URL di destinazione.

Fai **attenzione alle informazioni che condividi**, anche involontariamente, sui social.

Se la tua SIM cessa improvvisamente di funzionare, contatta immediatamente il tuo operatore telefonico e la tua filiale.

Controlla regolarmente i movimenti e mantieni aggiornati i riferimenti di contatto collegati con il conto bancario.

COSA FARE IN CASO DI (SOSPETTA) TRUFFA

COSA FARE IN CASO DI (SOSPETTA) TRUFFA?

Se sospetti di essere vittima di una frode o di un tentativo di frode:

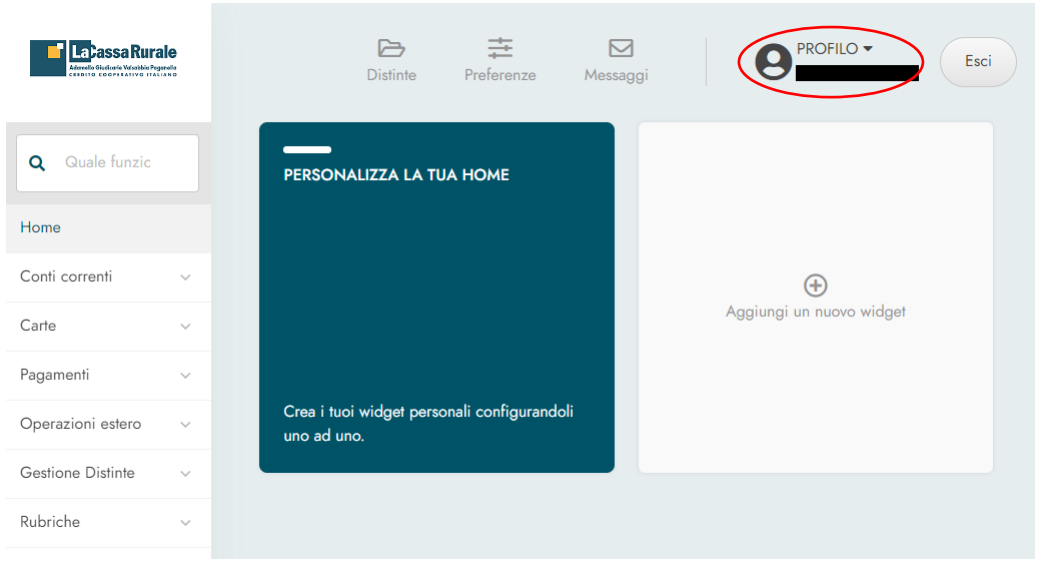
CAMBIA IMMEDIATAMENTE LA PASSWORD (SE POSSIBILE)

COSA FARE IN CASO DI (SOSPETTA) TRUFFA?

Se sospetti di essere vittima di una frode o di un tentativo di frode:

Con **Inbank web**

CAMBIA IMMEDIATAMENTE LA PASSWORD (SE POSSIBILE)

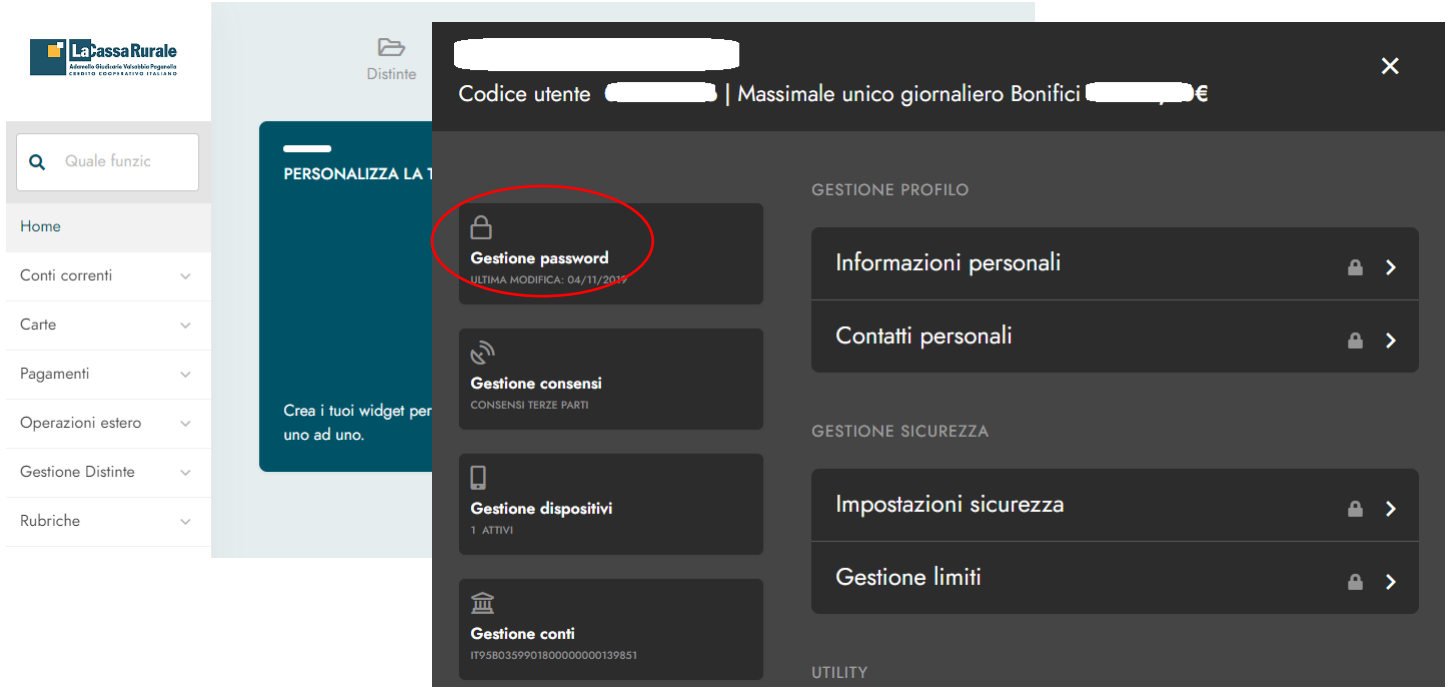


COSA FARE IN CASO DI (SOSPETTA) TRUFFA?

Se sospetti di essere vittima di una frode o di un tentativo di frode:

Con **Inbank web**

CAMBIA IMMEDIATAMENTE LA PASSWORD (SE POSSIBILE)

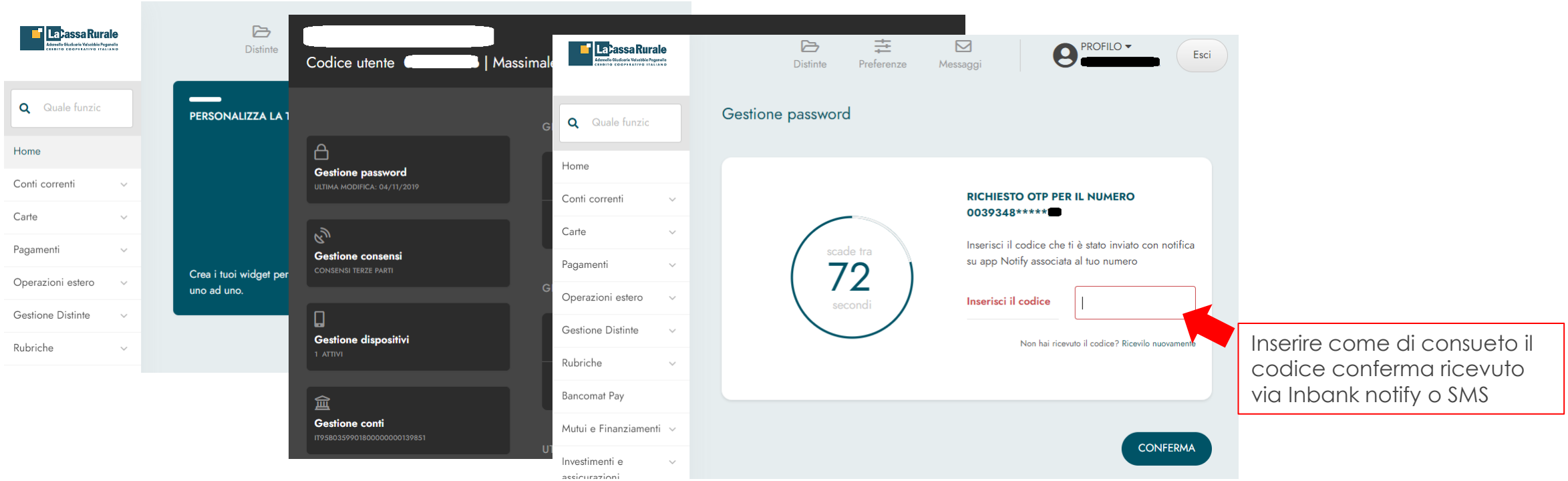


COSA FARE IN CASO DI (SOSPETTA) TRUFFA?

Se sospetti di essere vittima di una frode o di un tentativo di frode:

Con **Inbank web**

CAMBIA IMMEDIATAMENTE LA PASSWORD (SE POSSIBILE)



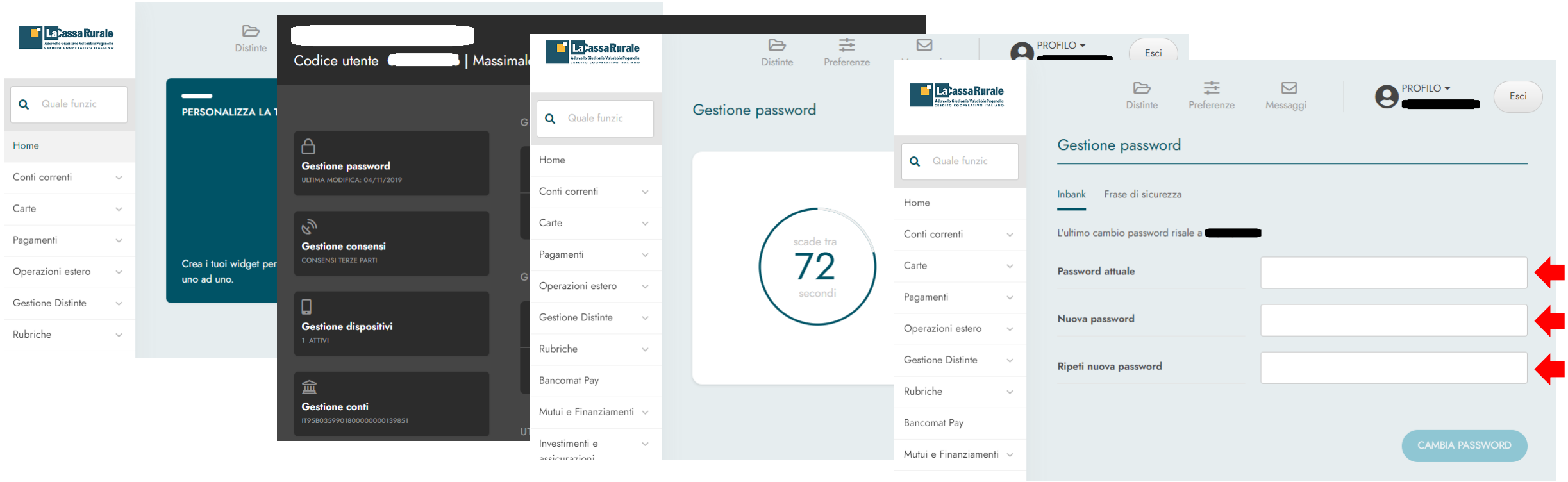
Inserire come di consueto il codice conferma ricevuto via Inbank notify o SMS

COSA FARE IN CASO DI (SOSPETTA) TRUFFA?

Se sospetti di essere vittima di una frode o di un tentativo di frode:

Con **Inbank web**

CAMBIA IMMEDIATAMENTE LA PASSWORD (SE POSSIBILE)

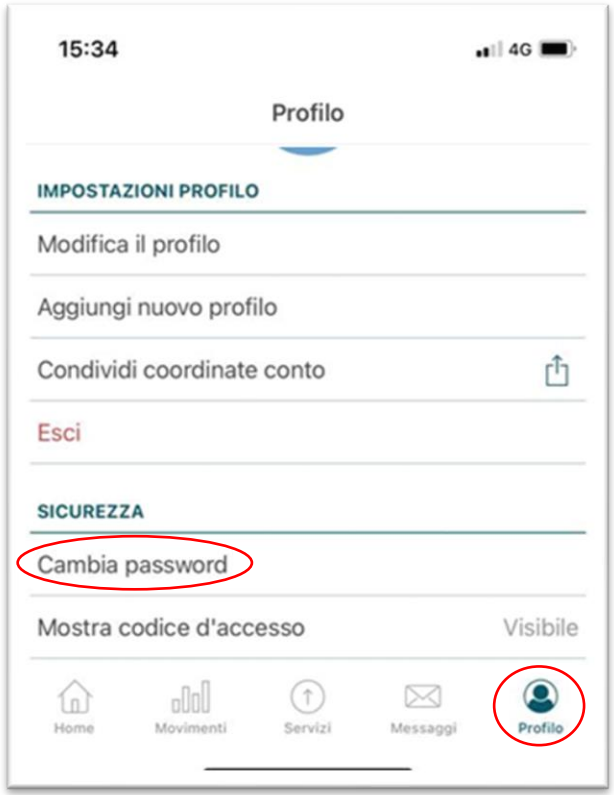


COSA FARE IN CASO DI (SOSPETTA) TRUFFA?

Se sospetti di essere vittima di una frode o di un tentativo di frode:

CAMBIA IMMEDIATAMENTE LA PASSWORD (SE POSSIBILE)

Oppure, in maniera analoga, con **Inbank App**:



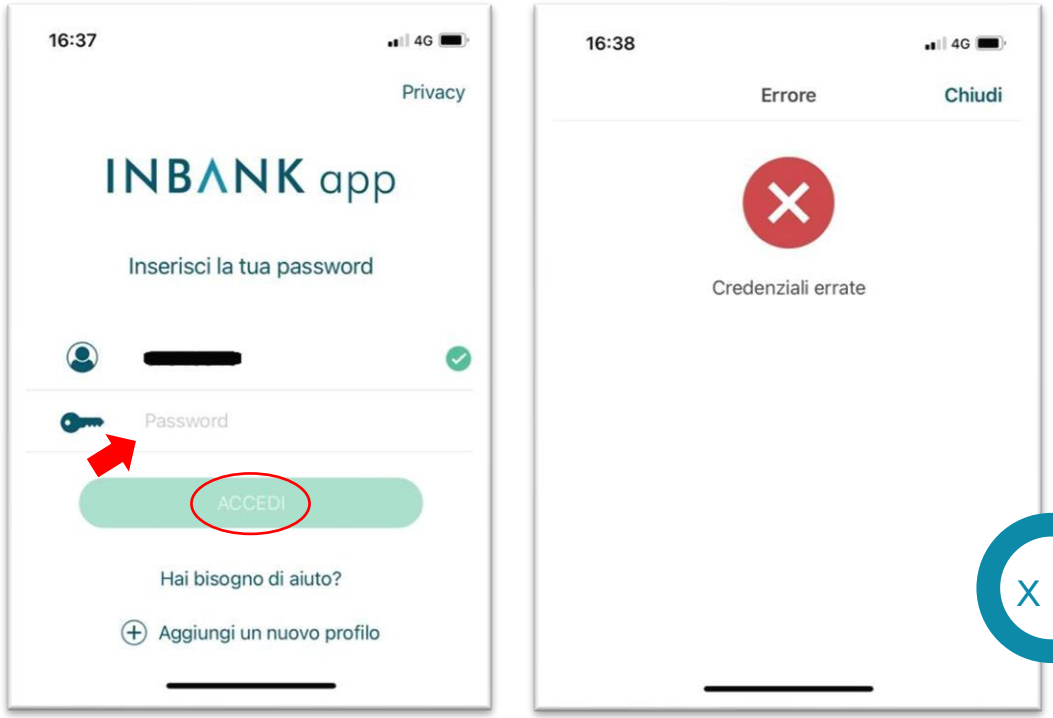
COSA FARE IN CASO DI (SOSPETTA) TRUFFA?

Se sospetti di essere vittima di una frode o di un tentativo di frode:

CAMBIA IMMEDIATAMENTE LA PASSWORD (SE POSSIBILE)

BLOCCA LA TUA POSTAZIONE INBANK

Effettua **almeno 5 accessi** al tuo Inbank **con una password errata**: in questo modo la postazione Inbank verrà bloccata automaticamente



COSA FARE IN CASO DI (SOSPETTA) TRUFFA?

Se sospetti di essere vittima di una frode o di un tentativo di frode:

CAMBIA IMMEDIATAMENTE LA PASSWORD (SE POSSIBILE)

BLOCCA LA TUA POSTAZIONE INBANK

BLOCCA LE CARTE DI PAGAMENTO ASSOCIATE

NUMERI DI TELEFONO PER IL BLOCCO DELLE CARTE:

CARTE DI DEBITO E PREPAGATE

ITALIA 800822056 - ESTERO +390260843768

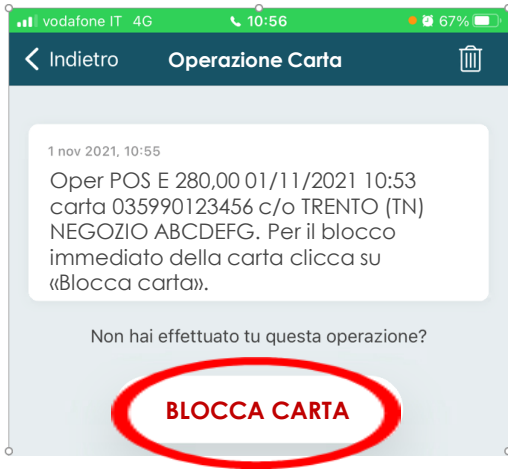
CARTA DI CREDITO NEXI

ITALIA 800151616 - ESTERO +390234980020

CARTA AMERICAN EXPRESS

ITALIA 0672900347 - ESTERO 80026392279

Oppure, se, ti è arrivata la notifica automatica (tramite Inbank notify) di un pagamento tramite carta di debito che non è stato disposto da te, puoi bloccare la carta di debito direttamente dalla notifica



COSA FARE IN CASO DI (SOSPETTA) TRUFFA?

Se sospetti di essere vittima di una frode o di un tentativo di frode:

CAMBIA IMMEDIATAMENTE LA PASSWORD (SE POSSIBILE)

BLOCCA LA TUA POSTAZIONE INBANK

BLOCCA LE CARTE DI PAGAMENTO ASSOCIATE

SEGNALA L'ACCADUTO ALLA TUA FILIALE

Contatta la tua filiale utilizzando il numero telefonico o l'e-mail già in tuo possesso
(e non eventuali numeri/e-mail da cui si sono ricevuti messaggi o chiamate)
Puoi reperire i numeri e le e-mail dal sito istituzionale https://www.lacassarurale.it/filiali/

COSA FARE IN CASO DI (SOSPETTA) TRUFFA?

Se sospetti di essere vittima di una frode o di un tentativo di frode:

CAMBIA IMMEDIATAMENTE LA PASSWORD (SE POSSIBILE)

BLOCCA LA TUA POSTAZIONE INBANK

BLOCCA LE CARTE DI PAGAMENTO ASSOCIATE

SEGNALA L'ACCADUTO ALLA TUA FILIALE

Contatta la tua filiale utilizzando il numero telefonico o l'e-mail già in tuo possesso
(e non eventuali numeri/e-mail da cui si sono ricevuti messaggi o chiamate)
Puoi reperire i numeri e le e-mail dal sito istituzionale https://www.lacassarurale.it/filiali/

Infine, se sei stato vittima di una frode:

DENUNCIA SEMPRE ALLE FORZE DELL'ORDINE

GRAZIE A TUTTI PER L'ATTENZIONE

DOMANDE?

Sede legale

Via 3 novembre, 20 – 38079 Tione di Trento (TN)

Tel. 0465.896896

lacassarurale.it

Sede legale e Direzione Generale

Via Segantini, 5 - 38122 Trento

Tel. 0461.313111

cassacentrale.it

La Cassa Rurale
Adamello Giudicarie Valsabbia Paganella
CREDITO COOPERATIVO ITALIANO

CASSA CENTRALE BANCA
CREDITO COOPERATIVO ITALIANO