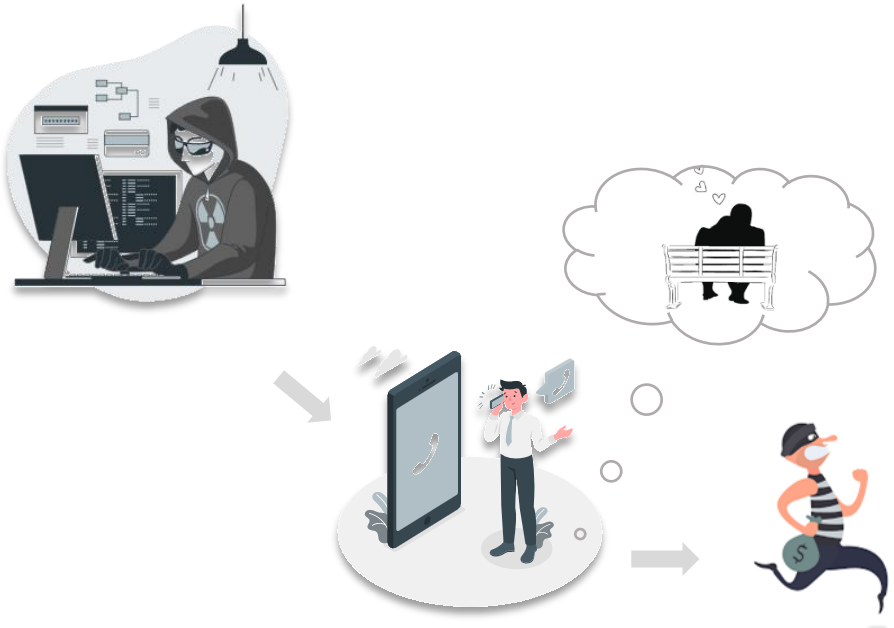
Impariamo a riconoscere le frodi e le truffe online.
Quali strategie dobbiamo adottare per difenderci?

4 Aprile 2024

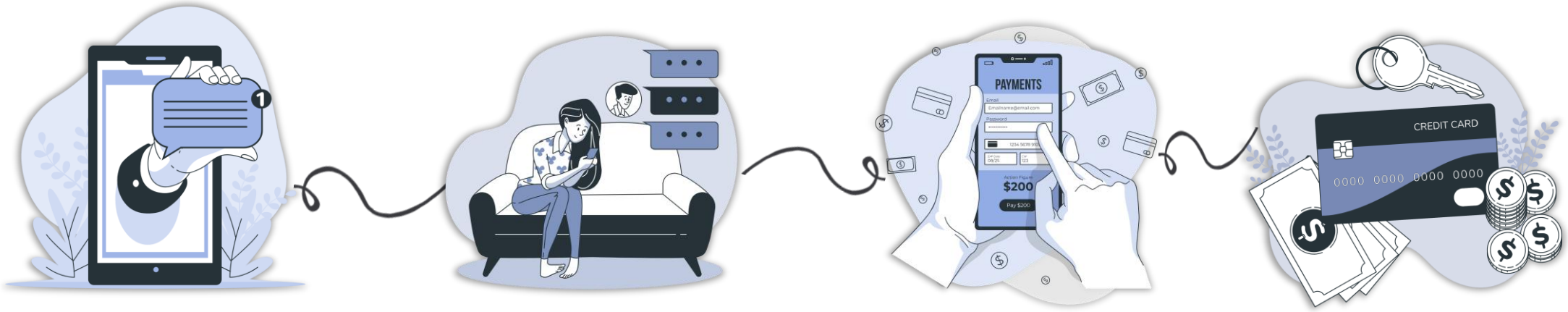
Distinzione tra frode e truffa

Si parla di **FRODE** quando l'**operazione di pagamento viene effettuata ed autorizzata dal frodatore**, utilizzando le credenziali che il cliente stesso ha ceduto al frodatore in un precedente momento.



Si parla di **TRUFFA** quando l'**operazione di pagamento viene effettuata ed autorizzata direttamente dal cliente** persuaso e manipolato dal truffatore

Una reale **Emergenza Familiare?**



1

Il truffatore invia un sms al cliente in cui si finge un familiare o amico in una situazione di emergenza e chiede di essere **contattato su un numero di telefono diverso** da quello usato solitamente.

2

Il cliente dà seguito alla conversazione spesso su un App di messaggistica istantanea o social network.

3

Il truffatore dopo alcuni messaggi di circostanza **chiede al cliente di eseguire dei pagamenti urgenti (bonifici, western union, altri) per ovviare ad una situazione di emergenza**.

4

Il **cliente esegue** i **pagamenti richiesti** pensando di aiutare un familiare o un amico in difficoltà, i fondi vengono invece trasferiti verso il truffatore.

INTESA SANPAOLO

Una reale **Emergenza Familiare?** **No, un tentativo di truffa!**

IMPARA A RICONOSCERE I SEGNALI E DIFENDERTI…

- **DIFFIDA DA COMUNICAZIONI CONTENENTI LINK O NUMERI DI TELEFONO SCONOSCIUTI**
- **PRESTA ATTENZIONE A RICHIESTE «URGENTI»**
- **VERIFICA IN PARALLELO (SUI CANALI GIÀ CONOSCIUTI) SE LA PERSONA A CUI SCRIVI È EFFETTIVAMENTE CHI DICE DI ESSERE**

1

Il truffatore invia un sm
in cui si finge un f
amico e chiede
contattato su un n
telefono diverso da qu
solitamente.

4

esegue i **pagamenti**
ensando di aiutare un
un amico e fornendo
i casi l'evidenza
uto pagamento o
umero carte.

INTESA SANPAOLO

Una grande **opportunità di investimento?**

1

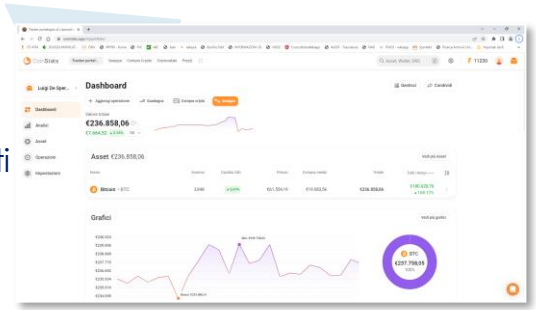
Il cliente viene contattato telefonicamente: una voce registrata gli propone **investimenti con grandi profitti,** spesso utilizzando il nome di grandi società (es. Amazon, Tesla...)

2

Ingolosito il cliente con **prospettiva di facili guadagni**, la telefonata viene inoltrata **ad un falso consulente finanziario** che, tramite ingegneria sociale, convince la vittima ad **iscriversi ad una finta piattaforma di trading,** spesso supportandolo nel processo tramite strumenti di condivisione schermo (es. TeamViewer)

3

Con il supporto del falso consulente, **la vittima effettua un primo deposito iniziale** di basso importo tramite bonifico o pagamento con carta.



4

Nei giorni successivi il truffatore mostra al cliente, tramite la finta piattaforma di trading, **dati falsi su presunti profitti derivanti dall'investimento iniziale**. La vittima è così incoraggiata a depositare ulteriori fondi. **I truffatori continuano a tentare di manipolare la vittima.**

5

Quando la vittima desidera prelevare i fondi presumibilmente guadagnati, **viene informata che deve effettuare un altro deposito per raggiungere la soglia di prelievo o per pagare le tasse**; Nessun fondo viene restituito alla vittima, che **si rende conto di essere stata truffata**.

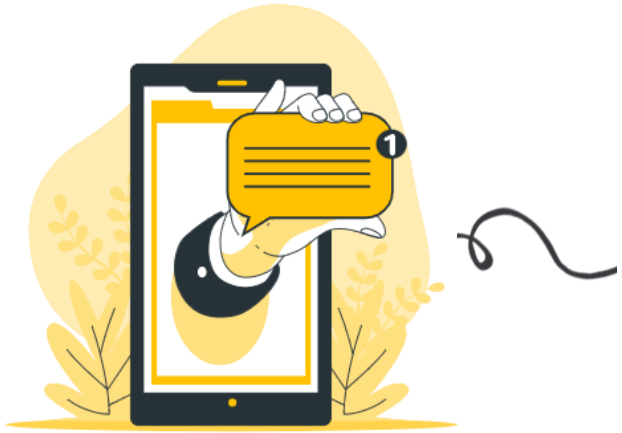
INTESA SANPAOLO

Una grande **opportunità di investimento?** **No, un tentativo di truffa!**

IMPARA A RICONOSCERE I SEGNALI E DIFENDERTI…

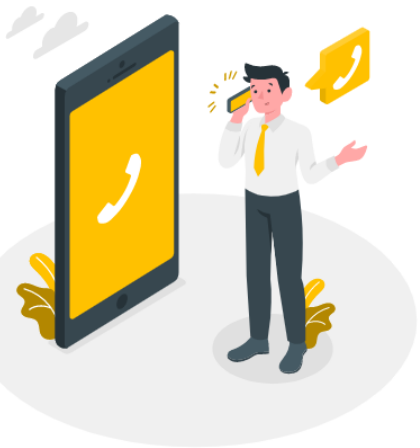
- **DIFFIDA DA COMUNICAZIONI CONTENENTI LINK O NUMERI DI TELEFONO SCONOSCIUTI**
- **NON LASCIARTI INGANNARE DALLE PROMESSE DI GUADAGNI FACILI**
- **VERIFICA L'ATTENDIBILITÀ DELLA PIATTAFORMA DI TRADING SU CUI STAI INVESTENDO**

Ti comunicano di **mettere in «salvo» i tuoi fondi?**



1

Il cliente riceve un **SMS di phishing**, apparentemente proveniente dalla Banca, con un link che rimanda **ad un sito simile** all'Internet Banking della Banca utilizzato dai truffatori per rubare le sue credenziali bancarie e, successivamente, ulteriori dati (es. saldo, movimenti etc.)



2

I truffatori contattano al telefono il cliente e, **fingendosi operatori antifrode della Banca e/o della Polizia Postale** per acquisire la sua fiducia, lo allertano circa **false «operazioni fraudolente momentaneamente bloccate»** sul suo conto corrente.

3

I truffatori convincono il cliente a **recarsi «con urgenza» in filiale** per eseguire, da sportello, operazioni di pagamento (tipicamente bonifici istantanei) verso un nuovo conto corrente appena aperto a suo nome e **al fine di «mettere in sicurezza» i propri fondi.**

4

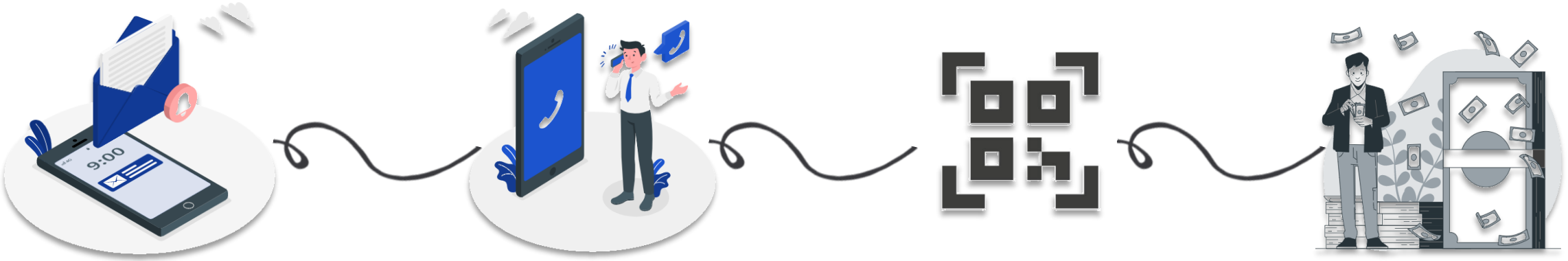
Una volta in filiale, il cliente viene persuaso ad eseguire un **bonifico** verso un **nuovo IBAN fraudolento** fornito dai frodatori e, convinto di «mettere in sicurezza i proprio risparmi», **li trasferisce verso i frodatori.**

Ti comunicano di **mettere in «salvo» i tuoi fondi?** **No, è un tentativo di truffa!**

IMPARA A RICONOSCERE I SEGNALI E DIFENDERTI…

- **DIFFIDA DA COMUNICAZIONI CONTENENTI LINK O NUMERI DI TELEFONO SCONOSCIUTI**
- **PRESTA ATTENZIONE A RICHIESTE «URGENTI»**
- **CHIUDI LA TELEFONATA E CONTATTA DIRETTAMENTE LA BANCA O UNA PERSONA FIDATA PER FARTI AIUTARE**

Ti contatta l'Ufficio Antifrode della tua Banca?



1

Il cliente riceve **un SMS di phishing che lo allerta circa l'esecuzione di pagamenti verso l'estero** (es. Svizzera), all'interno del quale è presente un link per disconoscere l'operazione.

2

Il cliente accede al link ed inserisce i propri dati personali. Successivamente viene contattato telefonicamente dal **frodatore** che, **fingendosi operatore della banca,** gli offre **assistenza per stornare i pagamenti.**

3

Il cliente, convinto di effettuare lo storno delle operazioni, **inquadra dal proprio device mediante App della Banca molteplici QR code** che il frodatore gli invia tramite App di messaggistica istantanea (es. whatsapp).

4

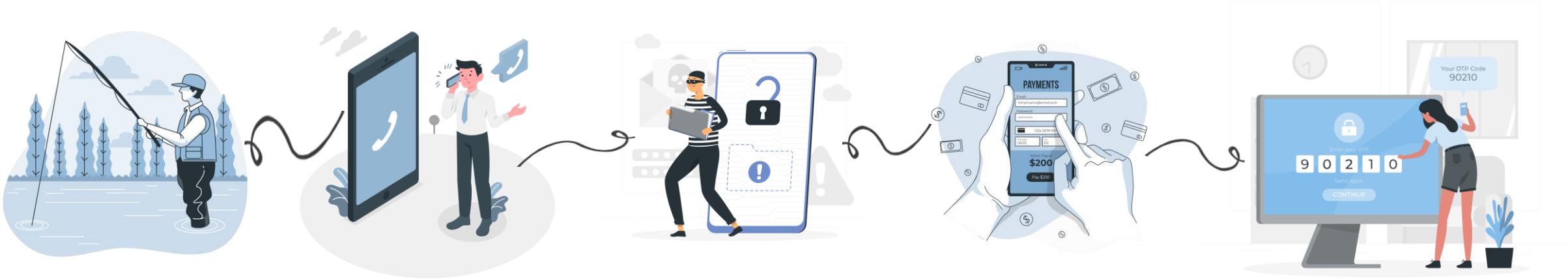
Il frodatore da ATM effettua i prelievi di contante autorizzati dal cliente tramite scansione dei QR Code.

Ti contatta l'Ufficio Antifrode della tua Banca? **No, è un tentativo di truffa!**

IMPARA A RICONOSCERE I SEGNALI E DIFENDERTI…

- **DIFFIDA DA COMUNICAZIONI CONTENENTI LINK O NUMERI DI TELEFONO SCONOSCIUTI**
- **PRESTA ATTENZIONE A RICHIESTE «URGENTI»**
- **CHIUDI LA TELEFONATA E CONTATTA DIRETTAMENTE LA BANCA O UNA PERSONA FIDATA PER FARTI AIUTARE**

Ti richiedono il **Controllo Remoto** del tuo device?



1

Il cliente cade vittima di un tentativo di **phishing** (via SMS o mail) e cede le credenziali di accesso al conto.

2

Il truffatore la **contatta al telefono** per comunicarle che ci sono **operazioni sospette** sul suo conto bancario che devono essere immediatamente revocate.

3

Il cliente accetta il **controllo** da **remoto** del **proprio PC** (es. assistenza rapida di Windows)

4

Il **truffatore inserisce** diverse **dispositive** di **pagamento** sul conto corrente del cliente utilizzando il controllo da remoto.

5

Il **cliente cede** i **codici OTS** necessari per autorizzare le dispositive di pagamento inserite dal truffatore.

Ti richiedono il **Controllo Remoto** del tuo device? **No, è un tentativo di truffa!**

1

Il cliente cade vittim
un tentativo di **phish**
(via SMS o mail) e ce
le credenziali di acc
al conto.

5

Il **cliente cede** i **codici OTS** necessari per autorizzare le dispositive di pagamento inserite dal truffatore.

IMPARA A RICONOSCERE I SEGNALI E DIFENDERTI…

- **DIFFIDA DA COMUNICAZIONI CONTENENTI LINK O NUMERI DI TELEFONO SCONOSCIUTI**
- **CHIUDI LA TELEFONATA E CONTATTA DIRETTAMENTE LA BANCA O UNA PERSONA FIDATA PER FARTI AIUTARE**
- **RICORDA CHE LA BANCA NON TI CONTATTERÀ MAI PER CHIEDERTI DI ESEGUIRE STORNI O SIMULAZIONI DI OPERAZIONI**

Una **nuova applicazione da installare?**

1

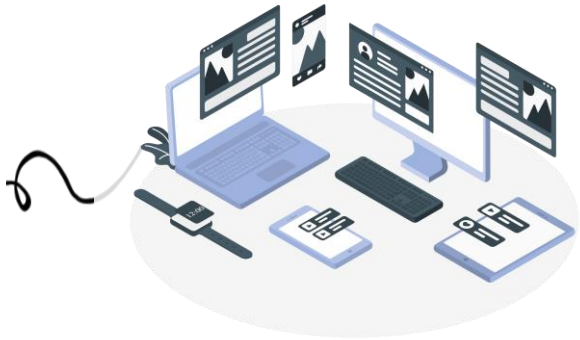
Il **frodatore** invia un **sms al cliente** contenente un link ad un'applicazione malevola da installare.

2

Convinto mediante con social engineering, **il cliente installa** l'applicazione sul proprio dispositivo.

3

Il frodatore attraverso il malware prende **il controllo da remoto del dispositivo** ed accedendo all'applicazione della banca esegue una o più operazioni di pagamento.



4

Ad operazioni eseguite, il **malware resetta** alle impostazioni di fabbrica il **dispositivo** del **cliente**.

Una **nuova applicazione da installare?** **No, un tentativo di frode!**

1

Il **frodatore** invia un
cliente contenente u
un'applicazione male
installare.

l'applicazione sul proprio
dispositivo.

accedendo all'applicazione
della banca esegue una o più
operazioni di pagamento.

4

zioni eseguite, il
re resetta alle
oni di fabbrica il
dispositivo del **cliente**.

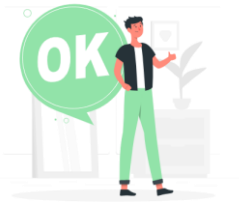
IMPARA A RICONOSCERE I SEGNALI E DIFENDERTI…

RICORDA CHE LA BANCA NON TI FORZERÀ MAI AD INSTALLARE APPLICAZIONI

Impariamo a riconoscere gli SMS genuini da quelli fraudolenti…

SMS 1

SMS 2

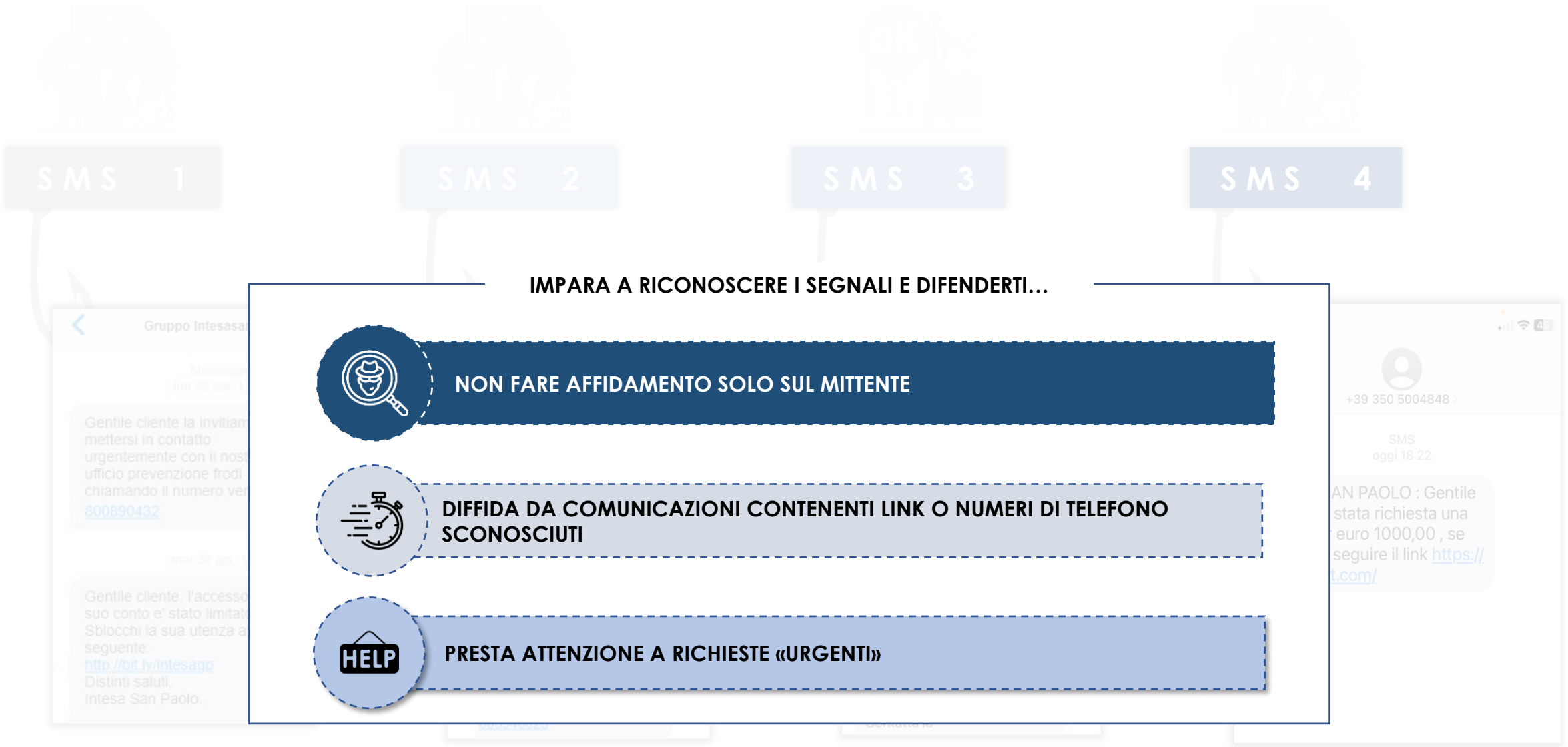


SMS 3

SMS 4

INTESA SANPAOLO

Impariamo a riconoscere gli SMS genuini da quelli fraudolenti. In che modo?

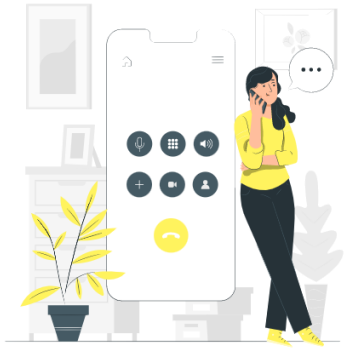


Impariamo a riconoscere le chiamate della Banca…

CHIAMATA 1

«Buongiorno, sono Laura Rossi, la chiamo dal servizio Antifrode di Intesa Sanpaolo. Parlo con il Sig. Mario Bianchi?
*La chiamo perché abbiamo notato **dei movimenti sospetti** sul suo conto e avremmo bisogno URGENTE delle sue credenziali per poterli annullare..*
*Le arriverà un codice **via SMS** e me lo dovrà comunicare per concludere le operazioni..»*

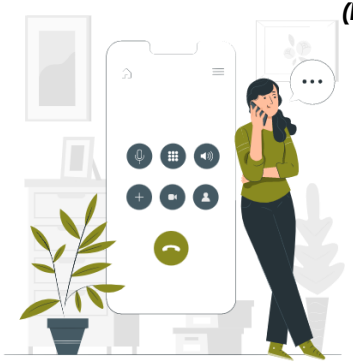
800.303.303



CHIAMATA 2

«Buongiorno, sono Maria Bianchi e la chiamo dalla Filiale di Padova di Intesa Sanpaolo. Posso parlare con il Signor Paolo Bianchi?
La contatto in quanto abbiamo notato dei bonifici effettuati da Lugano.
Se mi fornisce le credenziali possiamo stornarli, effettuando nuovi bonifici che le saranno successivamente riaccreditati sul conto corrente..»

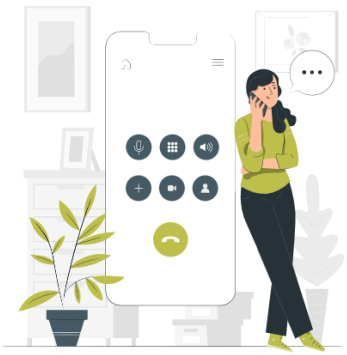
049.848.1211
(Filiale ISP di Padova)



CHIAMATA 3

*«Buongiorno, sono Marie Rossi e la contatto per conto della società **Morgan Stanley**, a cui siamo affiliati.*
*La chiamo per proporle un **piano di investimenti** mirato a far crescere in poco tempo i suoi guadagni, avrà sempre il controllo degli andamenti..»*

+34 657 001156



INTESA SANPAOLO

Impariamo a riconoscere le chiamate della Banca. In che modo?

CHIAMATA 1

«Buongiorno, sono Laura Rossi, la chiamo dal servizio Antifrode di Intesa Sanpaolo. Parlo con il Sig. Mario Bianchi?
*La chiamo perché abbiamo notato **dei movimenti sospetti** sul suo conto e avremmo bisogno URGENTE delle sue credenziali per poterli*
Le arriverà un codice
dovrà comunicare per
operazioni..»

CHIAMATA 2

«Buongiorno, sono Maria Bianchi e la chiamo dalla Filiale di Padova di Intesa Sanpaolo. Posso parlare con il Signor Paolo

CHIAMATA 3

*«Buongiorno, sono Marie Rossi e la contatto per conto della società **Morgan Stanley**, a cui siamo affiliati.*
*La chiamo per proporle un **piano di***
irato a far crescere in poco
uadagni, avrà sempre il
andamenti..»

+34 657 001156

IMPARA A RICONOSCERE I SEGNALI E DIFENDERTI…

NON FARE AFFIDAMENTO SOLO SUL MITTENTE

PRESTA ATTENZIONE A RICHIESTE «URGENTI»

CHIUDI LA TELEFONATA E CONTATTA DIRETTAMENTE LA BANCA O UNA PERSONA FIDATA PER FARTI AIUTARE

Take Away: i consigli utili del team Antifrode!

- Diffida da comunicazioni contenenti link o numeri di telefono sconosciuti
- Presta attenzione a richieste «urgenti»
- Verifica sui canali già conosciuti se la persona a cui scrivi è effettivamente chi dice di essere
- Non lasciarti ingannare dalle promesse di guadagni facili
- Verifica l'attendibilità della piattaforma di trading su cui stai investendo
- Chiudi la telefonata e contatta direttamente la Banca o una persona fidata per farti aiutare
- Ricorda che la Banca non ti contatterà mai per chiederti di eseguire storni o simulazioni di operazioni
- Ricorda che la Banca non ti forzerà mai ad installare applicazioni
- Non fare affidamento solo sul mittente!