



GUIDA TRUFFE WHATSAPP

In collaborazione con [Forenser S.r.l.](#) – Torino (TO)

Come riconoscerle e, caso per caso, tutti i passaggi per risolvere: recuperare l'account, bloccare i danni, riavere i soldi, denunciare.

IN UNA RIGA

Chi ti chiede soldi o codici via chat va verificato a voce, sul numero che conosci. Se c'è fretta, è quasi sempre una truffa.

ATTENZIONE · HAI UN IPHONE?

Su iPhone **non aggiornati** l'account WhatsApp può essere clonato **senza che tu faccia nulla**: niente link, niente codici. Controlla subito di avere l'ultima versione di iOS (

Impostazioni → Generali → Aggiornamento software) e di WhatsApp, e leggi la scheda [#01](#).

Come usare questa guida

1. Trova il tuo caso nell'indice qui sotto.
2. Segui i passaggi **nell'ordine** in cui sono scritti: i primi sono quelli che fermano il danno.
3. Se hai già pagato o dato dati, dopo il tuo caso vai alla [Parte C](#).
4. Alla fine, denuncia e segnala con i contatti della [Parte D](#).

Indice

PARTE A — REGOLE VALIDE PER TUTTE LE TRUFFE

PARTE B — LE TRUFFE UNA PER UNA, CON LA SOLUZIONE

- | | |
|---|--|
| 01 Account clonato senza fare nulla (iPhone non aggiornati) | 02 Account rubato o "truffa della ballerina" |
| 03 Telefono perso/rubato o SIM clonata | 04 Soldi chiesti da un contatto in rubrica |
| 05 "Ciao mamma, ho cambiato numero" | 06 Voce clonata con l'IA |
| 07 Link di phishing | 08 Finto operatore della banca |
| 09 Finto supporto WhatsApp e app modificate | 10 Condivisione schermo e controllo remoto |

11 Finte offerte di lavoro

13 Truffe sentimentali

15 Compravendite online

17 Premi, concorsi e buoni falsi

19 Allegati e app infette

21 False convocazioni di polizia ed enti

23 Finte raccolte fondi e biglietti falsi

12 Investimenti, trading e cripto

14 Sextortion e immagini intime

16 Affitti e case vacanza inesistenti

18 Chiamate da prefissi esteri

20 Finto recupero dei soldi persi

22 Finti prestiti e finanziamenti

PARTE C — HO GIÀ PAGATO O DATO DATI: COSA FARE

PARTE D — DENUNCE, SEGNALAZIONI E CONTATTI UTILI

PARTE A

Regole valide per tutte le truffe

I campanelli d'allarme ricorrenti

URGENZA

"Subito", "entro oggi", "altrimenti blocchiamo il conto".

SOLDI

Qualunque richiesta di pagamento, bonifico, ricarica.

CODICI

Richiesta di un codice SMS, PIN, OTP, password.

CANALE DIVERSO

"Non chiamarmi", "spostiamoci su Telegram", "clicca questo link".

SEGRETEZZA

"Non dirlo a nessuno", "è una sorpresa".

TROPPO BELLO

Guadagni facili, premi, prezzi stracciati.

Le 8 regole d'oro

1. Il codice a 6 cifre di WhatsApp e i codici SMS della banca non si danno mai a nessuno, nemmeno ad amici o parenti. Nessuno ha motivo di chiederli.
2. Se qualcuno chiede soldi via chat, chiamalo a voce sul numero che conosci già, non sul numero che ti scrive.
3. Non cliccare link ricevuti via chat per pagare, accedere, verificare, "sbloccare" o "votare".
4. Banche, Poste, forze dell'ordine e WhatsApp non ti chiedono mai di spostare soldi, installare app o dare codici.
5. Non installare app suggerite da sconosciuti e non condividere lo schermo con nessuno.
6. Non digitare sul telefono codici con * e # suggeriti da altri.
7. Attiva la verifica in due passaggi con un'email di recupero:
Impostazioni → Account → Verifica in due passaggi
8. Nel dubbio, fermati. Una truffa vive di fretta: aspettare un'ora non fa danni, pagare sì.

Proteggi ora il tuo WhatsApp (5 minuti)

1. Impostazioni → Account → Verifica in due passaggi → Attiva : scegli un PIN di 6 cifre che non usi altrove e inserisci un'email di recupero a cui hai accesso.
2. Impostazioni → Privacy → Chiamate → Silenzia chiamate da numeri sconosciuti
3. Impostazioni → Privacy → Gruppi → I miei contatti : gli sconosciuti non possono aggiungerti ai gruppi.
4. Impostazioni → Privacy : Immagine profilo, Info e Ultimo accesso su "I miei contatti".
5. Impostazioni → Chat → Backup delle chat : attiva il backup su Google Drive o iCloud, così in caso di problemi recuperi le conversazioni.
6. Controlla ogni tanto Impostazioni → Dispositivi collegati e scollega quello che non riconosci.
7. Salva in rubrica il numero antifrode della tua banca (lo trovi sul retro della carta o sul sito ufficiale).

PARTE B

Le truffe una per una, con la soluzione

Per ogni caso: come riconoscerlo e tutti i passaggi per risolverlo, nell'ordine giusto.

#01

IL PIÙ GRAVE

Account clonato senza che tu abbia fatto nulla (iPhone non aggiornati)

ransomNews

COME SUCCEDDE

È l'attacco più pericoloso in circolazione perché **non richiede nessuna azione**: non devi cliccare link, dare codici, scansionare QR code o aprire file. I truffatori sfruttano falle di sicurezza di iPhone e WhatsApp non aggiornati, prendono la sessione del tuo WhatsApp, leggono le chat recenti e scrivono ai tuoi contatti chiedendo bonifici, spesso con IBAN.

- **Chi è a rischio**: chi ha un iPhone con il sistema operativo non aggiornato. I casi italiani, iniziati a maggio 2026, riguardano soprattutto iPhone rimasti su **iOS 16**.
- **Le falle usate**: una di WhatsApp (CVE-2025-55177, corretta dalla versione 2.25.21.73) e una di Apple sull'elaborazione delle immagini (CVE-2025-43300, corretta su iOS 16 dalla 16.7.12).
- Secondo l'analisi di Forenser, la tecnica è riconducibile anche all'exploit kit **Coruna**, che colpisce iPhone con iOS dalla 13.0 alla 17.2.1 quando si apre con Safari un sito compromesso o falso.

Attenzione: in questo attacco il dispositivo dei truffatori **può non comparire** in

Dispositivi collegati, e i messaggi inviati a tuo nome possono comparire nella tua chat come "Tu" oppure essere cancellati, così non li vedi. Quindi il controllo dei dispositivi collegati, che serve negli altri casi, qui **non basta**.

COME ACCORGERSENE

- I contatti ti dicono di aver ricevuto da te richieste urgenti di soldi che non hai mai mandato.
- Nelle tue chat trovi messaggi segnati come "Tu" che non hai scritto.
- Hai un iPhone che non aggiorni da tempo, e in Dispositivi collegati non risulta nulla di strano.

PASSO 1 **Avvisa subito i contatti**

1. Avvisa tutti, meglio con un canale diverso da WhatsApp (telefonata, SMS, social), di **non rispondere** a richieste di soldi arrivate dal tuo numero:

Il mio WhatsApp è stato clonato. Non ho chiesto soldi a nessuno. Non pagate e non rispondete a richieste di denaro a mio nome. Se avete dubbi, chiamatemi.

2. Se qualcuno ha già pagato, digli di chiamare subito la sua banca ([Parte C](#)).

PASSO 2 **Conserva le prove prima di toccare il telefono**

1. Non reinstallare WhatsApp e non ripristinare l'iPhone finché non hai conservato le prove: dopo, molte tracce dell'attacco vanno perse.
2. Fai screenshot dei messaggi "Tu" che non hai scritto e chiedi ai contatti gli screenshot dei messaggi ricevuti, con data, ora e IBAN.
3. Se ti servono prove tecniche (per una denuncia, una causa, il rimborso di chi ha pagato), porta l'iPhone a un professionista di analisi forense prima di qualsiasi altro intervento.

PASSO 3 **Denuncia**

1. Denuncia alla Polizia Postale (www.commissariatodips.it) o in questura, allegando screenshot e IBAN indicati nei messaggi.
2. Indica modello di iPhone e versione di iOS: le trovi in `Impostazioni → Generali → Info`.

PASSO 4 **Ripulisci l'iPhone**

1. Dopo aver conservato le prove, fai il ripristino ai dati di fabbrica:
`Impostazioni → Generali → Trasferisci o inizializza iPhone → Inizializza contenuto e impostazioni`.
2. Aggiorna iOS all'ultima versione disponibile:
`Impostazioni → Generali → Aggiornamento software`. Sui modelli fermi a iOS 16 l'ultima patch è la 16.7.16.
3. Reinstalla WhatsApp nell'ultima versione dall'App Store.

Aggiornare iOS o WhatsApp da solo non basta se l'account è già stato clonato: l'aggiornamento non elimina la sessione già rubata e non garantisce che il telefono sia pulito.

PASSO 5 **Riprendi l'account e rinnova l'accesso**

1. Registra di nuovo WhatsApp con il tuo numero e il codice SMS: la reinstallazione disconnette la sessione clonata.
2. Attiva o rinnova la verifica in due passaggi con un PIN nuovo e un'email di recupero:
`Impostazioni → Account → Verifica in due passaggi`.
3. Controlla `Dispositivi collegati` e scollega quello che non riconosci.

4. Se dopo questi passaggi i contatti ricevono ancora messaggi che non hai scritto, rivolgiti a un professionista di analisi forense.

PREVENZIONE Come non farti clonare l'account

1. **Aggiorna iOS** all'ultima versione disponibile per il tuo iPhone e tieni attivi gli aggiornamenti automatici.
2. **Aggiorna WhatsApp** dall'App Store.
3. Se il tuo iPhone non si aggiorna più oltre iOS 16, valuta di **sostituirlo**: resterà esposto anche alle falle future.
4. Attiva la verifica in due passaggi e controlla ogni tanto Dispositivi collegati.
5. Se sei una persona particolarmente esposta, valuta la **Modalità di isolamento** di Apple (Impostazioni → Privacy e sicurezza → Modalità di isolamento) o le impostazioni restrittive dell'account WhatsApp: limitano alcune funzioni, ma riducono il rischio.
6. Verifica sempre a voce, sul numero che conosci, qualsiasi richiesta di soldi.

Fonte: analisi del laboratorio di informatica forense Forenser (forenser.it), che ha replicato l'attacco e lo ha segnalato a Meta.

#02 Account WhatsApp rubato o collegato di nascosto ("truffa della ballerina"): recupero completo

ransomNews

COME SUCCEDDE

Il truffatore ottiene il tuo codice di verifica e con quello registra il tuo numero sul suo telefono (tu vieni disconnesso) oppure collega di nascosto un suo dispositivo al tuo account (tu non ti accorgi di nulla). Poi scrive ai tuoi contatti chiedendo soldi (es. *"Ho comprato un po' di cose online, la carta ha superato il limite, mi anticipi 1.520 euro? Domani te li ridò"*). Le esche più comuni:

- *"Scusa, ti ho mandato un codice per sbaglio, me lo giri?"*
- **"Truffa della ballerina"**: un contatto ti chiede di votare la figlia di un'amica a un concorso di danza o per una borsa di studio, con foto e link. La pagina chiede il tuo numero e il codice che ricevi. Quel codice collega il tuo WhatsApp a un dispositivo dei truffatori (*ghost pairing*): **il tuo WhatsApp continua a funzionare**, quindi non te ne accorgi, mentre loro leggono le chat e scrivono ai tuoi contatti a tuo nome.
- Una pagina che chiede di inserire numero e codice.
- Una telefonata che ti fa digitare *21*numero# : è una deviazione di chiamata, e così il truffatore riceve la chiamata vocale con il codice.
- Qualcuno usa un attimo il tuo telefono e collega WhatsApp Web al suo computer (scansiona il QR code).

PASSO 1 Capisci in che situazione sei

- WhatsApp sul tuo telefono funziona ancora, ma i contatti ricevono messaggi che non hai scritto → qualcuno usa un dispositivo collegato (è il caso tipico della "truffa della ballerina"). Vai al Passo 2.
- WhatsApp ti ha disconnesso (es. avviso che il numero è registrato su un altro telefono, o ti chiede di verificare di nuovo il numero) → l'account è stato rubato. Vai al Passo 3.
- Il telefono non ha più linea (nessun segnale, "solo emergenza") → potrebbe essere una SIM clonata. Vai alla scheda [#03](#).
- Non hai dato codici, non hai cliccato nulla e hai un iPhone non aggiornato → potrebbe essere l'attacco senza clic. Vai alla scheda [#01](#).

PASSO 2 Hai ancora accesso: scollega l'intruso

1. Apri [Impostazioni → Dispositivi collegati](#).
2. Tocca ogni dispositivo che non riconosci e scegli Disconnetti (o Esci). Nel dubbio, disconnettili tutti: potrai ricollegare i tuoi in seguito.
3. Se hai inserito un codice su un sito per "votare", fai questo controllo anche se WhatsApp sembra normale.
4. Se in [Dispositivi collegati](#) non trovi nulla ma i contatti continuano a ricevere messaggi a tuo nome, segui la scheda [#01](#): in quell'attacco l'intruso può non comparire nell'elenco.
5. Attiva la verifica in due passaggi: [Impostazioni → Account → Verifica in due passaggi → Attiva](#), PIN di 6 cifre + email di recupero.
6. Controlla che nome, foto e info del profilo non siano stati cambiati, e che non siano stati creati o abbandonati gruppi a tuo nome.
7. Prosegui dal Passo 6.

PASSO 3 Sei stato buttato fuori: riprendi l'account

1. Apri WhatsApp sul tuo telefono (se non si apre, disinstallalo e reinstallalo da App Store o Google Play).
2. Inserisci il tuo numero di telefono e richiedi il codice di verifica.
3. Inserisci il codice a 6 cifre che ricevi via SMS o chiamata: chi sta usando il tuo account viene disconnesso automaticamente.
4. Se WhatsApp ti chiede il PIN della verifica in due passaggi e lo conosci, inseriscilo. Se non lo conosci, vai al Passo 4.
5. Se il codice non arriva, vai al Passo 5.
6. Appena rientrato, attiva o cambia subito la verifica in due passaggi (PIN nuovo + email di recupero) e controlla [Dispositivi collegati](#). Poi prosegui dal Passo 6.

Le chat sono salvate sul tuo telefono e protette dalla crittografia end-to-end: chi ha preso l'account da un altro dispositivo non può leggere le tue conversazioni precedenti. Se avevi il backup su Google Drive o iCloud, potrai ripristinarle.

PASSO 4 WhatsApp chiede un PIN che non conosci

1. Probabilmente il truffatore ha attivato la verifica in due passaggi con un suo PIN.
2. Tocca **PIN dimenticato?**: se l'email di recupero è la tua, ricevi un link per disattivare la verifica in due passaggi e rientri subito. Se l'ha impostata il truffatore, l'email non ti arriverà e devi seguire il punto successivo.
3. Devi aspettare **7 giorni** dall'ultimo utilizzo dell'account. Allo scadere, tocca **PIN dimenticato? → Ripristina** e verifica di nuovo il numero con il codice SMS: rientrerai senza PIN, ma i messaggi in attesa verranno cancellati.
4. **Nel frattempo il truffatore non può più usare l'account**: quando hai inserito il codice SMS è stato disconnesso, e senza il tuo telefono non può ricevere un nuovo codice.
5. Non lasciar passare troppo tempo: dopo **30 giorni** senza rientrare, alla verifica l'account viene eliminato e ne viene creato uno nuovo.
6. Usa questi 7 giorni per avvisare i contatti (Passo 6) e denunciare (Passo 7).

Se ricevi un'email per disattivare la verifica in due passaggi che non hai chiesto tu, non cliccare il link.

PASSO 5 Il codice di verifica non arriva

1. Controlla se è attiva una deviazione di chiamata: apri il tastierino, digita ***#21#** e premi chiama. Se compare un numero che non conosci, le tue chiamate sono deviate.
2. Disattiva **tutte** le deviazioni: digita **##002#** e premi chiama. Attendi il messaggio di conferma.
3. Torna su WhatsApp e richiedi di nuovo il codice (SMS o chiamata). Se compare un conto alla rovescia, aspetta che finisca: è normale dopo più tentativi.
4. Se il telefono non ha linea o non riceve SMS e chiamate, chiama il tuo operatore da un altro telefono: potrebbe trattarsi di una SIM clonata (scheda **#03**).

PASSO 6 Avvisa subito i contatti

1. Pubblica uno stato WhatsApp (appena rientri) e un post sui tuoi social, ad esempio:

Il mio WhatsApp è stato rubato. Non ho chiesto soldi a nessuno. Non pagate e non rispondete a richieste di denaro a mio nome. Se avete dubbi, chiamatemi.

2. Scrivi direttamente (o chiama) chi ha ricevuto i messaggi, soprattutto familiari, amici stretti e i gruppi di cui fai parte.
3. Chiedi a chi ha ricevuto richieste di soldi di **fare screenshot** e mandarteli: ti servono per la denuncia.
4. Se qualcuno ha già pagato, digli di chiamare subito la sua banca ([Parte C](#)).

PASSO 7 Segnala e denuncia

1. A WhatsApp: Impostazioni → Aiuto → Contattaci (oppure [whatsapp.com/contact](https://www.whatsapp.com/contact)), descrivendo il furto dell'account.

2. Alla Polizia Postale: segnalazione online su www.commissariatodips.it oppure denuncia in questura o dai carabinieri.
3. Allega gli screenshot dei messaggi inviati dal truffatore, data e ora del furto, e i numeri o IBAN su cui chiedeva i soldi.

PASSO 8 Metti in sicurezza tutto il resto

1. Se hai usato lo stesso codice o la stessa password altrove, cambiali.
2. Controlla email, banca e gli altri servizi che usano gli SMS per l'accesso: cambia le password e attiva la verifica in due passaggi.
3. Se l'account risulta bloccato (es. per lo spam inviato dal truffatore), usa nell'app il pulsante per richiedere la revisione e spiega che l'account era stato rubato.
4. Ripristina le chat dal backup, se ti servono.

WhatsApp non può localizzare il telefono, non può dirti chi ha avuto accesso al tuo account né da dove, e non disattiva l'account al posto tuo se non riesce a verificare che il numero è tuo. Il recupero passa sempre dal codice SMS sul tuo numero.

#03 Telefono perso o rubato, SIM clonata (SIM swap)

ransomNews

COME SUCCEDDE

Il telefono viene perso o rubato, oppure il truffatore si fa intestare un duplicato della tua SIM (SIM swap): da un momento all'altro il tuo telefono resta senza linea, mentre lui riceve SMS e codici al tuo posto, compresi quelli di WhatsApp e della banca.

RISOLVI PASSO PER PASSO

PASSO 1 Blocca la SIM

1. Da un altro telefono, chiama subito il tuo operatore e fai **bloccare la SIM**.
2. Se il telefono funziona ma all'improvviso non ha più linea, chiedi all'operatore se è stato emesso un duplicato della SIM a tua insaputa.

PASSO 2 Proteggi soldi e account

1. Chiama la banca: segnala il rischio, fai bloccare carte e accessi all'home banking e controlla i movimenti.
2. Dal computer o da un altro dispositivo cambia la password dell'email principale, poi quelle degli altri servizi importanti.
3. Se il telefono è perso o rubato, usa la funzione di localizzazione e blocco del telefono (Trova il mio dispositivo di Google o Dov'è di Apple) e, se serve, cancellalo a distanza.

PASSO 3 Recupera il numero e WhatsApp

1. Vai dall'operatore con un documento e richiedi una **nuova SIM con lo stesso numero**.

2. Inserisci la SIM nel nuovo telefono, installa WhatsApp e verifica il numero con il codice: il telefono perso o rubato viene **disconnesso automaticamente** (WhatsApp funziona su un solo telefono per numero).
3. Ripristina le chat dal backup e attiva la verifica in due passaggi.
4. Finché non hai la nuova SIM, puoi chiedere aiuto a WhatsApp da whatsapp.com/contact. Ricorda che il telefono rubato può usare WhatsApp sul Wi-Fi anche con la SIM bloccata: recuperare il numero è la via più rapida per chiuderlo fuori.

PASSO 4 Denuncia

1. Furto del telefono o SIM swap: denuncia in questura o dai carabinieri (serve anche per operatore e banca).
2. Telefono smarrito: la segnalazione di smarrimento si può fare online su denunceonline.poliziadistato.it.
3. Avvisa i contatti come nel Passo 6 della scheda [#02](#).

#04 Richiesta di soldi da un contatto in rubrica

ransomNews

COME SUCCEDDE

Ricevi un messaggio da un amico o parente salvato in rubrica: *"Ho problemi con la carta, mi anticipi 1.520 euro? Domani te li ridò", "Devo pagare il notaio", "Fammi una ricarica"*. Una variante del 2026 allega un falso preventivo di un centro dentistico con l'IBAN di un privato. Quasi sempre l'account del tuo contatto è stato rubato (scheda [#02](#)).

RISOLVI PASSO PER PASSO

NON HAI ANCORA PAGATO

1. Non pagare e non rispondere con dati personali o codici.
2. Chiama la persona **a voce**, con una normale telefonata (non una chiamata WhatsApp, che arriverebbe al truffatore).
3. Se non risponde, contatta qualcuno che le sta vicino.
4. Se è una truffa: fai screenshot della chat, avvisa la persona con un altro canale (telefonata, SMS, altro social) e mandale la scheda [#02](#).
5. Segnala il messaggio: tieni premuto il messaggio → **Segnala**.

HAI GIÀ PAGATO

1. Chiama **subito** la tua banca o l'emittente della carta e chiedi di bloccare o richiamare il pagamento ([Parte C](#)).
2. Fai denuncia indicando IBAN, numero della carta prepagata o altri estremi su cui hai pagato, e allega gli screenshot.
3. Avvisa la persona di cui è stato rubato l'account: anche lei deve denunciare.

#05 "Ciao mamma, ho cambiato numero"

ransomNews

COME SUCCEDDE

Un messaggio da un numero **sconosciuto**: "Ciao mamma/papà, mi si è rotto il telefono, questo è il mio nuovo numero". Dopo qualche messaggio arriva la richiesta di pagare una bolletta, una fattura o un bonifico urgente. Spesso il truffatore dice di non poter chiamare o parlare.

RISOLVI PASSO PER PASSO

NON HAI ANCORA PAGATO

1. Chiama il **vecchio** numero del figlio o parente, oppure qualcuno che è con lui.
2. Fai una domanda che solo lui può sapere.
3. Non salvare il nuovo numero in rubrica finché non hai verificato.
4. Fai screenshot della chat, poi **blocca e segnala** il numero (apri la chat → nome in alto → Blocca / Segnala).
5. Avvisa gli altri familiari: spesso il truffatore scrive a più persone della stessa famiglia.

HAI GIÀ PAGATO

1. Chiama subito la banca e chiedi il richiamo del bonifico o il blocco del pagamento ([Parte C](#)).
2. Denuncia, con screenshot, numero di telefono del truffatore e IBAN del beneficiario.

#06 Voce clonata con intelligenza artificiale

ransomNews

COME SUCCEDDE

Un vocale o una chiamata con la voce quasi identica a quella di un familiare, che chiede soldi per un'emergenza: incidente, arresto, ospedale. Bastano pochi secondi di audio presi da video o vocali per clonare una voce. Il nome che compare può essere quello giusto, se l'account è stato rubato.

RISOLVI PASSO PER PASSO

NON HAI ANCORA PAGATO

1. Non decidere durante la chiamata. Riattacca.
2. Richiama **tu** la persona sul suo numero abituale, con una normale telefonata, oppure chiama qualcuno che è con lei.
3. Ricorda: polizia, avvocati e ospedali non chiedono soldi al telefono o via WhatsApp.
4. Concorda in famiglia una "parola d'ordine" da chiedere nelle emergenze vere.
5. Salva il vocale o fai screenshot, poi blocca e segnala.

HAI GIÀ PAGATO O CONSEGNATO SOLDI

1. Chiama subito la banca ([Parte C](#)). Se hai consegnato contanti o gioielli a qualcuno venuto a casa, chiama il **112**.

2. Denuncia, portando il vocale o il numero da cui è arrivata la chiamata.

#07 Link di phishing (corrieri, pedaggi, multe, Poste, banche)

ransomNews

COME SUCCEDDE

"Il tuo pacco è in giacenza", "Pedaggio autostradale non pagato", "Multa da saldare", "Il tuo conto è stato bloccato". Il link porta a un sito falso che imita quello vero e chiede credenziali, dati della carta, codici o documenti.

RISOLVI PASSO PER PASSO

NON HAI CLICCATO O NON HAI INSERITO NULLA

1. Non cliccare. Per controllare, apri tu il sito o l'app ufficiale **scrivendo l'indirizzo a mano** nel browser.
2. Se hai cliccato senza inserire nulla: chiudi la pagina e non scaricare file.
3. Blocca e segnala il mittente.

HAI INSERITO DATI: AGISCI IN BASE A COSA HAI DATO

- **Dati della carta** → blocca subito la carta (app della banca o numero sul retro), controlla i movimenti, disconosci le operazioni che non hai fatto ([Parte C](#)).
- **Credenziali o codici della banca** → chiama subito la banca, fai bloccare l'accesso all'home banking e cambia le credenziali da un dispositivo sicuro.
- **Password di email o social** → cambia subito la password (e ovunque l'hai riusata), disconnetti tutte le sessioni attive, attiva la verifica in due passaggi, controlla che nella tua email non siano state aggiunte regole di inoltramento automatico.
- **Credenziali SPID** → cambia la password dal sito del tuo gestore SPID, controlla lo storico degli accessi e, se trovi accessi non tuoi, contatta il gestore e chiedi la sospensione dell'identità.
- **Foto di documenti o codice fiscale** → denuncia (ti protegge se qualcuno usa i tuoi dati), poi nei mesi successivi controlla che non siano stati aperti finanziamenti o contratti a tuo nome, ad esempio richiedendo i tuoi dati alla Centrale dei rischi della Banca d'Italia.

IN OGNI CASO

1. Fai screenshot del messaggio e del sito falso (con l'indirizzo visibile).
2. Segnala alla Polizia Postale su www.commissariatodips.it; se c'è un danno, denuncia.

#08 Finto operatore della banca / "conto sicuro"

ransomNews

COME SUCCEDDE

Messaggio o chiamata, anche con il nome della banca sul display, dall'"ufficio antifrode": "C'è un accesso sospetto, dobbiamo mettere al sicuro i tuoi soldi". Ti fanno fare un bonifico su un "conto

sicuro", ti chiedono i codici, o ti mandano un finto carabiniere o finanziere a "confermare".

RISOLVI PASSO PER PASSO

DURANTE LA CHIAMATA

1. Riattacca. Non dare codici, non fare bonifici, non installare app.
2. Chiama **tu** la banca al numero sul retro della carta o sul sito ufficiale (meglio da un altro telefono, o aspetta qualche minuto prima di richiamare).
3. Ricorda: nessuna banca ti chiede **mai** di spostare soldi su un altro conto per proteggerli.
4. Se mentre fai un bonifico l'app segnala che nome e IBAN **non corrispondono**, fermati.

HAI FATTO IL BONIFICO O DATO CODICI

1. Chiama subito la banca: chiedi il richiamo del bonifico, il blocco dell'home banking e delle carte.
2. Cambia le credenziali dell'home banking da un dispositivo sicuro.
3. Se hai installato un'app su loro indicazione, segui anche la scheda [#10](#).
4. Denuncia e poi presenta reclamo scritto alla banca ([Parte C](#)).
5. Se qualcuno si presenta a casa per "ritirare" carte, contanti o gioielli, chiama il **112**.

#09 Finto supporto WhatsApp e app modificate

ransomNews

COME SUCCEDDE

"Il tuo account verrà sospeso, verifica qui", "Passa a WhatsApp Gold / WhatsApp Plus con nuove funzioni". Servono a rubare il codice o a farti installare app infette. Le versioni modificate possono anche far bloccare il tuo account da WhatsApp.

RISOLVI PASSO PER PASSO

1. Non cliccare: WhatsApp non ti scrive in chat per minacciarti di sospensione e non chiede codici.
2. Se hai dato il codice di verifica, segui subito la scheda [#02](#).
3. Se hai installato una versione modificata: fai prima il backup delle chat, poi disinstallala e installa WhatsApp **solo** da App Store o Google Play.
4. Se l'account risulta bloccato, usa nell'app il pulsante per richiedere la revisione.
5. Cambia le password importanti (email, banca) da un altro dispositivo e attiva la verifica in due passaggi su WhatsApp.
6. Se l'app modificata chiedeva permessi speciali, segui anche la scheda [#19](#).

#10 Condivisione schermo e app di controllo remoto

ransomNews

COME SUCCEDDE

Un finto tecnico (banca, operatore telefonico, Amazon, Microsoft) ti chiede di condividere lo schermo durante una videochiamata WhatsApp, o di installare app come AnyDesk o TeamViewer. Così vede i codici che ricevi e può operare sul tuo conto.

RISOLVI PASSO PER PASSO

1. Interrompi subito la chiamata e la condivisione dello schermo.
2. Metti il telefono (o il computer) in **modalità aereo** o staccalo da internet.
3. Disinstalla l'app di controllo remoto.
4. Da **un altro telefono**, chiama la banca: blocca carte e home banking e controlla i movimenti.
5. Da un altro dispositivo cambia password e PIN di banca, email e servizi principali.
6. Se non sei sicuro che il dispositivo sia pulito, fai il backup dei tuoi file e il ripristino ai dati di fabbrica.
7. Denuncia e, se ci sono operazioni non tue, segui la [Parte C](#).

#11 Finte offerte di lavoro (like, recensioni, "task")

ransomNews

COME SUCCEDDE

"Guadagna 50-200 euro al giorno mettendo like o recensioni". All'inizio ti pagano piccole somme vere per conquistare fiducia. Poi ti spostano su Telegram o su un sito e ti chiedono di "investire" o "sbloccare" i guadagni versando soldi, sempre di più. I soldi non tornano.

RISOLVI PASSO PER PASSO

1. Fermati: non versare altro, nemmeno per "sbloccare" o "recuperare" quanto hai già messo.
2. Salva tutto: screenshot delle chat, nomi e numeri dei contatti, indirizzo del sito, ricevute dei pagamenti, IBAN o indirizzi dei wallet.
3. Blocca e segnala i contatti su WhatsApp e su Telegram, esci dai gruppi.
4. Se hai pagato, chiama subito la banca ([Parte C](#)).
5. Se hai inviato foto di documenti o dati personali, segui anche il punto ["Foto di documenti"](#) della scheda #07.
6. Denuncia alla Polizia Postale.

#12 Gruppi di investimento, trading e criptovalute

ransomNews

COME SUCCEDDE

Vieni aggiunto a un gruppo con un finto "professore", a volte con la faccia di un personaggio noto (anche falsa, fatta con l'IA). Complici nel gruppo mostrano guadagni enormi. Ti fanno aprire un

conto su una piattaforma finta, dove il saldo sembra crescere. Quando provi a prelevare, ti chiedono "tasse" o "commissioni".

RISOLVI PASSO PER PASSO

1. Non versare altro e non pagare "tasse" o "commissioni" per sbloccare un prelievo: il saldo che vedi non esiste.
2. Salva tutto: chat, nome e indirizzo della piattaforma, ricevute, indirizzi dei wallet e ID delle transazioni.
3. Esci dal gruppo, segnalalo e blocca gli amministratori.
4. Chiama la banca o l'exchange da cui sono partiti i soldi e segnala la frode ([Parte C](#)).
5. Se hai dato accesso remoto al telefono o al computer, segui anche la scheda [#10](#).
6. Denuncia alla Polizia Postale e segnala la piattaforma alla **Consob** (www.consob.it).
7. Prima di investire in futuro, controlla sul sito Consob gli avvisi sulle società abusive.

#13 Truffe sentimentali

ransomNews

COME SUCCEDDE

Una persona conosciuta online, o arrivata con un "numero sbagliato", costruisce in settimane o mesi una relazione. Poi arrivano le richieste: biglietto aereo, spese mediche, dogana, oppure un "investimento" insieme.

RISOLVI PASSO PER PASSO

1. Se non l'hai mai incontrata di persona e chiede soldi, è una truffa.
2. Verifica: cerca le sue foto con una ricerca per immagini (Google Immagini o Google Lens) e proponi una videochiamata: di solito trova sempre scuse.
3. Non mandare altri soldi, regali, codici di buoni o foto intime.
4. Salva le chat, poi interrompi i contatti, blocca e segnala.
5. Se hai pagato, chiama subito la banca ([Parte C](#)) e denuncia.
6. Parlane con una persona di fiducia: queste truffe giocano sulla vergogna, ma sono organizzate da professionisti.

#14 Sextortion e immagini intime

ransomNews

COME SUCCEDDE

Dopo una conversazione o videochiamata intima arriva il ricatto: "Pubblico il video se non paghi". Oppure un messaggio generico che sostiene di averti registrato.

RISOLVI PASSO PER PASSO

1. **Non pagare:** pagare porta solo a nuove richieste.

2. Non rispondere più e **non cancellare** le chat: fai screenshot di profilo, numero, messaggi e richieste di pagamento.
3. Blocca e segnala il profilo su WhatsApp e sugli altri social dove ti ha contattato.
4. Se temi che le immagini vengano pubblicate, fai la segnalazione al **Garante Privacy** con il modulo online (garanteprivacy.it/revengeporn): indica le piattaforme dove temi la diffusione. Il Garante decide entro 48 ore e può ordinare alle piattaforme di bloccare il materiale. Possono segnalare anche i ragazzi dai 14 anni, per i più piccoli i genitori.
5. Se sei maggiorenne puoi usare anche **StopNCII.org**: crea un'impronta digitale delle immagini sul tuo dispositivo, senza caricarle, e le piattaforme aderenti la usano per bloccarle.
6. Denuncia alla Polizia Postale (www.commissariatodips.it): estorsione e minaccia sono reati.
7. Se è coinvolto un **minore**, è un reato gravissimo da trattare in urgenza: rivolgiti subito alla Polizia Postale. Per i minorenni esiste anche il servizio **Take It Down** per far rimuovere le immagini.

#15 Compravendite online (Vinted, Subito, Marketplace)

ransomNews

COME SUCCEDDE

Come venditore: un finto acquirente ti sposta su WhatsApp e ti manda un link per "ricevere il pagamento" o "confermare la spedizione". Il link ruba i dati della carta. **Come acquirente:** paghi in anticipo fuori dalla piattaforma (bonifico, ricarica) e la merce non arriva mai.

RISOLVI PASSO PER PASSO

PREVENZIONE

1. Resta nella chat e nel sistema di pagamento della piattaforma.
2. Per **ricevere** soldi non serve mai inserire i dati della tua carta né codici.

SE CI SEI CASCATO

1. Hai inserito i dati della carta → bloccala subito e disconosci le operazioni ([Parte C](#)).
2. Hai pagato e la merce non arriva → se hai pagato sulla piattaforma, apri una contestazione dall'app; se hai pagato con carta o PayPal, chiedi il rimborso tramite la contestazione del tuo circuito; se hai fatto un bonifico o una ricarica, chiama subito la banca o l'emittente.
3. Segnala l'utente alla piattaforma, con gli screenshot.
4. Denuncia, indicando profilo, numero di telefono, IBAN o carta su cui hai pagato.

#16 Affitti e case vacanza inesistenti

ransomNews

COME SUCCEDDE

Annuncio con prezzo molto basso, il "proprietario" è all'estero e chiede una caparra via bonifico o ricarica per "bloccare" la casa. La casa non esiste o non è sua.

RISOLVI PASSO PER PASSO

1. Prima di pagare: cerca le foto dell'annuncio con una ricerca per immagini, chiedi di vedere la casa o un contratto verificabile, preferisci piattaforme con pagamento protetto.
2. Se hai pagato: chiama subito la banca o l'emittente della carta ricaricata ([Parte C](#)).
3. Se la prenotazione era partita da una piattaforma (Airbnb, Booking ecc.), segnala subito l'annuncio e chiedi assistenza alla piattaforma.
4. Salva annuncio, chat e ricevute, e denuncia.

#17 Premi, concorsi, regali e buoni falsi

ransomNews

COME SUCCEDDE

"Hai vinto un iPhone", "Buono da 500 euro per l'anniversario del supermercato", "Rispondi al sondaggio e ricevi un premio". Ti chiedono dati, una piccola "spesa di spedizione" con la carta (che in realtà attiva abbonamenti), o di inoltrare il messaggio.

RISOLVI PASSO PER PASSO

1. Non hai vinto nulla a cui non hai partecipato: non cliccare e non inoltrare il messaggio.
2. Se hai inserito la carta: bloccala e disconosci gli addebiti ([Parte C](#)). Controlla l'estratto conto anche nei mesi successivi: questi abbonamenti addebitano piccole cifre ricorrenti.
3. Se hai inserito il numero di telefono e ti arrivano addebiti sul credito, chiedi all'operatore di disattivare i servizi a pagamento non richiesti e di attivare il blocco.
4. Segnala il messaggio e, se c'è un danno, denuncia.

#18 Chiamate e messaggi da prefissi esteri

ransomNews

COME SUCCEDDE

Chiamate o messaggi da numeri con prefissi esteri sconosciuti (+62, +84, +254, +92 e altri): offerte di lavoro, "numero sbagliato", proposte di investimento. Sono spesso l'inizio delle truffe [#11](#), [#12](#) e [#13](#).

RISOLVI PASSO PER PASSO

1. Non rispondere e non richiamare.
2. Blocca e segnala: apri la chat → nome in alto → **Blocca e Segnala**.
3. Attiva .

4. Attiva Impostazioni → Privacy → Gruppi → I miei contatti .

5. Se hai già iniziato a parlarci, segui la scheda corrispondente ([#11](#), [#12](#) o [#13](#)).

#19 Allegati e app infette da installare

ransomNews

COME SUCCEDDE

Ti inviano un file (.apk su Android, documenti, la "foto del pacco" di un finto corriere, un "invito al matrimonio", una "fattura") o ti chiedono di installare un'app per "tracciare il pacco", "ricevere il rimborso", "parlare con l'operatore". L'app ruba dati, legge gli SMS o controlla il telefono.

RISOLVI PASSO PER PASSO

1. Metti subito il telefono in **modalità aereo**.
2. Disinstalla l'app. Su Android, se non si lascia disinstallare, controlla in Impostazioni → Sicurezza le app con permessi di amministratore e in Impostazioni → Accessibilità le app con accesso speciale: toglì i permessi, poi disinstallala.
3. Su Android esegui la scansione di Google Play Protect (Play Store → foto profilo → Play Protect).
4. Da **un altro dispositivo**, chiama la banca e cambia le password di banca, email e servizi principali.
5. Se non sei sicuro che il telefono sia pulito, fai il backup delle foto e delle chat e il **ripristino ai dati di fabbrica**. Dopo il ripristino, non reinstallare l'app sospetta.
6. Se ci sono operazioni non tue, segui la [Parte C](#) e denuncia.

Non aprire allegati inattesi nemmeno se arrivano da amici: il loro account potrebbe essere stato rubato. Installa app solo dagli store ufficiali.

#20 Finto recupero dei soldi persi

ransomNews

COME SUCCEDDE

Dopo una truffa, qualcuno ti contatta fingendosi avvocato, agenzia, ente pubblico o "hacker etico": *"Possiamo recuperare i tuoi soldi, serve un anticipo"*. È la seconda truffa sulla stessa vittima.

RISOLVI PASSO PER PASSO

1. Nessuno recupera soldi truffati in cambio di un anticipo: non pagare e non dare accesso al telefono o al conto.
2. Rivolgiti solo alla tua banca, alla Polizia Postale o a un avvocato scelto da te.
3. Salva i messaggi e aggiungili alla denuncia che hai già fatto.

4. Se hai già pagato, segui la [Parte C](#).

#21 False convocazioni di polizia ed enti pubblici

ransomNews

COME SUCCEDDE

Un messaggio o un PDF con loghi della Polizia, dei Carabinieri, della Polizia Postale, dell'INPS o dell'Agenzia delle Entrate, a volte firmato con il nome di un vero dirigente. Ti accusa di reati gravi o ti segnala una "pendenza", minaccia arresto o sanzioni e ti chiede di rispondere, mandare dati o pagare per "chiudere il caso" o ottenere un rimborso.

RISOLVI PASSO PER PASSO

1. Mantieni la calma: polizia ed enti pubblici **non** chiedono soldi o dati via WhatsApp, email o SMS sotto minaccia di procedimenti.
2. Non rispondere, non aprire allegati, non cliccare link, non pagare, non inviare documenti.
3. Se vuoi verificare, usa solo i canali ufficiali che trovi tu: poliziadistato.it, il sito dell'ente, il numero della questura o della caserma più vicina. Mai i contatti scritti nel messaggio.
4. Fai screenshot e segnala alla Polizia Postale su www.commissariatodips.it, poi blocca il mittente.
5. Se hai già risposto o inviato dati, segui la scheda [#07](#); se hai pagato, la [Parte C](#), e denuncia.

#22 Finti prestiti e finanziamenti

ransomNews

COME SUCCEDDE

Ti offrono un prestito veloce, senza garanzie e "anche ai cattivi pagatori". Per erogarlo chiedono prima un anticipo: "spese di istruttoria", "assicurazione", "tasse", "sblocco della pratica". Dopo il pagamento ne chiedono un altro, e il prestito non arriva mai. Spesso chiedono anche foto dei documenti.

RISOLVI PASSO PER PASSO

1. Un prestito vero non si sblocca pagando in anticipo: non versare nulla.
2. Prima di qualsiasi finanziamento, verifica che la società sia iscritta negli elenchi della **Banca d'Italia** (banche e intermediari finanziari) o dell'**OAM** (agenti e mediatori creditizi).
3. Se hai pagato: chiama subito la banca o l'emittente della carta ricaricata ([Parte C](#)).
4. Se hai inviato documenti o codice fiscale, segui il punto ["Foto di documenti"](#) della scheda [#07](#).
5. Salva chat e ricevute, blocca, segnala e denuncia.

COME SUCCEDDE

Raccolte fondi: dopo un'emergenza (alluvione, terremoto, guerra) o per un "bambino malato", arriva un appello con un IBAN o un link per donare, spesso inoltrato da amici in buona fede.

Biglietti: concerti e partite esauriti offerti in chat o nei gruppi, da pagare con bonifico o ricarica; i biglietti non arrivano, sono falsi o già venduti a più persone.

RISOLVI PASSO PER PASSO

1. Dona solo dai siti ufficiali delle organizzazioni, scrivendo l'indirizzo a mano, non da link o IBAN ricevuti in chat. Gli enti del terzo settore si possono verificare sul Registro unico nazionale del terzo settore (RUNTS).
2. Compra biglietti solo dai canali ufficiali o dalle piattaforme di rivendita autorizzate dall'organizzatore.
3. Non inoltrare appelli che non hai verificato.
4. Se hai pagato: chiama subito la banca o l'emittente ([Parte C](#)); se hai pagato con carta o PayPal, apri una contestazione.
5. Salva chat, profilo del venditore e ricevute, segnala e denuncia.

PARTE C

Ho già pagato o dato dati: cosa fare

Agisci subito: i primi minuti e le prime ore contano.

Ho fatto un bonifico

1. Chiama subito la banca e chiedi il richiamo del bonifico. Il bonifico istantaneo è irrevocabile, ma chiedi comunque: la banca può tentare il recupero presso la banca del beneficiario e segnalare il conto.
2. Denuncia, indicando IBAN e intestatario del beneficiario, e porta la denuncia alla banca.
3. Un bonifico disposto da te, anche se ingannato, per la legge è "autorizzato": il rimborso non è automatico. Puoi comunque presentare reclamo (vedi sotto).

Pagamenti con carta o dati della carta

1. Blocca la carta (app della banca o numero sul retro).
2. Chiedi alla banca il disconoscimento delle operazioni che non hai autorizzato tu. Hai tempo fino a 13 mesi dall'addebito, ma fallo subito.
3. Per le operazioni non autorizzate la banca deve rimborsare entro la giornata lavorativa successiva, salvo che dimostri tua colpa grave (es. aver comunicato tu i codici).
4. Denuncia: la copia serve per la pratica di rimborso.

Ricarica (Postepay, prepagate, buoni)

1. Contatta subito l'emittente della carta o dei buoni e chiedi il blocco.
2. Denuncia, indicando il numero della carta ricaricata o i codici dei buoni.

Criptovalute

1. Salva indirizzo del wallet, ID della transazione, chat.
2. Se hai usato un exchange, avvisalo subito con questi dati.
3. Denuncia: sono difficili da recuperare, ma le transazioni sono tracciabili.

Codici, password o accesso al telefono

1. Chiama la banca e fai bloccare gli accessi.
2. Cambia le password, l'email per prima, da un dispositivo sicuro.
3. Attiva la verifica in due passaggi ovunque possibile.

In ogni caso

- Non cancellare nulla: chat, numeri, screenshot, ricevute.
- Annota data e ora di ogni passaggio.
- Non pagare nessuno che promette di recuperare i soldi (scheda [#20](#)).

Se la banca non rimborsa: reclamo e Arbitro Bancario Finanziario

1. Invia un reclamo scritto alla banca (PEC, raccomandata A/R o modulo online) con: i tuoi dati, i dati del conto o della carta, le operazioni contestate, la richiesta di rimborso e in allegato denuncia, estratto conto e prova del blocco.
2. La banca deve rispondere entro 15 giorni lavorativi (fino a 35 in casi eccezionali motivati).
3. Se rifiuta o non risponde, puoi ricorrere all'Arbitro Bancario Finanziario (www.arbitrobancariofinanziario.it): si fa online, sulla base dei documenti, senza bisogno di un avvocato.

PRIMA DI PAGARE: LA VERIFICA DEL BENEFICIARIO

Dal 9 ottobre 2025, prima di ogni bonifico (ordinario o istantaneo) la banca confronta il nome che hai scritto con l'intestatario reale dell'IBAN. Se l'app mostra mancata corrispondenza o corrispondenza parziale, fermati e verifica a voce con un canale che già conosci.

PARTE D

Denunce, segnalazioni e contatti utili

Cosa portare alla denuncia

- Screenshot delle chat, con numero di telefono o profilo del truffatore ben visibile.
- Data e ora dei fatti, annotate passo per passo.
- Ricevute dei pagamenti, IBAN, numeri di carte ricaricate, indirizzi dei wallet.

- Indirizzi dei siti falsi e nomi delle app installate.
- Un documento d'identità.

Polizia Postale e denuncia

- Segnalazione online:
www.commissariatodips.it
- Denuncia: in questura, in un ufficio della Polizia Postale o presso i carabinieri.
- Denunce online:
denunceonline.poliziadistato.it (anche da app IO). La pre-denuncia per truffe e frodi è in sperimentazione solo in alcuni uffici di Lazio e Umbria e va confermata di persona entro 48 ore; la segnalazione di smarrimento del telefono vale in tutta Italia.
- Canale WhatsApp ufficiale della Polizia di Stato (scheda "Aggiornamenti") per gli avvisi sulle nuove truffe.

WhatsApp

- Tieni premuto il messaggio o apri la chat → **Segnala / Blocca**.
- Account rubato o bloccato:
Impostazioni → Aiuto → Contattaci oppure
whatsapp.com/contact

Soldi e banche

- La tua banca: numero sul retro della carta o sul sito ufficiale. Salvalo **ora** in rubrica.
- Arbitro Bancario Finanziario:
www.arbitrobancariofinanziario.it
- Consob (investimenti e società abusive):
www.consob.it

Immagini intime e altri contatti

- Garante Privacy, segnalazione immagini intime: garanteprivacy.it/revengeporn
- StopNCII.org (maggioresni) e Take It Down (minoresni).
- Emergenze: **112**
- Piattaforme (Vinted, Subito, Marketplace, Airbnb, Booking): segnala l'utente dall'app.

IN UNA RIGA

Chi ti chiede soldi o codici via chat va verificato a voce, sul numero che conosci. Se c'è fretta, è quasi sempre una truffa.