%(EYEBROW)S

%(cover_title)s

%(cover_sub)s

%(byline)s **%(byline_b)s**

%(pub)s **%(pub_b)s**

%(PRICE_LBL)S

€6

%(price_was)s ~~%(was_price)s~~

Non fartiingannare

Come funzionano **davvero** le truffe e le frodi online — e come proteggere te stesso, la tua famiglia e il tuo denaro. Una guida visiva sul campo distillata da un manuale di 100 capitoli: la psicologia, il copione, il catalogo di 45 tipi di truffa, i dati sul rischio dei pagamenti e il piano di recupero.

9
Parti
100
Capitoli
45+
Tipi di truffa
36
Tabelle di dati
70k
Parole di fonte

Anteprima gratuita · Il Rapporto sulla Difesa dalle Truffe

Stai leggendo l'*anteprima gratuita*. La difesa completa è nel manuale.

Quello che hai davanti è il rapporto visivo: la psicologia della truffa, il copione in sette passi, il catalogo dei tipi di truffa, i dati sul rischio dei pagamenti, i controlli di verifica e le prime mosse di recupero. È già molto — ma è **una distillazione**. Il manuale completo *Non farti ingannare* (100 capitoli) aggiunge proprio le parti che contano di più quando i soldi sono già partiti.

01
Carte regalo e Steam card Perché i truffatori le pretendono, come funziona la richiesta, le bandierine rosse da riconoscere e la procedura dei primi dieci minuti se hai già grattato e inviato il codice.
02
Rintracciare i truffatori Intestazioni delle email, indirizzi IP, indagini WHOIS sui domini, tracce su IBAN e wallet di criptovalute: cosa puoi fare davvero da solo, con i limiti spiegati con onestà.
03
Recuperare il denaro Richiamo bancario, chargeback, azione legale, assicurazione — e una tabella chiara di ciò che è recuperabile e ciò che non lo è.
04
Checklist, modelli e risorse italiane Strumenti compilabili, lettere alla banca, denuncia e querela, contatti delle autorità italiane ed europee.

Offerta di lancio · tempo limitato
€6
invece di ~~€7,99~~

Compra la guida completa — €6 Checklist gratuita

Panoramica

Un crimine che attacca i *sentimenti*, non l’intelligenza

Le truffe sono una delle più grandi industrie del mondo. Raggiungono ogni Paese, ogni fascia d’età, ogni livello di istruzione. Medici, avvocati, direttori di banca e agenti di polizia vengono tutti truffati. Il motivo è semplice — ed è l’idea più importante di questo rapporto.

La tesi

I truffatori non attaccano la tua intelligenza

Attaccano i tuoi sentimenti. Una truffa è una storia raccontata per farti agire prima di pensare. La difesa non è essere più furbi — è costruire comunque il tempo per pensare.

La scala

Centinaia di milioni di euro, solo in Italia

Le denunce di frode online si contano a decine di migliaia ogni anno in Italia, con perdite per centinaia di milioni. In tutta l’UE la cifra raggiunge i miliardi; nel mondo, alcune stime superano i mille miliardi di dollari l’anno.

Il costo nascosto

La maggior parte delle truffe non viene mai denunciata

Le vittime provano vergogna, quindi le cifre ufficiali sono solo quelle che conosciamo. Gli esperti ritengono che il totale reale sia diverse volte superiore — e dietro ogni statistica c’è una persona che non se lo meritava.

«Una truffa è una storia raccontata per farti agire prima di pensare. La tua difesa è pensare comunque.»

L’unica frase da ricordare

In sintesi

3
Cose che vuole un truffatore: denaro, informazioni, aiuto
10
Pulsanti psicologici che preme
7
Passi in ogni truffa
20
Bandierine rosse d’oro

Parte I · Capire le truffe

L’anatomia di una *truffa*

Quasi ogni truffa al mondo cerca di ottenere da te una di tre cose. Capisci questo, e capisci l’intera macchina.

Cosa cerca davvero il truffatore

Obiettivo 01

Il tuo denaro

Inviare denaro, trasferire denaro, pagare una commissione, comprare carte regalo o consegnare i dati bancari perché lo prendano da soli. L’obiettivo più ovvio — e il metodo di pagamento è sempre una loro scelta, mai la tua.

Obiettivo 02

Le tue informazioni

A volte non chiedono affatto denaro. Vogliono la tua password, il numero della carta, il PIN, un codice inviato al tuo telefono, una copia del passaporto o la tua data di nascita — per rubare più tardi, aprire conti a tuo nome o impossessarsi dei tuoi account.

Obiettivo 03

Il tuo aiuto

Quello che sorprende le persone. Vogliono che tu riceva denaro, inoltri un pacco, compri con la tua carta o apra un conto. Credi di aiutare o di guadagnare. In realtà sei uno scudo — e ora il reato è in parte a tuo nome.

I dieci pulsanti psicologici

Pulsante 01

Speranza e avidità

Qualcosa per nulla — sempre «appena credibile». Non un miliardo di euro, ma cinquantamila. Abbastanza grande da cambiarti la vita, abbastanza piccolo da sembrare possibile.

Pulsante 02

Paura

«Il tuo conto è stato violato.» «C’è un mandato di arresto.» La paura spegne il pensiero attento, e il truffatore offre la via più rapida per farla cessare.

Pulsante 03

Amore e solitudine

Il pulsante più potente di tutti, e il più crudele. La vittima spesso difende il truffatore, perché credere alla verità significa perdere l’unica persona che sembra tenere a lei.

Pulsante 04

Autorità

Polizia, banche, fisco: obbediamo. Usano loghi ufficiali, linguaggio ufficiale, identificativo del chiamante falsificato e indirizzi email quasi perfetti. Quando parla l’autorità, smettiamo di dubitare.

Pulsante 05

Urgenza

«Entro 24 ore.» La velocità è l’alleata del truffatore e la nemica della vittima. Una scadenza viene fabbricata per impedirti di controllare.

Pulsante 06

Vergogna

Contano sul tuo silenzio. Se sei troppo imbarazzato per dirlo a qualcuno, nessuno può avvertirti — e la truffa continua indisturbata.

Pulsante 07

Il piede nella porta

Un piccolo primo sì — un piccolo favore, un piccolo pagamento — rende il successivo, più grande sì, coerente e naturale.

Pulsante 08

La trappola dei costi affondati

Hai già pagato, quindi pagare ancora una volta sbloccherà finalmente le «vincite». Ecco perché le vittime pagano ancora e ancora.

Pulsante 09

Prova sociale

Un gruppo di chat pieno di «clienti» felici, tutti falsi. Se lo fanno tutti, dev’essere sicuro — peccato che «tutti» sia anche il truffatore.

Pulsante 10

Illusione di controllo

«Puoi prelevare quando vuoi.» Il pannello, i numeri, i livelli VIP — tutto progettato per farti sentire padrone del tuo denaro.

Il copione del truffatore — sette passi, ogni volta

1 · L’approccio, o l’amo
Contatto inatteso — email, SMS, chiamata, richiesta di amicizia, un «numero sbagliato»
2 · Costruire la fiducia, o il corteggiamento
Calore, una storia triste, «prove» di guadagni, un gruppo di chat di finti clienti felici
3 · Creare il bisogno
Un motivo urgente ed emotivo — e la soluzione è sempre che tu invii denaro
4 · Il primo pagamento
Una piccola somma, o un’informazione — progettata per sembrare innocua
5 · L’escalation
Somme più grandi, più pressione, una nuova scadenza ogni volta
6 · L’estrazione
Tutto — risparmi, prestiti, persino il denaro di altre persone
7 · La sparizione, o il ghosting
Silenzio, oppure una nuova identità e un nuovo bersaglio

La stessa macchina, un costume diverso

Tipo di truffa	Passo 1 — l’approccio	Passo 3 — il bisogno
Sentimentale	Numero sbagliato o app di incontri	Parente malato, spese di viaggio
Investimenti	Annuncio sui social o invito a un gruppo	Deposito per iniziare a guadagnare
Falso lavoro	Offerta di lavoro su WhatsApp	Quota di formazione, quota per l’attrezzatura
Phishing bancario	SMS: «il tuo conto è bloccato»	Conferma i tuoi dati o sposta il denaro
Lotteria	Email: «hai vinto»	Tassa per sbloccare il premio
Affitti	Annuncio immobiliare sotto il prezzo di mercato	Caparra prima della visita
Assistenza tecnica	Pop-up: «il tuo computer è infetto»	Pagare l’«assistenza» o dare accesso remoto

Storia diversa. Stessa macchina. Riconoscere la struttura — non il dettaglio — è ciò che ti protegge.

Parte I · Capitolo 2

Niente è nuovo — sono cambiati solo gli *strumenti*

Per capire le truffe moderne, aiuta sapere da dove vengono. Dai mercati antichi al clonaggio vocale con l’IA, la truffa è la stessa: conquistare la fiducia, poi usarla contro chi l’ha data.

Mondo antico
Commercio e viaggi
Merci false, reliquie false, pesi truccati
1800
Posta e telegrammi
Prigioniero spagnolo, lingotto d’oro, truffa del filo
1900
Lettere e fax
Lettere con anticipo, lotterie false
1990
Email
Phishing di massa, lettere «nigeriane», premi falsi
2000
Siti web e chat
Negozi falsi, incontri falsi, lavori falsi
2010
Social media
Truffe sentimentali, furto d’identità, profili falsi
Dal 2017
Cripto e app
Investimenti falsi, pig butchering, furto di wallet
2020
IA
Clonaggio vocale, video deepfake, chat automatica

Ogni nuova tecnologia ha ampliato la portata della truffa — non ne ha mai cambiato la logica.

L’economia della truffa — dove va il denaro

Tappa 01

Il tuo pagamento

Un pagamento esce da te. Il suo tipo decide quanto sarà difficile recuperarlo — e il truffatore sceglie sempre il più difficile da invertire.

Tappa 02

Il prestanome

Un «money mule» lo riceve — spesso reclutato con un falso lavoro: «ricevi pagamenti, tieni il cinque per cento».

Tappa 03

Gli strati

Viene spostato, di solito suddiviso in somme più piccole, attraverso conti in diversi Paesi.

Tappa 04

L’incasso

Convertito in cripto o contanti e sparito nel giro di ore. Ecco perché la velocità conta così tanto.

Chi c’è dietro

L’industria

I «compound delle truffe» nel Sud-Est asiatico

Le più grandi operazioni organizzate non sono in Africa. In Myanmar, Cambogia e Laos, complessi recintati ospitano centinaia o migliaia di lavoratori che gestiscono pig butchering, investimenti falsi e truffe sentimentali a turni, con manager, obiettivi e reparti risorse umane. Molti dei lavoratori sono essi stessi vittime — attirati da falsi lavori, con i passaporti sequestrati, costretti a lavorare sotto minaccia di violenza.

La sottocultura

I «Yahoo Boys» e la cultura della frode

In alcune parti dell’Africa occidentale, la frode informatica è diventata una sottocultura che tratta la truffa come un gioco e uno status symbol — fotografie di lusso comprate con denaro rubato, un proprio gergo, musica ed eroi. Danneggia tutti, compresi i cittadini onesti e le imprese dei Paesi in cui esiste.

«Non immaginare un criminale solitario. Potresti parlare con una persona che è essa stessa prigioniera, che legge un copione scritto da qualcun altro, in un edificio dall’altra parte del mondo.»

Capitolo 5 — Chi sono i truffatori?

Parte II · Il grande catalogo

Quarantacinque modi per essere *ingannati* — e come riconoscere ciascuno

Il capitolo mostruoso del manuale cataloga ogni grande truffa in circolazione. Qui sono raggruppate per il canale attraverso cui arrivano, ciascuna contrassegnata da un livello di rischio relativo tratto dal modo in cui la fonte stessa la tratta.

I classici e i grandi soldi

Gli archetipi della frode con anticipo e le frodi sugli investimenti ad alte perdite che dominano le perdite di oggi.

Frode con anticipo (la «419») «Pig butchering» — la più pericolosa oggi Investimenti falsi e cripto Forex, bot di trading e «profitto garantito» Schemi Ponzi e piramidali Eredità e «cliente defunto» Lotteria, premio e concorso falsi

Amore, solitudine e la truffa lunga

Truffe che prima costruiscono una relazione — spesso per settimane o mesi — prima della prima richiesta di denaro.

Truffe sentimentali e falso amore Truffe sulle app di incontri Sextortion e ricatto La truffa dei nonni / emergenza familiare Messaggio «conto di un familiare»

Denaro, lavoro e la promessa di guadagni facili

Dove l'offerta di reddito o credito è l'esca, e la quota che paghi è il prodotto.

Falso lavoro e lavoro da casa Truffe su prestiti e credito «Riparazione del credito» e cancellazione dei debiti Prestanome — quando diventi tu il criminale «Contributo per piccole imprese» «Agenzia per il lavoro» che prende i documenti

Il messaggio in tasca

Phishing via email, SMS e telefono — le truffe più diffuse al mondo, e le più facili da riconoscere una volta che conosci i segnali.

Phishing — email che rubano la tua vita Smishing e vishing — SMS e telefono Finte chiamate bancarie e «conto bloccato» Impersonare polizia, fisco e governo Finte consegne e corrieri Truffe di assistenza tecnica Codice QR, app di pagamento e POS

Piattaforme, negozi e social

Frodi che si nascondono dentro le app che usi ogni giorno, dai marketplace alle piattaforme video.

Negozi online falsi Frodi sui marketplace (Vinted, Subito, Facebook) Truffe su WhatsApp Truffe su Telegram Truffe su Facebook e Instagram TikTok, YouTube e influencer Affitti e immobili Biglietti, eventi e viaggi

Imprese, documenti e identità

Le truffe che prendono di mira aziende, processi ufficiali e le carte di una vita.

Compromissione email aziendale (BEC) Frode sulle fatture e frode del CEO SIM swapping e furto del numero Visti, immigrazione e documenti Università e borse di studio false Recupero di «account violato»

Il secondo attacco e la nuova frontiera

Lo strato più crudele — truffe che cacciano chi è già stato truffato — e il kit di strumenti IA che alimenta ciò che verrà.

Truffe del recupero — il secondo attacco IA, deepfake e clonaggio vocale Finte beneficenze e soccorsi per disastri Animali, cuccioli e pet Arte, antiquariato e oro falsi Trappole di abbonamenti e prove gratuite «Cessione del credito» e rimborso bollette energetiche

I livelli di rischio sono giudizi editoriali, non tratti dalle tabelle della fonte · fonte: Capitoli 9–46

I termini che dovrebbero farti fermare

La tabella del «linguaggio dei truffatori» del manuale, per intero. Queste frasi non sono errori — sono copioni, e ciascuna ha uno scopo.

La parola o frase	Cosa significa davvero
«Urgente», «immediatamente», «entro 24 ore»	Non vogliamo che tu abbia il tempo di pensare
«Riservato», «non dirlo a nessuno»	Nessuno deve poter ti avvertire
«Piccola commissione per sbloccare i fondi»	Il primo di molti pagamenti che non rivedrai mai
«Profitto garantito», «senza rischio»	Ogni investimento ha un rischio; questa promessa è una bugia
«Conto sicuro»	Non esiste; una bugia per spostare il tuo denaro
«Il conto è bloccato, conferma i tuoi dati»	Vogliamo la tua password o il numero della carta
«Il tuo pacco non può essere consegnato»	Vogliamo un piccolo pagamento o i dati della tua carta
«Paga con carte regalo»	Vogliamo denaro che non si può tracciare né rimborsare
«Invialo in cripto»	Vogliamo denaro che non si può invertire
«Rispondi a questa email personale, non a quella ufficiale»	Non siamo chi diciamo di essere

Fonte: Capitolo 8 — Il linguaggio dei truffatori

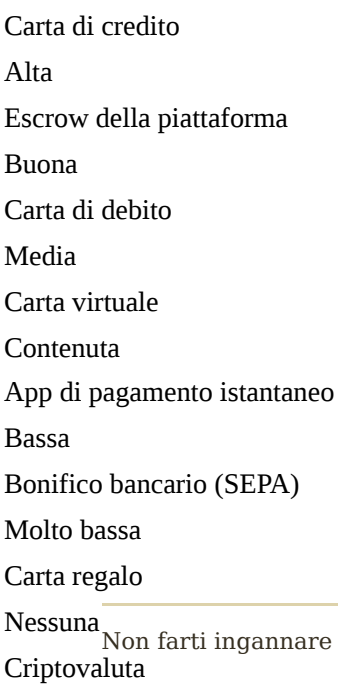
Dati · Parti II, V, VI

I numeri che *contano*

Due cifre decidono come finisce una truffa: quanto è reversibile il metodo di pagamento e quanto in alto sale la vittima sulla scala dell’escalation. Le tabelle della fonte, trasformate in grafici.

Grafico 1 · Quanto è reversibile ogni metodo di pagamento?

Recuperabilità, da «nessuna» ad «alta». Il truffatore sceglie il metodo di pagamento proprio perché è in fondo a questa lista — più bassa è la barra, meglio è per lui.



Nessuna

Fonti: Capitolo 6.1 (tabella di inversione) e Capitolo 96.3 (tabella di sicurezza dei metodi di pagamento). La lunghezza della barra è una codifica illustrativa delle valutazioni qualitative della fonte.

La via più rapida per fermare il denaro

Tipo di pagamento	Cosa si può fare	Quanto in fretta
Pagamento con carta, in sospeso	Annullarlo o bloccarlo	Ore
Pagamento con carta, completato	Richiesta di chargeback	Giorni–settimane
Bonifico SEPA, recente	Richiamo + cooperazione tra banche	Ore–giorni
Bonifico SEPA, più vecchio / inoltrato	Molto difficile	Quasi mai
Trasferimento in cripto	Tracciabile, non reversibile; blocco sull’exchange solo con la polizia	Ore, con la polizia
Carte regalo, non ancora usate	Segnalazione all’emittente, a volte possibile	Ore
Carte regalo, usate / contanti	Perse — denuncia alla polizia con urgenza	Chiuso

Fonte: Capitolo 65.1 — Fermare il denaro. La velocità decide tutto.

La scala dell’escalation di una truffa sentimentale

Le richieste crescono in cinque fasi. Le cifre della fonte mostrano come una prima piccola commissione diventa «tutto».

€200–500
Fase 1
Tassa per il visto, bolletta ospedaliera, riparazioni del telefono
€1k–3k
Fase 2
Dogana per un «regalo» che ti viene inviato
€5k–20k
Fase 3
Operazione medica, viaggio urgente
€20k+
Fase 4
«Contratto bloccato, ho bisogno di aiuto»
Tutto
Fase 5
Problemi senza fine, prestiti, risparmi

Fonte: Capitolo 10.3 — Le richieste di denaro, in ordine di comparsa.

Vero o falso? Due confronti da memorizzare

Investimento reale	Investimento falso
Regolamentato e registrato	Non si trova in nessun registro
Rendimenti descritti come possibili	Rendimenti descritti come certi
Prelevi liberamente	Il prelievo è sempre bloccato
Documenti che puoi verificare	Screenshot che non puoi controllare

Investimento reale	Investimento falso
Contatto tramite canali ufficiali	Contatto solo su app di chat
Nessuna pressione a decidere in fretta	Pressione costante e scadenze

Istituzione reale	Come ti contatta davvero
Polizia e Carabinieri	Non chiedono mai denaro per telefono o messaggio
Agenzia delle Entrate	In modo formale, per iscritto, canali ufficiali
INPS	Portale ufficiale o posta, non chat
Comune	Avvisi formali, mai SMS urgenti
Banche	Non ti chiedono mai di spostare denaro su un «conto sicuro»

Fonti: Capitolo 14.1 e Capitolo 28.2 — le due tabelle da ricordare prima di pagare o di credere.

Caso di studio · L’«accademia di trading» che è svanita

Capitolo 14.4

Una coppia, un gruppo Telegram e €150.000

Una coppia italiana sulla cinquantina si iscrisse a un’«accademia di trading» su Telegram consigliata da un amico che vi aveva già «guadagnato» — egli stesso una vittima, pagato con una piccola commissione per reclutare altri. Cominciarono con €1.000, videro profitti giornalieri sul pannello e in otto mesi investirono quasi €150.000, compresi un prestito bancario e la vendita di un’auto. Quando chiesero di prelevare, la piattaforma pretese una «tassa di sblocco del 22%». Ne pagarono una parte. Poi il sito, il gruppo e ogni amministratore sparirono.

Capitolo 12.4

Un commercialista, una «analista finanziaria» e €200.000

Un commercialista di 40 anni della Lombardia ricevette un messaggio WhatsApp da una donna che si presentò come analista finanziaria. Dopo tre mesi di conversazioni quotidiane, aveva trasferito quasi €200.000 su una piattaforma che mostrava un saldo di oltre €300.000 — e aveva parlato a suo fratello del «miglior investimento della sua vita». Il prelievo fu rifiutato a meno che non pagasse una «tassa» del 20%. Prese in prestito €40.000 per pagarla. Poi il sito andò offline. I fondi avevano attraversato diversi Paesi verso le cripto nel giro di ore da ogni trasferimento. Sta ancora estinguendo il prestito.

«Un rendimento dell’1% al giorno è impossibile ed è sempre una bugia. Una piattaforma che mostra profitti che non puoi prelevare non è una piattaforma di trading — è un sito con dei numeri sopra.»

La regola del pig butchering · Capitolo 12.4

Parte III · Truffatore o autentico?

Fidati del processo, non dell’*impressione*

Le vecchie difese consistevano nel notare gli errori. Le nuove difese consistono nel verificare. Una persona o un’azienda che si oppone a essere controllata ti sta dicendo qualcosa.

Le venti bandierine rosse d’oro

Uno sconosciuto ti contatta per primo Ti ha scelto come bersaglio

2

C’è urgenza o una scadenza Non vuole che tu pensi

3

Ti chiede segretezza Non vuole che qualcuno ti avverta

4

Il guadagno è troppo bello per essere vero Non è vero

5

Bisogna pagare denaro prima di riceverne La commissione è la truffa

6

Un profitto o rendimento «garantito»È una bugia per definizione

7

Pagamento con carta regalo, cripto o bonifico Vogliono denaro che non si può invertire

8

Ti chiede un codice inviato al tuo telefono Vuole entrare nel tuo conto

9

Ti chiede il PIN o la password Nessuna istituzione reale lo fa mai

10

Ti chiede di spostare denaro su un «conto sicuro»Un conto del genere non esiste

11

La relazione va troppo in frettaÈ fabbricata

12

Rifiuta una videochiamata, o ha sempre una scusa Non è chi dice di essere

13

Le fotografie compaiono su altri profili Sono rubate

14

L’indirizzo email è quasi, ma non esattamente, giustoÈ un dominio falso

15

Il sito è nuovo, senza storiaÈ stato costruito per prendere denaro

16

Nessun indirizzo, telefono o numero di partita IVA reale Non esiste alcuna azienda reale

17

Non si trova in nessun registro ufficiale Non è regolamentato

18

Ti chiede di installare un software di accesso remoto Vuole il tuo dispositivo

19

Ti chiede denaro per ricevere un lavoro, un prestito o un premioÈ il trucco della frode con anticipo

20

Ti chiede di ricevere e inoltrare denaro Vuole un prestanome

Fonte: Capitolo 47.1 — Le venti bandierine rosse d’oro

Se hai due minuti, controlla questo

Cosa controlli	Dove	Tempo necessario
Una foto	Ricerca inversa delle immagini	1 minuto
Un sito web	WHOIS, recensioni, test di contatto	5 minuti
Un’azienda	Registro imprese, partita IVA	5 minuti

Cosa controlli	Dove	Tempo necessario
Una società di investimento	Lista delle autorizzate dall’autorità di vigilanza	2 minuti
Un IBAN	Validazione, controllo del nome, ricerca	2 minuti
Un numero di telefono	Ricerca, con «truffa»	1 minuto
Un indirizzo email	Intestazioni, controllo del dominio	2 minuti

Fonte: Capitolo 96.4 — La tabella di verifica. Dieci minuti di controlli costano meno di una vita di rimpianti.

Il test più chiaro di tutti

Togli l’urgenza — e guarda cosa succede

Di’ «fammi pensarci» o «ti richiamo domani». Un’offerta autentica sopravvive a una pausa. Una truffa no, perché tutto il suo disegno dipende dal fatto che tu agisca prima di pensare. La reazione ti dice tutto.

La reazione	Cosa significa
«Ma certo, prenditi il tuo tempo»	Autentico
«Come puoi non fidarti di me?»	Manipolazione
«C’è una nuova scadenza oggi»	Urgenza
«Mi stai facendo perdere tempo»	Pressione
Silenzio, poi una nuova storia	Cambio di copione
Ti blocca	Eri un bersaglio

Fonte: Capitolo 54.3 — Cosa ti dice la reazione.

Parti V, VI, VII · Recupero

Se sei già stato *truffato*

La velocità conta più di ogni altra cosa. Nelle prime ore il denaro si può ancora fermare; dopo qualche giorno, di solito no. Fai queste cose in ordine — e fai per prima la cosa che *non* devi fare: non lasciare mai che la vergogna ti tenga in silenzio.

Le prime 24 ore — agisci in questo ordine

Ora 01

Chiama la tua banca

Chiedi di fermare o richiamare il pagamento. Chiedi il richiamo per iscritto e annota il riferimento. Non aspettare il mattino.

Ora 01

Blocca e congela

Annulla le carte, congela i conti, cambia le password e attiva la 2FA — a partire dalla tua email, la chiave maestra di tutto.

Primo giorno

Raccogli le prove

Screenshot, messaggi, l’IBAN del truffatore, email con le intestazioni complete. Non cancellare nulla e non fare «pulizia».

Primo giorno

Denuncia alla polizia

Presenta una denuncia o una querela (Capitolo 73). La denuncia è ciò che apre le porte che un singolo non può aprire da solo.

Ferma il denaro — cosa è e cosa non è possibile

La tua situazione	Il passo giusto, in ordine
Denaro prelevato senza la tua autorizzazione	Segnala subito alla banca, chiedi il rimborso, poi la polizia
Sei stato ingannato e hai autorizzato un bonifico	Segnala rapidamente a banca e polizia; vie di richiamo e chargeback
Hai pagato un venditore online e non hai ricevuto nulla	Diritti del Codice del Consumo, la piattaforma, AGCM, un’associazione dei consumatori
Un venditore in un altro Paese dell’UE	ECC-Net Italia
I tuoi dati personali sono stati usati in modo improprio	Garante per la protezione dei dati personali
Vuoi un risarcimento dal truffatore	Azione civile, o parte civile nel procedimento penale

Fonte: Capitolo 90 — Assicurazione e risarcimento, tabella per situazione.

La truffa del recupero — l’attacco che arriva per secondo

Chiunque ti offra di recuperare il tuo denaro dietro una commissione anticipata è di nuovo un ladro. Le vittime sono i bersagli più facili, perché sono le più disperate. I segnali d’allarme sono inconfondibili.

Segnale 01

Ti contatta per primo

Il vero lavoro di recupero non inizia con una chiamata in uscita. Se qualcuno ti ha trovato, chiedi come — e perché proprio ora.

Segnale 02

Promette il recupero

Nessuno può promettere il recupero di fondi rubati. Non un avvocato, non uno studio, non uno «specialista informatico».

Segnale 03

Vuole una commissione in anticipo

I veri professionisti si fanno pagare il tempo, o prendono una percentuale di ciò che viene recuperato — mai un pagamento anticipato.

Segnale 04

Chiede cripto o carte regalo

Nessun servizio legittimo richiede un pagamento in questo modo. Mai.

Segnale 05

Recensioni perfette e anonime

Le recensioni vere citano difficoltà, ritardi e fallimenti. Un muro di post a cinque stelle senza macchia è scritto dal suo proprietario.

Segnale 06

Vuole documenti e urgenza

Chiede i tuoi dati bancari, un documento e le chiavi — e una decisione prima che tu possa controllare. Entrambe sono il marchio della frode.

Non sei stupido

La verità

Sei stato attaccato da un professionista

Ogni truffa del manuale di origine è messa in atto da persone che lo fanno di mestiere, che l'hanno fatto centinaia di volte e che studiano i sentimenti umani come un ingegnere studia una macchina. Se qualcuno si è allenato tutto il giorno per ingannarti, e tu ti sei fidato per qualche giorno, la colpa è sua — non tua.

Cosa dice una vittima	Cosa significa di solito
«Mi hanno hackerato»	Spesso una password riutilizzata, o un codice ceduto
«Ha rubato la mia identità»	Sono stati usati documenti o dati personali
«La banca ha detto che non si può fare nulla»	Chiedi di nuovo, per iscritto, e fai escalation
«La polizia non ha risposto»	Le denunce non sono aggiornamenti sul caso; chiedi per iscritto
«È stata colpa mia»	Non lo è stata
«Mi sento stupido»	Sei stato ingannato da un professionista

Fonte: Capitoli 74.2 e 98.2 — Il recupero emotivo, e le parole che usano le vittime.

Le dieci regole da ricordare per sempre

Regola 01

Rallenta

Ogni truffa dipende dalla velocità. Il tempo è la tua difesa più forte.

Regola 02

Non pagare mai denaro per ricevere denaro

Qualsiasi commissione da pagare in anticipo — per un premio, un'eredità, un prestito o un lavoro — è una truffa.

Regola 03

Non dare mai un codice, un PIN o una password

Nessuna banca, agente di polizia o tecnico ne ha bisogno. Il codice sul tuo telefono è solo per te.

Regola 04

Non esiste un «conto sicuro»

Chi ti chiede di spostare il tuo denaro per proteggerlo lo sta rubando.

Regola 05

Verifica tramite un canale che hai scelto tu

Riaggancia e richiama su un numero che hai trovato da solo. Non fidarti mai del numero o del link nel messaggio.

Regola 06

Fidati del processo, non dell'impressione

Giudica con i controlli, non con i sentimenti. Una persona che si oppone a essere controllata ti sta dicendo qualcosa.

Regola 07

Se è troppo bello per essere vero, non lo è

Un profitto garantito, un premio con una commissione, uno sconosciuto che ti ama in una settimana: niente di tutto ciò è reale.

Regola 08

Conserva le prove e agisci in fretta

Nelle prime ore, chiama la tua banca. Non cancellare nulla. Denuncia alla polizia.

Regola 09

Non vergognarti e non tacere

Parlane con qualcuno. La vergogna protegge il truffatore; l'apertura lo sconfigge.

Regola 10

Attento alla seconda truffa

Chiunque ti offra di recuperare il tuo denaro dietro una commissione anticipata è un ladro, di nuovo.

Fonte: Capitolo 100 — Parole finali: dieci regole da ricordare per sempre

Parte VIII · Sezione speciale per i lettori italiani

Chi chiamare in *Italia* — e cosa fa ciascuno

L’ente giusto dipende dal problema. Rivolgersi all’ufficio sbagliato costa giorni che potresti non avere. Questa è la mappa della fonte delle autorità italiane ed europee, nell’ordine in cui usarle.

Matrice · il tuo problema → l’ente giusto

Il tuo problema	L’ente giusto, in ordine
Frode online, phishing, furto d’identità	Polizia Postale, poi denuncia in qualsiasi commissariato
Un pagamento o un bonifico da fermare	Prima la tua banca, poi l’ABF se la banca rifiuta
Un’offerta di investimento	Consob, per controllare la società, poi la polizia se fraudolenta
Un negozio scorretto o un annuncio ingannevole	AGCM, e un’associazione dei consumatori
Una controversia con un venditore estero nell’UE	ECC-Net Italia
Uso improprio dei tuoi dati personali	Garante per la protezione dei dati personali
Un problema assicurativo	IVASS, e l’arbitro assicurativo
Una banca che rifiuta di aiutare	ABF, e il canale reclami della Banca d’Italia

Fonte: Capitolo 71.1–71.6

La directory

Polizia e giustizia

Polizia Postale — servizio specialistico per i crimini online, con il portale Commissariato di P.S. Online. **Carabinieri** e **Polizia di Stato** — denuncia in qualsiasi stazione. **Guardia di Finanza** — criminalità finanziaria. **Procura della Repubblica** — querela.

Autorità finanziarie

Banca d’Italia — vigilanza bancaria, canale reclami. **Consob** — autorità di mercato, lista delle società autorizzate. **ABF** — arbitro bancario gratuito. **OAM** — agenti e mediatori creditizi. **IVASS** — assicurazioni.

Consumo, dati e concorrenza

AGCM — pratiche scorrette, pubblicità ingannevole. **Garante privacy** — protezione dei dati. **Associazioni dei consumatori** — consulenza gratuita, azione collettiva. **ECC-Net Italia** — controversie transfrontaliere nell’UE.

Europee e internazionali

Europol — cooperazione di polizia transfrontaliera. **Eurojust** — cooperazione giudiziaria. **ECC-Net** — centri europei dei consumatori. **EBA** — regole bancarie europee. **Interpol** — polizia internazionale.

Note culturali — perché il lettore italiano è preso di mira, e i punti di forza da usare

Fiducia

Le istituzioni, e come si usa la fiducia

Una fiducia profonda e guadagnata nelle istituzioni è un punto di forza — e una leva. I truffatori prendono in prestito i loghi, i moduli e il tono dello Stato, perché quei segnali viaggiano più in fretta.

Famiglia

La forza e la trappola

La vicinanza delle famiglie italiane è una difesa potente — e l'emozione esatta che prende di mira la truffa dei nonni. Rivolgila verso l'esterno: concordate una parola d'ordine di famiglia e rendete normale il controllo.

Vergogna

Come dissolverla

La vergogna è la più grande alleata del truffatore, perché tiene le vittime in silenzio e irraggiungibili. Nominarla — «è successo a migliaia di persone, non è colpa tua» — è ciò che spezza il suo potere.

Fonte: Capitolo 94 — Note culturali per i lettori italiani

Indice completo

Tutte e nove le parti, tutti e cento i *capitoli*

La struttura completa del manuale di origine — una mappa navigabile di tutto, da che cos'è una truffa alle dieci regole da ricordare per sempre.

Parte I · Capire le truffe

1. Che cos'è una truffa? La verità nuda e cruda
2. Breve storia della frode, dalle lettere a Internet
3. La psicologia della frode: perché le persone intelligenti ci cascano
4. Il copione del truffatore: i sette passi di ogni truffa
5. Chi sono i truffatori? La verità sulla Nigeria e sul mondo
6. L'economia della truffa: come si muove il denaro
7. La storia delle lettere 419
8. Il linguaggio dei truffatori: parole che dovrebbero farti fermare

1. Frode con anticipo (la truffa “419”)
2. Truffe sentimentali e falso amore
3. Truffe sulle app di incontri
4. “Pig butchering”: la truffa più pericolosa oggi
5. Finte offerte di lavoro e truffe del lavoro da casa
6. Investimenti falsi e truffe sulle cripto
7. Forex, bot di trading e “profitto garantito”
8. Schemi Ponzi e piramidali
9. Lotteria, premio e concorso falsi
10. Eredità e truffe del “cliente defunto”
11. Finte beneficenze e soccorsi per disastri
12. Phishing: email che rubano la tua vita
13. Smishing e vishing: phishing via SMS e telefono
14. Finte chiamate bancarie e “il tuo conto è bloccato”
15. Truffe di assistenza tecnica
16. Negozi online falsi
17. Frodi sui marketplace: Vinted, Subito, Facebook Marketplace
18. Truffe su affitti e immobili
19. Truffe su prestiti e credito
20. Impersonare polizia, fisco e governo
21. Truffe su WhatsApp
22. Truffe su Telegram
23. Truffe su Facebook e Instagram
24. Truffe su TikTok, YouTube e influencer
25. Finte consegne e truffe dei corrieri
26. Compromissione email aziendale (BEC)
27. Frode sulle fatture e frode del CEO
28. Sextortion e ricatto
29. La truffa dei nonni e l’emergenza familiare
30. SIM swapping e furto del numero di telefono
31. Prestanome: quando diventi tu il criminale
32. Truffe su biglietti, eventi e viaggi
33. Truffe su animali e cuccioli
34. Truffe su visti, immigrazione e documenti
35. Truffe del recupero: il secondo attacco
36. Truffe con codice QR, app di pagamento e POS
37. IA, deepfake e clonaggio vocale
38. Altre truffe che dovresti conoscere

Parte III · Truffatore o autentico?

1. Le venti bandierine rosse d’oro
2. Come verificare una persona
3. Come controllare una foto: ricerca inversa delle immagini
4. Come controllare un sito web
5. Come controllare un’azienda
6. Come controllare un conto bancario (IBAN)
7. Come controllare un numero di telefono e un’email
8. Come mettere alla prova un contatto sospetto

Parte IV · Proteggersi

1. Password: il primo muro
2. Autenticazione a due fattori
3. Home banking sicuro
4. Acquisti online sicuri
5. Privacy sui social media
6. Cosa non dovresti mai condividere
7. Proteggere il telefono e il computer
8. Parlare con la famiglia e i parenti anziani
9. Il piano di sicurezza familiare

Parte V · Se sei già stato truffato

1. Le prime 24 ore
2. Fermare il denaro
3. Come parlare con la tua banca
4. Procedure di chargeback e richiamo
5. Congelare i conti e proteggere la tua identità
6. Raccogliere e conservare le prove
7. Denunciare alla polizia
8. Autorità italiane: chi fa cosa
9. Organismi europei e aiuto transfrontaliero
10. Come presentare una denuncia o querela in Italia
11. Recupero emotivo: non sei stupido

Parte VI · Rintracciare i truffatori

1. Prove digitali: le regole
2. Rintracciare un numero di telefono
3. Rintracciare un indirizzo email
4. Indirizzi IP: cosa possono e non possono dirti
5. Rintracciare un conto bancario (IBAN)
6. Rintracciare wallet di criptovalute
7. WHOIS e indagine sui domini
8. Database di segnalazione e verificatori di truffe
9. Come funziona la cooperazione di polizia internazionale
10. Aspettative realistiche: cosa può e non può fare la polizia

Parte VII · Recuperare il tuo denaro

1. Richiami bancari: come funzionano
2. Chargeback e regole dei circuiti di carte
3. Tracciamento e servizi di recupero delle cripto
4. Come evitare le truffe del recupero
5. Azione legale e cause civili
6. Assicurazione e risarcimento

Parte VIII · Sezione speciale per i lettori italiani

1. Legge italiana e i tuoi diritti di consumatore
2. Modelli di segnalazione in italiano
3. Contatti italiani ed europei: la lista completa
4. Note culturali per i lettori italiani

Parte IX · Strumenti e riferimento

1. Checklist principali
2. Tabelle di riferimento rapido
3. Modelli di lettere ed email
4. Glossario dei termini
5. Domande frequenti
6. Parole finali: dieci regole da ricordare per sempre

Fonte: indice del manuale · 9 parti · 100 capitoli · 36 tabelle · ~70.000 parole


Benito Russo, analista di sicurezza informatica
L’autore

Chi è *Benito Russo*

Analista di sicurezza informatica con oltre quindici anni di esperienza, Benito Russo affianca banche e intermediari finanziari nella prevenzione delle frodi. Sul campo ha indagato centinaia di casi reali — phishing e finti siti bancari, frodi sui bonifici, richieste di carte regalo e carte Steam, truffe sulle criptovalute — e ha aiutato molte vittime a denunciare, avviare un chargeback e gestire la mediazione con la banca.

Ha scritto *Non farti ingannare* perché, in italiano, mancava una guida pratica che dicesse cosa fare davvero, nell’ordine giusto, quando i soldi sono già partiti.

Analista di sicurezza informaticaInvestigatore antifrodeConsulente per il recupero fondiDifensore dei consumatoriDivulgatore e formatore
Leggi il manuale completo

Fin qui l’anteprima · Ora la parte che protegge i tuoi soldi

Questa era l’*anteprima*. Il manuale completo è ciò che usi quando serve davvero.

Il rapporto che hai letto ti insegna **a riconoscere** una truffa. Il manuale *Non farti ingannare* ti insegna anche **a reagire**: cosa fare nelle prime ore, come si rintraccia un pagamento, come si presenta una denuncia e cosa si può realisticamente recuperare. Cento capitoli, nove parti, strumenti compilabili.

Cosa non c'è qui

Carte regalo e Steam card, il copione della richiesta e la procedura di emergenza se hai già pagato.

Cosa non c'è qui

Il capitolo tecnico completo: intestazioni, IP, WHOIS, IBAN, wallet di criptovalute e costruzione del fascicolo di prove.

Cosa non c'è qui

Recupero realistico: richiamo bancario, chargeback, azione legale e assicurazione, con aspettative oneste.

E inoltre

Checklist, modelli di lettere, moduli di denuncia e querela, contatti delle autorità italiane ed europee — gli strumenti pratici che trasformano la consapevolezza in azione.

Offerta di lancio
€6
invece di ~~€7,99~~
Compra la guida completa — €6

Copertura: ebook e cartaceo · Soddisfatti o rimborsati entro 30 giorni · Pagamento sicuro

Non farti *ingannare*
Scritto da **Benito Russo** · Pubblicato da **Golden Vista Global** · Edizione Visuale MMXXVI

Informazioni su questo rapporto

Una guida visiva sul campo distillata dal manuale di 100 capitoli *Non farti ingannare — Guida completa alle truffe e alle frodi online*, scritto per i lettori italiani. Struttura, statistiche, tabelle e casi di studio sono tratti dalla fonte; il layout, i grafici e la navigazione sono il contributo di questa edizione.

Contenuti

- L'anatomia di una truffa
- Il catalogo delle truffe
- I numeri
- Truffatore o autentico?
- Se sei stato truffato
- Indice completo

Regole d'oro

- Rallenta — il tempo è la tua difesa
- Non pagare mai denaro per ricevere denaro
- Non dare mai un codice, un PIN o una password
- Non esiste un «conto sicuro»
- Verifica tramite un canale che hai scelto tu
- Non vergognarti e non tacere

%(ctag)s

%(cth2)s

%(ctp)s

info@goldenvistaglobal.com

%(CTFINE)S