# NON ABBOCCARE.

*Guida alla sopravvivenza nell'era delle truffe digitali*

**Andrea Citton**

NON ABBOCCARE
*Guida alla sopravvivenza nell'era delle truffe digitali*

*Un progetto editoriale indipendente di Andrea Citton.*

*Testi: Andrea Citton*
*Prefazione: Luca Poma e Germano Milite*
*Progetto grafico e impaginazione: Lisa Trettene*
*Consulenza: Kind9*

*© Andrea Citton, 2026*

*Tutti i diritti riservati.*

*Prima edizione: giugno 2026*

*Stampato in Italia.*

*La differenza tra chi viene truffato e chi no,*
*alla lunga, non è l'intelligenza.*

*È l'abitudine al dubbio.*

# PRENDERSI CURA

*Introduzione a cura di Germano Milite[1] e Luca Poma[2]*

L'ultima in ordine di tempo – ma la lista è purtroppo lunghissima – è l'influencer e star della piattaforma per adulti OnlyFans che è finita sotto i riflettori dopo un servizio de Le Iene che ha messo in discussione alcune delle sue più recenti narrazioni pubbliche, come la presunta adozione a distanza di un bambino in Senegal, con capi di abbigliamento firmati e costosi recapitati dalla donna in uno sperduto villaggio africano a (presunto) beneficio di un bimbo africano. La stessa influencer che aveva dichiarato in passato che i meridionali "hanno un odore diverso", manipola e sfrutta la povertà per fare hype e guadagnare più soldi.

È il principio del "bene o male, purché se ne parli", che può produrre un ritorno immediato, ma difficilmente costruisce valore nel tempo, funzionava, forse, nel secolo scorso, e ancora. Ed è la flex-culture, la cultura del "mettere in mostra" (flexare, appunto, nel linguaggio giovanile dei Social) al fine di dimostrare di essere perché si ha qualcosa: il valore materiale degli oggetti che si possiedono come misura di tutte le cose.

Il problema non è essere atipici, provocatori o controversi: il problema è pensare di ottenere denaro speculando sulla povertà e

[1] Giornalista professionista e imprenditore digitale, è ideatore di Fufflix, il più importante progetto di sensibilizzazione e informazione in Italia sul tema delle truffe on-line e dei fuffaguru e fondatore e direttore della testata giornalistica www.young.it

[2] Professore in Reputation management all'Università LUMSA di Roma, insegna in 2 corsi di laurea e in 8 master, ha pubblicato 17 volumi e più di 200 tra saggi e articoli, ed è tra i massimi esperti in Italia nel tema della costruzione della reputazione e della gestione delle crisi reputazionali. Dirige la rivista online CreatoridiFuturo.it

le difficoltà della gente. Il denaro non può essere e non deve essere l'unico pilastro per il successo, ed è sconcertante che il caso che ha devastato l'impero Ferragni non abbia insegnato nulla a un mondo, quello degli influencer, che è già sottoposto a forte scrutinio pubblico: dopo il Pandoro Gate il rapporto tra comunicazione commerciale, beneficenza, trasparenza e fiducia è diventato uno dei temi centrali nel dibattito sulla creator economy.

Certo, questo tipo di influencer e di content creator non si pongono il tema di esserci ancora tra 10 anni, e di costruire buona reputazione che duri nel tempo: un follower vale altro, e chi li abbandona oggi verrà sostituito da chi arriverà domani, in un flusso senza fine di persone con scarsi strumenti intellettuali e critici – oppure in stato di bisogno, illusi dalle sirene del guadagno facile e senza sforzo – che abboccheranno alle iper-semplificazioni del truffatore.

E tra tutti i content creator farlocchi forse i più pericolosi sono proprio quelli finanziari. Il Trading, ovvero l'analisi dei mercati al fine di ottenere profitti e di speculare sui movimenti dei mercati, che comprende l'acquisto, la vendita di titoli e obbligazioni, è un'attività che richiede delle competenze e una centratura mentale particolarmente solida, oltre che impegnare molte ore tutti i giorni. Il trading fatto in maniera seria richiede non solo un budget di partenza significativo, da usare a leva, ma richiede anche molte ore per analizzare nel dettaglio i mercati. Nel tempo però si è trasformato in una proposta di guadagno facile. Questo tipo di Fuffaguru – i cosiddetti finfluencer - è particolarmente pericoloso perché si rivolge ad un target debole, spesso padri di famiglia che non hanno grandi possibilità economiche e sperano di arrotondare con queste attività di trading, per aiutare la propria famiglia, il che rende questo genere di proposte particolarmente malsane. Ad esempio tramite finte attività di trading, con il Forex, all'unico scopo di spingere le persone, attraverso canali Telegram, le cosiddette "sale segnali" (sic!), a investire su broker ai quali l'influencer è affiliato

con un accordo, e dai quali prende un contributo per ogni iscritto che porta in piattaforma e che deposita del denaro (in molti casi questi personaggi, infatti, guadagnano dalle perdite di chi hanno portato al broker affiliato).

Ovviamente – come meglio di noi spiega Citton in questo libro - la maggior parte dei ”broker” di questo genere non seguono le norme italiane ed europee secondo le quali per fare questo lavoro è necessario avere tutta una serie di autorizzazioni, quindi non sono in realtà neanche facoltizzati ad operare nel territorio dell'Unione Europea. In molti casi, appaiono proprio dei disclaimer che avvertono chi vuole usare questi servizi che quel tipo di attività è illegale nel territorio dell'UE, ma molti, forse per avidità, ingenuità o superficialità, ignorano queste red flag, che di fatto rendono teoricamente consapevole chi ne sta per usufruire che effettivamente non c'è garanzia sui depositi e sulle operazioni fatte. Si tratta se non di truffa quanto meno di pubblicità ingannevole, che promette di guadagnare cifre altissime con minimo investimento. In realtà, c'è anche il potenziale reato di esercizio abusivo della professione finanziaria, perché di fatto si propone consulenza senza essere iscritti all'albo o abilitati a fare investimenti su criptovalute o su prodotti finanziari, che – tra l'altro – in molti casi neppure esistono.

La verità è che le carenze in materia di alfabetizzazione finanziaria limitano drammaticamente la capacità dei cittadini di valutare correttamente rischi e opportunità dei prodotti finanziari. Un avvertimento ai risparmiatori italiani va allora dato, e questo libro vuole appunto darlo: va richiamata l'attenzione dei cittadini sui pericoli legati a scelte d'investimento prese in modo affrettato, superficiale ed emotivo, facendosi trascinare dall'effetto gregge, o presumendo erroneamente che un finfluencer possa offrire un servizio equiparabile a quello di un professionista autorizzato. La Consob ha ricordato infatti in più occasioni che un finfluencer non è un consulente finanziario abilitato e che può avere conflitti d'interesse:

i risparmiatori devono in particolare prestare attenzione a quelle offerte che vengono incautamente presentate come molto redditizie e prive di rischio, ha evidenziato recentemente l'autorità a riguardo, ricordando che una delle regole basilari in materia di scelte d'investimento è la correlazione fra rischio e rendimento: alla promessa di rendimenti alti, corrispondono di regola rischi molto elevati.

Va data quindi priorità al rafforzamento dell'alfabetizzazione finanziaria in ambito digital: questo è un obiettivo cruciale, poiché è connesso alla capacità dei cittadini di comprendere e utilizzare in modo consapevole i nuovi strumenti della finanza digitale. Sul fronte tech, vi sono in particolare tre finalità prioritarie da perseguire, recentemente sottolineati da alcuni interventi divulgativi sempre della Consob: è necessario promuovere l'uso responsabile e consapevole degli strumenti finanziari digitali; poi, rafforzare la capacità di giudizio degli utenti nella valutazione di informazioni e servizi disponibili online, potenziando l'abilità di distinguere contenuti affidabili da fonti fuorvianti, manipolatorie o potenzialmente fraudolente; infine, è indispensabile educare alla sicurezza digitale, formando i cittadini al riconoscimento tempestivo di pratiche abusive, frodi e truffe online, alla protezione dei dati personali e alla gestione responsabile delle proprie risorse economiche in ambiente digitale.

Citton, come ha già fatto in passato con altri volumi che ha realizzato, stampato e distribuito di propria iniziativa e, è necessario sottolinearlo, a proprie spese, vuole "prendersi cura" di tutto ciò, nel suo piccolo, non girando lo sguardo dall'altra parte: questo agile manuale, viene quindi incontro a questa pluralità di obiettivi, in modo attuale e innovativo. E di tutto questo gli va reso convintamente merito.

**Luca Poma e Germano Milite**

# PREFAZIONE

*A cura dell'autore*

Non abboccare

**Chiamiamoli con il loro nome.**

Non "truffatori". Non "malintenzionati". Non "soggetti che operano in modo non trasparente".

Ladri. Delinquenti. Predatori che ogni giorno scelgono deliberatamente le loro vittime tra le persone più vulnerabili: anziani soli, famiglie in difficoltà, persone che si fidano ancora della parola altrui.

Lo fanno con una telefonata. Con un messaggio. Con un link. Con una voce patinata che finge cortesia mentre fruga nel conto corrente di qualcuno che non ha fatto nulla di sbagliato, se non rispondere al telefono.

***Questo libro nasce dalla rabbia.***

Dalla rabbia di chi ha ascoltato troppi racconti — reali, documentati, devastanti — di persone che hanno perso i risparmi di una vita in pochi minuti. Di anziani convinti di parlare con la banca, con i carabinieri, con il nipote in pericolo. Di genitori abbindolati da false emergenze costruite ad arte da chi conosce bene la grammatica dell'urgenza e della paura.

Questi criminali non sono geni. Non sono hacker cinematografici davanti a schermi pieni di codice. Sono impostori mediocri armati di un copione rodato, di numeri rubati e di una cosa sola che funziona sempre: la nostra umanità.

E proprio lì colpiscono. Nella fiducia. Nell'affetto. Nel riflesso condizionato di chi vuole aiutare, di chi non vuole sembrare scortese, di chi ancora crede che dall'altra parte del telefono ci sia sempre una persona in buona fede.

**Smettila di sentirti in colpa se ti hanno ingannato. La colpa è solo loro.**

Ma da oggi hai anche uno strumento in più.

Queste pagine non sono un manuale tecnico. Sono uno specchio — per riconoscere le truffe prima che si avvicinino, per sapere cosa rispondere, cosa non fare, come proteggere te stesso e chi ami. Sono il distillato di anni di casi reali, di meccanismi smontati pezzo per pezzo, di trappole descritte con la precisione chirurgica di chi le ha studiate a fondo.

Se sei già stato truffato: non sei stupido. Sei stato aggredito da qualcuno che lo fa di mestiere.

Se non sei ancora stato truffato: non sentirti al sicuro. Nessuno lo è, finché non sa come funziona il meccanismo.

***Questo libro è la risposta che meritavi.***

**Andrea Citton**
*Lido di Venezia, 2026*

# INTRODUZIONE

*Prima di tutto, viene l'inizio.*

## Perché ho deciso di scrivere questo libro?

Perché sono stanco, sono stanco da professionista di questo settore da una vita ormai: vedere gente che spinta dall'avidità si fa mangiare tutti i risparmi sotto il naso, ignorando i consigli degli esperti, di chi conosce le truffe e le vede arrivare lontano chilometri.

È una frase scontata, lo so, ma a questo mondo nessuno regala niente. Se una promessa vi sembra troppo bella per essere vera, spesso è proprio così. Specialmente se viene fatta da chi vi sta chiedendo dei soldi e vendendo l'entrata passiva. Gli unici passivi in questo caso siete voi, che prendete le bastonate e neanche ve ne rendete conto. Almeno finché non è troppo tardi

***Ma non solo.***

Questo libro è anche per le persone che vedono i fantasmi dappertutto e che hanno paura persino di rispondere al telefono perché inconsapevoli di cosa li aspetta.

Siamo nel 2026, non più nel 2000. Se pensate che il mondo della finanza sia ancora quello delle strette di mano e dei consigli rassicuranti del "buon padre di famiglia", siete fuori strada.

Non sono qui per biasimare queste persone, anzi. Nel 2026, quindi oltre un quarto di secolo da quando internet è entrato nelle nostre case, i truffatori hanno affinato le tecniche e non esiste più un momento in cui "siamo al sicuro". Dobbiamo saperci difendere 24/7. Hanno imparato che se usano le parole giuste e ci mettono fretta, molto spesso ce la fanno. Oggi la minaccia non bussa alla porta, ma arriva via SMS, via social o con una telefonata che sfrutta gli affetti più cari.

***Non si fanno scrupoli davanti ad anziani o con disabilità.***

Mi è successo personalmente:

Entra nel mio ufficio una signora di 82 anni. È sconvolta, trema. Mi dice che deve fare un bonifico istantaneo di 14mila euro subito, perché un sedicente carabiniere l'ha chiamata dicendo che sua figlia rischia di perdere la casa per un mutuo non pagato. Mentre mi parla, il telefono le squilla in borsa: sono ancora loro, i "lupi", che la pressano, che non le lasciano il tempo di respirare. In quel momento, io non sono il suo consulente finanziario: sono lo scudo tra lei e il baratro. Le ho tolto il telefono di mano, l'ho portata in ufficio a prendersi un caffè, le ho dato un bicchiere d'acqua e le ho spiegato che sua figlia non rischiava nulla. Dopodiché mi sono fatto passare il telefono della signora e ho parlato direttamente con il "carabiniere". Diciamo che non sono stato carino nei suoi confronti, ma almeno per quella volta ho evitato che una signora anziana perdesse una cifra significativa.

Questo libro è rivolto a chi vorrebbe il pasto gratis; a chi ha paura di uscire di casa e non si fida più nemmeno del sistema o dei consulenti tradizionali. È anche per chi, per ingenuità o troppa fiducia, rischia di diventare carne da macello per i predatori finanziari — e tutti possiamo essere ingenuI in un certo momento. È successo anche a me, che faccio questo mestiere da 37 anni, di essere poco lucido e cliccare un link che non dovrei. Morale: ho rischiato di perdere tutto. Mi è costato 600 euro e una settimana senza computer. Succede. Per questo serve sempre la massima attenzione.

Sono fortemente convinto che serva fare educazione in questa materia. Il danno di una truffa non finisce nel portafoglio. In trentasette anni di mestiere ho visto persone oneste, gente che ha sudato ogni singolo euro, scivolare nella depressione o ammalarsi di sdegno per la vergogna di essere stati raggirati. La fiducia tradita brucia molto più del denaro perso.

A voi che leggete questo libro, che siete umani quanto lo sono io, chiedo giusto un paio di cose. Lo faccio da padre, zio, fratello e professionista stagionato:

Siate sempre scettici, come dicevo, non esistono pasti gratis. Se qualcuno vi promette delle percentuali cheassurde, ci sono altri quelle cifre le stanno pagando, o le pagherete voi senza saperlo.

La finanza è una materia complessa, che richiede studio ed esperienza. Se un consulente che vi sta proponendo l'affare della vita, fino a sei mesi fa faceva tutt'altro... magari anche no, abbiate il coraggio di dire di no.

Infine, la mia regola d'oro: prima di pensare ad arricchirvi, mettete in sicurezza la salute, la casa e la famiglia. Il guadagno facile, semmai, viene dopo. Il rendimento senza protezione è un bagno di sangue.

Il dubbio e lo scetticismo sono armi formidabili se usate con la testa, controllare tutto, leggere i documenti, chiedere una seconda opinione. Sarà una scocciatura, ma è molto meglio prevenire che curare

Questo libro, quindi, non nasce per farvi i complimenti o annoiarvi con grafici incomprensibili, ma per darvi quello "scappellotto" mentale necessario a svegliarvi prima che sia troppo tardi. Perché oggi, essere ingenui non è più una svista: è un lusso che non potete più permettervi.

A chi è rivolto, quindi, questo libro? A chiunque sia stanco di sentirsi una preda. Non mi serve che abbiate una laurea in economia; quello che vi chiedo è di tirare il freno a mano e accendere il cervello prima di cliccare su un link o dire "sì" a uno sconosciuto al telefono. Prima ancora delle competenze tecniche, questo libro esige un cambiamento di atteggiamento: la prudenza deve venire prima del rendimento.

# RINGRAZIAMENTI

Questo libro non esisterebbe senza il contributo di tre persone che hanno rappresentato le colonne portanti della mia ricerca: il Prof. Luca Poma, il Dr. Germano Milite e il Dr. Luca Yuri Toselli. La loro competenza, la loro disponibilità e il rigore con cui hanno accompagnato questo lavoro sono stati per me un riferimento costante e prezioso.

Un ringraziamento particolare va al Dr. Gianmarco Crinieri, per la cura e la precisione con cui ha condotto la ricerca bibliografica, e alla D.ssa Lara Badiali e al Dr. Giuseppe Aliprandi per il supporto morale e tecnico che hanno saputo offrire nei momenti giusti.

Un pensiero grato va alla D.ssa Valeria Guerriero, per il lavoro quotidiano prezioso e insostituibile, e ai miei colleghi di Venezia, il cui appoggio costante ha reso questo percorso meno solitario.

Ma il pensiero più profondo va alla mia famiglia: a Paola, a Riccardo, a Enrico, a Marianna e a Carlotta. Senza la loro presenza, la loro pazienza e il loro affetto silenzioso, queste pagine non avrebbero avuto né il calore né il senso che spero abbiano.

# TASSONOMIA E INTRODUZIONE

Prima di addentrarci nel pratico, è utile stendere un glossario, evitando di dare le cose per scontate.

Quelli che leggerai ti sembreranno termini assurdi, quasi inventati, ma fidati: tutto esiste ed è documentato.

- Partiamo dalla cosa più comune: l'**email phishing** (o, più genericamente, **phishing**). Si tratta di email inviate in massa che imitano comunicazioni ufficiali (banche, corrieri o, servizi digitali) e contengono link a pagine false o allegati pericolosi. Lo scopo è quello di farti compilare volontariamente ma inconsapevolmente i campi necessari ad accedere al tuo account, anche bancario, per questo è così pericoloso. Nel caso degli allegati, questi possono contenere virus o simili che entrano nel tuo dispositivo e causano problemi ancora maggiori (tipo accedere ai tuoi file, la tua webcam, eccetera).

- **Smishing**: lo stesso discorso del phishing ma via SMS (unisce infatti le parole SMS e phishing). Si tratta infatti di tutti quei messaggi che imitano banche, corrieri, INPS/agenzie pubbliche e inducono a cliccare link malevoli o chiamare numeri falsi. Il meccanismo è lo stesso dell'email phishing.

- Il **Romance o dating scam** (ossia lo scam della relazione romantica) è forse la truffa più meschina: il truffatore costruisce una relazione affettiva online per ottenere denaro, investimenti o informazioni sensibili. Per attuarla ci vogliono giorni o addirittura settimane.

- Il **Pig-butchering** (*macellazione del maiale*) è per mol-

ti versi assimilabile al romance scam. È uno schema a lungo termine dove il truffatore costruisce una relazione (romantica o amicale) e poi "ingrassa" la vittima con finti consigli finanziari, convincendola a investire in piattaforme crypto false. Svuotano il conto del malcapitato dopodiché chiudono i contatti improvvisamente una volta che la bestia è stata macellata.

- **Tech-support scam o Remote access scam** (supporto tecnico/accesso da remoto): lo attua chi finge di essere assistenza tecnica di Microsoft, Apple, banca o gestore telefonico e convince la vittima a installare software di controllo remoto sul dispositivo. Il loro metodo si basa sul creare panico (per esempio ti dicono "il tuo computer è infetto!"). Lo scopo è farti scaricare TeamViewer, AnyDesk, QuickAssist o qualsiasi software di controllo da remoto del tuo computer o telefono. Questo lo fanno per poter effettuare bonifici fraudolenti o furti d'identità. In altri casi il truffatore ti fa credere, appunto, che tu abbia virus nel computer e a pagamento ti *sistema* il computer.

- Un'altra strategia molto in voga ultimamente è la creazione di profili social (specialmente su Instagram) **identici** a quelli di persone reali per truffare amici e contatti. Il truffatore copia foto, nome e bio, poi contatta le vittime chiedendo aiuto economico o proponendo falsi investimenti. È successo a me in primis di recente, creandomi non poco fastidio.

- **Overpayment scam o Marketplace scam** (letteralmente "pagato troppo"): Truffa molto comune su Facebook Marketplace, Subito, Vinted, eccetera. Il falso acquirente "paga troppo" e chiede di restituire la differenza via bonifico, gift card o servizi non tracciabili come le criptovalute. Il pagamento iniziale però è falso o non valido e quindi viene rimbalzato dalla banca. Ed è così che ti fregano.

- **Sextortion/Revenge-porn extortion** (da "sex", "extortion" e "porno di vendetta"): uno degli schemi più pericolosi, perché spesso indirizzato a minorenni o quasi, ed è uno di quelli che sta subendo una grossa spinta evolutiva grazie all'intelligenza artificiale. Lo abbiamo visto per esempio con Jolanda Renga.[1] Si tratta di minacce di pubblicare foto intime (vere, ottenute con l'inganno, o inventate, create con l'intelligenza artificiale) se non si paga un riscatto. Spesso succede ai ragazzi che frequentano le app di incontri. In questi casi dall'altra parte quasi mai c'è realmente una ragazza: spesso c'è un truffatore che induce il ragazzo a mandare foto intime e poi lo estorce. Queste situazioni possono avere conseguenze gravissime, incluso il suicidio della vittima.

Adesso che abbiamo un minimo di vocabolario possiamo delineare meglio gli attori coinvolti in questo teatrino degli orrori.

## Chi c'è dietro queste truffe? A chi mirano e perché?

L'immaginario collettivo vuole che i ladri digitali siano ragazzotti nigeriani senza prospettive. Alla ricerca di una via d'uscita facile, truffando poveri malcapitati per tirare avanti al giorno dopo.

La realtà è invece molto più complessa, sfumata e preoccupante di così.

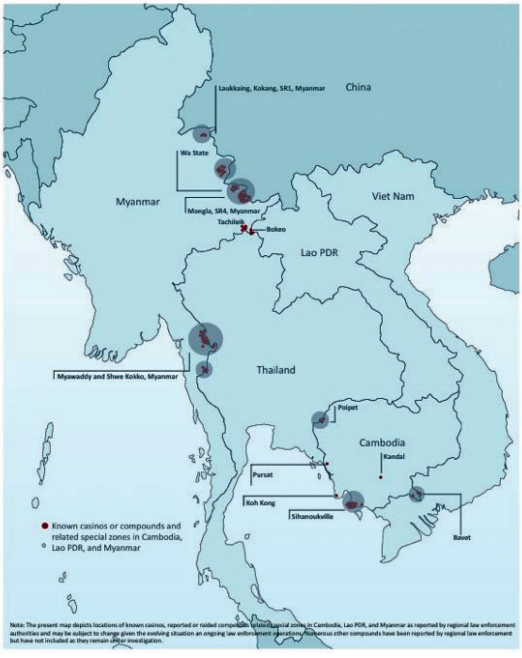
Certo ci sono dei piccoli gruppi di ragazzi, spesso provenienti dall'Africa occidentale, che, come lo stereotipo vuole, raggirano delle persone, come dicevamo prima.

## Ma questa è solo una minoranza.

Spesso si tratta di organizzazioni che superano i confini nazionali e sfruttano le leggi troppo morbide o situazioni politiche di-

[1] "Ecco perché ho denunciato chi minacciava di diffondere foto di me nuda. Dopo ho ricevuto insulti da tanti adulti": Jolanda Renga parla alla Camera - Il Fatto Quotidiano

sagiate per proliferare. In altre parti del mondo (soprattutto paesi come il Myanmar, le Filippine, la Cambogia e il Laos) ci sono dei veri e propri uffici, edifici interi dediti a questo "mercato" nel quale i lavoratori sono spesso stati portati lì con l'inganno o, peggio ancora, vittime di un sistema di traffico di esseri umani. Questo non lo sto dicendo per giustificare quelli che di fatto sono criminali, lungi da me, ma per farvi capire che in alcuni casi sì, ci sono delle grosse organizzazioni che vivono solo di questo, ma che in fondo alla catena alimentare si trovano delle persone obbligate a parlare con voi, potenzialmente con una pistola puntata alla testa, in alcuni casi non metaforicamente.[2] [3]




[2] Online Scam Operations and Trafficking into Forced Criminality In Southeast Asia

[3] Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia

Chi cercano questi truffatori? Siamo tutti a rischio o alcuni di noi lo sono più o meno di altri? Ovviamente in base al tipo di schema attuato, il target cambia, in alcuni casi dipende dalla piattaforma che si usa. Per esempio se parliamo di una truffa su Vinted o sul negozio di Facebook, nessuno è davvero al sicuro, ci stiamo esponendo "volontariamente". Tutti noi possiamo essere leggeri e fidarci senza pensare troppo, specialmente se non conosciamo i segnali problematici (o, in inglese, red flag). Anche in questo caso lo stereotipo vuole che la "vittima designata" sia la persona anziana con una bassa alfabetizzazione digitale, ma secondo le indagini dell'Unione Europea i nonni hanno solo una probabilità più alta di "cascarci", ma non sono il solo target, anzi. Secondo gli studi, maggiore è la presenza online, più alto è il rischio di essere intercettati. Ciò significa che i millennial e la generazione Z sono i più esposti ai tentativi di truffa[4] [5] – ossia la fascia di età tra i 18 e i 37 anni. Ed è anche qui che nasce l'esigenza di una guida come questa, a diffondere consapevolezza e strumenti a chi non ne ha.

**Tutti siamo potenziali vittime, ed è questo un altro motivo che mi ha spinto a creare questa guida: più strumenti abbiamo meno queste truffe riescono a proliferare.**

[4] Iocta, Internet Organised Crime Threat Assessment - Publications Office of the EU

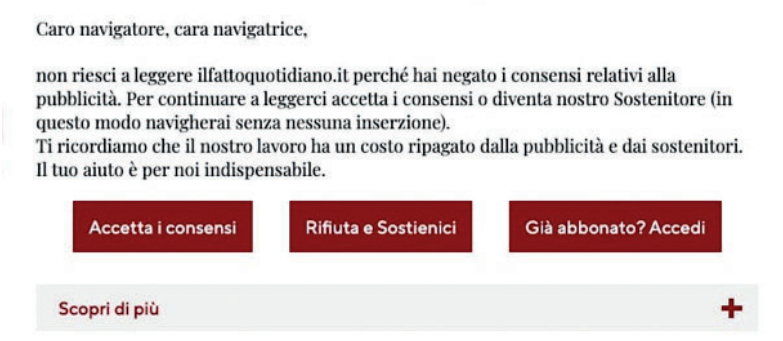
[5] ENISA Threat Landscape 2025

# COME SI ARRIVA ALLE VITTIME

Abbiamo spiegato quali sono gli schemi più usati, chi sono le potenziali vittime (tutti) e cosa è successo in passato. Ma come arrivano a noi i truffatori? Sparano alla cieca migliaia di email al giorno nella speranza che qualcuno abbocchi o ci sono strategie più raffinate, specifiche?

**Dipende. Da quanta informazione su di te è già in giro.**

Chiunque sia online lascia una traccia digitale: l'iscrizione a Facebook, l'accettazione dei cookie.




I dati che queste pagine raccolgono possono, volontariamente (tramite la vendita) o involontariamente (tramite i cosiddetti "data leak", cioè fuoriuscite di dati), finire altrove. Non è per forza un male. Dipende da come vengono usati quei dati. Nella maggioranza dei casi le informazioni che si posseggono servono a rendere le pubblicità più mirate. Pensa a quando cerchi scarpe su Google. Poi torni a leggere notizie e–boom–pubblicità di scarpe ovunque. Succede così: i dati della ricerca ti "seguono".

Purtroppo i truffatori usano gli stessi dati. Possono essere generici… o pericolosamente precisi. La specificità varia in base a quanto vogliono spendere su di te i truffatori e quante informazioni sono riusciti ad ottenere.

Se parliamo di phishing – ossia quei messaggi o email che mirano a farti aprire link o allegati o a farti contattare un numero esterno – generalmente si parla di "spray and pray" (spruzza e prega) ossia gettare nel mucchio e sperare che qualche sprovveduto o disattento ci caschi.

Quando si utilizza questo approccio non si prende di mira una persona specifica: si inviano link che rimandano a pagine false, oppure allegati malevoli che infettano il dispositivo. Spesso si fingono una banca e ti chiedono le credenziali: "account sospeso", "aggiorna password".

***Tu ci caschi, loro entrano.***

In alternativa, il phishing può essere usato per ottenere i dati di accesso ai social network. Spesso i truffatori mandano un'email identica – o quasi – a quella che manderebbe Instagram o Facebook, segnalando problemi. Devi verificare l'account. Clicchi, inserisci la password in una pagina che all'apparenza è legittima. Fine: non hai verificato nulla, hai consegnato le chiavi. Il trucco è semplice ma funziona.



**Gentile cliente,**

Ti comunichiamo che l'accesso e le funzioni del tuo conto **sono state temporaneamente disabilitate**. Questa misura è stata presa perchè hai ignorato la nostra precedente richiesta di effettuare la **verifica obbligatoria** del tuo profilo Online Banking.

Prima che riabilitiamo l'uso della tua carta abbiamo bisogno che ci confermi la tua identità compilando una serie di dati già inseriti sul nostro sito al momento della tua registrazione sul portale di UniCredit.

**Ti invitiamo a cliccare sul bottone seguente e seguire le indicazioni.**

ACCEDI AI SERVIZI ONLINE

Tieni presente che l'accesso ai servizi (tra quali, prelievi e pagamenti) e il loro utilizzo sono limitati finchè l'aggiornamento non viene effettuato correttamente.

Rimaniamo a tua disposizione per qualsiasi tipo di chiarimento e informazione!

**Gruppo UniCredit!**

Da cyberselfawarenesscom.wordpress.com

In poche parole, lo "spray-and-pray" indica un phishing senza target specifico, che sfrutta dati in circolazione da tempo e generalmente economici. Ha quindi un tasso di successo molto basso: la strategia punta sulla quantità ed è spesso la prima scelta dei truffatori online.

Spear phishing: il contrario. Mirato. Studiato. Poche email, grande effetto. Quale dei due pensi che faccia più danni?

È usata pochissimo – 0,1% dei casi – eppure ha causato oltre la metà dei danni. Capisci la leva? Pochi colpi, effetto devastante[1].

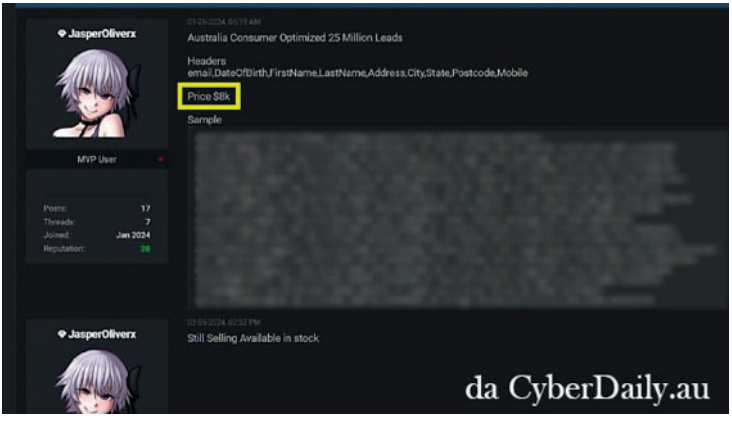
Questo approccio richiede molto più impegno, una raccolta di dati molto più sostanziosa e una scelta di parole più rigorosa, Questo aspetto è stato potenziato dall'utilizzo dell'intelligenza artificiale, che rende i messaggi più credibili.

Prima però servono profili dettagliati: una scrematura dei dati reperibili sui social (LinkedIn, Instagram, ecc.) e di altre informazioni pubbliche. È, a tutti gli effetti, una schedatura delle vittime.

[1] Barracuda_report_2023-spear-phishing-trends.pdf

Poi comprano dati sul dark web – quella parte "nascosta", anonima e spesso criminale della rete – e mettono tutto insieme. Risultato: messaggi perfetti per ingannare.

Questi dati, come dicevamo all'inizio, provengono spesso da attacchi subiti da grandi raccoglitori di informazioni (per esempio Yahoo, che nel 2013 vide esposti tre miliardi di account) e poi vengono messi in vendita – i prezzi variano a seconda del tipo di dato, da pochi euro fino a qualche migliaio – oppure, addirittura, pubblicati gratuitamente.



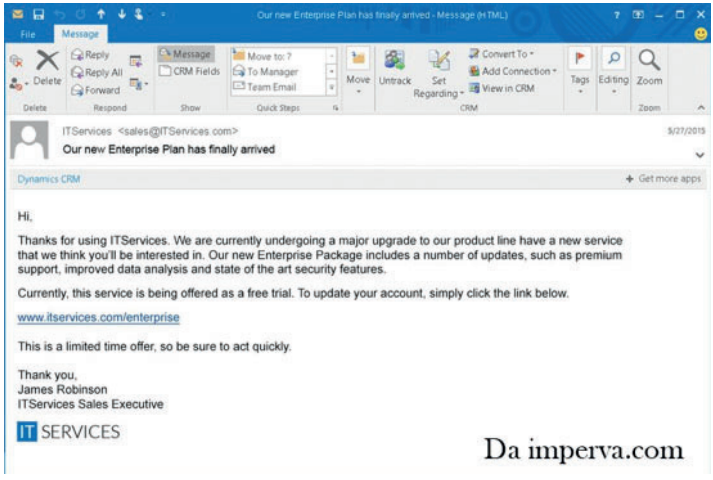

Le imprese non sono affatto esenti da questo tipo di tentativi, anzi, una porzione molto significativa degli attacchi phishing è pensata per colpire organizzazioni perché lì i guadagni sono molto più alti. Non solo, riuscire a infettare una rete aziendale dà accesso a tutto lo staff con tanto di informazioni, fornitori (quindi altre aziende da poter puntare), eccetera. Insomma: entrare senza farsi beccare è come trovare una miniera d'oro. Quante scuole potremmo costruire con 15 miliardi[2]? Pensaci. La risposta è tra le 1000 e le 1500, praticamente rifaremmo il piano scolastico di più regioni messe insieme.

[2] Phishing Statistics By Demographic, Healthcare, Industry And Country (2025)

Nel caso delle organizzazioni la tecnica più usata dai truffatori è lo spear phishing, che può servire sia a sottrarre denaro sia a ottenere l'accesso a computer o caselle email aziendali. Da qui deriva, però, una delle minacce più dannose per le imprese: il Business Email Compromise (BEC, compromissione della posta elettronica aziendale).

Il truffatore si finge una figura di fiducia (amministratore, fornitore, dipendente) e chiede alla vittima un bonifico urgente o – nel caso di un fornitore/dipendente autentico – di cambiare l'IBAN al quale indirizzare i pagamenti. È una truffa estremamente raffinata: le email non finiscono nello spam perché sono inviate da account legittimi o si inseriscono in flussi di posta preesistenti.

Questo schema richiede studio, attenzione, ma è molto profittevole, anzi, è la strategia più profittevole di tutte. Nel 2023: 20mila segnalazioni e 2,5 miliardi di perdite[3]. Numeri che parlano chiaro.




Fin qui abbiamo parlato di tecniche diverse. In realtà, la logica è sempre la stessa.

[3] 2023 INTERNET CRIME REPORT

Il phishing è una grande campana: sotto ci finiscono strategie diverse, ma con una cosa in comune: l'inganno è il mezzo per arrivare allo scopo.

Nella bibliografia abbiamo citato, per esempio, la clonazione dei profili social (il messaggio privato che ti arriva da un profilo che sembra quello di un tuo amico, ma non lo è). In questi casi la logica dell'attacco non cambia. Cambia solo il canale. Al posto dell'email o del sito falso, viene falsificata un'identità, e con lei la fiducia che avevi già concesso.



**Come difendersi, dunque? E si può davvero impedire che entrino nei nostri dispositivi?**

Per te che sei privato: poche regole semplici. Le principali sono:

- È fondamentale attivare l'autenticazione a due fattori, così che non basti conoscere la password per accedere agli account ma che ci sia una conferma da un altro dispositivo al login[4].
- Altro punto chiave, ma che nessuno fa, è avere password uniche per ogni account. Usa password diverse per ogni account. Lo so: è una rogna. Ma evita che, con una sola password, ti entrino ovunque. Usare un password manager non è un lusso – è obbligatorio. In rete ce ne sono diversi (anche gratuiti). Non fare il pigro.

Per le aziende vale lo stesso discorso sull'autenticazione a due fattori, ma gli esperti raccomandano di non approvare richieste critiche (pagamenti, modifica di coordinate bancarie, dati sensibili) basandosi solo sull'email. Bisognerebbe confermare la richiesta con un canale alternativo, non passante per l'email; per esempio:

- una telefonata su un numero già registrato e verificato (non quello presente nell'email sospetta).
- Un messaggio tramite un'altra piattaforma aziendale.
- Una conferma diretta di persona, quando possibile[5].

Questa verifica impedisce agli aggressori di sfruttare la casella email o un indirizzo falso per ottenere un'autorizzazione fraudolenta per una transazione, salvando potenzialmente milioni di euro che sparirebbero quasi magicamente.

**La pigrizia è un'arma per i truffatori. Un po' di attenzione salva soldi. Mi raccomando: non abbassare la guardia.**

---

[4] How to Safeguard Against Business Email Compromise | EMPIST

[5] What is business email compromise (BEC)? | Wiz

# STORIA DELLE TRUFFE INFORMATICHE

Ma come siamo arrivati a questo punto? Quali sono stati i passaggi che ci hanno fatto arrivare dove siamo? Com'erano le truffe informatiche prima di adesso? Alcune esistono ancora?

I reati informatici esistono da che esistono i computer, quindi ben prima di internet e del suo antenato ARPANET. In passato virus e tutti i suoi sottogeneri (malware, ransomware, eccetera) erano fisicamente all'interno dei floppy disk, che chi è della mia generazione ha maneggiato molte volte. La strategia era di sfruttare buchi di sistema noti sui quali al tempo era ovviamente meno semplice intervenire tempestivamente.

Con l'arrivo di internet nelle nostre case sono nati degli schemi che per una buona parte sono rimasti sostanzialmente invariati. Questi crimini hanno cambiato semmai l'approccio, affinato le strategie, ma il nucleo è essenzialmente rimasto invariato.

Pensiamo per esempio alla truffa informatica per eccellenza: il principe nigeriano, ossia la strategia che prevede l'arrivo di una email da parte di un completo sconosciuto, il cui mittente sostiene che voi siate l'ultimo erede di un principe nigeriano (i dettagli possono variare) sul letto di morte. Voi siete stati scelti per ereditare tutta la sua fortuna milionaria/miliardaria; per ottenerla però dovete sbloccare la transazione (per motivi di tasse notarili, ad esempio). Servono giusto qualche migliaio di euro: somme inesistenti se le mettiamo a confronto con la cifra promessa.

***E sappiamo tutti come finisce questa storia.***

Greetings to you my friend,

I know this will come to you as a surprise because you do not know me.
I am [redacted] I work in Central Bank of Nigeria, packaging and courier department.

I got your contact among others from a search on the internet and I was inspired to seek your co-operation, I want you to help me clear this consignment that is already in theEurope which I shipped through our CBN accredited courier agent. The content of the package is $20,000,000.00 all in $100 bills but the courier company does not know that the consignment contains money.

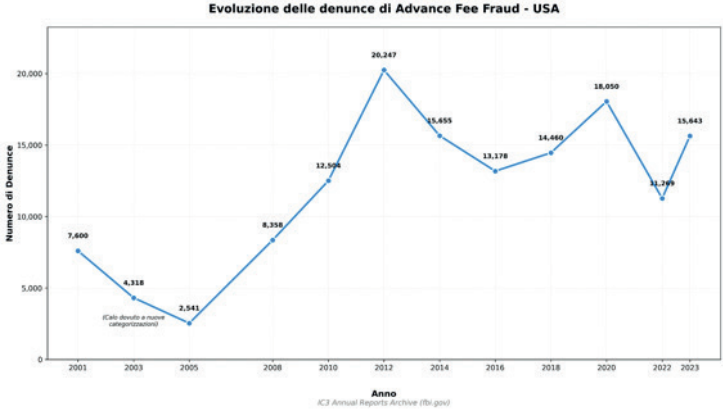
All I want you to do for me now is to give me your mailing address, your private phone and fax number and I believe that at the end of the day you will have 50% and 50% will be for me. My identity must no be revealed to anybody.

If this arrangement is okay by you, you can call [redacted]

Da historicalemails.com

Il fenomeno – chiamato "advanced fee fraud" (truffa del pagamento anticipato) – è così ampio che l'FBI include questa categoria nei suoi report annuali[1].

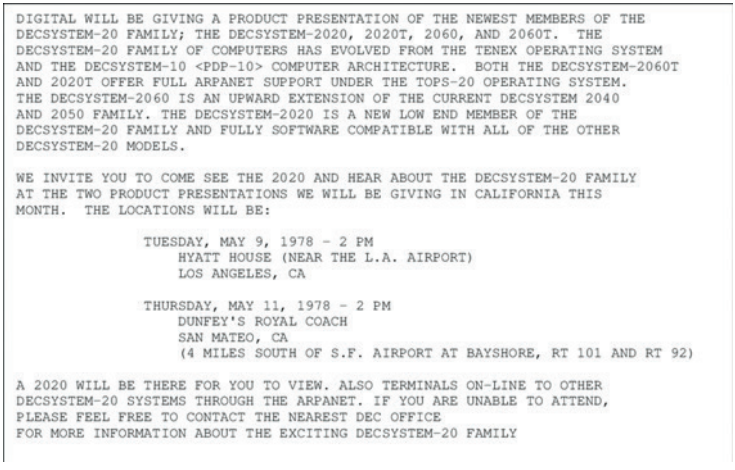
Oggi la truffa del principe nigeriano è meno diffusa, ma fondamenta, metodo e strategia restano gli stessi. L'advanced fee fraud rimane molto usata e i documenti delle agenzie di sicurezza ce lo confermano. Si fa leva sulla nostra avidità allo stesso modo in cui si faceva prima, solo un po' meglio e in scala, perché ci caschiamo sempre.




[1] FBI: INTERNET CRIME REPORT 2024

Comunque, che ci crediate o no, il primo esempio dei moderni crimini informatici, risale addirittura al 1978. All'epoca non c'era ancora internet ma il suo antenato ARPANET.

Questo primo "crimine informatico" non è altro che una email di spam[2], ossia quelle email che normalmente il nostro provider (Gmail, Outlook, eccetera) filtra più o meno autonomamente perché potenzialmente pericolosa.



DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST MEMBERS OF THE
DECSYSTEM-20 FAMILY; THE DECSYSTEM-2020, 2020T, 2060, AND 2060T. THE
DECSYSTEM-20 FAMILY OF COMPUTERS HAS EVOLVED FROM THE TENEX OPERATING SYSTEM
AND THE DECSYSTEM-10 <PDP-10> COMPUTER ARCHITECTURE. BOTH THE DECSYSTEM-2060T
AND 2020T OFFER FULL ARPANET SUPPORT UNDER THE TOPS-20 OPERATING SYSTEM.
THE DECSYSTEM-2060 IS AN UPWARD EXTENSION OF THE CURRENT DECSYSTEM 2040
AND 2050 FAMILY. THE DECSYSTEM-2020 IS A NEW LOW END MEMBER OF THE
DECSYSTEM-20 FAMILY AND FULLY SOFTWARE COMPATIBLE WITH ALL OF THE OTHER
DECSYSTEM-20 MODELS.

WE INVITE YOU TO COME SEE THE 2020 AND HEAR ABOUT THE DECSYSTEM-20 FAMILY
AT THE TWO PRODUCT PRESENTATIONS WE WILL BE GIVING IN CALIFORNIA THIS
MONTH. THE LOCATIONS WILL BE:

TUESDAY, MAY 9, 1978 - 2 PM
HYATT HOUSE (NEAR THE L.A. AIRPORT)
LOS ANGELES, CA

THURSDAY, MAY 11, 1978 - 2 PM
DUNFEY'S ROYAL COACH
SAN MATEO, CA
(4 MILES SOUTH OF S.F. AIRPORT AT BAYSHORE, RT 101 AND RT 92)

A 2020 WILL BE THERE FOR YOU TO VIEW. ALSO TERMINALS ON-LINE TO OTHER
DECSYSTEM-20 SYSTEMS THROUGH THE ARPANET. IF YOU ARE UNABLE TO ATTEND,
PLEASE FEEL FREE TO CONTACT THE NEAREST DEC OFFICE
FOR MORE INFORMATION ABOUT THE EXCITING DECSYSTEM-20 FAMILY

Nel 1983, alla University of Southern California, un giovane dottorando di nome Fred Cohen ha realizzato un esperimento molto semplice ma rivoluzionario: ha scritto qualche riga di codice informatico e ha creato quello che il suo professore ha definito per la prima volta "virus informatico".

Il software creato da Cohen era in grado di inserirsi in altri programmi, copiarne una parte e continuare a diffondersi autonomamente. Durante una dimostrazione pubblica, questo è riuscito a propagarsi in pochi minuti all'interno di un sistema informatico.

[2] A Brief History of Malware and Cybercrime | CIO

Era appena stato dimostrato per la prima volta che un computer poteva essere contagiato come un organismo vivente.

L'esperimento non era assolutamente pensato per fare danni, ma per illustrare un concetto teorico: che esistono programmi capaci di replicarsi senza controllo e che, soprattutto, non era possibile creare un metodo infallibile per individuarli tutti.

Oggi questo rimane in parte vero, infatti gli antivirus che dovremmo avere installati aggiornano il proprio database piuttosto frequentemente appena emergono nuovi virus, per garantire la massima protezione dei nostri dispositivi.

```
program virus:=
{1234567;

subroutine infect-executable:=
        {loop:file = get-random-executable-file;
        if first-line-of-file = 1234567 then goto loop;
        prepend virus to file;
        }

subroutine do-damage:=
        {whatever damage is to be done}

subroutine trigger-pulled:=
        {return true if some condition holds}

main-program:=
        {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}

next:}
```

Dalla tesi di dottorato di Fred Cohen

Cinque anni dopo, nel 1988, è avvenuta la prima condanna al mondo per un reato commesso su internet.

Robert Morris era anche lui un dottorando, nel noto college americano MIT, che tentava di provare quella che fino a quel momento era solo teorico: creare un programma che fosse in grado di infettare, copiarsi e trasferirsi autonomamente da un computer all'altro. In gergo questo tipo di programma si chiama *worm*. Suo malgrado il sistema da lui creato, denominato poi Morris Worm, e progettato per auto-replicarsi, sfruttando diversi punti deboli già conosciuti dei sistemi, funzionò molto meglio del previsto.

L'intento dichiarato da Morris era quello di stimare la grandezza di internet, ma un errore di progettazione fece sì che il worm si copiasse ripetutamente sugli stessi sistemi, consumandone risorse e rendendoli inutilizzabili.

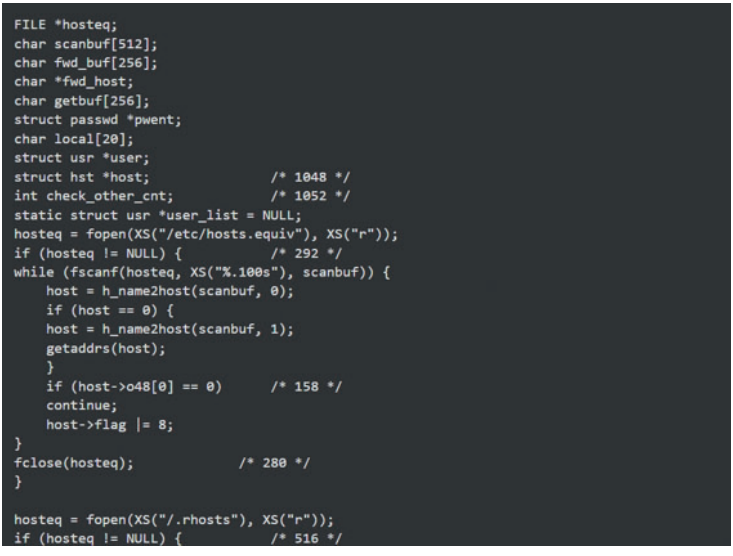
Come se non bastasse, il worm ebbe anche un'ampia diffusione: si stima che colpì il 10% dei circa 60.000 computer allora connessi.

Tra questi sono stati infettati e paralizzati server universitari, centri di ricerca e strutture governative, causando danni calcolati in milioni di dollari[3].

Come detto Morris fu involontariamente un pioniere del sistema e fu condannato nel 1990 con la neonata legge americana sui reati informatici[4].

[3] Morris Worm — FBI

[4] La storia del malware | IBM



```
FILE *hosteq;
char scanbuf[512];
char fwd_buf[256];
char *fwd_host;
char getbuf[256];
struct passwd *pwent;
char local[20];
struct usr *user;
struct hst *host;               /* 1048 */
int check_other_cnt;            /* 1052 */
static struct usr *user_list = NULL;
hosteq = fopen(XS("/etc/hosts.equiv"), XS("r"));
if (hosteq != NULL) {           /* 292 */
while (fscanf(hosteq, XS("%.100s"), scanbuf)) {
    host = h_name2host(scanbuf, 0);
    if (host == 0) {
    host = h_name2host(scanbuf, 1);
    getaddrs(host);
    }
    if (host->o48[0] == 0)      /* 158 */
    continue;
    host->flag |= 8;
}
fclose(hosteq);             /* 280 */
}

hosteq = fopen(XS("/.rhosts"), XS("r"));
if (hosteq != NULL) {           /* 516 */
```

Capisco sia necessaria una piccola nota tecnica: virus e worm si somigliano molto, ma differiscono in un punto fondamentale. Il virus ha bisogno di un vettore (documento o programma); il worm viaggia in autonomia tra i sistemi, e quindi è più pericoloso.

A metà degli anni ‘90, più precisamente nel 1995, con la diffusione dei computer domestici e dei primi servizi online come America Online (AOL), nasce qualcosa di nuovo rispetto all’hacking “tecnico” degli anni precedenti. La truffa informatica si slega dal tecnicismo e comincia a basarsi sull’inganno delle persone più che delle macchine. In questo periodo compaiono le prime forme documentate di phishing e strumenti come AOHell, un vero e proprio toolkit (cioè un pacchetto di strumenti già pronti) creato da mascalzoni per automatizzare furti di credenziali (email e password) su AOL.

Questo ha reso queste campagne molto più semplici e diffuse, abilitando anche chi non aveva competenze tecniche. Non era più necessario violare i sistemi informatici: bastava convincere i malcapitati a consegnare spontaneamente i propri dati.

Questo segna un passaggio fondamentale, perché per la prima volta la frode digitale diventa scalabile (può colpire molte persone insieme), economica (non richiede grandi competenze tecniche) e psicologica: il punto debole non è più il computer, ma la fiducia dell'utente[5] che suo malgrado ci casca.

Oggi AOHell non esiste più perché col tempo è diventato obsoleto, ma ha fatto scuola, introducendo logiche che oggi ritroviamo in sistemi molto più avanzati e dannosi.




Infine, nel 2000, ci fu un evento chiave che ha gettato le basi per tutto quello che è venuto dopo. Di cui sono rimasto molto colpito per la sua attualità.

Nel maggio del 2000, mentre Vladimir Putin veniva insediato come Presidente della Federazione Russa, un worm noto come ILOVEYOU si è diffuso rapidamente in tutto il mondo sfruttando una trappola emotiva che ha fatto scuola: arrivava via email con oggetto "ILOVEYOU" e un messaggio che invitava ad aprire l'allegato apparentemente innocuo, chiamato "LOVE-LETTER-FOR-YOU.TXT".

[5] AOHell | WIRED

Una volta aperto, però, questo eseguiva un codice che sovrascriveva file e si auto-replicava, per poi inviarsi a tutti i contatti della vittima e ripetere il ciclo.

Alle spalle di questa catastrofe informatica c'era Onel de Guzman, un giovane studente filippino che ha sviluppato il worm originariamente con l'idea di accedere gratuitamente a connessioni Internet, senza però prevederne la portata distruttiva. Nel giro di pochi giorni ILOVEYOU è riuscito a infettare decine di milioni di computer Windows, causando gravissime interruzioni nei sistemi di aziende, governi e istituzioni – inclusi, pensate, il Pentagono, la CIA e il Parlamento Britannico.

I danni economici furono nell'ordine dei miliardi di dollari – si stimano tra i 5 e i 10 miliardi di dollari[6]. Questo dimostrò che non era più necessario avere abilità tecniche informatiche per rappresentare una minaccia, era sufficiente convincere la potenziale vittima ad aprire un allegato, che all'apparenza non destava nessun sospetto, per fare danni di portata enorme.

A riprova di quanto questo evento sia stato "pionieristico" De Guzman non ha nemmeno mai ricevuto alcuna condanna, banalmente perché al tempo non esistevano leggi filippine che coprissero casi come il suo. La prima è stata approvata solo un mese dopo[7].

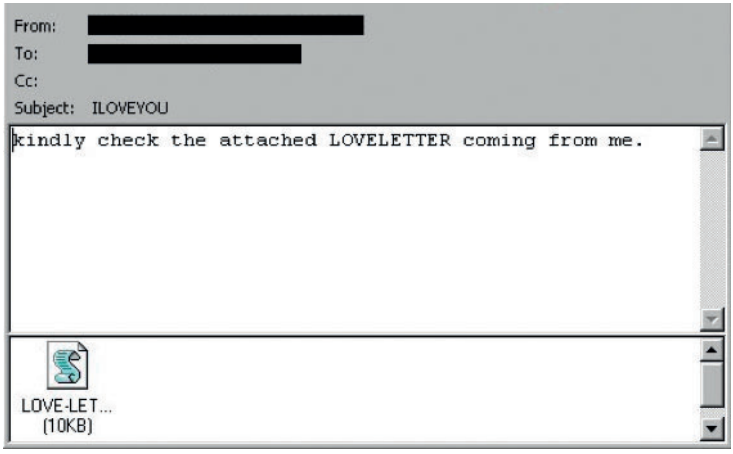
Lo studente filippino ha subito però pesanti conseguenze mediatiche e sociali, proprio come accade oggi sui social; De Guzman infatti è stato etichettato come "l'uomo che ha messo in ginocchio internet".

Dopo la gogna mediatica si è ritirato a vita privata, e ricompare sporadicamente per concedere interviste in cui ha continuato a sostenere di aver sottovalutato il potenziale della sua creazione.

---

[6] This 20-Year-Old Virus Infected 50 Million Windows Computers In 10 Days: Why The ILOVEYOU Pandemic Matters In 2020

[7] Love Bug's creator tracked down to repair shop in Manila




La strategia usata in ILOVEYOU – ossia indurre il potenziale pollo a compiere attivamente delle azioni, chiamata "social-engineering" – è ancora molto utilizzata, perché è estremamente efficace e difficile da contrastare. Parliamo di una delle strategie preferite dei grossi gruppi hacker, tra cui quelli nordcoreani legati al leader Kim Jong-un, per infettare sistemi governativi o grosse reti private.

Il regime nordcoreano finanzia attivamente diversi gruppi hacker per fare cassa. Il crimine online rappresenta infatti, secondo diverse stime, circa metà dell'intero PIL nordcoreano[8] [9]. Questo non fa altro che dimostrare quanto strategie come quella di De Guzman siano profittevoli, relativamente semplici da applicare e spesso difficili da contrastare.

Quindi, se ti arriva una email sospetta, non aprire mai l'allegato, altrimenti sono guai.

---

[8] North Korea Earns $4 Billion Through Crypto Theft in Two Years Amid UN Sanctions | The Economy

[9] Lazarus Group, Labyrinth Chollima, HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY, Diamond Sleet, Group G0032 | MITRE ATT&CK®

# STRATEGIE - TECH SUPPORT

Navigando in rete ti sarà probabilmente capitato di finire su una pagina con un pop-up di Windows/Apple che dice: “Il tuo computer è infettato, chiama il numero xyz per risolvere”. È una cosa che succede spesso.

Se hai chiamato, hai parlato al telefono con un giovanotto che sostiene di essere un tecnico di Windows/Apple. Questo ti ha convinto a scaricare un software per il controllo da remoto (AnyDesk o TeamViewer) e una volta in controllo della tua macchina, ti ha fatto vedere alcune schermate che non hai capito, ha parlato in linguaggio tecnico, incomprensibile, affermando che il computer ha una serie di problemi incredibili.



Questo è il manuale della "Tech Support Scam" – la frode del supporto tecnico. Questo schema mira direttamente a chi non è pratico di computer e non riesce a rendersi immediatamente conto che si tratta di una fregatura. Di solito punta agli over-60: non hanno ancora sviluppato questo filtro e quindi credono più facilmente ai pop-up finti[1].

Una volta preso il controllo, il "tecnico" fa credere che ci siano un sacco di problemi – e che solo lui possa risolverli. Ti mostrano dati di sistema del tutto innocui, raccontandolì però in modo falso, contando sul fatto che la vittima non possa controbattere e si fidi del sedicente esperto.

Ovviamente la riparazione della macchina non è gratuita: questa finta riparazione costa alla vittima tra i 150 e gli 800 dollari[2] (in un caso la vittima ha pagato ben 25.000 dollari[3]). Spesso per essere pagati chiedono Bitcoin o buoni regalo: soldi difficili da rintracciare una volta incassati.

Questo genere di truffa rientra nella categoria chiamata "imposter scam", truffa dell'impostore. Nel 2024, negli Stati Uniti, sono state registrate quasi un milione di segnalazioni – e ricordiamo che chi denuncia è solo una minoranza. La perdita stimata: quasi 3 miliardi di dollari[4].

**È una cifra impressionante, che non accenna a ridursi.**

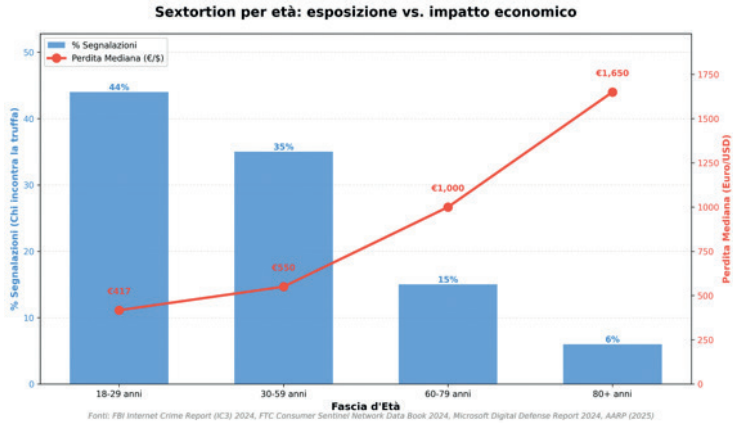
---

[1] Tech Support Scams Are Rampant

[2] S. Rept. 114-208 - FIGHTING FRAUD: U.S. SENATE AGING COMMITTEE IDENTIFIES TOP 10 SCAMS TARGETING OUR NATION'S SENIORS | Congress.gov

[3] Darien resident loses $25,000 to cybersecurity scammers, police say

[4] Consumer Sentinel Network Data Book 2024




## Perché questo schema funziona?

Il truffatore al telefono ha spesso davanti a sé un copione pieno di tecnicismi e supercazzole, pensato per farlo sembrare un esperto. La regola è una: mettere pressione per far sì che la vittima prenda decisioni impulsive, non ragionate. Esempi: "ti entrano nel computer", "perderai i tuoi dati", e, la migliore: "perderai i tuoi soldi". Funziona sempre, altrimenti non tirerebbero su quasi tre miliardi di dollari in un solo anno.

Tutto è fondato sull'ignoranza e la buona fede della vittima, difatti non è raro che il truffatore cerchi di convincere il pollo a tenere la bocca chiusa: sa che nel momento in cui dovesse parlare, uno più smaliziato riconoscerebbe la fregatura. A quel punto addio pollo e addio soldi.

## Cosa possiamo fare per difenderci?

- Innanzitutto: non chiamare mai il numero nel pop-up. Se ti serve assistenza, cerca il numero ufficiale dell'azienda sul sito e chiama quello. Attenzione ai risultati sponsorizzati in alto: non sempre sono affidabili[5].

[5] How To Spot, Avoid, and Report Tech Support Scams | Consumer Advice

- Un tecnico di Windows o Apple non ti chiederà mai di installare software per il controllo remoto del computer. Se ti viene chiesto chiudi immediatamente la chiamata e spegni il computer.

- Se ti chiedono il pagamento in Bitcoin o carte regalo, vale lo stesso discorso: non pagare e chiudi tutto immediatamente.

- Se pensi di essere stato truffato, non vergognarti: chiama la polizia e denuncia. Più siamo a segnalare questi criminali più efficace sarà la difesa.

Se hai genitori o conosci persone anziane che usano Internet, stai loro vicino come faresti con un bambino. Spesso sono inesperti e non pronti al cinismo della rete. Seguili e proteggili sempre.

# STRATEGIE - SEXTORTION

Ricordo come fosse ieri il giorno in cui i giornali hanno scoperto la "sextortion", fu un terremoto: Jolanda Renga sconvolse l'Italia intervenendo alla Commissione parlamentare di inchiesta sul femminicidio. Qualche tempo prima era stata contattata e ricattata da uno sconosciuto che la minacciò di pubblicare in rete foto che la ritraevano nuda se non avesse ricevuto 10.000 euro.

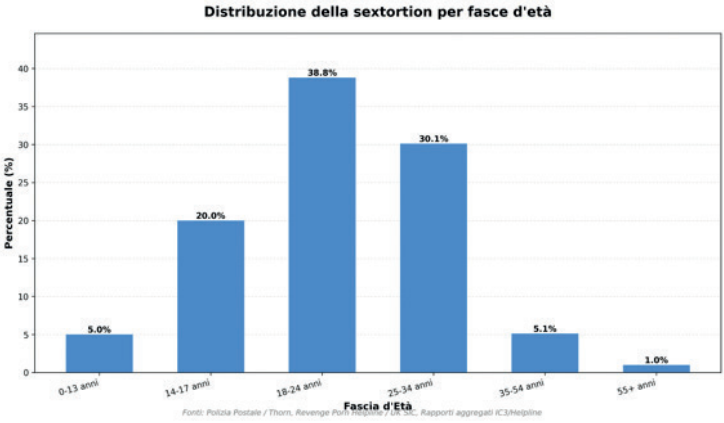
Peccato che quelle foto fossero state generate artificialmente, semplicemente addestrando un'intelligenza artificiale con foto pubbliche e non intime reperibili sui social della ragazza[1].

La "sextortion" (unione di "sex", sesso, ed "extortion", estorsione) è una forma di estorsione online: qualcuno ottiene – o crea – materiale intimo e lo usa per ricattare la vittima.

Quella subita da Jolanda Renga è una sua evoluzione, la più recente.

Questa è una strategia che prende di mira principalmente i giovani maschi, anche minorenni[2]; perché spesso molto attivi sui social network e in una fase della loro vita in cui cadono più facilmente vittime di alcune trappole.

[1] Jolanda Renga 'educazione affettiva sin da piccoli' - Notizie - Ansa.it
[2] Sextortion: A Growing Threat Preying Upon Our Nation's Teens — FBI




Il metodo più utilizzato in questo tipo di ricatto è quello chiamato "grooming" – adescamento e manipolazione: Il truffatore tenta inizialmente di costruire una relazione di fiducia con la vittima. Lo fa fingendosi un'attraente ragazza e mira a convincerlo, talvolta usando foto false, a inviare materiale compromettente[3]. A quel punto lo ha in pugno e svela il suo trucco. La favola finisce. Il truffatore esige di essere pagato per rimanere in silenzio. Nello specifico minaccia di diffondere ad amici e parenti il materiale che ha ottenuto se non verrà pagato.




[3] Online Sexual Exploitation, Grooming, and Extortion of Youth - Children and Screens

## Il ragazzo va nel panico.

I dati a nostra disposizione ci dicono che mediamente la cifra richiesta per comprare il silenzio è di circa 650 euro[4]. Una cifra spaventosa per un giovane adulto, ancora di più per un adolescente.

## Che fare?

Un terzo dei giovani intervistati sostiene di aver pagato. Ma c'è un problema: spesso, dopo il primo pagamento, il truffatore continua a ricattare, pretendendo ancora di più per non diffondere il materiale[5].

Ed è così che molti ragazzi cominciano a valutare di farla finita: la vergogna, la pressione, i troppi soldi. È tutto troppo da gestire.

Almeno venti ragazzi, alcune fonti dicono addirittura 36[6]. Tra il 2021 e il 2025. Solo negli Stati Uniti[7]. Chissà quanti in giro per il mondo di cui non sappiamo niente. Non è retorica. Succede.

## Perché questi truffatori mirano a giovani ragazzi?

Come detto sopra: sono più esposti degli adulti, sono in una fase della loro vita meno consapevole e meno smaliziata, sentono di più la pressione sociale, ma non solo.

Secondo gli studi, giovani e adolescenti tendono ad avere maggiore disinvoltura nell'invio di immagini intime o nel fidarsi di contatti digitali, perché sottovalutano i rischi o non riescono a riconoscere segnali di manipolazione8. Questo non è necessariamente perché i ragazzi sono leggeri, ma perché, spesso, l'estorsore è una persona già nota (un contatto online o qualcuno incontrato), quindi la barriera psicologica è più bassa[9].

Un ragazzo su cinque tra i 13 e i 20 anni è stato vittima di sextortion[10]. Una cifra impensabile.

[4] Financial sextortion study in young boys and adolescents | European Union
[5] Helpline - Cyber Rights Organization
[6] NCMEC Releases New Data: 2024 in Numbers
[7] Sextortion: A Growing Threat Targeting Minors — FBI
[8] Sextortion: A Scoping Review - PMC
[9] Sexual Extortion & Young People: Navigating Threats in Digital Environments
[10] Sexual Extortion & Young People: Navigating Threats in Digital Environments

***Come possiamo proteggere i nostri ragazzi da tutto questo? Come possiamo in qualità di genitori o tutori evitare che si tolgano la vita per qualche foto compromettente fatta per ingenuità o inesperienza?***

L'educazione e il dialogo sono fondamentali:

- Parla regolarmente e apertamente con tuo figlio di cosa fa online – non usare solo regolamenti e divieti. Dialoga sinceramente sui rischi e su come ricattatori e truffatori operano (ad esempio, iniziando come amici o flirt online). Questo aiuta a creare fiducia e fa sì che il ragazzo si senta libero di raccontare eventuali problemi prima che sia troppo tardi[11].

- Spiegagli che non è colpa sua se dovesse succedere qualcosa e che può venire sempre da te per aiuto senza paura di punizioni o rimproveri. Questo riduce il rischio che tenga la cosa nascosta[12].

- Chiedi a tuo figlio di mantenere i profili social privati e di accettare solo persone che conosce. Rivedi con lui le impostazioni di privacy[13].

- Mai condividere foto o video intimi online, anche con persone "di cui ci si fida", perché una volta inviati non si ha più controllo su dove finiscano[14].

---

[11] FBI: 'Financial sextortion' of teens is a 'rapidly escalating threat.' How parents can protect their kids

[12] Advice for parents or carers of children who are being sexually extorted or 'sextorted'

[13] FBI: 'Financial sextortion' of teens is a 'rapidly escalating threat.' How parents can protect their kids

[14] Sextortion — FBI

Se invece tuo figlio ti dice che lo stanno già ricattando con delle foto compromettenti, niente panico:

- Non pagare. Mai. Nessun pagamento garantisce che l'estorsione finisca.
- Blocca e segnala l'account dell'estorsore sulle piattaforme.
- Non cancellare subito le prove (foto o messaggi): possono aiutare le indagini.
- Contatta le autorità competenti.[15] [16]

Queste indicazioni valgono anche per le ragazze che hanno subito le stesse minacce con foto false che ha subito Jolanda Renga.

La sextortion non si previene con il silenzio e non si cura con la vergogna. Si previene togliendo ai ricattatori l'unica arma che hanno: l'isolamento della vittima. Finché un ragazzo penserà di essere solo, loro continueranno a vincere.

Oggi non servono nemmeno più foto vere. Basta una manciata di immagini pubbliche e un algoritmo.

**Venti ragazzi in due anni, solo negli Stati Uniti. Non sono numeri: sono silenzi che nessuno ha intercettato in tempo.**

[15] Safeguarding Alert: Sextortion and the Rise of AI

[16] Advice for parents or carers of children who are being sexually extorted or 'sextorted'

***La sextortion non uccide perché esistono delle foto. Uccide perché convince chi le subisce che non esiste alternativa al panico.***

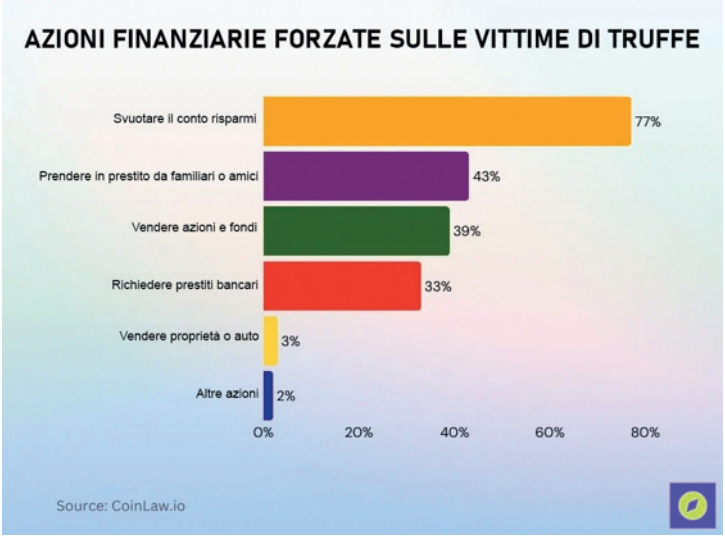
E ogni volta che un adulto risponde con il giudizio invece che con l'ascolto, sta facendo metà del lavoro del ricattatore.

# STRATEGIE - PIG BUTCHERING

"Pig butchering" significa letteralmente "macellazione del maiale". È una definizione brutale, ma dannatamente appropriata.

Il nome nasce dalla metafora del contadino che alleva la bestia, la fa ingrassare nutrendola e dandole un tetto... e infine la macella. E non è una metafora innocua.

Pig butchering è il nome dato a una strategia di truffa che sfrutta questo stesso principio: allevare la propria vittima, ingrassare la somma che la vittima spende, fidelizzandola, e poi lasciarla morire. È una strategia che negli Stati Uniti ha mietuto e miete ancora moltissime vittime. Secondo l'FBI, le perdite totali legate alle truffe di investimento (inclusi pig butchering) erano oltre quattro miliardi di dollari nel 2023[1]. E no, non è un numero astratto. È il conto di vite rovinate.




[1] IC3 2023 Cryptocurrency Fraud Report

Questo schema inizia in modo banale ma comune: la vittima riceve un messaggio "per errore" (phishing). Se abbocca, inizia la danza. Settimane, mesi, il tempo non conta. Si costruisce una relazione amicale o "romantica".

Da qui, la storia può prendere due strade. Se il truffatore sfrutta la fiducia per chiedere soldi – emergenze mediche, viaggi improvvisi, gift card – stiamo parlando di romance scam, la truffa sentimentale. Se invece l'obiettivo è convincere la vittima a investire su piattaforme false, eccoci nel territorio del pig butchering.

Stesso incipit, percorsi diversi. In tutti i casi, la vittima pensa di avere un legame reale con qualcuno che non esiste. Niente è lasciato al caso: profili falsi, foto rubate, storie costruite.

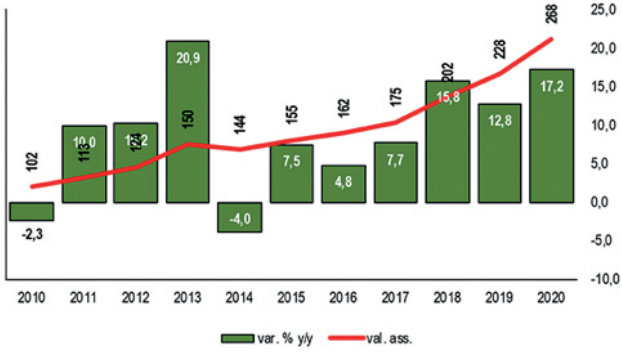
Nel pig butchering, ostentare ricchezza serve a rendere credibile l'investimento: villa, orologi, lifestyle da imprenditore. Nel romance scam, la stessa ostentazione è solo esca emotiva, giustifica richieste immediate. In entrambi i casi, i siti proposti non sono affidabili: portali sconosciuti o copie di servizi noti.

Ma il pig butchering non vive di emergenze. Vive di tempo, fiducia e capitali. Ed è qui che il conto inizia davvero a salire.

In poche parole quei soldi non vengono investiti, ma finiscono più o meno direttamente nelle tasche del truffatore. Questa è la fase di ingrassatura del maiale. L'obiettivo è uno solo: spremere il più possibile la vittima, e non fermandosi certo ai soldi già disponibili. Sempre allo stesso modo. Non sono rari i casi in cui le persone vengono spinte a usare il fondo pensione o a chiedere prestiti pur di aumentare "l'investimento"[2]. Quando la truffa viene scoperta, il danno è doppio: ai soldi persi si aggiunge una situazione personale ed economica ancora più difficile da gestire. È anche per questo che molte vittime non denunciano. La vergogna di essere state raggirate

[2] FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"

pesa più della rabbia, e così il rospo viene ingoiato in silenzio.



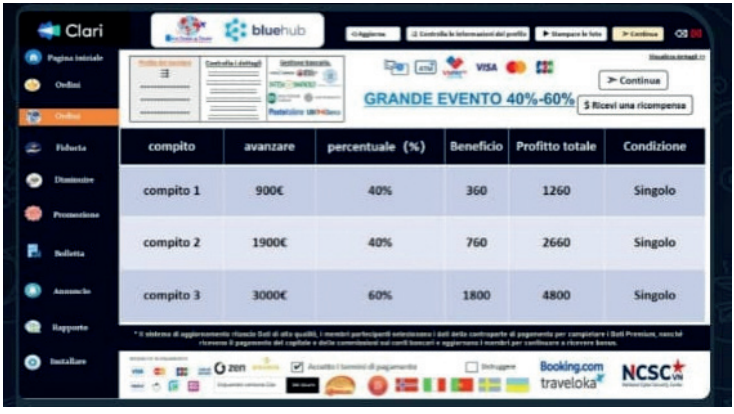

**Dinamica decennale denunce di delitti, truffe, frodi informatiche per regione e ripartizione**
**2010-2020, var. % cumulata – Elaborazione Ufficio Studi Confartigianato su dati Istat**

## Ma cosa fare se ci si rende conto di essere finiti dentro uno schema di questo tipo? La prima cosa è agire subito[3].

1. Tagliare ogni contatto. Subito. Senza rimorsi[4].
2. Conservare tutte le prove. Screenshot come se fossero testimoni[5].
3. Sporgere denuncia. Non vergognarti. Serve agli altri, oltre che a te[6].
4. Segnalare l'accaduto alla piattaforma su cui è avvenuto il primo contatto[7].
5. Se sono coinvolti conti, carte o bonifici, avvisare immediatamente la propria banca o l'ente emittente[8].

[3] Cryptocurrency Investment Fraud — FBI
[4] Avoid Scams: Investment Fraud and Pig Butchering
[5] Cryptocurrency Investment Fraud — FBI
[6] Pig Butchering Scams | Federal Deposit Insurance Corporation OIG
[7] CFTC Partners with Federal and Private Groups to Distribute Cryptocurrency Relationship Investment Scam Information
[8] FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"

Facciamo un passo indietro: come riconosco un macellaio? Domande semplici: promette “garantito”? Ti spinge con urgenza? La piattaforma ti suona strana o non l’hai mai sentita nominare? Non è investimento. È marketing dell’inganno. Spesso quelli usati dai truffatori sono siti che imitano piattaforme famose e affidabili, a volte persino nell’indirizzo web (l’URL). In realtà sono solo facciate: non c’è nessuna vera funzionalità, a volte nemmeno un deposito reale di Bitcoin, solo un portafoglio a cui mandare i soldi. Il resto serve a una cosa sola: fregarti.




È una strategia meschina, impietosa e cinica. Inoltre spesso, ricordiamolo, chi la esegue non lo fa per scelta, ma perché costretto, ricattato o intrappolato in meccanismi più grandi di lui. Questo non rende il danno meno reale, ma aiuta a capire quanto il sistema sia sporco fino in fondo.

Quindi, in futuro, se una persona che non conosci ti propone degli investimenti garantiti… l’unica cosa garantita è che ti fai molto male. Non investire su piattaforme che non conosci.

# TESTIMONIANZE

Andiamo oltre i numeri. Parliamo di persone. Persone violate. Persone che spesso non denunciano. L'abbiamo già visto in altri capitoli.

Quello che segue sono storie vere. Persone che hanno voluto raccontare. Per due ragioni: esorcizzare il danno e avvertire altri. Ecco i pattern, le conversazioni, i segnali. Da leggere con attenzione.

Gino si espone con nome e cognome su un forum[1] di consulenza legale. Merita rispetto. Estremo rispetto.

Racconta di aver subito uno dei più classici e tutt'ora proficui esempi di truffa in circolazione: ha ricevuto un SMS da qualcuno che si fingeva Poste Italiane.

Attenzione: non è il sito numero delle Poste. È un trucco per apparire come chi non è, una specie di camuffamento digitale. Gli addetti del settore chiamano questa cosa spoofing, ma non serve conoscere la parola per capire il rischio. Serve solo sapere una cosa: mai fidarsi di chi ti chiama o ti manda un link inaspettato. Mai.

Il messaggio gli chiedeva di fare una verifica di sicurezza. Altrimenti, gli dicevano, avrebbe perso il conto. In allegato: un link. Ha aperto il link. Si è tranquillizzato: sembrava il sito di Poste. Ha inserito i propri dati e poco dopo ha ricevuto una chiamata da un sedicente operatore di Poste Italiane che lo ha chiamato per nome. Gli ha chiesto il codice temporaneo ricevuto via SMS. "Serve per la verifica", gli ha detto. Dopodiché gli ha fatto disinstallare l'applicazione di Poste Italiane dal cellulare. Avrebbe ricevuto un messaggio

[1] truffa posteinfo | La Legge Per Tutti

con le credenziali e che poi sarebbe potuto ri-accedere. Gino non ha mai ricevuto quel messaggio.

Probabilmente allarmato, ha chiamato il numero verde delle Poste dove ha scoperto l'amara verità: è stato truffato.

La persona che poco prima era con lui al telefono gli ha sfilato quasi 1.400 euro e stava tentando di spenderne altri 300 nel momento in cui Gino è arrivato allo sportello per bloccare il conto.

Purtroppo in questi casi c'è poco da fare.Tecnicamente, le credenziali sono state consegnate dal truffato – senza che lui sapesse cosa stava facendo. Ecco perché i messaggi dicono: "Non condividere questo codice con nessuno." Non è un avviso di facciata. Nessuno significa nessuno. Un operatore della Posta non vi chiederà mai questo codice, non ne ha bisogno.

Gino ha sporto denuncia ai Carabinieri. È necessario per formalizzare l'accaduto e tutelarsi. Ma lo dico con franchezza: per quanto esistano tutele, nulla è garantito[2]. Spesso rintracciare questi criminali è complicato: richiede tempo e anche quando vengono individuati, il procedimento può essere lungo e complesso, spesso operano dall'estero, talvolta fuori dall'Unione Europea, il che complica le indagini, come abbiamo detto precedentemente.

La prossima storia viene invece da un utente online che ha scelto di rimanere anonimo. Ha cancellato il proprio profilo, capirai con me perché.

La sua storia[3] è fortemente disturbante e in un certo senso anche distopica: è un esempio pratico di quello di cui abbiamo parlato quando ho descritto il fenomeno del "pig butchering".

Un'app di incontri, una qualsiasi – non importa quale.

[2] Payment Services Directive - Finance - European Commission

[3] How I was tricked into a pig butchering scam so you don't have to.

Entri in contatto con una ragazza – carina, interessante – che al momento è in estremo oriente, a Singapore, per motivi vari. Nessun appuntamento di persona finché lei non torna.

Questo non vi impedisce però di cominciare a costruire un rapporto, sentirvi ogni giorno, scambiarvi foto, pensieri, dediche. Quella che era una semplice amicizia scivola velocemente nella relazione – se così vogliamo chiamarla. Però ne possiede tutte le caratteristiche: l'intimità, i nomignoli, la conoscenza profonda, persino la dieta fatta insieme. Non si tratta solo di messaggi: vi scambiate canzoni, voice clip, piccoli video, e a volte vi trovate a giocare online insieme. Tutto questo contribuisce a creare un legame che, giorno dopo giorno, diventa sempre più reale nella vostra testa, anche se l'incontro di persona è ancora lontano.

Dopo un paio di mesi la ragazza, che purtroppo non è ancora riuscita a rientrare da Singapore per problemi suoi, ti propone un investimento che nella sua famiglia (che hai saputo essere molto ricca) le hanno consigliato. Si tratta di criptovalute. Ti convince a investire 2.500 euro su un sito che lei ti consiglia; vedi i numeri crescere fino a 100.000 euro e a quel punto decidi di volerli ritirare.

Ma non è così semplice: per riscattare servono tasse per 5.000 euro – troppi, non puoi permettertelo.

Lei promette che ne coprirà metà; così tu paghi.

Quando tocca a lei versare la sua parte, improvvisamente sua madre ha un infarto e non può pagare.

Le chiedi una foto di sua madre in ospedale.

Lei ti dice solo "perché?". Poi ti blocca ovunque, e sparisce.

Solo dopo arriva tutto e realizzi: sei stato preso in giro e manipolato.

Ecco perché non voleva che ne parlassi con genitori e amici: tu gliel'avevi già detto e loro erano subito sospettosi.

Capisci perché abbia provato a convincerti a chiedere un prestito per investire una somma maggiore.

Vista dall'esterno, questa storia appare una truffa fin dal primo momento, anche per chi non fa il mio mestiere. Ma quando ci sei dentro le cose sono molto meno scontate.

Ed è questo il punto: renderti cieco davanti alle evidenze, e in casi come questi si impegnano tantissimo per fartela credere. È così che la razionalità perde terreno: piccoli gesti quotidiani che convincono.

Nessuno può giudicare. Avremmo potuto essere tutti al suo posto. Lui però ha avuto il coraggio di raccontare la sua storia, anche se questo lo fa apparire "debole". Quanti hanno lo stesso coraggio?

***Questo per dirvi di non giudicare mai chi si espone, traiamone solo insegnamenti e accogliamo chi ha avuto un momento di debolezza. Come diceva Caterina Caselli nel lontano '66: nessuno mi può giudicare, nemmeno tu.***

# EVOLUZIONI E SVILUPPI

Abbiamo parlato del passato e abbiamo parlato del presente. Ma cosa ci aspetta per il futuro? Come pensano gli esperti che si evolverà il settore? Sarà vero che dobbiamo avere più paura?

Ovviamente l'intelligenza artificiale – come abbiamo già menzionato – è entrata a fare parte di questo sistema in diversi modi.

Fino a poco tempo fa, per fare spear phishing – cioè inviare email curate, mirate e specifiche – occorreva molto lavoro: raccolta di informazioni pubbliche e, talvolta, compravendita di dati. Oggi i cybercriminali delegano tutto a un algoritmo che mette insieme le informazioni e scrive il testo da inviare. Il truffatore deve occuparsi solo del "prima" e del "dopo"[1].

L'ho visto con i miei occhi: clienti che mi portano screenshot increduli.

Non solo. Grazie a strumenti come ChatGPT abbiamo capito che un robot, se allenato bene, è in grado di messaggiare con un essere umano in modo convincente.

Io stesso quando ho delle email noiose da scrivere o che richiedono poca attenzione a volte faccio riferimento a questo strumento, la sua utilità è fuori discussione.

Tutte le truffe che richiedono l'instaurazione di un rapporto di fiducia (per esempio pig butchering o romance scam) possono essere automatizzate, senza dover coinvolgere malcapitati che non parlano una sillaba di inglese; in questo modo il loro contributo diventa molto limitato.

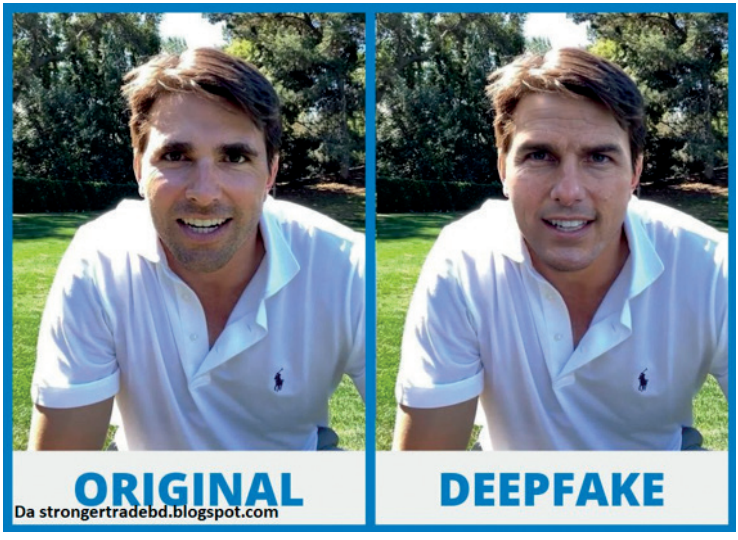
[1] Kaspersky: evoluzione del phishing tra AI, biometria e firme digitali

### Ancora di più.

Raccogliendo sufficienti campioni della voce di una persona – alcuni parlano addirittura di pochi secondi[2] – si può addestrare una macchina a riprodurla fedelmente. A quel punto basta chiamare amici e parenti e quella va da sola.

### Distopico. Lo so.

Quando abbiamo parlato di sextortion abbiamo menzionato i deepfake, cioè immagini o video generati artificialmente che ritraggono persone che fanno o dicono cose[3]. Dopo la diffusione dei deepfake, il mondo è andato nel panico: si temeva che non esistesse più una realtà visiva condivisa e che la verità potesse essere piegata in modo spaventosamente realistico e accessibile.




[2] Warning social media videos could be exploited by scammers to clone voices | Scams | The Guardian

[3] A commentary on sexting, sextortion, and generative AI: Risks, deception, and digital vulnerability - Pater - 2025 - Family Relations - Wiley Online Library

Ma non riguarda solo la geopolitica internazionale.

I video falsi possono convincere genitori o parenti che il loro caro abbia un'emergenza, che li stia videochiamando in quel momento e che stia chiedendo soldi[4].

Un dipendente può ricevere una videochiamata falsa dal proprio datore di lavoro che chiede un bonifico[5] [6].

O per rendere le truffe di investimento più convincenti, usando senza consenso figure pubbliche molto note. Accade tranquillamente anche su YouTube[7].

Questi sono, purtroppo, scenari reali. Abbiamo già visto accadere queste cose. Più passerà il tempo e più questi strumenti diventeranno accessibili e diffusi. Sempre.

Per fortuna non tutto accade indisturbato: esperti e ricercatori si sono attivati da tempo per trovare soluzioni che aiutino utenti e professionisti dell'informazione a verificarne l'origine. La stessa tecnica impiegata dai truffatori può essere rivolta contro di loro. Se si allena un'intelligenza artificiale con video o foto non reali, questa imparerà a distinguerle e potenzialmente diventerà bravissima, rappresentando così un'ottima difesa[8].

Soprattutto si cerca di inserire nei contenuti generati artificialmente segnali che ne certifichino la provenienza: watermark (filigrane digitali), metadati o simili. Controllate sempre i metadati, non fidatevi solo degli occhi.

---

[4] AI-generated videos, photos used in new virtual kidnapping scams, FBI warns
[5] Deepfake CFO Video Calls Result in $25MM in Damages | Trend Micro (US)
[6] Exploring autonomous methods for deepfake detection: A detailed survey on techniques and evaluation - ScienceDirect
[7] Warren Buffett DeepFakes on TikTok—Here's How To Spot Them Every Time
[8] NIST Guidelines Can Help Organizations Detect Face Photo Morphs, Deter Identity Fraud



| | |
|---|---|
| file_name | [redacted].pdf |
| file_size | 400 kB |
| file_type | PDF |
| file_type_extension | pdf |
| mime_type | application/pdf |
| pdf_version | 1.7 |
| linearized | No |
| author | [redacted] |

Se guardiamo a queste trasformazioni non come singoli eventi sensazionali ma come modificazioni del nostro ecosistema dell'attenzione, allora la posta in gioco diventa più chiara: non è soltanto il denaro che viene sottratto, è la capacità collettiva di fidarsi, di riconoscere canali affidabili, di mantenere uno spazio pubblico in cui l'esperienza visiva e narrativa conservi qualche vincolo con la realtà.

## Ecco il punto.

Le tecnologie che consentono oggi di fabbricare una voce, una relazione o un'immagine convincente sono anche tecnologie che ridefiniscono la quantità e la qualità delle informazioni che possiamo processare e condividere. Di conseguenza, la risposta non può essere solo tecnica né solo repressiva: serve una riorganizzazione della nostra attenzione pubblica – standard tecnici che attestino provenienza e trasformazioni, pratiche giornalistiche e di controllo della qualità che ristabiliscano fiducia, e un'educazione civica digitale che sappia pensare in termini collettivi e non solo individuali. Solo così potremo trasformare la stessa macchina che oggi facilita l'inganno in uno strumento di difesa comune.

# APPUNTI GUIDA

Struttura del libro:

1. Prefazione di Luca Poma
2. Prefazione di Germano Milite
3. Intervista a citton (perché, cosa lo ha spinto a scrivere questo libro, come ha visto cambiare negli anni questo fenomeno a chi pensa sia rivolta la guida e quali obiettivi ha
    a. Cosa ci rende oggi più vulnerabili rispetto al passato? Lo siamo?
    b. Se potessi lasciare al lettore una sola regola, non tecnica ma umana, quale sarebbe?
    c. A chi è davvero rivolto questo libro?
    d. Cosa succede se continuiamo a rimandare una vera educazione alla prudenza?
    e. Qual è l'atteggiamento umano che questo libro chiede al lettore prima ancora di qualsiasi competenza?
4. Taxonomia delle truffe — una classificazione pratica (phishing, vishing, smishing, CEO fraud / BEC, SIM-swap, account takeover, investment/ponzi, romance scam, fake apps, deepfake/voice cloning, scam via QR/payment request, malware/RAT, business email compromise).
    a. Introduzione al contesto
5. La storia delle truffe telematiche
    a. Quali sono stati i primi esempi
6. Chi sono le vittime preferite (segmentazione, bias cognitivi)

a. Vale la pena menzionare anche i tentativi di truffa alle imprese tramite link di phishing o richieste di bonifici falsi

7. Come arrivano alle vittime
   a. Dataleak / data broker / OSINT
   b. Social engineering (phishing, vishing, smishing)
   c. Malware / fake apps / QR / payment-request
   d. Tentativi verso imprese (BEC/CEO fraud) — breve box
8. Statistiche e impatto economico
9. Quali sono le strategie più utilizzate e come difendersi
10. Casi studio
    a. Intervistare 2-3 persone che sono cadute vittime di schemi diversi
       i. Hai voglia di raccontare, con parole tue, cosa è successo e quando (data approssimativa)?
       ii. Come sei entrato in contatto con il truffatore (email, telefono, social, app)?
       iii. Qual è stato il primo segnale che ti ha insospettito (se ce n'è stato uno)?
       iv. Hai eseguito qualche azione che ha permesso il furto (es. clic su link, invio di codice OTP, bonifico)?
       v. Quanto tempo è passato dalla prima comunicazione al momento in cui ti sei accorto della frode?
       vi. Hai salvato prove (email, screenshot, numeri di telefono)? Le hai consegnate a qualche autorità o banca?
       vii. Hai contattato la banca/istituzione e cosa ti hanno risposto?

viii. Cosa avresti voluto sapere prima per evitare la trappola? (consiglio pratico rivolto ai lettori)

ix. Quali effetti pratici e psicologici ha avuto l'evento su di te? (attenzione: gestire con delicatezza)

x. Sei disposto a comparire con nome reale, o preferisci anonimato? Se anonimato, specificare come vuoi essere citato.

xi. Vuoi aggiungere qualcosa che secondo te è utile per gli altri lettori?

11. Come si sta evolvendo il fenomeno, quali scenari si stanno presentando e quali complicazioni potrebbero portare (deepfake, AI-assisted scams, supply-chain)

12. Risorse e contatti — dove segnalare (Polizia Postale, ABI, Banca d'Italia, CONSOB, CERT nazionale) e link a guide ufficiali

Negli ultimi anni gli attacchi ai privati si sono evoluti: l'email resta il vettore più usato ma SMS, WhatsApp/Telegram, chiamate vocali (vishing), social e le truffe romantiche/investimento sono in forte crescita; inoltre l'uso di AI e deepfake ha aumentato la credibilità degli attacchi e creato nuovi scenari (es. "virtual kidnapping").

1. Email phishing (broad phishing)
   a. Descrizione: email broad con link a pagine false o allegati malevoli.
   b. Perché funziona: volume elevato + messaggi formulati per Urgenza/Autorità.
   c. Segni: saluti generici, link che non combacia con il dominio, allegati con password.

d. Impatto: furto credenziali, malware, perdita denaro.

Per approfondire: report APWG/KnowBe4 su trend 2024–25.

2. Romance / Dating scams
    a. Descrizione: costruzione di legami emotivi online per estorcere denaro o dati.
    b. Perché funziona: leva emozionale e isolamento; spesso target: over-50.
    c. Impatto: altissime perdite medie per vittima e grave danno psicologico.
3. Tech-support / Remote access scams
    a. Descrizione: “assistenti” che convinceranno a installare software di controllo remoto.
    b. Perché funziona: vittima vuole risolvere problema tecnico e concede accesso.
    c. Segni: link per scaricare TeamViewer/AnyDesk, richiesta di OTP o password.
4. Clonazione profili
    a. Descrizione: profili falsi identici a chi stanno impersonando anche come nickname
    b. perché funziona: la vittima si fida perché pensa si tratti di un’altra persona
    c. Segni: profilo nuovo, richiesta di pagamento, invito a investire
5. Pig-butchering (long con + crypto / investment scam)
    a. Breve: il truffatore costruisce una relazione (messaggi, dating/social), finge consigli di investimento e convince la vittima a “investire” in schemi crypto falsi; alla fine svuota i conti.

b. Perché funziona: leva emotiva + finta prova di rendimenti + pagamenti in crypto difficili da recuperare.

c. Segnali: rapporti lunghi ma mai incontrati di persona, richiesta di trasferire solo in crypto, piattaforme/bot "di trading" che bloccano i prelievi.

6. Sextortion / revenge porn extortion

   a. Breve: minacce di pubblicare materiale intimo (vero o falso) a meno che non si paghi.

   b. Segnali: richieste di pagamento in crypto, email con password (talvolta vecchie) usate per credervi.

7. Fake verification / admin messages (es. "sei stato segnalato" su social)

   a. Breve: messaggi che chiedono di "verificare" account tramite link che rubano credenziali.

   b. Segnali: richiesta di login tramite link, minacce di ban urgenti.

# CONSIDERAZIONI FINALI

A chi legge questo libro con la testa e con il cuore.

Siamo arrivati alla fine di questo percorso insieme.

Hai letto di truffe, di meccanismi, di vittime e di predatori. Hai visto come funziona il sistema dall'interno. Hai capito che non esiste un profilo preciso di chi "ci casca" — perché ci caschiamo tutti, in momenti diversi, per ragioni diverse.

Permettimi di chiudere non con un elenco di regole, ma con qualcosa di più semplice e più umano.

Quello che ti chiedo è solo questo: rallenta.

**Prima di cliccare, rallenta.**

**Prima di rispondere, rallenta.**

**Prima di trasferire, rallenta.**

Un secondo di pausa vale più di qualsiasi antivirus.

**Sul denaro:** Non esistono rendimenti garantiti senza rischio. Prima di muovere qualsiasi somma, parla con qualcuno di fiducia. Il confronto è gratis. Il rimpianto, no.

**Sulle emozioni:** I truffatori non attaccano la tua intelligenza. Attaccano la tua umanità. Quando senti urgenza, quando senti paura, quando senti che devi decidere subito — fermati. Chi ha qualcosa di serio da offrirti può aspettare cinque minuti.

**Sui tuoi cari:** Parla con loro. Non per spaventarli — per prepararli. Una conversazione di dieci minuti può fare la differenza tra una brutta mattina e una catastrofe.

**Su te stesso:** Se in passato ti hanno fregato — sappi che non c'è nulla di cui vergognarsi. Nulla. La colpa non è mai della vittima. Mai.

Una regola sola:

***Il dubbio non è debolezza. È intelligenza.***

Ora condividi questo libro — con chi ami, con chi è vulnerabile, con chi ancora non sa quanto sia facile trovarsi dall'altra parte di una truffa ben costruita. La difesa migliore non è tecnica. È collettiva.

Buon viaggio !!

# BIBLIOGRAFIA


1. [2407.12896] A Survey of Scam Exposure, Victimization, Types, Vectors, and Reporting in 12 Countries
2. ENISA Threat Landscape 2025
3. Iocta, Internet Organised Crime Threat Assessment - Publications Office of the EU
4. “Ecco perché ho denunciato chi minacciava di diffondere foto di me nuda. Dopo ho ricevuto insulti da tanti adulti”: Jolanda Renga parla alla Camera - Il Fatto Quotidiano
5. 1 2024 IC3 ANNUAL REPORT
6. A Brief History of Malware and Cybercrime | CIO
7. AOHell | WIRED
8. La storia del malware | IBM
9. Morris Worm — FBI
10. This 20-Year-Old Virus Infected 50 Million Windows Computers In 10 Days: Why The ILOVEYOU Pandemic Matters In 2020
11. Love Bug’s creator tracked down to repair shop in Manila
12. North Korea Earns $4 Billion Through Crypto Theft in Two Years Amid UN Sanctions | The Economy
13. 250+ Phishing Statistics and Trends You Must Know in 2025
14. Barracuda_report_2023-spear-phishing-trends.pdf
15. Biggest Data Breaches in US History (Updated 2025) | UpGuard

16. (PDF) THE DARK WEB ECONOMY: CYBERCRIMINAL BUY AND SELL YOUR DATA
17. Phishing Statistics By Demographic, Healthcare, Industry And Country (2025)
18. 2023 INTERNET CRIME REPORT
19. How to Safeguard Against Business Email Compromise | EMPIST
20. What is business email compromise (BEC)? | Wiz
21. Truffe online, +9% nel 2024, vittime 2,8 milioni di italiani - Notizie - Ansa.it
22. Nel 2024 truffe online per 181 milioni di euro - Cybersecurity - Ansa.it
23. IC3 2023 Cryptocurrency Fraud Report
24. FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as “Pig Butchering”
25. Cryptocurrency Investment Fraud — FBI
26. Avoid Scams: Investment Fraud and Pig Butchering
27. Pig Butchering Scams | Federal Deposit Insurance Corporation OIG
28. CFTC Partners with Federal and Private Groups to Distribute Cryptocurrency Relationship Investment Scam Information
29. Tech Support Scams Are Rampant
30. S. Rept. 114-208 - FIGHTING FRAUD: U.S. SENATE AGING COMMITTEE IDENTIFIES TOP 10 SCAMS TARGETING OUR NATION’S SENIORS | Congress.gov
31. Consumer Sentinel Network Data Book 2024
32. Darien resident loses $25,000 to cybersecurity scammers, police say

33. How To Spot, Avoid, and Report Tech Support Scams | Consumer Advice
34. Jolanda Renga 'educazione affettiva sin da piccoli' - Notizie - Ansa.it
35. Sextortion: A Growing Threat Preying Upon Our Nation's Teens — FBI
36. Online Sexual Exploitation, Grooming, and Extortion of Youth - Children and Screens
37. Financial sextortion study in young boys and adolescents | European Union
38. Helpline - Cyber Rights Organization
39. Sextortion: A Growing Threat Targeting Minors — FBI
40. Sextortion: A Scoping Review - PMC
41. Sexual Extortion & Young People: Navigating Threats in Digital Environments
42. FBI: 'Financial sextortion' of teens is a 'rapidly escalating threat.' How parents can protect their kids
43. Advice for parents or carers of children who are being sexually extorted or 'sextorted'
44. Sextortion — FBI
45. Safeguarding Alert: Sextortion and the Rise of AI
46. Kaspersky: evoluzione del phishing tra AI, biometria e firme digitali
47. AI-generated videos, photos used in new virtual kidnapping scams, FBI warns
48. Exploring autonomous methods for deepfake detection: A detailed survey on techniques and evaluation - ScienceDirect
49. Warren Buffett DeepFakes on TikTok—Here's How To Spot Them Every Time

50. Warning social media videos could be exploited by scammers to clone voices | Scams | The Guardian
51. A commentary on sexting, sextortion, and generative AI: Risks, deception, and digital vulnerability - Pater - 2025 - Family Relations - Wiley Online Library
52. Deepfake CFO Video Calls Result in $25MM in Damages | Trend Micro (US)
53. NIST Guidelines Can Help Organizations Detect Face Photo Morphs, Deter Identity Fraud
54. NCMEC Releases New Data: 2024 in Numbers
55. Payment Services Directive - Finance - European Commission
56. How I was tricked into a pig butchering scam so you don't have to.
57. Truffa posteinfo | La Legge Per Tutti

# INDICE

Prendersi cura ..... 7
Prefazione ..... 11
Introduzione ..... 13
Ringraziamenti ..... 17
Tassonomia e introduzione ..... 19
Come si arriva alle vittime ..... 25
Storia delle truffe informatiche ..... 33
Strategie - tech support ..... 43
Strategie - sextortion ..... 47
Strategie - pig butchering ..... 53
Testimonianze ..... 57
Evoluzioni e sviluppi ..... 61
Appunti guida ..... 65
Considerazioni finali ..... 71
Bibliografia ..... 73
Indice ..... 77