



# Rendimenti da sogno? No, perdite da incubo!

Tutto ciò che dovrete sapere sulle truffe sugli investimenti online

La vostra polizia e la Prevenzione Svizzera della Criminalità (PSC) – un servizio intercantonale della Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia (CDDGP)

## Investite il vostro denaro con discernimento!

In questo periodo di politica dei “tassi zero” e d’incertezza economica e borsistica, è diventato difficile mettere al sicuro i propri beni, per non parlare di farli fruttare. Per questo motivo, molti investitori sono sempre più spesso alla ricerca di investimenti stabili (per esempio in oro, immobili) e di **nuove tipologie d’investimento** che promettono alti rendimenti anche in tempi di crisi, come le **criptovalute**. Questa situazione è prontamente sfruttata da truffatori che si spacciano per fornitori di servizi finanziari innovativi. Questi imbrogliatori incitano i piccoli investitori insicuri a fare investimenti dai presunti lauti guadagni, che poi si tramutano però in perdite secche. Questa pratica è chiamata **truffa sugli investimenti online** (dall’inglese “investment fraud”) e in questo opuscolo vi spieghiamo come funziona.



### 1ª fase: l’adescamento

In generale, la strategia dei truffatori consiste nel diffondere su larga scala **annunci pubblicitari** in Internet (pop-up, banner pubblicitari, mail di spam, ecc.) e nei portali di notizie online, ma anche effettuando telefonate indesiderate e tentativi di contatto sulle reti sociali e persino sulle piattaforme di incontri online.

Il loro scopo è inizialmente solo quello di **suscitare il vostro interesse** per una nuova forma d’investimento e di invogliarvi a lasciare loro i vostri **dati di contatto**. Inoltre, non appena inserite certe parole chiave nel vostro motore di ricerca online, sarete indirizzati verso siti Internet apparentemente serissimi (e ottimizzati per i motori di ricerca!), ma purtroppo gestiti da truffatori. Lì, vi vengono presentati argomenti convincenti che si avvalgono anche di **“testimonianze”** di personalità di spicco verosimilmente molto soddisfatte dei loro investimenti.



## 2<sup>a</sup> fase: il primo contatto

Se vi siete poi registrati su un tale sito, poco tempo dopo riceverete una **chiamata da parte di un presunto consulente per gli investimenti**. Dato che inizialmente potreste ancora nutrire un certo scetticismo, questa persona non cercherà di convincervi ad effettuare subito investimenti importanti, ma vi proporrà di investire solo piccoli importi, come CHF 250 o CHF 500, “tanto per provare”. Avrete così l'impressione di essere voi a decidere. Poi riceverete l'accesso al vostro “account” sul sito web che vi consentirà di monitorare la presunta performance del vostro investimento. E ogni volta che vi collegherete, constaterete che i vostri investimenti stanno fruttando. **L'obiettivo che i truffatori perseguono, e che in questo caso hanno anche raggiunto, è di convincervi ad investire di più.**



## 3<sup>a</sup> fase: la conquista della fiducia

Constatando la buona performance dei vostri investimenti, il vostro scetticismo scompare e potreste addirittura essere contenti di ricevere una nuova chiamata del vostro consulente. Questo è proprio lo scopo dei truffatori: farvi credere di poter contare su una **consulenza personalizzata** per i vostri futuri investimenti. Questi malfattori padroneggiano bene l'arte della cosiddetta “ingegneria sociale”. Sanno infatti quali tecniche interpersonali usare per manipolare le loro vittime. In altri termini, all'inizio non sarete messi **direttamente sotto pressione**, ma solo indirettamente con **offerte** apparentemente disponibili solo **in misura limitata o per poco tempo**. Inoltre, questa nuova relazione di fiducia serve ad allontanarvi da ex partner finanziari di cui vi fidavate (per esempio la vostra banca). I truffatori aprono poi un conto (portafoglio o *wallet*) a vostro nome e con la vostra legittimazione presso veri e propri *trader* di criptovalute. Tuttavia, ad avere i diritti d'accesso al conto non siete solo voi (se mai lo siete), ma sono sempre i truffatori. Succede addirittura che questi malfattori prendano il controllo del vostro computer usando un software di manutenzione remota ed effettuino poi delle transazioni tramite il vostro e-banking.



#### 4ª fase: versamenti aggiuntivi

Ecco però cosa succede in realtà. Il giorno in cui decidete per un motivo qualsiasi di ritirare una parte del denaro investito dopo aver visto aumentare i vostri profitti per qualche tempo, scoprirete che non potete farlo. Allora il vostro consulente vi spiegherà, per esempio, che c'è stato un **crollò improvviso** o che avete dovuto dapprima pagare **un'elevata tassa**. A questo punto, il vostro consulente cercherà di convincervi – questa volta esercitando pressioni dirette e persino intimidendovi con vere e proprie minacce – della natura speciale dell'investimento, che richiede un'ulteriore iniezione di denaro affinché possiate assicurarvi i guadagni. In alcuni casi entra addirittura in scena anche un presunto superiore o addirittura il **"capo"** della supposta società finanziaria, che con la sua dichiarata autorevolezza cerca di tranquillizzarvi promettendovi ulteriori guadagni, a condizione di tener duro. Se però insistete nel volerne uscirne, vi verrà allora proposta **un'assicurazione contro le perdite** che avreste apparentemente potuto sottoscrivere fin dall'inizio, ma che, come gesto di buona volontà, vi consentono di concludere con effetto retroattivo. Niente di tutto questo è vero! Alla fine, sospettate di poter essere vittima di una truffa, ma nonostante il buon senso vi aggrappate ancora di più al vostro consulente di fiducia. Alla fine quest'ultimo sosterrà che può ancora trovare un modo per permettervi di recuperare il vostro denaro, a condizione però di **effettuare un pagamento anticipato per coprire le spese bancarie, legali o notarili...**



#### 5ª fase: la realizzazione della perdita

Qualsiasi cosa tentiate, **non ricupererete mai il vostro denaro**, tranne forse nella 1ª fase. Ma anche in quel caso si tratterà solo di piccole somme per tranquillizzarvi e continuare ad allettarvi. Ora avete finalmente capito di essere stati truffati.





## Alcune regole generali

- Guadagnare soldi facili senza rischiare perdite è un'illusione!
- Nessuno rivela "le dritte da insider" pubblicamente in Internet. Chi lo fa è perché in realtà non ne ha.
- Nessuno condivide strategie d'investimento promettenti con perfetti sconosciuti. D'altronde, perché dovrebbe?
- I consigli d'investimento pubblicizzati da personalità di spicco sono quasi sempre fasulli e servono solo da esca. Di solito, queste celebrità non sanno neppure che la loro immagine è utilizzata a questo fine.

## Cosa fare prima di lanciarsi in nuove forme d'investimento

- Siate molto prudenti, specialmente quando vi promettono alti rendimenti e settori d'investimento complessi come le criptovalute, il forex trading e il presunto trading di opzioni binarie. Prendetevi il tempo e informatevi consultando il maggior numero possibile di fonti diverse. Non lasciatevi mai mettere sotto pressione, né da consulenti né da offerte limitate nel tempo.
- Non lasciatevi accecare da promesse di rendimenti irrealistici. Nessun fornitore di servizi finanziari serio promette profitti superiori alla media in poco tempo.
- Verificate se il fornitore in questione è in possesso di una licenza FINMA ([www.finma.ch](http://www.finma.ch) → FINMA Public → Istituti, persone e prodotti autorizzati) o se figura sulla lista di allerta FINMA ([www.finma.ch](http://www.finma.ch) → FINMA Public → Lista di allerta). Se vi imbattete in offerte sospette, dovrete segnalarle alla FINMA con il modulo di notifica ([www.finma.ch](http://www.finma.ch) → FINMA Public → Notificare). Queste informazioni permettono alla FINMA di individuare i fornitori non autorizzati e di bandirli dal mercato.
- Consultate l'indice centrale delle ditte [www.zefix.ch](http://www.zefix.ch) e controllate l'estratto del registro di commercio per vedere se il vostro fornitore è presente.
- Nel caso di fornitori che operano dall'estero, effettuate una ricerca in Internet per capire chi ha messo le offerte online. Se vedete apparire anche solo uno o due avvisi di truffa, meglio lasciar stare.
- Rivolgetevi al vostro consulente bancario e a degli esperti di vostra fiducia per una valutazione professionale.

- Non affidate mai il vostro denaro a qualcuno che conoscete solo virtualmente.
- Non permettete mai a qualcuno che conoscete solo virtualmente di accedere in remoto al vostro computer (utilizzando software di manutenzione remota come TeamViewer, Anydesk, Supremo, ecc.)
- «Non buttate soldi dalla finestra!», ossia non tentate di recuperare i vostri soldi iniettando nuovi fondi. Non funziona!

## Cosa fare se siete vittima di una truffa sugli investimenti online

- Informate subito la vostra polizia comunale o cantonale e sporgete denuncia!
- Informate subito la vostra banca che le transazioni in questione erano fraudolente. Eventualmente, la banca riuscirà a bloccare il denaro prima che finisca nelle tasche dei truffatori.
- Se qualche tempo dopo siete contattati per telefono o e-mail da un presunto investigatore privato, avvocato o procuratore pubblico, è molto probabile che questo individuo faccia parte della stessa banda di truffatori. Non trasferite denaro neppure in quel caso.

Maggiori informazioni: [www.ebas.ch/investmentfraud](http://www.ebas.ch/investmentfraud)





Prevenzione Svizzera della Criminalità  
Casa dei Cantoni  
Speichergasse 6  
3001 Berna

[www.skppsc.ch](http://www.skppsc.ch)

Questo pieghevole è stato realizzato in collaborazione  
con la **Scuola Universitaria Professionale di Lucerna**  
e «**eBanking – ma sicuro!**».

[www.ebas.ch](http://www.ebas.ch) | [www.ebankingmasicuro.ch](http://www.ebankingmasicuro.ch)

Lucerne University of  
Applied Sciences and Arts

**eBanking ma sicuro!**

**HOCHSCHULE  
LUZERN**

**Informatik**  
FH Zentralschweiz

Marzo 2021

