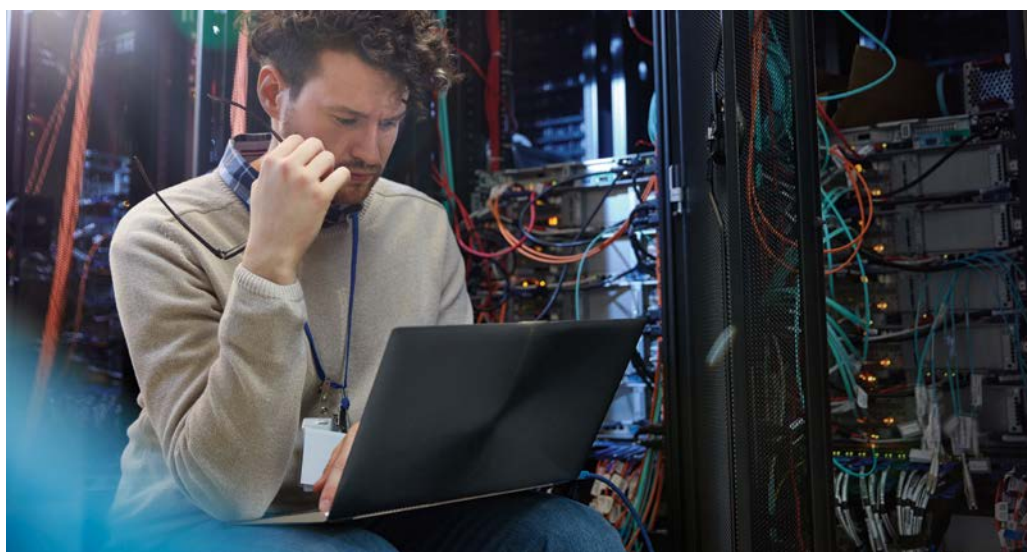


# Truffe nel traffico dei pagamenti – ecco come tutelare la vostra azienda

Le truffe nel traffico dei pagamenti espongono il mondo imprenditoriale svizzero a notevoli danni finanziari, e la tendenza è in crescita. Quali sono i segnali d'allarme e come potete tutelare attivamente voi e la vostra azienda?



## Business e-mail compromise

Il business e-mail compromise è considerato una delle maggiori minacce cibernetiche sia per l'economia sia per le singole aziende. Di seguito illustriamo come si svolge questa truffa.

1

### Spionaggio

- I truffatori raccolgono le informazioni disponibili pubblicamente sull'azienda e sui suoi collaboratori.
- I truffatori entrano nell'infrastruttura informatica dell'azienda o di un partner d'affari (p. es. attraverso attacchi phishing).

2

### Inganno

- I truffatori contattano il reparto finanziario dell'azienda via e-mail.
- Con un pretesto chiedono di effettuare un pagamento in scadenza su un conto bancario finora sconosciuto.

3

### Esecuzione del pagamento

- Una persona ingannata del reparto finanziario dispone il pagamento sul conto bancario controllato dai truffatori.



Una truffa da parte di presunti CEO andata a buon fine può portare la vostra azienda alla bancarotta. I truffatori vogliono accedere al vostro patrimonio aziendale. Di seguito illustriamo come si svolge questa truffa:



### Cosa occorre sapere:

- Ogni impresa può finire nel mirino dei truffatori, indipendentemente da dimensioni, settore o domicilio.
- Un'infrastruttura informatica non adeguatamente protetta apre un varco ai truffatori.
- Le comunicazioni via e-mail non sono sicure e possono essere manipolate.

Come imprenditori non siete inermi di fronte a questi rischi. Con i seguenti accorgimenti renderete più difficile il lavoro dei truffatori ed eviterete danni finanziari.

### Ecco come tutelarvi:

- Proteggete la vostra infrastruttura informatica con gli standard più aggiornati.
- Definite con i vostri clienti e fornitori diversi canali di comunicazione e mantenetevi aggiornati (p. es. telefono, cellulare, e-mail, indirizzo postale).
- Se ricevete dai vostri partner d'affari istruzioni di pagamento divergenti (p. es. una banca o un numero di conto diversi), verificateli. Importante: fatelo su un canale sicuro, ad esempio utilizzando un numero di telefono già convalidato.

- Instaurate processi contabili in grado di impedire l'esecuzione di transazioni fraudolente, ossia:
  - informate i vostri reparti interni interessati in merito ai fenomeni del business e-mail compromise e della truffa del CEO.
  - evitate i diritti di firma individuale.
  - esortate i vostri collaboratori a segnalare immediatamente a un servizio interno centrale osservazioni ed eventi sospetti.
- Verificate quali informazioni sulla vostra azienda e sui vostri collaboratori desiderate pubblicare. Limitatele al minimo.
- Valutate l'opportunità di denunciare la frode anche se non avete subito danni finanziari.
- In caso di frode, informate immediatamente la vostra banca principale. In questo modo la banca può prendere le misure di protezione necessarie e reclamare una transazione fraudolenta in caso di danni.

Il vostro consulente sarà lieto di rispondere a tutte le vostre domande.



**CREDIT SUISSE (Svizzera) SA**

Casella postale 100

CH-8070 Zurigo

**credit-suisse.com**

Le informazioni fornite nel presente documento costituiscono materiale di marketing. Non si tratta di una consulenza d'investimento o di altro tipo basata su una considerazione della situazione personale del destinatario né del risultato di una ricerca obiettiva o indipendente. Le informazioni fornite nel presente documento non sono giuridicamente vincolanti e non costituiscono né un'offerta né un invito a effettuare alcun tipo di operazione finanziaria. Queste informazioni sono state redatte da Credit Suisse Group AG e/o dalle sue affiliate (di seguito «CS») con la massima cura e secondo scienza e coscienza. Le informazioni e le opinioni contenute nel presente documento sono quelle di CS al momento della redazione e possono cambiare in qualsiasi momento senza preavviso. Esse sono state ricavate da fonti ritenute attendibili. CS non fornisce alcuna garanzia circa il contenuto e la completezza delle informazioni e, dove legalmente consentito, declina qualsiasi responsabilità per eventuali perdite connesse all'uso delle stesse. Salvo indicazioni contrarie, tutti i dati non sono certificati. Le informazioni fornite nel presente documento sono a uso esclusivo del destinatario. Né le presenti informazioni né eventuali copie delle stesse possono essere inviate, consegnate o distribuite negli Stati Uniti o a US Person (ai sensi della Regulation S dello US Securities Act del 1933, e successive modifiche). Il presente documento non può essere riprodotto, né totalmente né parzialmente, senza l'autorizzazione scritta di CS. I suoi dati personali saranno trattati in conformità con la politica sulla privacy di Credit Suisse, disponibile dal suo domicilio tramite il sito web ufficiale di Credit Suisse <https://www.credit-suisse.com>. Al fine di fornirle documentazione di marketing relativa a prodotti e servizi, Credit Suisse Group AG e le sue società affiliate possono trattare i suoi dati personali di base (ovvero dettagli di contatto, come nome e indirizzo e-mail) fino a quando lei non provveda a comunicarci che non desidera più ricevere tale documentazione. Può decidere di non ricevere più la documentazione informando in qualsiasi momento il suo Relationship Manager.

Copyright © 2020 Credit Suisse Group AG e/o sue affiliate. Tutti i diritti riservati.