

# RISCHI LEGATI A POSSIBILI UTILIZZI DI UNA CARTA DI CREDITO O DI UN CONTO CORRENTE

## INTRODUZIONE

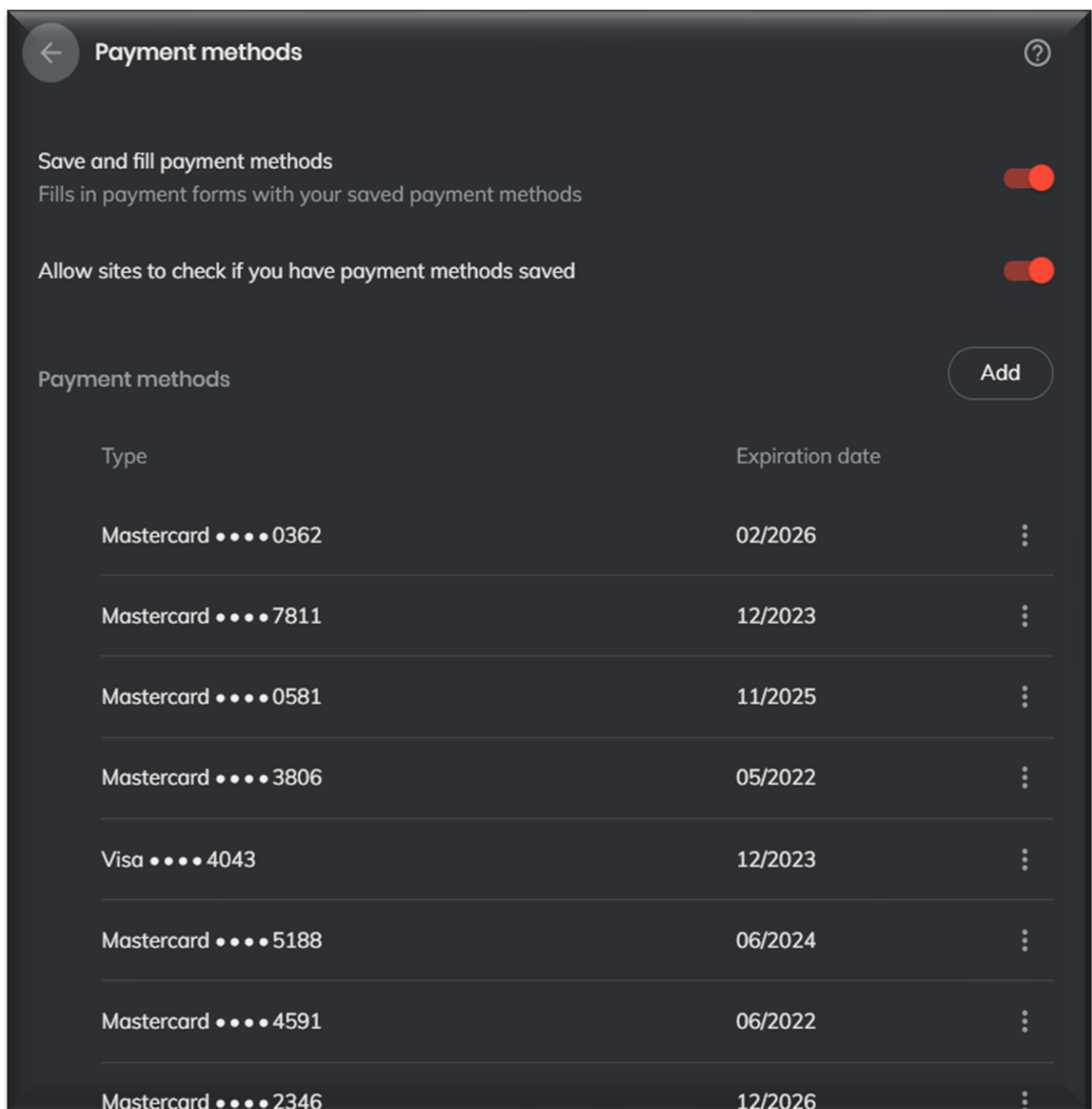
### FORMATO DELLE CARTE DI CREDITO

Le carte di credito sono realizzate in modo molto semplice: **numero di 16 cifre** stampato sul **fronte**, ben in evidenza, **data di scadenza** e, sul **retro**, in dimensioni minori, il codice **CVV di 3** (massimo 4, per alcune carte) **cifre**; quest'ultima **brevissima sequenza** consente **innumerevoli utilizzi**, se conosciuta. E' molto semplice per un malintenzionato venire a conoscenza di questi 3 dati.



## COME SI VIENE A CONOSCENZA DI QUESTI DATI?

Poniamo il caso che per qualche motivo siano venuti in possesso del numero, data di scadenza e CVV della vostra carta di credito e si tratti di un parente, amico o conoscente, magari che non vi è proprio simpatico, il quale vorrebbe vendicarsi per un torto subito, o altro; potreste avergli ad esempio **prestato** la carta **in passato** per pagare addebiti online, se in quel momento non aveva disponibile la cifra richiesta, anche per **pagamenti di poco conto**, come 1-2 €, dimenticandovene. Ora vi ritrovate **memorizzati nel browser** di quella persona i dati della vostra carta, e vorrebbe utilizzarla in qualche modo poco legittimo.



## METODI DI UTILIZZO

### COSA E' POSSIBILE E NON E' POSSIBILE FARE

Ebbene, le possibilità sono tante. Ovviamente **non si potranno mai prelevare contanti dagli ATM**, almeno **non direttamente**, ma ci sono numerosi casi di utilizzo, che ora vediamo.

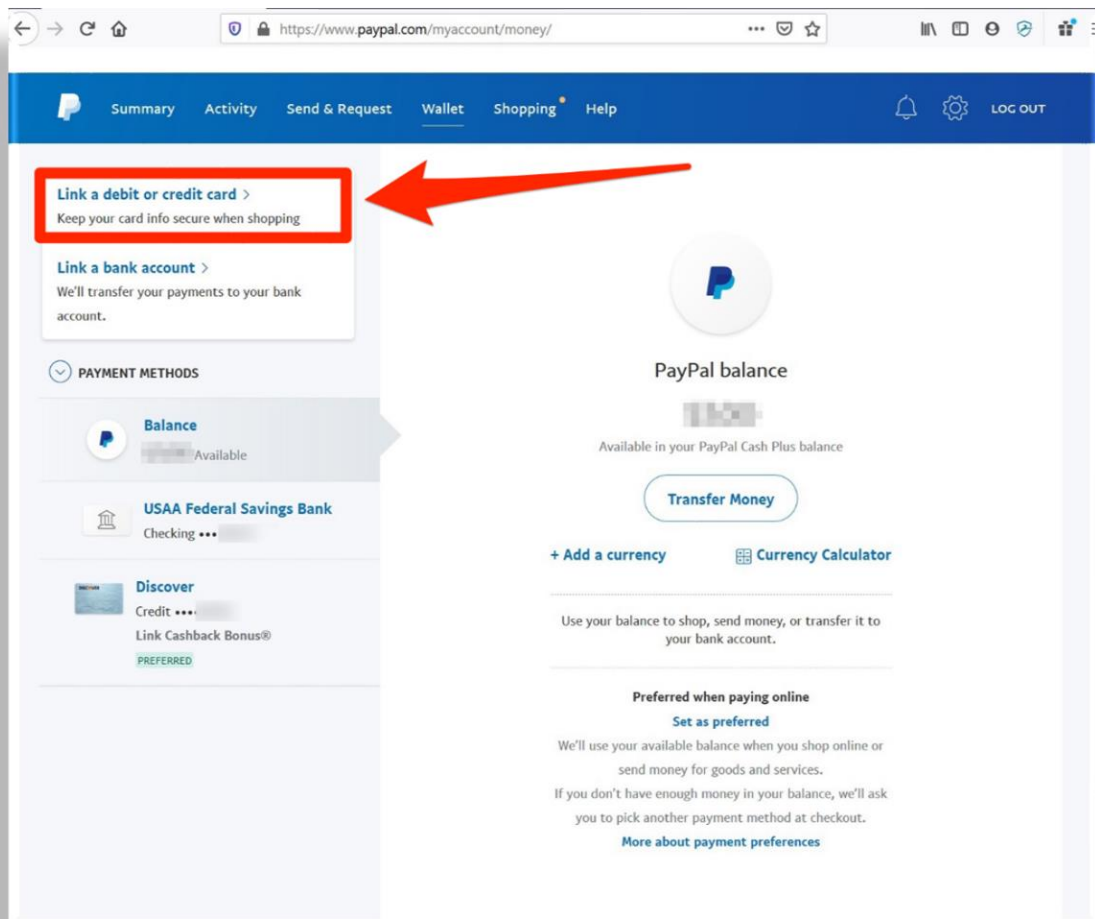


### ASSOCIAZIONI A METODI DI PAGAMENTO VIRTUALI

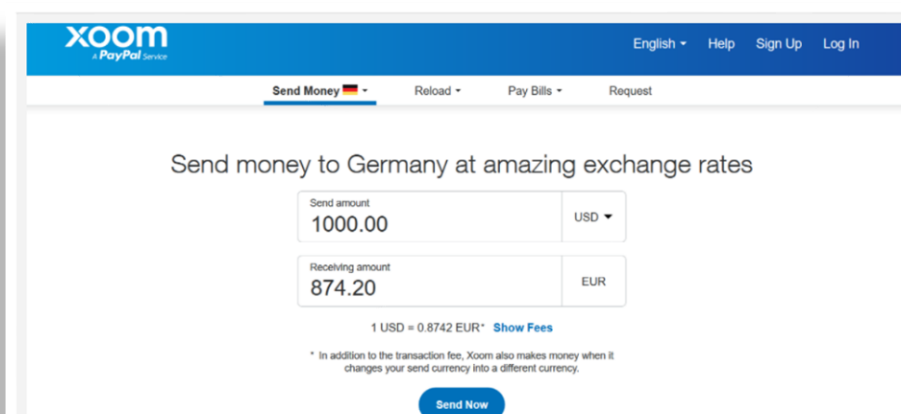
1. **Associare la carta ad un conto PayPal:** partendo da una connessione protetta da **VPN**, che copre il reale indirizzo IP, che è un po' come la targa dell'automobile e consente di risalire immediatamente al proprietario della linea dalla quale si è connessi, si crea un account fake di PayPal, ovvero inserendo **dati random**, non riferiti ad alcun soggetto esistente, con una **e-mail** altrettanto **fittizia** (magari tramite servizi che generano caselle **e-mail temporanee**) e, in caso venisse richiesto obbligatoriamente anche un **numero di telefono**, fornendo un **numero VoIP**, di fatto senza essere intestato a nessuno.

A questo punto è possibile **associare la carta** avente i dati in possesso: numero di 16 cifre, data di scadenza e CVV; nel caso tale carta non fosse già associata ad alcun conto PayPal, sarà ora semplicissimo effettuare acquisti online utilizzando i fondi presenti su questa carta di credito, poiché PayPal è un metodo di pagamento **accettato** pressoché **ovunque**, da tutti gli e-commerce. Sarà inoltre possibile **inviare denaro virtuale** ad un altro account PayPal. In questo caso può essere effettuato un **passaggio intermedio**: acquistare da siti come **bundle.com** una **carta Visa o Mastercard virtuale**, che è possibile intestare a chi si desidera, utilizzando **dati a piacere**; tale carta verrà associata all'account PayPal secondario. Il denaro inviato arriverà sotto forma di **credito PayPal** disponibile, che poi verrà **trasferito** sulla **carta virtuale**. Ora,

con essa, si può inviare direttamente il denaro tramite app di credito tipo *Revolut*, *Hype*, *N26*, etc. al proprio conto legittimo, oppure, per maggiore cautela, acquistare dei Bitcoin o altre criptomonete, che potranno essere ripulite inviandole ad un Mixer (servizio a pagamento + fee che riceve in entrata Bitcoin e li rimanda al wallet ripuliti da tutte le transazioni precedenti, quindi di fatto non rintracciabili alla fonte d'acquisto).



Ultimamente, PayPal ha avviato anche un servizio di invio e ricezione denaro in tutto il mondo, chiamato **Xoom**. E' quindi possibile effettuare il login a Xoom direttamente dall'account PayPal creato appositamente per associare la carta altrui ed utilizzarla per inviare il denaro in essa contenuto a chi si vuole (anche a se stessi, ma è una pratica del tutto sconsigliata). La truffa ideale sarebbe quindi inviarli ad una terza persona che collabori e faccia finta di essere all'oscuro di tutto. Il denaro verrà incassato in contanti in un punto Xoom abilitato (sono numerosi, in tutta Italia).



2. **Amazon e Amazon Pay:** il secondo metodo più rapido per poter beneficiare del credito presente in questa carta è quello di **associarla ad un account Amazon**. È possibile **aprire un account Amazon senza fornire documenti** di identità o altre informazioni sensibili e **associare carte e conti bancari**. In questo caso quindi, qualora si fosse a conoscenza di un **IBAN** e relativo codice **BIC/SWIFT**, sarà possibile eseguire la stessa operazione. Ora si può utilizzare il metodo di pagamento scelto per fare **acquisti** di ogni tipo sulla **piattaforma Amazon**. In questo caso, diversamente da PayPal, è dunque possibile acquistare **soltanto articoli in vendita su Amazon**.

Credit & Debit Cards Expires [Add credit/debit card](#)

Amazon.com accepts all major credit & debit cards.

Enter your credit card (Step 1 of 2)

Card number

Name on card

Expiration date

06 2015

Cancel Next

In alcuni casi, soprattutto quando il nominativo e l'indirizzo del proprietario della carta (o dell'IBAN) non coincidono con quelli del destinatario della merce, può essere richiesta una **verifica**, che non consiste in altro che nel **reinserimento** delle 3 cifre del codice **CVV**.

amazon

**Please re-enter your payment information.**

We want to make sure this is an authorized use of your account. This is for verification purposes and any gift card or promotional balances will be automatically applied to your order before attempting to charge your card.

**Enter your card information**

**Credit or Debit Card**  
Enter your card information

Name on card Card number Expiration date

01 2017

[Add your card](#)

Do you need help? Explore our [Help pages](#) or [contact us](#)

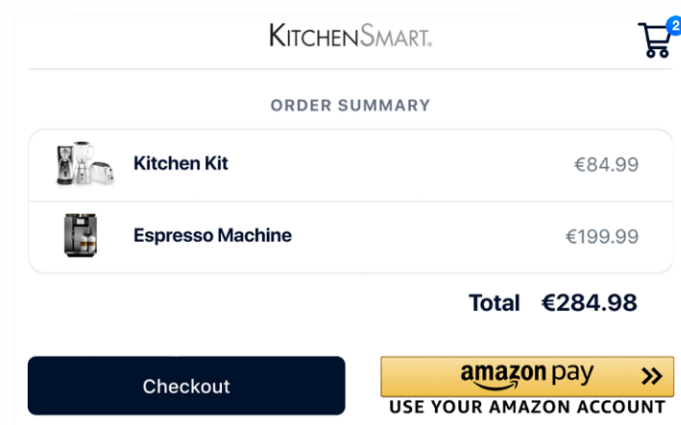


N.B.: quasi mai viene scelto l'indirizzo personale di casa, ma vengono fatti inviare i prodotti acquistati ad un **Locker**, possibilmente abbastanza lontano dalla vera località di residenza, dove ci si recherà con un **codice** che verrà fornito da Amazon per poter aprire lo sportello del locker e ritirare la merce.

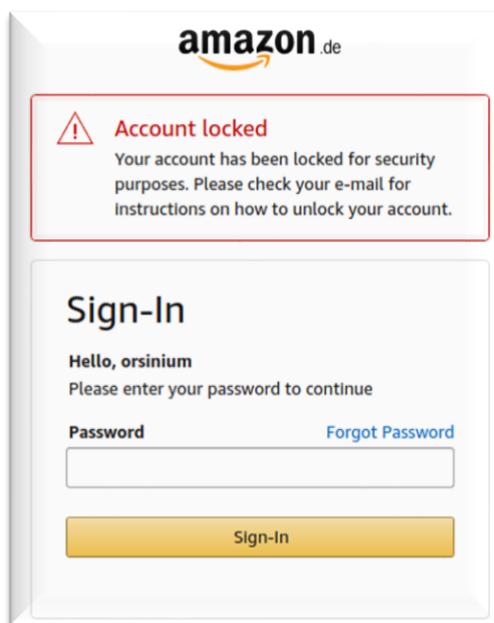
Piccola nota: non viene mai inserito il vero numero di cellulare, ma utilizzando un **numero virtuale** in grado di ricevere SMS, oppure un **VoIP gratuito** ottenuto, ad esempio, tramite **app** come *Dingtone*.



Non tutti sanno, inoltre, che esiste un **metodo di pagamento** del tutto simile a PayPal, chiamato **Amazon Pay** e legato strettamente ai **metodi di pagamento associati all'account Amazon**. Non tutti i venditori accettano Amazon Pay, ma negli ultimi tempi si sta diffondendo ed ha ora una buona reputazione e affidabilità. Qualora ci si imbatta in un articolo in vendita online acquistabile con **Amazon Pay**, è possibile utilizzare la **carta** in precedenza **associata ad Amazon** per pagare.

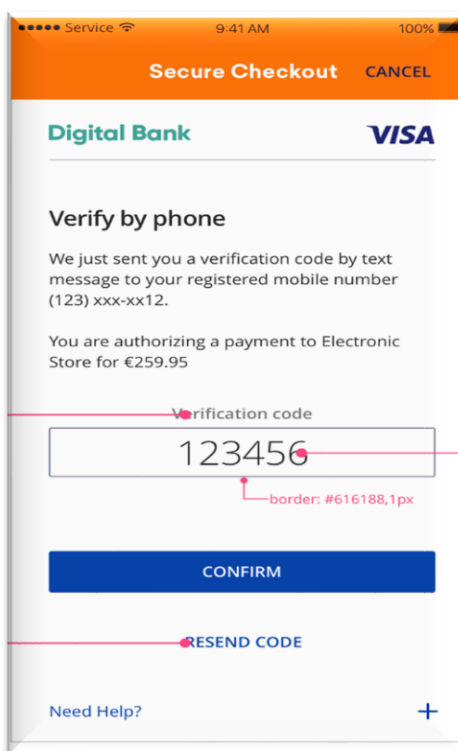


In rari casi è accaduto che Amazon abbia bollato come tentativo di frode l'utilizzo di una carta avente per proprietario un soggetto con un **nome** ed un **indirizzo** differenti da quelli indicati in fase di creazione dell'**account fittizio**. In questi casi si sono riservati il diritto di **annullare** tutti gli **ordini effettuati**, impedendo così la ricezione della merce. In seguito è stato anche apposto a tale account un **ban permanente**.



## 3D SECURE: IN COSA CONSISTE E QUANDO E' PRESENTE

Il **vantaggio** enorme, per i truffatori, consiste nel fatto che, una volta associata la carta ad Amazon, viene **abolito** il sistema **3D Secure**, ovvero la **verifica in 2 passaggi** per l'acquisto, che consiste nell'invio di un **SMS** (o una **notifica push**) al telefono del **proprietario della carta** contenente un **codice**, che quindi, non disponendo del cellulare di quella persona, **non potrebbe essere conosciuto** e inserito nella casella di controllo, e sarebbe allora **impossibile completare** il pagamento.

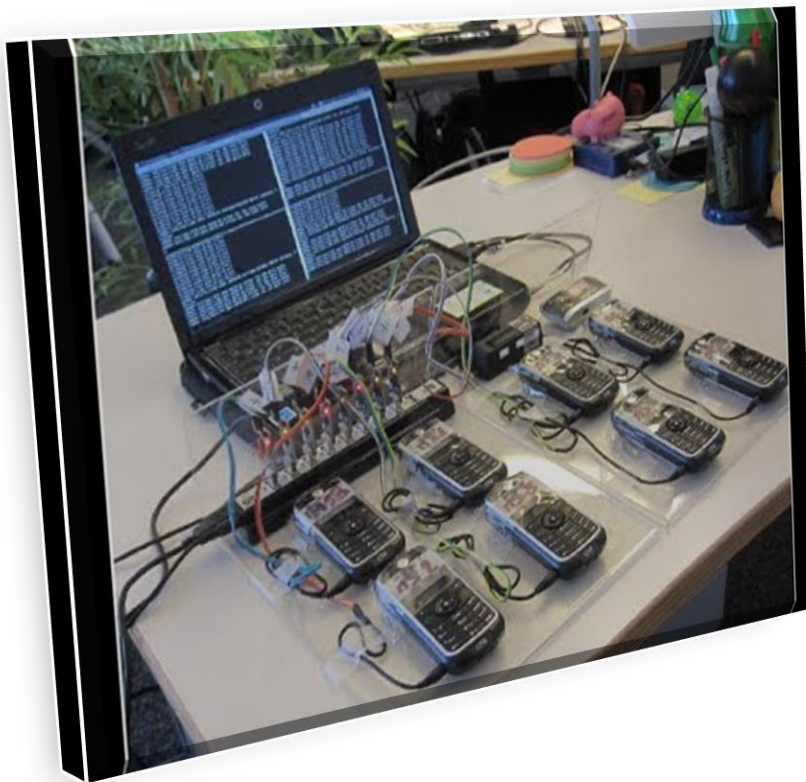


## BYPASS DI 3D SECURE

**Siti poco popolari:** esistono inoltre alcuni siti che permettono gli acquisti con carta di credito, **senza utilizzare il 3D Secure**. In questo caso è sufficiente quindi inserire i dati della carta di credito, **senza invio del codice SMS** al numero del proprietario della carta.

**SMS sniffing e Social Engineering:** se non è stato possibile associare la carta ad un account PayPal o Amazon (ma anche Skrill, etc.) e si vuole a tutti i costi fare un trasferimento di denaro o degli acquisti, ma il sistema avvia il **3D Secure**, si può **intercettare l'SMS** contenente il codice da inserire **per completare la transazione**, che altrimenti verrà negata.

A questo scopo può essere utilizzato un **IMSI Catcher**, ma funziona soltanto se il **cellulare** del quale si vogliono leggere gli SMS è relativamente **vicino**.



Oppure è possibile leggere il messaggio tramite un **RAT (Remote Administration Tool)** inviato al proprietario della carta. Un RAT non è altro che un **malware** composto da due parti: **Client** e **Server**. Attraverso il **Client** si può osservare e **manovrare da remoto** il telefono della **vittima**, sul quale verrà installato il lato **Server**. I metodi per installare un RAT sono infiniti, ma la strategia più semplice è il **Social Engineering**: se abbastanza abili, potranno tentare l'**invio del server del RAT** allo smartphone del proprietario della carta con una **scusa**, dicendo, ad esempio, di stare passando un'**app utile**, interessante,



oppure ancora un **gioco** divertente o altro, sulla base dei **gusti** del soggetto e di **quanto lo si conosce bene e si fida**, altrimenti non aprirà mai il file ed il client RAT non verrà avviato.



Il **Social Engineering** può essere applicato in **altri modi**, oltre che per l'installazione di un Server RAT. Una possibile strategia consiste nell'avviare la transazione con la carta in questione, inviare l'SMS col codice 3D Secure al numero del proprietario e subito **inviargli un SMS**, da un **numero diverso dal numero reale** e conosciuto, con scritto qualcosa del tipo: **«Ciao, ho sbagliato ad inviare un codice al tuo numero, ma serve per un mio accesso, me lo puoi comunicare per favore? Grazie mille e scusa»**; se il soggetto vittima non è troppo astuto (ed è abbastanza gentile da perdere il tempo e 15 cents di SMS), **risponderà al numero che utilizzato**, scrivendo il **codice** che necessario per la **convalida** dell'operazione.

In realtà i **metodi** per ottenere il codice **possono essere infiniti**, basta essere abbastanza ingegnosi e scaltri da non essere riconosciuti.

## CONTO CORRENTE AL POSTO DI CARTA DI CREDITO

**Bonifici SEPA**: alcuni siti permettono il **pagamento** tramite **addebito diretto** con **bonifico SEPA**; in questo caso si deve **conoscere l'IBAN** e il codice **BIC** (o **SWIFT**), talvolta neanche del tutto preciso, basta

che **almeno 5 caratteri** siano identici a quello reale. Anche in questo caso, però, non è difficile venire a conoscenza del BIC tramite l'*Ingegneria Sociale* suddetta.

**Secure Order Form**

Payment Options For **France**

- ☐ Credit & Debit Cards
- ☒ **SEPA** SEPA Direct Debit
- ☐ **Skrill** (Moneybookers)
- [More Payment Options](#)

IBAN \* DE09100100101234567893 ✓

BIC \*

Shopper Details

First Name \* Jane ✓

Last Name \* Shopper ✓

Email Address \* jane.shopper@email.com ✓

Address \* 71 rue Jean Vilar ✓

City \* Toulouse ✓

Country \* France (change) ✓

Zip/Postal Code \* 33130 ✓

Order Information Currency: EUR

sepa prod €8.73

1

[Have a coupon?](#)

Total €8.73

**McAfee SECURE**  
CLICK TO VERIFY

**COMODO**  
AUTHENTIC  
SECURE  
COMODO SSL

## CONCLUSIONI

Inavvertitamente potreste rivelare informazioni finanziarie importantissime, pur non ritenendole di nessuna utilità, mentre sono preziosi dati utilizzati da malintenzionati per effettuare truffe o sperperare il credito di ignari utenti.

*Novara, 23/04/2021*

Dr. Kira Smith