



CONFCONSUMATORI
CONFEDERAZIONE
GENERALE DEI
CONSUMATORI

L'ULTIMA FRONTIERA DELLE TRUFFE: DALLO SMARTPHONE AL WEB

Avv. Manuela Friggeri - Consulente Confconsumatori

Realizzato nell'ambito del Programma generale di intervento della Regione Emilia-Romagna con l'utilizzo dei fondi del Ministero dello sviluppo economico. D.M. 10/08/2020

PRIMA DI TUTTO...COSA SIGNIFICA TRUFFA?

Articolo 640 Codice Penale

- ▶ *Chiunque, con artifici o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.*

QUINDI... affinché si possa parlare di truffa dal punto di vista penale devono verificarsi due presupposti fondamentali:

1. **ARTIFIZIO** = simulazione o dissimulazione della realtà, tale da indurre in errore il soggetto passivo
2. **RAGGIRO** = ogni macchinazione atta a far scambiare il falso con il vero

...E il Codice del Consumo cosa dice?

- **PRATICHE COMMERCIALI SCORRETTE** = sono quelle idonee a falsare in misura apprezzabile il comportamento economico del consumatore medio al quale sono dirette. Si distinguono in:
- **INGANNEVOLI**: quando sono idonee a indurre in errore il consumatore medio, falsandone il processo decisionale
- **AGGRESSIVE**: quando l'impresa agisce con molestie, coercizione o altre forme di indebito condizionamento

I PIÙ COMUNI TIPI DI TRUFFA

- ▶  **Vishing:** frode attraverso contatto telefonico o messaggio vocale
- ▶  **Smishing:** estorsione di informazioni tramite un SMS sul cellulare
- ▶  **Phishing:** e-mail che riproducono i loghi e la grafica di quelle ufficiali

In tutti i casi la finalità è quella di **ottenere dati personali** che verranno utilizzati per accedere ai nostri soldi o ricavarne altri vantaggi.

TRUFFE TELEFONICHE e CHIAMATE INGANNEVOLI



Esempio di approcci telefonici INGANNEVOLI:

- Il contratto di energia sta scadendo...
- Il mercato tutelato finisce a fine anno...
- La normativa vigente prevede di installare un rilevatore di gas...
- C'è una promozione per cui ci mettono la fibra gratis...
- Il precedente contratto con il suo gestore è stato disdetto e abbiamo assorbito tutto noi...

È MOLTO FACILE CADERE NELLA TRAPPOLA!

... perché dopo averci elencato tutti i vantaggi dell'offerta, l'operatore attiva una procedura di registrazione del contratto il più delle volte **incomprensibile**, richiedendoci di fornire dati personali e consensi.

Esempio =



ATTENZIONE!

Il contratto concluso telefonicamente è valido a tutti gli effetti ed è praticamente impossibile, a posteriori, dimostrare che quanto abbiamo registrato è difforme da quanto ci è stato detto solo pochi minuti prima.

Viene registrata solo la parte dei **consensi** e non anche la parte di telefonata nella quale mi hanno spiegato i costi e i vantaggi di questa offerta.

COME MI TUTELO PREVENTIVAMENTE?

- ▶ Individua chi ti chiama. Chi ti contatta deve dichiarare lo **scopo** della chiamata e la **società** per la quale ti contatta.
- ▶ Non avere fretta. Prenditi il **tempo** per capire e fare domande.
- ▶ Occhio al **prezzo finale** e diffida di sconti eccessivi.
- ▶ Non c'è obbligo di accettare nessun contratto proposto telefonicamente.
- ▶ Se mi chiama un mio fornitore (es. di servizi telefonici o energetici) **NON mi chiederà mai i DATI personali** (del contratto, bancari, PIN del bancomat, Codice fiscale, etc).
- ▶ **NON** possono fare **modifiche unilaterali** del contratto per telefono.

COSA POSSIAMO FARE QUANDO ACCETTIAMO TELEFONICAMENTE UN CONTRATTO DIVERSO DA QUELLO PROMESSO?

Fortunatamente ci viene in soccorso il **diritto di recesso**, detto comunemente «diritto al ripensamento» che possiamo esercitare **entro 14 giorni** dalla conclusione del contratto.

PERCHÉ HANNO IL NOSTRO NUMERO?

- ▶ Spesso lo abbiamo fornito noi, inconsapevolmente, quando abbiamo sottoscritto un contratto o attivato una tessera fedeltà.
- ▶ Nell'informativa sul trattamento dati personali che ci viene fornita, tra le caselle che barriamo distrattamente ne sono alcune che autorizzano l'utilizzo dei dati per attività ulteriori rispetto all'oggetto e allo scopo del contratto principale (messaggi promozionali, profilazione, etc.).

**COME
POSSIAMO
REVOCARE IL
CONSENSO
ALL'USO DEI
NOSTRI DATI
PER SCOPI
PROMOZIONALI?**

- 1) Chiedere all'operatore di eliminare il nostro contatto
- 2) Iscrivere al **Registro delle opposizioni (RPO)** da luglio 2022 attivo anche per il cellulari.

Si accede tramite il sito

<https://registrodelleopposizioni.it/cittadino/> e ci sono vari canali di iscrizione. **RICORDATE: l'iscrizione non è immediata** e il divieto è riferito solamente ai consensi già dati. Se dopo l'iscrizione fornisco altri consensi, questi **NON** sono inclusi!

- 3) Rivolgersi al **Garante della Privacy:**

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/4535524>

A photograph of a man with grey hair and glasses, seen from the side, looking at a smartphone. In the background, a laptop screen displays a data chart. The image is partially obscured by a white diagonal shape that contains text.

SMS E MAIL INGANNEVOLI

Sempre più spesso le truffe avvengono attraverso SMS e tramite mail, generalmente contenenti **link** da cliccare e/o documenti da scaricare finalizzati a:

- **Carpire dati personali**
- **Introdurre virus**
- **Prelevare somme dal credito telefonico e/o da eventuale carta di credito o dal conto corrente (vedi truffe bancarie)**

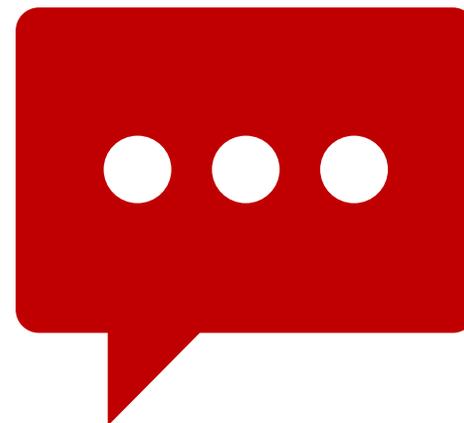
COME RICONOSCERE LE MAIL O GLI SMS INGANNEVOLI/FALSI?

ESEMPI DI TRUFFE PIÙ DIFFUSE:

- ▶ Conto corrente bloccato
- ▶ Pagamento non andato a buon fine
- ▶ Pacco trattenuto o in consegna
- ▶ Vincita di un premio
- ▶ Problemi di sicurezza legati ad un conto corrente
- ▶ Messaggio dell'INPS
- ▶ Messaggio del Ministero della Salute sul Green Pass

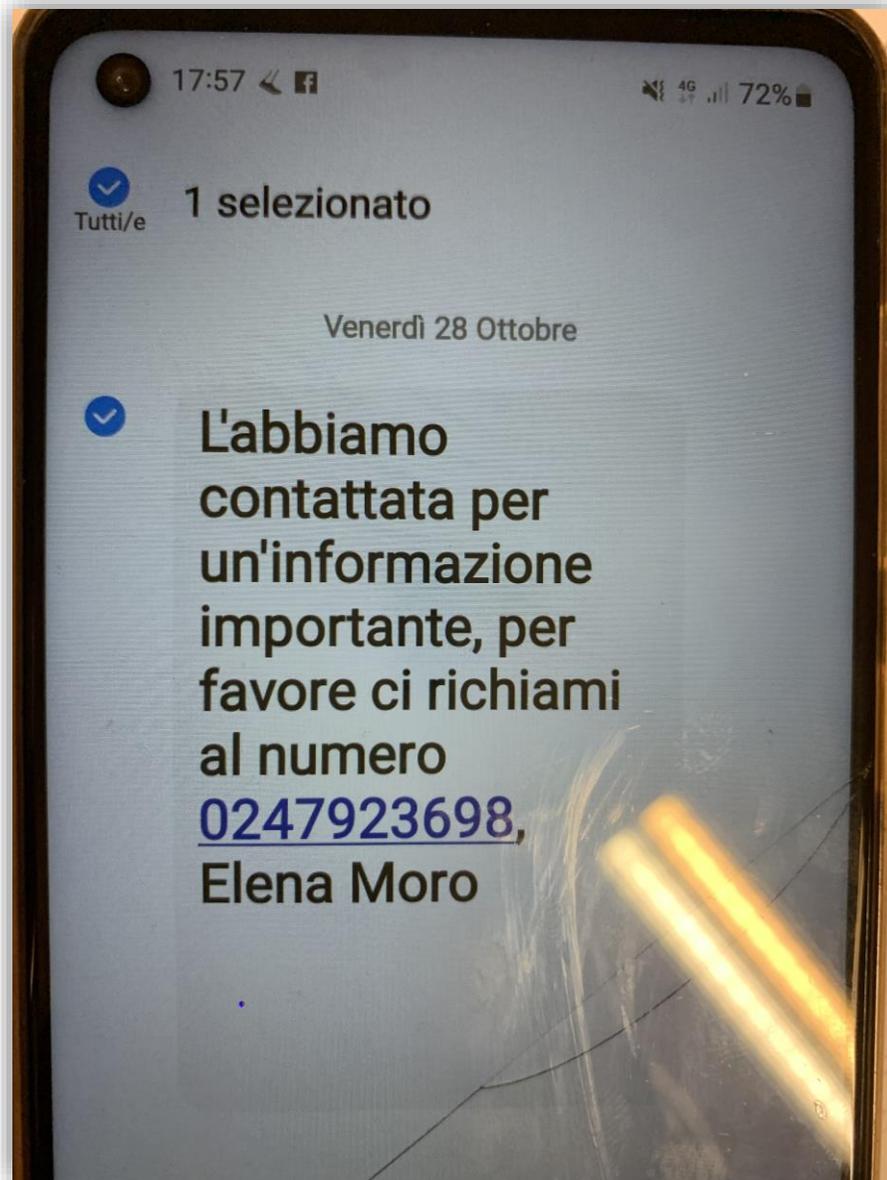
COME RICONOSCERE UN MESSAGGIO DI TESTO FALSO?

- ▶ ***Il messaggio non è pertinente:*** l'utente non ha motivo di aspettarsi il messaggio ricevuto, che non è legato a nessuna attività intrapresa negli ultimi giorni.
- ▶ ***Il messaggio trasmette una certa urgenza:*** nel testo viene comunicata un'emergenza e viene richiesto di intervenire il prima possibile per evitare conseguenze disastrose.
- ▶ ***Il mittente è un numero sconosciuto:*** il numero non è presente nella rubrica o contiene meno cifre rispetto a un numero di telefono normale.
- ▶ ***Il messaggio contiene errori ortografici e grammaticali:*** nella maggior parte degli esempi i messaggi sono scritti male sia dal punto di vista stilistico che grammaticale, e a volte contengono anche errori di ortografia grossolani.
- ▶ ***Il messaggio contiene un link sospetto:*** i link fraudolenti spesso iniziano con il prefisso HTTP (senza la S finale) oppure simulano il nome dell'azienda autentica inserendo altre parole o lettere, come unicredit-bank-italia.com.



COME DIFENDERSI?

- ▶ **Disattivare le comunicazioni pubblicitarie** da parte delle aziende e dei negozi presso cui fai acquisti - la maggior parte dei servizi si affidano a partner terzi per il **marketing**, questi potrebbero gestire gli elenchi dei contatti in modi illeciti.
- ▶ **Non rispondere ai messaggi non richiesti**, neanche per chiedere di smettere di riceverli.
- ▶ **Non fare clic sui link** contenuti in messaggi di mittenti sconosciuti o sospetti.
- ▶ **Non condividere i dati personali e finanziari** tramite il link di SMS o mail.
- ▶ **Non condividere numero di telefono e indirizzo e-mail online**, ad esempio per partecipare a offerte o accedere a contenuti
- ▶ **Aggiornare periodicamente il sistema operativo del telefono**



17:57

4G 72%

Tutti/e 1 selezionato

Venerdì 28 Ottobre

L'abbiamo
contattata per
un'informazione
importante, per
favore ci richiami
al numero
0247923698,
Elena Moro

17:17 ↗

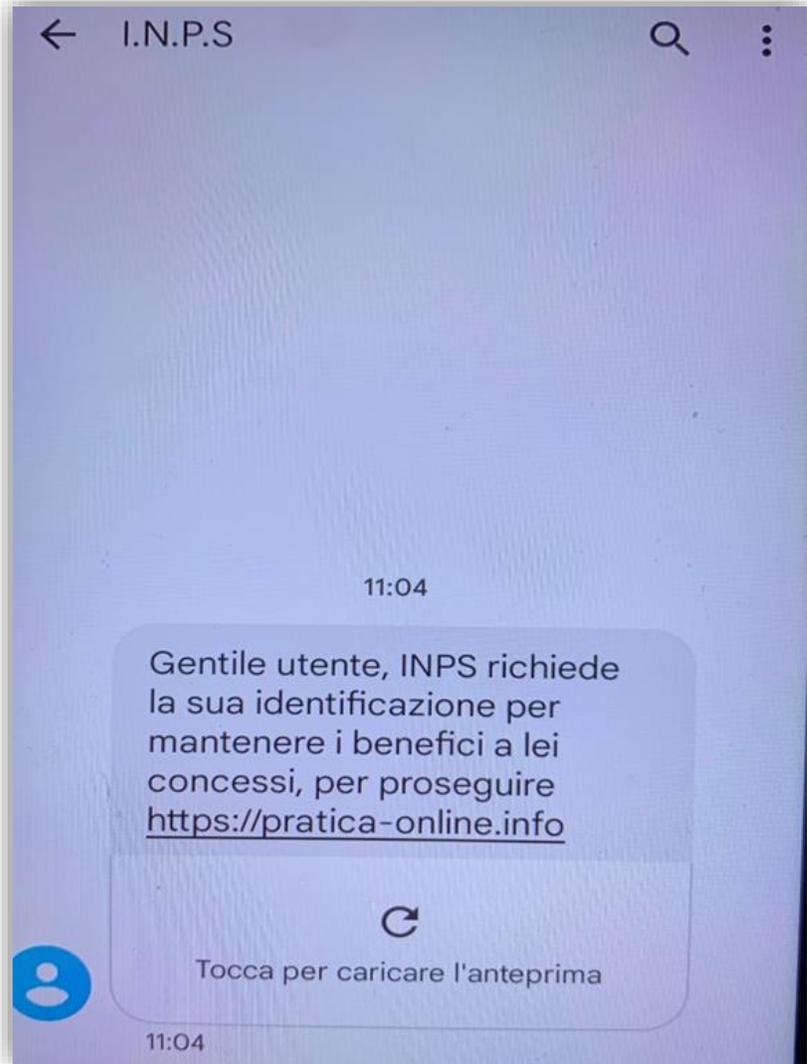


+39 350 1194225 >

SMS

30 ott 2021, 11:36

Il tuo pacco è stato trattenuto presso il nostro centro di spedizione. Si prega di seguire le istruzioni qui: <http://inutol.com/GIIRhzP>



Il metodo piu facile per risparmiare energia



E-Energy <umkiwv@askolsers.hz.cz>

A

Criteria di conservazione Junk Email (30 giorni)

Fine validità 18/12/2022

 L'elemento scadrà tra 26 giorni. Per mantenere l'elemento più a lungo, applicare criteri di conservazione diversi.
I collegamenti e altre funzionalità all'interno del messaggio sono stati disabilitati. Per riattivare le funzionalità, spostare il messaggio nella cartella Posta in arrivo.
Messaggio inoltrato in data 18/11/2022 08:54.
Le interruzioni di riga in eccesso sono state rimosse dal messaggio.

Il modo più semplice per risparmiare energia elettrica >> <<https://kimonerti.wiki/eu2/>>

Usate gli elettrodomestici esattamente come prima E PAGATE DUE VOLTEMENO!

Iniziate a risparmiare con E-Energy <<https://kimonerti.wiki/eu3/>> già oggi!

E-Energy conserva questa energia ricevuta e la ridà sotto forma di consumo attivo all'elettrodomestico che si trova sullo stesso circuito.

Risparmio del -50%! + Sconto -50%!

Il tempo necessario per risparmiare quanto speso in una famiglia di 3 persone è di due mesi e mezzo di utilizzo.

Dove si usa E-Energy Electricity Saver

Appartamenti e case private. Uffici.

Palestre e centri estetici. Negozi.

Bar e ristoranti. Officine meccaniche.

Principio di funzionamento di E-Energy >> <<https://kimonerti.wiki/eu4/>>

Investimento intelligente per difendere il budget.

La Settimana del Black Friday è arrivata



Amazon.it <promotion-it@amazon.it>

A [redacted]

Criteri di conservazione Junk Email (30 giorni)

Fine validità 18/12/2022

Rispondi Rispo

i L'elemento scadrà tra 26 giorni. Per mantenere l'elemento più a lungo, applicare criteri di conservazione diversi. I collegamenti e altre funzionalità all'interno del messaggio sono stati disabilitati. Per riattivare le funzionalità, spostare il messaggio nella cartella Posta in arrivo. Completare. Completato venerdì 18 novembre 2022. Il messaggio è stato convertito in formato di testo normale.

<<http://g-ecx.images-amazon.com/images/G/01/e-mail/img/softlines/sp.gif>>

Risparmi fino al 40% fino al 28 novembre <https://www.amazon.it/gp/f.html?C=1MSDH8HMEIVM0&K=36ETL2UQCRJ3W&M=urn:rtn:msg:202211180016473fa46ffa76424f6693861b143330p0eu&R=37HI39S53B9P&T=C&U=https%3A%2F%2Fwww.amazon.it%2Fgp%2F..%2Fblack3Dpe_52863321_735984511_pe_super%2F%2F&H=LNGTB5EQMZ48IMFPCOJYVYH5BWAA&ref_pe_52863321_735984511_pe_super>

<<http://g-ecx.images-amazon.com/images/G/01/e-mail/img/softlines/sp.gif>>

<https://www.amazon.it/gp/r.html?C=1MSDH8HMEIVM0&K=36ETL2UQCRJ3W&M=urn:rtn:msg:202211180016473fa46ffa76424f6693861b143330p0eu&R=3R4TDPYJNKTE&T=O&U=https%3A%2F%2Fimages-eu.ssl-images-amazon.com%2Fimages%2FG%2F01%2Fnav%2Ftransp.gif&H=MOQDFM728XK2FVAGO9UMLWXGIVEA&ref_pe_52863321_735984511_opens>

<<http://g-ecx.images-amazon.com/images/G/01/e-mail/img/softlines/sp.gif>>

<<http://g-ecx.images-amazon.com/images/G/01/e-mail/img14/kc/sp.gif>>

<https://www.amazon.it/gp/r.html?C=1MSDH8HMEIVM0&K=36ETL2UQCRJ3W&M=urn:rtn:msg:202211180016473fa46ffa76424f6693861b143330p0eu&R=2UXFZ4WYD82BN&T=C&U=https%3A%2F%2Fwww.amazon.it%2Fref%3Dpe_52863321_735984511_pe_sef_logo&H=WCCDYKZT1XMLWAB0HNEWVUBOWMA&ref_pe_52863321_735984511_pe_sef_logo>

Il mio Amazon <https://www.amazon.it/gp/r.html?C=1MSDH8HMEIVM0&K=36ETL2UQCRJ3W&M=urn:rtn:msg:202211180016473fa46ffa76424f6693861b143330p0eu&R=3LCX4VUQGU1C1&T=C&U=https%3A%2F%2Fwww.amazon.it%2Fgp%2Fyourstore%3Fref%3Dpe_yourstore_52863321_735984511&H=DVJ8NFHM8PXAVUT1AE5HWB7KIK&ref_pe_52863321_735984511>

Offerte <https://www.amazon.it/gp/f.html?C=1MSDH8HMEIVM0&K=36ETL2UQCRJ3W&M=urn:rtn:msg:202211180016473fa46ffa76424f6693861b143330p0eu&R=3O8C2Fwww.amazon.it%2Fgp%2Fgoldbox%2Fref%3Dpe_52863321_735984511_pe_todaysdeal%2F&H=FYXWKA7QLT8IAIGEYOQ0FLD3LM4A&ref_pe_52863321_735984511_pe_todaysdeal>

Tutte le categorie <https://www.amazon.it/gp/f.html?C=1MSDH8HMEIVM0&K=36ETL2UQCRJ3W&M=urn:rtn:msg:202211180016473fa46ffa76424f6693861b143330p0eu&R=AZHUWOGO8XMX&T=C&U=https%3A%2F%2Fwww.amazon.it%2Fgp%2Fsite-directory%2Fref%3Dpe_52863321_735984511_pe_tuttecategorie%2F&H=IASJJO3F4KQHXOCUP9WVUYURS7EA&ref_pe_52863321_735984511_pe_tuttecategorie>

<<http://g-ecx.images-amazon.com/images/G/01/e-mail/img/softlines/sp.gif>>

<https://www.amazon.it/gp/f.html?C=1MSDH8HMEIVM0&K=36ETL2UQCRJ3W&M=urn:rtn:msg:202211180016473fa46ffa76424f6693861b143330p0eu&R=3F8X1CNCQMCN8&T=C&U=https%3A%2F%2Fwww.amazon.it%2Fgp%2F..%2Fblackfriday%2F%2Fref%3Dpe_52863321_735984511_pe_3FLanguage%3D&H=IQDVANSOYXZPFOOKPFKZRLAM3AKA&ref_pe_52863321_735984511_pe_>

<<http://g-ecx.images-amazon.com/images/G/01/e-mail/img14/kc/sp.gif>>

<<http://g-ecx.images-amazon.com/images/G/01/e-mail/img14/kc/sp.gif>>

Approfitta delle nostre offerte fa-pe-lo-se! <https://www.amazon.it/gp/f.html?C=1MSDH8HMEIVM0&K=36ETL2UQCRJ3W&M=urn:rtn:msg:202211180016473fa46ffa76424f6693861b143330p0eu&R=34JLQSCQCP1G&T=C&U=https%3A%2F%2Fwww.amazon.it%2Fgp%2F..%2Fblack3Dpe_52863321_735984511_pe_%2F%2F%3FLanguage%3D&H=AJV5IMB91NI18NLFALFOA5GEU8A&ref_pe_52863321_735984511_pe_>

<<http://g-ecx.images-amazon.com/images/G/01/e-mail/img14/kc/sp.gif>>

Non è ancora il momento di suonare Jingle Bells, ma da oggi e fino al 28 novembre basteranno le nostre strepitose offerte a farti cantare il cuore in attesa del Natale. <https://www.amazon.it/gp/f.html?C=1MSDH8HMEIVM0&K=36ETL2UQCRJ3W&M=urn:rtn:msg:202211180016473fa46ffa76424f6693861b143330p0eu&R=220CDND1FNSU8&T=C&U=https%3A%2F%2Fwww.amazon.it%2Fgp%2F..%2Fblackfriday%2F%2Fref%3Dpe_52863321_735984511_pe_%2F%2F%3FLanguage%3D&H=E800FLAZ1C1MPOAHBM9WMEG73YSA&ref_pe_52863321_735984511_pe_>

<<http://g-ecx.images-amazon.com/images/G/01/e-mail/img14/kc/sp.gif>>

Scopri le offerte <https://www.amazon.it/gp/f.html?C=1MSDH8HMEIVM0&K=36ETL2UQCRJ3W&M=urn:rtn:msg:202211180016473fa46ffa76424f6693861b143330p0eu&R=3O1JP203DCPFI&T=C&U=https%3A%2F%2Fwww.amazon.it%2Fgp%2F..%2Fblackfriday%2F%2Fref%3Dpe_52863321_735984511_pe_2F%3FLanguage%3D&H=HXI1X3EQ4KLE3ERATVFKSJPG26EA&ref_pe_52863321_735984511_pe_>

<<http://g-ecx.images-amazon.com/images/G/01/e-mail/img14/kc/sp.gif>>

<<http://g-ecx.images-amazon.com/images/G/01/e-mail/img14/kc/sp.gif>>

<<http://g-ecx.images-amazon.com/images/G/01/e-mail/img14/kc/sp.gif>>

<<http://g-ecx.images-amazon.com/images/G/01/e-mail/img14/kc/sp.gif>>

<https://www.amazon.it/gp/r.html?C=1MSDH8HMEIVM0&K=36ETL2UQCRJ3W&M=urn:rtn:msg:202211180016473fa46ffa76424f6693861b143330p0eu&R=1920Y3ER3AIL&T=C&U=https%3A%2F%2Fwww.amazon.it%2Fdeal%2F876acfb%3FshowVariations%3Dtrue%26ref_>



Maryjane Roberto <gj5221538@gmail.com>



--

Urgente dall'ospedale.

Mia cara amata, questa è la signora Maryjane Roberto. Vengo dall'Estonia. Sono sposato con il signor Lakic John, che ha lavorato con l'ambasciata dell'Estonia in Costa d'Avorio per nove anni prima di morire nel 2010. Siamo stati sposati per undici anni senza figli. Morì dopo una breve malattia durata solo quattro giorni.

Ci sono fondi che ho ereditato dal mio defunto marito amorevole, il signor Roberto Johnson, la somma di (\$ 3,5 milioni) che ha depositato in una banca prima della sua morte, ho bisogno di una persona onesta e fedele che possa utilizzare questi fondi per il lavoro umanitario.

Ho preso questa decisione perché non ho figli che erediteranno questi soldi e non voglio una situazione in cui questi soldi saranno usati in modo empio. Ecco perché sto prendendo questa decisione e il mio medico mi ha confermato che ho meno di tre settimane di vita, avendo conosciuto la mia condizione ho deciso di donare questo fondo a un ente di beneficenza o a un individuo che utilizzerà questo denaro per assistere i poveri e i bisognosi secondo le mie istruzioni.

Voglio che tu utilizzi il 70% di questi fondi per orfanotrofi, scuola e chiesa, vedove, propagazione della parola e altre opere per l'umanità, il restante 30% dovrebbe essere tuo per i tuoi sforzi come nuovo beneficiario, per favore se sei in grado di utilizzare questi fondi per il lavoro umanitario gentilmente mi risponda non appena avrò ricevuto la sua risposta, le darò ulteriori indicazioni su come deve procedere per le richieste di detti fondi.

La tua amata sorella,
Sig.ra Maryjane Roberto.



Godwillfound@mail.com

A: Recipients <Godwillfound@mail.com>

Ciao, mi chiamo Laura Spears, vincitrice della lotteria Michigan Millions da 3 milioni di dollari nel gennaio 2022. Ti donerò 500.000 dollari. Continua a leggere:

<https://www.independent.co.uk/news/world/americas/michigan-lottery-winner-spam-email-b1999558.html>



Woman finds \$3m lottery prize in her spam email folder

Woman finds \$3m lottery prize in her spam email folder. Laura Spears will now add the Michigan Lottery to her safe senders list

www.independent.co.uk

12:00

4G

< Indietro 9 di 1001

● Delivery Spedizione. 09:30:07 -
23/11/2022
22:36, mer 23 novembre 2022

Da:  **Bartolini**

[Dettagli](#)

DPD.Bartolini-ITALIA

Oggi 09:30:07 - 23/11/2022 abbiamo
tentato di consegnare il tuo pacco.

Il tuo pacco è tornato in sicurezza al
nostro deposito.

Per richiedere la consegna di questo
pacco, compila il modulo sul nostro
sito:

[* Pianifica una nuova consegna](#)

Cordiali saluti.



Rispondi



Sposta



Inoltra



Spam



Elimina



Altro

LE TRUFFE BANCARIE (PHISHING, SMISHING, SPOOFING, SIM WRAPPING...)

Le truffe bancarie sono diventate sempre più sofisticate e i truffatori si servono delle tecniche «classiche» - anche combinate insieme - per prelevare somme spesso consistenti dai conti correnti degli utenti, attraverso una e-mail o un SMS, solo apparentemente proveniente da istituti finanziari (banche o società emittenti di carte di credito). Il messaggio mail o SMS (spesso inserito nella stessa chat del proprio istituto) invita, riferendo problemi di registrazione o di altra natura, a fornire i propri dati riservati di accesso al servizio. Solitamente nel messaggio, per rassicurare falsamente l'utente, è indicato un collegamento (link) che rimanda solo apparentemente al sito web dell'istituto di credito o un numero di telefono identico a quello della Banca stessa sul quale si insinua il truffatore. In realtà il sito a cui ci si collega è stato allestito in modo identico a quello originale.

Qualora l'utente inserisca i propri dati riservati, questi saranno nella disponibilità dei criminali.



© UniCredit S.p.A. <info@index.it>

A [redacted]@libero.it

Rispondi Rispondi a tutti Inoltra Elimina Altro ▾



Gentile [redacted]

Le tue credenziali (**Codice di Adesione e PIN**) per accedere ai servizi di UniCredit sono scadute.

Non potrà più effettuare alcun tipo di operazione online se non si procede con l'aggiornamento del tuo profilo.

Cosa puoi fare?

Accedi all'area riservata per aggiornare e gestire i dati del tuo profilo.

[Accedi ai servizi online](#)

La informiamo, che se l'aggiornamento non viene completato entro 24 ore dalla ricezione della presente email non potrà più effettuare alcun tipo di operazione online.

Il tuo account è stato limitato.



📧 Inbank <info@index.it>

A @libero.it

Rispondi Rispondi a tutti Inoltra Elimina Altro ▾

Gentile [REDACTED],

Il tuo Questionario di Conoscenza del Cliente è in scadenza il 22/09/2022.

inbank.it ti ricorda che hai l'obbligo di compilare il Questionario di Conoscenza del Cliente per consentirci di contribuire a prevenire il riciclaggio e il finanziamento del terrorismo, secondo la normativa vigente

La tua collaborazione è essenziale: il mancato aggiornamento obbliga la banca a chiudere tutti i rapporti contrattuali con te intrattenuti trascorsi 2 giorni dalla data di scadenza del Questionario stesso.

Procedi il prima possibile ad aggiornarlo/letarlo perché il mancato aggiornamento può determinare alcune limitazioni operative.

Per procedere alla tua Area Clienti di inbank, accedi cliccando sul bottone sottostante dove visualizzerai un avviso dettagliato che ti consentirà di accedere al Questionario e aggiornarlo:

[AREA PERSONALE](#)



Unicredit



Mercoledì 4 Maggio

Gentile Cliente
un dispositivo
non autorizzato
si è collegato
alla sua aerea
privata segua
la procedura di
accesso tramite
link [http://bit
.do/Unicredit
-Accesso](http://bit.do/Unicredit-Accesso)

18:18



11:49

4G



+39 379 1723871 >

SMS

mar 11 gen, 20:53

(INFOPOSTE)
Gentile cliente
verifica il tuo
dispositivo per
evitare la
sospensione del
conto [https://
assistenza-onlin-
com.preview-
domain.com/](https://assistenza-online.com.preview-domain.com/).
Grazie



SMS



Inviato: martedì 27 settembre 2022 10:43

A: Sportello unico Confconsumatori <sportello@confconsumatori.it>

Oggetto: Truffa bancaria UniCredit - diversa da tutte le altre

Buongiorno,

scrivo per sottoporre alla vostra attenzione una truffa che non avevo mai sentito di cui sono stata purtroppo vittima.

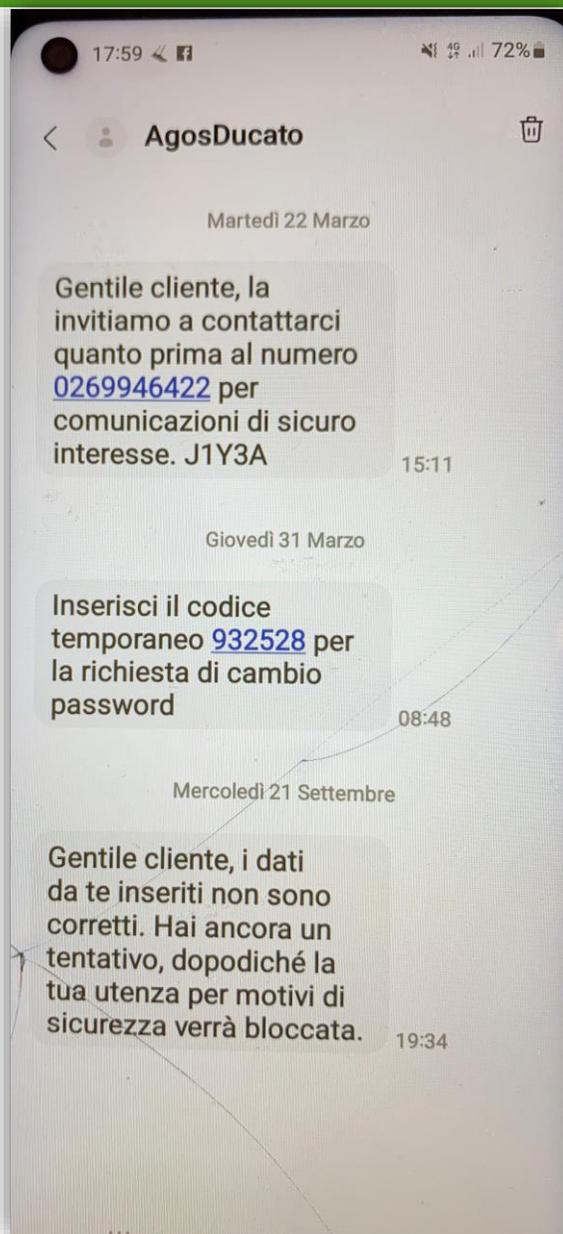
In data 2 settembre ho iniziato a ricevere - all'interno della solita chat di messaggi di UniCredit - molteplici messaggi di avvenuta autorizzazione di pagamento per somme anche ingenti, per esempio 1890 euro, 500 euro ecc. Ne ho ricevuti circa una decina con l'indicazione di chiamare il numero verde di UniCredit oppure il numero dell'ufficio Antifrodi.

Dapprima ho provato a chiamare il numero verde per bloccare la carta ma l'attesa era di circa 15 minuti, ho quindi optato per chiamare l'altro numero indicato nei messaggi (quello dell'ufficio Antifrodi) visto che continuavo a ricevere messaggi di avvenuto pagamento e avevo paura mi rubassero tutto il platfond.

Al numero dell'ufficio Antifrodi mi ha risposto un signore che si è identificato come operatore Unicredit e ha seguito la solita procedura degli operatori che ho sempre sentito quando chiamavo Unicredit. Mi ha quindi fatto bloccare subito la carta di credito ed effettuare tutti gli storni dei pagamenti che ho ricevuto. Sempre nella chat di Unicredit mi è arrivata la conferma di avvenuto blocco della carta. Per gli storni dei pagamenti fraudolenti il processo era questo: il finto operatore di Unicredit al telefono mi inviava delle notifiche push sull'app di Unicredit che io autorizzavo in quanto rimborsi e mi arrivava contestualmente il messaggio di avvenuto rimborso sempre nella chat di Unicredit.

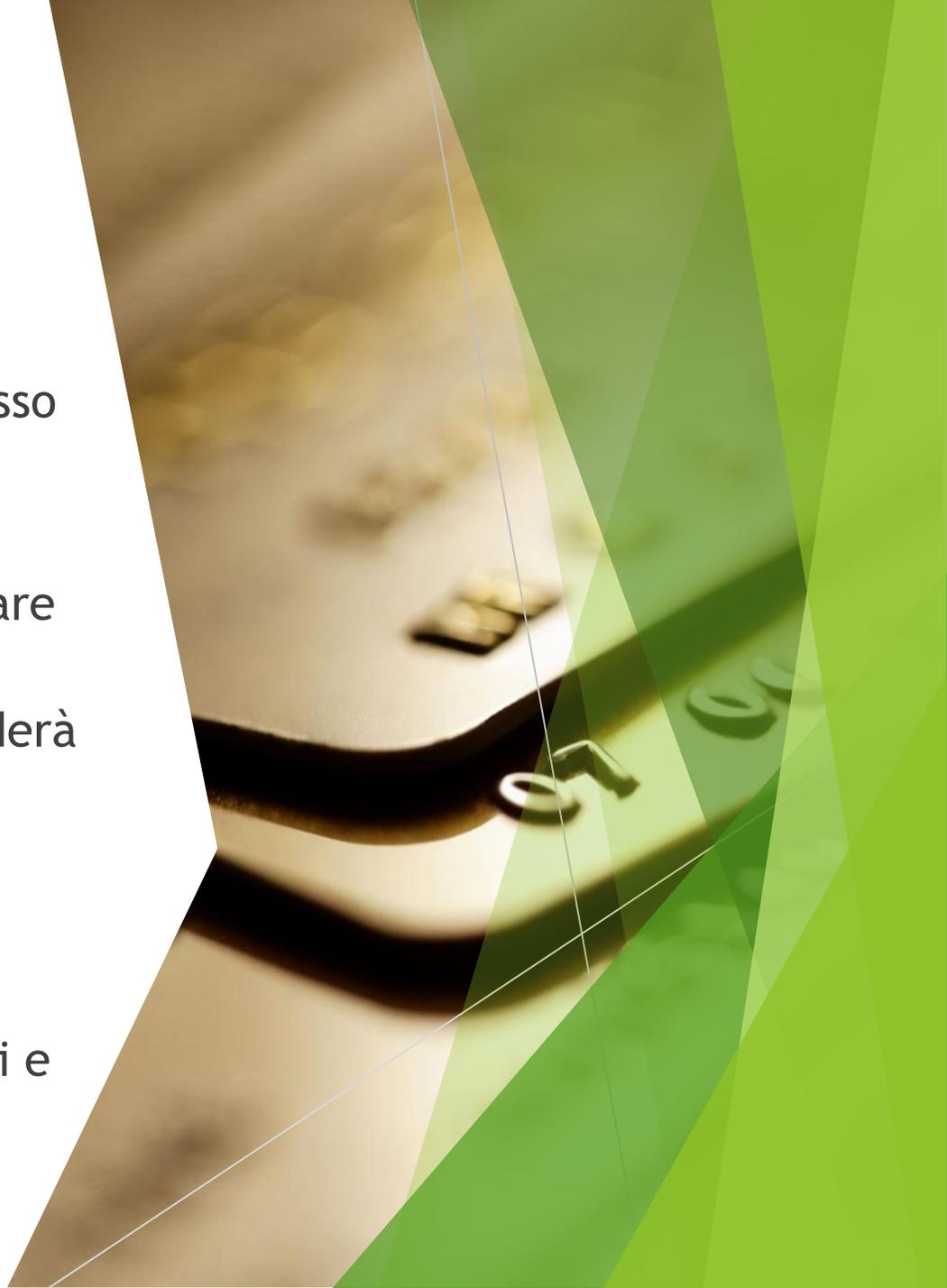
Sta di fatto che dopo qualche giorno, poiché non avevo ancora ricevuto la mia nuova carta di credito, ho chiamato il numero verde di UniCredit (quello dell'ufficio Antifrodi era inattivo) e ho scoperto di aver parlato direttamente con il mio truffatore, che non avevo mai bloccato la carta e che al posto dei rimborsi mi aveva fatto autorizzare i pagamenti.

UniCredit ha rifiutato la mia richiesta di rimborso, ora sono in mani ad un avvocato e spero di riavere indietro i miei soldi.



COME MI PROTEGGO?

- ▶ Contattare la propria Banca e parlare con operatore di fiducia.
- ▶ NON dare mai il proprio PIN o altri dati bancari di accesso
- ▶ Non conservare dati bancari o della carta di credito su Smartphone o dentro al portafoglio
- ▶ La banca non mi invia SMS o MAIL con richieste di cliccare link che mi fanno inserire i dati
- ▶ La mia banca NON conosce il mio PIN e non me lo chiederà MAI
- ▶ Avvisi urgenti di blocco del conto o delle carte sono campanelli d'allarme
- ▶ Controllare periodicamente il conto corrente
- ▶ Accertarsi di avere un sistema di alert legato ai prelievi e pagamenti elettronici sulla propria carta bancomat.



E SE CADO VITTIMA DI UNA TRUFFA?

- ▶ Faccio denuncia alla **Polizia Postale**
- ▶ Invio subito una **richiesta di blocco carta**
- ▶ Verifico con la mia banca l'accaduto e conservo **copia dell'estratto conto** contenente gli addebiti illegittimi
- ▶ Invio un **reclamo** scritto alla Banca con richiesta di rimborso e allego la denuncia
- ▶ Se la Banca risponde negativamente attivo una **ADR** (conciliazione con la banca se esistente e/o **ABF** = Arbitro Bancario Finanziario)
- ▶ Posso rivolgermi ad un'Associazione di consumatori per avere assistenza:

<https://www.confconsumatori.it/truffa-con-sms-spoofing-rimborsati-9-950-euro-a-roma/>

<https://www.confconsumatori.it/truffe-bancarie-digitali-recuperati-oltre-2-700-euro-a-grosseto/>

- ▶ Se l'ABF non va a buon fine o se la casistica è molto complessa devo valutare una **causa** con un legale.

MI INFORMO, MI TUTELO E SEGNALO...

- ▶ <https://www.confconsumatori.it/chi-ha-paura-del-web/>
- ▶ <https://inavigati.certfin.it/index.html#section-gli-esperti>
- ▶ <https://www.arbitrobancariofinanziario.it/>
- ▶ <https://www.commissariatodips.it/>
- ▶ <https://www.agcm.it/competenze/tutela-del-consumatore/>

IN CONCLUSIONE

Il **phishing** (ossia le frodi tramite email) e lo **smishing** (ossia le frodi tramite SMS) sono **reati di frode**: si basano sull'ingannare la vittima facendo cliccare un link per fornire informazioni. Il modo più semplice per proteggersi da questi attacchi è **non fare nulla**.

Finché non si risponde o non si esegue il comando del messaggio, un **SMS** o una **MAIL dannosi** non possono innescare la frode. Basta **ignorarli ed eliminarli** e resteranno innocui.

**GRAZIE PER
L'ATTENZIONE!**



CONFCONSUMATORI
CONFEDERAZIONE
GENERALE DEI
CONSUMATORI