Ingegneria Sociale

COS'È?

*L'ingegneria sociale,è una tecnica utilizzata da malintenzionati per ottenere dati privati,oppure avere accesso a sistemi protetti, utilizzando non le vulnerabilità ,ad esempio di un sito ma sfruttando la psicologia.*Una delle tecniche di ingegneria sociale molto utilizzata è il "**phishing**"

PHISHING

Il **phishing** e' una tecnica utilizzata per rubare credenziali o dati sensibili,attraverso l'uso (spesso) di email.Queste email, a livello grafico sono uguali a quelle legittime tranne per alcuni aspetti che vedremo nelle pagine successive.

Smishing
simile al phishing ma utilizza numeri di cellulare

Come comportarsi in caso succede?

Per evitare quanto abbiamo detto nelle pagine precedenti,ci sono alcuni parametri da tenere in considerazione:

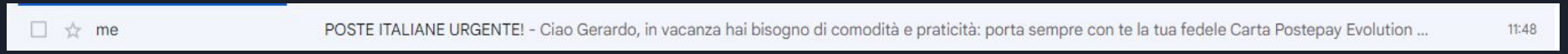
Mittente
controllare che il mittente si una email affidabile
esempio:email contenente un ordine amazon,non puo' avere come mittente pippo@gmail.com

SPF
ci aiuta a capire che l'email provenga da server senza alcun scopo illegale

DKIM
consiste nell'inserire una firma digitale alle email in modo da essere sicuri che il mittente sia legittimo

DMARC
controllo aggiuntivo di sicurezza e dipende da **spf** e **dkim**

Ecco un esempio pratico!



Come possiamo notare, a prima vista ci sembra una email normale inviata da poste italiane

ma...

EMAIL TRUFFA!!

1 di 646

POSTE ITALIANE URGENTE! Posta in arrivo ×

G gerardocarrabs28@gmail.com
a me

11:48 (0 minuti fa)

LA PRIMA COSA CHE NOTIAMO È IL MITTENTE (*non e' poste italiane*)

EMAIL VERA!!

9 di molte

Spedisci il tuo pacco con Poste, ti conviene! Posta in arrivo ×

Poste Italiane <mail@comunicazioni.poste.it>
a me

lun 27 nov, 20:14

Ciao GERARDO,

abbiamo riservato una promozione speciale per **i clienti PostePay come te**.

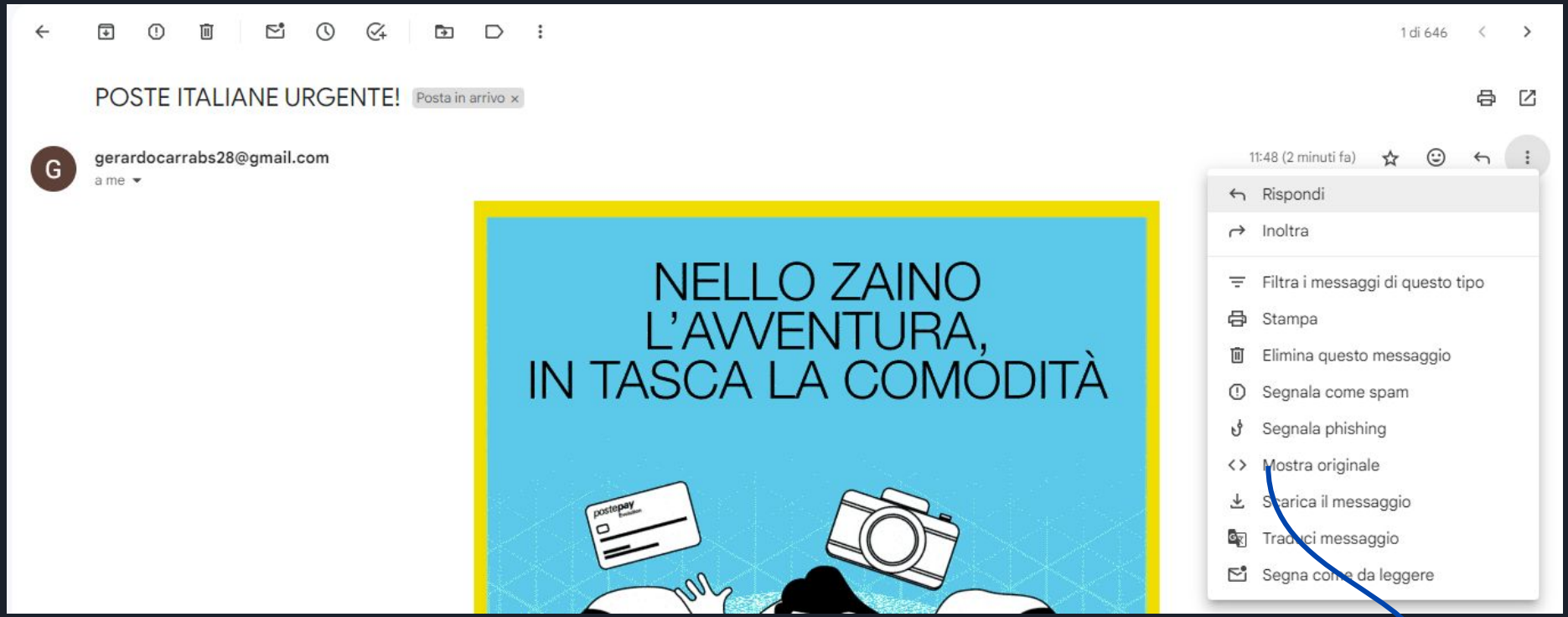
Fino al **31 dicembre 2023** riceverai subito uno **sconto del 10%*** sulle tue prime **3 spedizioni nazionali*** utilizzando il codice:

PROMONLINE

FAI UN PREVENTIVO

IN QUESTO CASO IL MITTENTE È AFFIDABILE

COME FARE?



CLICCARE SOPRA I 3 PUNTINI VERTICALI COLLOCATI IN ALTO A DESTRA, DI CONSEGUENZA SELEZIONARE LA VOCE "*<> MOSTRA ORIGINALE*"

EMAIL VERA

Messaggio originale

ID messaggio	<0.0.B4.DC7.1D9C5310D9FA932.0@omp.info.poste.it>
Creato alle:	2 agosto 2023 alle ore 13:04 (consegnato dopo 232 secondi)
Da:	Postepay <mail@info.poste.it>
A:	gerardocarrabs28@gmail.com
Oggetto:	Comodità all inclusive!
SPF:	PASS con l'IP 140.86.230.152 Ulteriori informazioni
DKIM:	'PASS' con il dominio info.poste.it Ulteriori informazioni
DMARC:	'PASS' Ulteriori informazioni

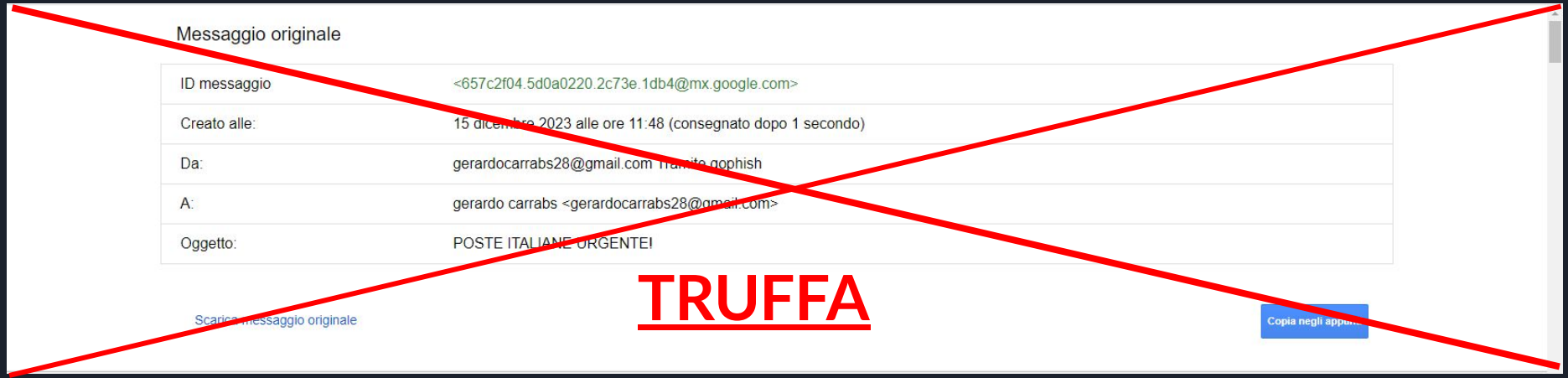
Scarica messaggio originale

Copia negli appunti

IL DMARK E IL DKIM ALCUNE VOLTE NON SONO PRESENTI MA L'EMAIL PUO' ESSERE SEMPRE AFFIDABILE

COME POSSIAMO NOTARE:
SPF PASS(OVVERO È STATO FATTO UN CONTROLLO E L'EMAIL RISULTA AFFIDABILE
DKIM PASS (QUESTO ANCHE VUOL DIRE CHE L' EMAIL RISULTA AFFIDABILE)
DMARC PASS (CONTROLLO AGGIUNTIVO CHE CI INDICA LA SICUREZZA DELL'EMAIL)

EMAIL TRUFFA!!



COME POSSIAMO NOTARE A VISTA , MANCANO I 3 PARAMETRI CHE ABBIAMO VISTO PRECEDENTEMENTE,INOLTRE COME ABBIAMO DETTO IL MITTENTE È DIVERSO DA QUELLO ORIGINALE