



Virus in arrivo, non aprite email con messaggi sospetti!

di Paolo Franzese



In questi giorni sta girando questa email confezionata ad hoc per una frode:

Da: "imaginepaolo Gmail" <manfred.petzina@aon.at>

Data: 23 gennaio 2017 10:28:54 CET

A: **in questa sezione troverete una lista di email a voi ben note.**

Oggetto: una storia incredibile

Caro amico!

Recentemente mi sono imbattuto in una storia incredibile, penso che si potrebbe

Ti prego di leggere qui [Aprire il messaggio](#)

Errori di battitura gentilmente offerti da mio iPhone, imaginepaolo Gmail

Ovviamente per i più esperti questa email è una email da **cestinare subito**, ora ti spiego il perchè:

- **Area mittente:**

- controllando bene l'indirizzo email del mittente ci sono alcune osservazioni:

- non c'è corrispondenza tra nome email e indirizzo reale;

"imaginepaolo Gmail" <manfred.petzina@aon.at>

- l'indirizzo in **blu** risulta su un dominio sconosciuto e non in sintonia con il mittente;

- **Area altri destinatari:**

- c'è una lista enorme di destinatari;

- **ATTENZIONE QUI → potrebbero esserci varie email di tuoi amici o colleghi di lavoro per confonderti ← ATTENZIONE QUI;**

- **Titolo messaggio:**



Oggetto: una storia incredibile

- un titolo interessante ma senza oggetto chiaro;
- un titolo che stimola la curiosità;
- ma un titolo che non dice nulla;
- *Contenuto del messaggio:*
 - Quando nel contenuto del messaggio c'è l'invito a cliccare su un **link non molto chiaro NON CLICCARRE MAI!**
- *Footer del messaggio:*
 - Questa è una novità preoccupante...

Errori di battitura gentilmente offerti da mio iPhone, imaginepaolo Gma

questa frase mi ha sbalordito, evidentemente il virus ha scavato tra le vostre email andando a ricopiare questa frase da qualche email inviata da iPhone.

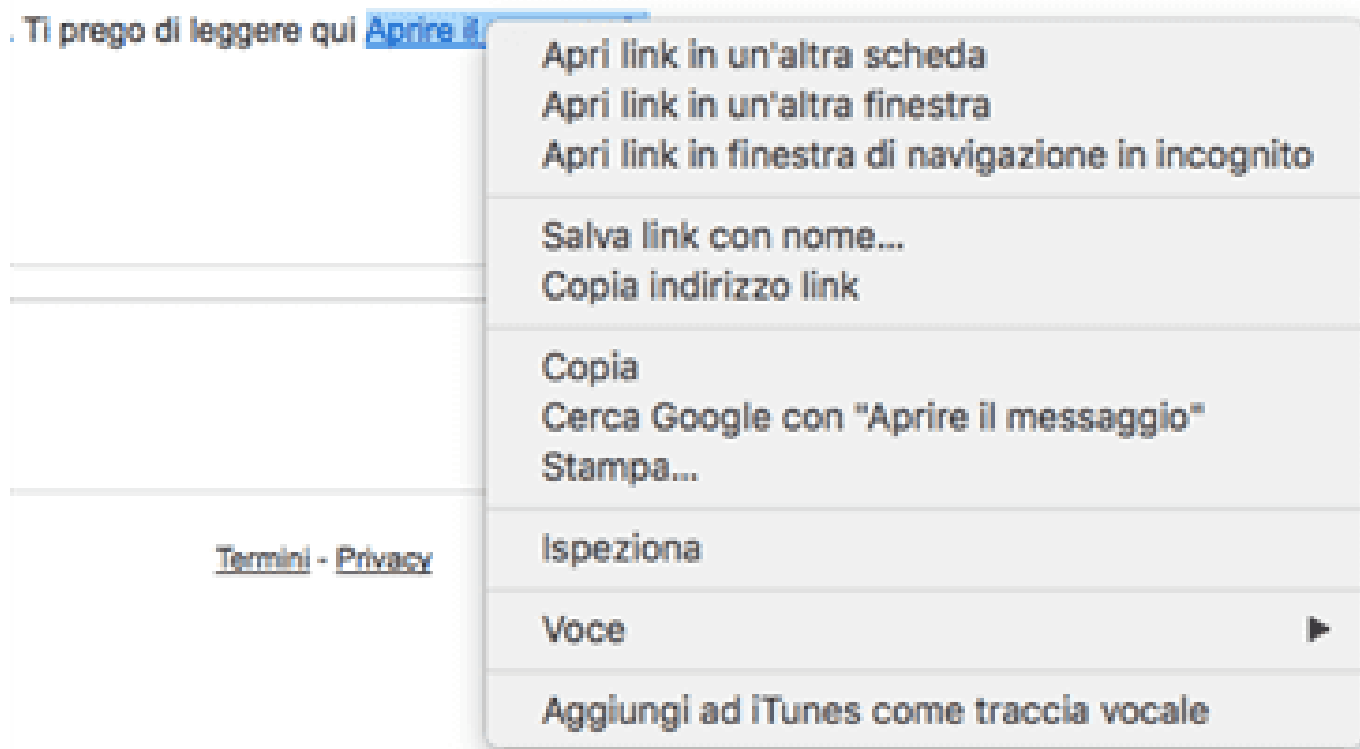
Alcuni suggerimenti per non prendere un virus.

- **Lavora in condizioni HARDWARE e SOFTWARE di MASSIMA SICUREZZA;**
- **Mantieni aggiornati Sistemi Operativi, Software e Antivirus;**
- **Cerca in Google**, mittente del messaggio e nome del domino;
- **Cerca alcune frasi del messaggio**, sicuramente troverai tra i risultati che ti trovi davanti ad un possibile tentativo di frode.
- **Leggi bene** l'email, se noti errori grammaticali grossolani **SII PRUDENTE!**

, penso che si potrebbe piacervi. Ti prego di leggere qui [Aprire il messaggio](#)

- Se c'è un allegato **NON CLICCARRE MAI** fate attenzione a questi file con queste estensioni (ne abbiamo parlato anche in questo [articolo](#)):
 - Le classiche estensioni eseguibili: **EXE, COM, BAT, PIF**
 - I documenti che possono contenere dei codici: **PDF, DOC, XLS, PPT**
 - File di sistema eseguibili: **DLL, CPL, MSC, CMD**
 - Installatori e file compressi: **MSI, ZIP, CAB, RAR**
 - Screensaver: **SCR** (sono dei programmi!)
 - File con doppia estensione (ad esempio **FILE.DOC.EXE**)
- **Analizza il link** poggiando il cursore sul link senza cliccare, oppure premendo contemporaneamente **CTRL** e il mouse, fai comparire la seguente finestra e copia il link per

analizzarlo



- Guarda cosa c'è nascosto dietro quel banalissimo link:

```
ui <a href="http://annalisa.albertbader.com/9594" data-saferedirecturl="https://www.google.com/url?hl=it&amp;q=http://annalisa.albertbader.com/9594&amp;source=gmail&ust=1485266268220000&usg=AFQjCNHlSeidAFdzSiHy0266SLkicyT7-g">Aprire il messaggio</a>
```

- Ti segnalo questi utili strumenti per aiutarvi in questa fase:
 - <https://www.unshorten.it/> (serve a sbloccare un eventuale link crittografato);
 - <https://www.mywot.com/> (vi fornisce una valutazione sulla reputazione del link);
- **Non rispondere MAI ad una email sospetta;**
- **Non inoltrare MAI una email sospetta;**
- Cerca di **controllare la posta sempre attraverso il web** e con **browser sicuri**;

Bene, ora, se hai altri suggerimenti, postali nei commenti qui sotto e condividi questo articolo per la sicurezza di tutti.

Da un articolo scritto da Paolo Franzese il 23 Gennaio 2017