



ISTRUZIONI PER LA RIMOZIONE DEL VIRUS

Numerosi utenti sono incappati in una pagina web su cui

- è stato fraudolentemente applicato il logo della Guardia di Finanza e lo slogan “Insieme per la legalità” copiati dal sito istituzionale “www.gdf.it”,
- viene detto che il computer adoperato presenta contenuti illegali (immagini pedopornografiche e messaggi terroristici),
- si chiede il pagamento di 100 euro (da eseguirsi in via elettronica) per il ripristino delle funzionalità dell’apparato che sarebbe stato bloccato per ragioni preventive.

La visualizzazione del pop-up ad apertura automatica comporta l’installazione di una serie di istruzioni maligne che compromettono il regolare utilizzo del pc.

Se non si è esperti, è preferibile rivolgersi ad un tecnico così da ottenere la rimozione del virus e dar corso ad altre eventuali attività di competenza per evitare il ripetersi di episodi di questo tipo (installazione/aggiornamento di antivirus, antimalware, firewall...).

Se si ha dimestichezza con l’informatica, per rimediare al problema è sufficiente procedere all’esecuzione di semplici operazioni.

- 1 spegnere il computer e farlo ripartire in “modalità provvisoria” tenendo premuto (per la fase di accensione) il tasto “F8”
- 2 cliccare con il mouse su START (oppure AVVIO o ancora sull'icona di Windows) posto in basso a sinistra della barra delle applicazioni
- 3 all’apertura del menu a tendina verticale fare clic su "Tutti i programmi", così da aprire l’elenco dei software installati
- 4 cercare la cartella "Esecuzione automatica" e, una volta individuata, fare clic con il mouse sull'icona corrispondente
- 5 sullo schermo viene visualizzata la lista dei programmi configurati per essere avviati automaticamente all’accensione del computer senza intervento di chi è alla tastiera

- 6 dovrebbe apparire, tra gli altri, il file "WPBTO.dll" oppure un file con nome identificativo del tipo "O.<una serie di altri numeri>.exe" (il file si può presentare in altre varianti sintattiche)
- 7 selezionare il file ed eliminarlo con il tasto "CANC" oppure "DEL" o spostando il file nel cestino presente sul desktop del computer
- 8 selezionare con il mouse il "cestino" sul desktop e fare clic con il tasto destro
- 9 all'apertura della finestra in corrispondenza del cestino, selezionare "svuota cestino" così da procedere alla definitiva eliminazione del malware
- 1 0 spegnere il computer e riavviarlo normalmente, così da poter constatare l'effettivo ripristino del regolare funzionamento dell'apparato a disposizione
- 1 1 provvedere all'installazione (e al costante aggiornamento) di un programma antivirus che possa preservare da futuri analoghi inconvenienti
- 1 2 per ogni eventuale ulteriore dubbio rivolgersi al GAT - Nucleo Speciale Frodi Telematiche della Guardia di Finanza telefonando al numero 06-229381 oppure inviando una mail a sos@gat.gdf.it

