**MODALITA’ OPERATIVE E CONSIGLI PRATICI DA SEGUIRE IN CASO IL PROPRIO DISPOSITIVO VENGA INFETTATO DA UN CRYPTOLOCKER - AZIENDA**

**\*\*\***

1. **Se possibile, disattivare la connettività del proprio dispositivo e lasciarlo acceso**.
2. **Non pagare il riscatto**.
3. **Non cancellare il file che contiene il malware e salvare una copia digitale dello stesso o della email nel quale questo (o il link) era contenuto.**
4. **Salvare il file contenente le istruzioni per il pagamento e lo sblocco del dispositivo** (il file solitamente è denominato "DECRYPT\_INSTRUCTIONS.TXT" e ha all'interno due cose importanti: la URL personale dove ci sono le indicazioni sul riscatto -in genere un Tor hidden service- e l'indirizzo bitcoin sul quale versare il riscatto – se presente-).
5. **Salvare almeno due file criptati di tipo DOC o XLS con dimensione maggiore di 1MB e se disponibili (es. presi da backup parziali) anche le due versioni in chiaro per facilitare le operazioni di decifratura e di sbloccaggio del dispostivo.**
6. **Compilare uno dei modelli di querela allegati** (mod.1 nel caso in cui sia stato già effettuato il pagamento del riscatto richiesto; mod. 2 nel caso in cui non sia stata pagata la somma richiesta).
7. **Depositare la denuncia querela compilata presso il comando di Polizia Postale più vicino** (per verificare il comando di Polizia Postale più vicino cliccare sul seguente indirizzo: <https://www.commissariatodips.it/profilo/contatti.html> ).
8. **Contattare un consulente informatico per il possibile rispristino della funzionalità del dispositivo e per l’acquisizione di eventuali prove digitali presenti all’interno dello stesso.**