



### 1 ATTENZIONE ALLE E-MAIL PROVENIENTI DA MITTENTI SCONOSCIUTI

Il presente documento ha lo scopo di **allertare** tutti i dipendenti degli Enti pubblici che utilizzano postazioni informatiche, si rende noto che, da alcuni giorni sta circolando, in maniera massiva, un virus-trojan che se lanciato codifica i vostri dati (word, excel, pdf, rtf, ecc...)

Il virus è una variante di CryptoLocker, esso è un trojan (cavallo di troia) comparso oramai da qualche anno che ha come prerogativa quella di infettare sistemi operativi windows, consiste nel criptare i dati della vittima e richiedere un pagamento per la decrittazione.

**ATTENZIONE:** Esso generalmente si diffonde come allegato di posta elettronica apparentemente lecito e inoffensivo che sembra provenire da istituzioni legittime, avvolte l'allegato si presenta come file ZIP, contiene un eseguibile con una icona e una certa estensione, una volta lanciato si installa ed inizierà a codificare i vostri dati, il tutto avviene in pochi secondi.

Anche se CryptoLocker venisse rimosso subito, i file rimarrebbero cifrati in un modo inviolabile in quanto si utilizza un algoritmo di cifratura a 256 bit. Non esiste nessun modo per recuperare i file, se non pagando per avere la chiave di decodifica. L'unico modo per essere sicuri dei vostri dati è avere una copia di backup non compromessa.

Si consiglia vivamente di non aprire assolutamente allegati di cui non siete certi della provenienza, nell'incertezza potete contattarci per verificarne la bontà e/o l'ambiguità.