



Ransomware: i consigli del Garante privacy per difendersi dal software che prende "in ostaggio" pc e smartphone

Il ransomware è un programma informatico dannoso diffuso per infettare un dispositivo elettronico (pc, tablet, smartphone, smart tv), bloccandolo o criptandone i contenuti (foto, video, file), e chiedere un riscatto (in inglese, ransom) per "liberarlo".

Davanti all'aumento di questo tipo di attacchi informatici, il Garante per la protezione dei dati personali pubblica una pagina informativa con alcune regole basilari per conoscere meglio questo malware e mettere in campo alcuni accorgimenti utili per non esserne vittima o per tentare di liberarsene nel caso in cui i dispositivi utilizzati siano già stati infettati e vi sia stata una richiesta di riscatto.

La scheda, disponibile alla pagina www.garanteprivacy.it/ransomware, è parte di una serie di prodotti di divulgazione ideati dal Garante per sensibilizzare gli utenti sulle diverse tematiche connesse alla protezione dei dati personali, in particolare quando si usano le nuove tecnologie.

La campagna informativa sul ransomware sarà portata avanti anche attraverso i profili social del Garante su [LinkedIn](https://www.linkedin.com/company/garante-privacy), [Instagram](https://www.instagram.com/garanteprivacy) e [Google+](https://plus.google.com/u/0/org/114017332926200000000/).

Roma, 13 dicembre 2017



20 1997-2017
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
A TUTELA DI UN DIRITTO FONDAMENTALE

ATTENZIONE AL RANSOMWARE

Il programma che prende «in ostaggio» PC e smartphone

- 1. COS'È IL RANSOMWARE?**

Il **ransomware** è un programma informatico dannoso che infetta un dispositivo (PC, tablet, smartphone, smart TV), **bloccando l'accesso ai contenuti** (foto, video, file) e **chiedendo un riscatto** (in inglese, *ransom*) per «liberarli». La **richiesta di pagamento** con le relative istruzioni è presentata in una finestra che appare automaticamente sullo schermo del dispositivo infettato. L'utente ha pochi giorni per pagare: **poi il blocco diventa definitivo**. Ci sono **due tipi principali di ransomware**: i **cryptor** (che criptano i file contenuti nel dispositivo rendendoli illeggibili) e i **blocker** (che bloccano l'accesso al dispositivo infettato).
- 2. COME SI DIFFONDE?**

Il ransomware si diffonde soprattutto attraverso **messaggi** - inviati via e-mail, sms o chat o che appaiono su pagine web e social network - che sembrano provenire da **sogetti conosciuti e sicuri** come corrieri espressi, gestori di servizi (*acqua, luce, gas*), operatori telefonici, soggetti istituzionali, ecc.. Chi li riceve è indotto ingannevolmente ad **aprire allegati** o a **clickare link o banner** collegati a software dannosi. Il dispositivo infettato può poi «contagiare» altri, perché il ransomware, impossessandosi della **rubrica dei contatti**, può utilizzarla per **spedire automaticamente messaggi** contenenti file dannosi.
- 3. COME DIFENDERSI?**

La prima difesa è evitare di aprire **messaggi provenienti da soggetti sconosciuti** o con i quali non si hanno rapporti (ad es. un operatore telefonico di cui non si è cliente, un corriere espresso da cui non si aspettano consegne, ecc.) e **non cliccare su collegamenti a siti sospetti**. E' utile installare un **antivirus** con estensioni per malware sui propri dispositivi e **mantenere aggiornato il sistema operativo**. E' fondamentale effettuare **backup periodici dei contenuti**: così, nel caso in cui fosse necessario formattare il dispositivo per sbloccarlo, i dati in esso contenuti non verranno persi.
- 4. COME LIBERARSI DAL RANSOMWARE?**

Pagare il riscatto è solo apparentemente la **soluzione più facile**. Oltre al danno economico, si corre infatti il rischio di **non ricevere i codici di sblocco**, o addirittura di finire in **liste di «pagatori»** potenzialmente soggetti a periodici attacchi ransomware. L'alternativa è quella di **rivolgersi a tecnici specializzati** capaci di sbloccare il dispositivo. Oppure si può **formattare il dispositivo**, ma con il rischio di perdere tutti i dati in esso contenuti se **non è disponibile un backup**. E' consigliabile sempre segnalare o denunciare l'attacco ransomware alla Polizia postale, anche per aiutare a prevenire ulteriori truffe.

La scheda ha mere finalità divulgative