

Italia: 16 milioni di cittadini colpiti dal cybercrime. L'insicurezza in 10 grafici

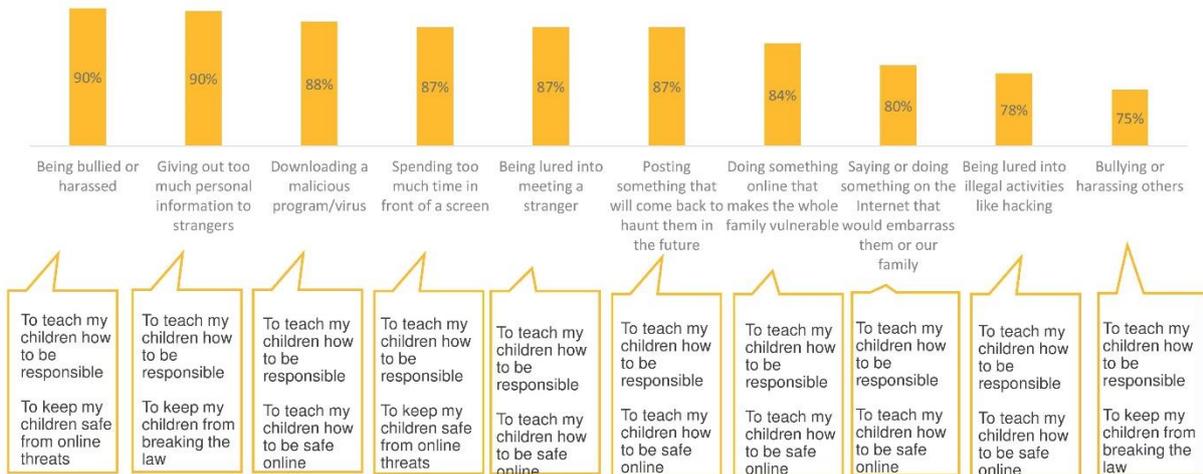
Sono numeri un po' alti. Un po' troppo alti forse. Ma almeno confermano quanto scritto sul libro bianco della cybersecurity sulla gravità dei crimini informatici. Secondo il sondaggio online realizzato su mille persone e contenuto all'interno del Norton Cyber Security Insights Report gli hacker cattivi sottraggono ben 146,3 miliardi di euro (172 miliardi di dollari) a 978 milioni di consumatori di 20 paesi.

In Europa, l'anno passato ha visto attestarsi a **98,2 milioni il numero delle vittime** di crimini informatici; **il totale del denaro sottratto è stato di 23,3 miliardi di euro**. Va subito detto che le definizioni di crimine informatico e di vittima del crimine informatico di Symantec sono piuttosto "larghe". Un crimine informatico viene definito come – ma non si limita a – un numero di attività specifiche, ivi compresi il furto d'identità, la frode a carte di credito o la compromissione della password di un account. Mentre una vittima di crimine informatico è un partecipante alla ricerca che ha confermato di essere stato vittima di una o più di questi incidenti. Tuttavia, anche con queste categorie i numeri descrivono un allarme vero.

In Italia? Oltre 16 milioni di utenti della rete sono caduti in trappole informatiche lo scorso anno, oltre un terzo della popolazione adulta (37%). Le perdite in Italia hanno totalizzato quasi 3,5 miliardi di euro, e ogni vittima ha perso in media più di 2 giorni lavorativi per occuparsi delle conseguenze del crimine informatico subito.

Chi sono le vittime? A livello globale, le vittime di crimini informatici condividono un profilo molto simile: utilizzano la rete con regolarità, sono sicuri di sé, utilizzano più dispositivi per connettersi sia da casa sia in mobilità; all'incirca una su tre vittime di crimini informatici utilizza un dispositivo smart per lo streaming (31%), rispetto al 20% di coloro che non sono state vittime di un crimine informatico. Inoltre, chi ha subito un crimine informatico generalmente possiede un dispositivo connesso in rete, ed effettua regolarmente acquisti online via mobile quando non è in casa rispetto alla controparte mai colpita da crimine informatico.

Parents are worried about many things when it comes to their child and the Internet – but fewer act



Q24. What are the reasons why you do those activities in relation to your children and their online activities?

Q25. How worried are you about each of the following when it comes to your child and the Internet?
Copyright © 2017 Symantec Corporation

Within the last year, cybercrime victims spent more than \$4 billion in Italy dealing with the consequences



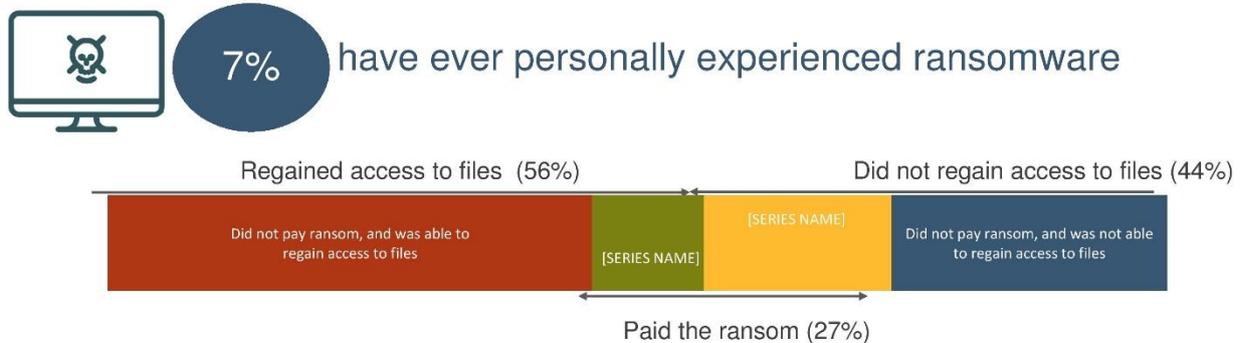
Q10. Have you (or someone you know) ever experienced any of the following situations?

Q10B. Which of these events have you experienced in the past 12 months?

Q13. How much have you lost financially over the past 12 months due to the events list below?

Tracking question

Ransomware affected 3% of people living in Italy in the last 12 months, 7% ever. 44% were unable to recover their files



Q10. Have you ever experienced any of the following situations?
Q11. What was the outcome of your ransomware attack?

Tracking question

27

Copyright © 2017 Symantec Corporation

Capitolo ransomware. Il ransomware è un riscatto, il computer risulta bloccato e o si paga e promettono di non fare entrare in possesso, il rischio è di non recuperare comunque il proprio patrimonio digitale.

I file digitali di uno su quattordici degli intervistati sono stati presi in ostaggio con richiesta di riscatto, e per coloro che hanno dovuto vivere questo incubo informatico, il prezzo da pagare è sempre stato molto salato. Le vittime di ransomware raccontano di aver perso una media di quasi 109 ore per occuparsi delle conseguenze del ricatto informatico e più di uno su 10 (il 12%) non ha ottenuto indietro nulla a fronte del pagamento del riscatto. Con quasi la metà (44%) degli utenti italiani che ammettono di non fare mai un backup di almeno uno dei dispositivi che utilizzano, e con sei italiani su dieci che ammettono di affidarsi al fornitore per gli aggiornamenti del software, un numero significativo di persone corre seri rischi di perdere definitivamente i propri dati.

I crimini informatici più comuni in Italia Ecco i numeri più sorprendenti. Diciamo subito che non ne usciamo bene.

- **Il 69% degli Italiani ha avuto a che fare con il crimine informatico** lo scorso anno.

- **Più della metà (il 55%) ha avuto un dispositivo infettato** da un virus o altre minacce alla sicurezza.
- **Al 41% è stato notificato che le proprie informazioni sensibili sono state compromesse** a seguito di una violazione di dati. Quasi un quarto degli intervistati ha abboccato alla truffa di un finto supporto tecnico.

In quali casi abbiamo perso più soldi.

- Accesso non autorizzato o hacking della mail o del profilo social media (€ 509)
- Furto d'identità (€ 192)
- Frode con carta di credito/debito (€ 183)
- Virus o altra minaccia alla sicurezza su PC /tablet/cellulare (€ 156)
- Furto di informazioni di pagamento dal telefono (€ 141)
- Perdita di un lavoro o di una promozione a causa di un post sui social media caricato da altri (€ 134)
- Acquisti online che si sono rivelati essere una truffa (€ 131)
- Ha subito un attacco di tipo ransomware (€ 77)
- Truffa da parte di un finto supporto tecnico (€ 71)

Come cambia la concezione della privacy. È piuttosto interessante notare, scrivono gli esperti di Symantec, che le vittime di crimini informatici sono più propense a pensare che non ci sia niente di sbagliato nell'inviare la privacy altrui o nell'accedere a informazioni sensibili senza chiedere permesso. Il 34% afferma che leggere le email di qualcuno senza un esplicito consenso è talvolta o sempre accettabile; dello stesso parere è solo il 18% delle persone che non hanno mai subito un crimine informatico. Il 21% ritiene che accedere senza permesso alle informazioni finanziarie di qualcuno sia talvolta o sempre accettabile; dello stesso parere è solo l'11% delle persone che non hanno mai subito un crimine informatico.

Il Norton Cyber Security Insights Report è una ricerca online condotta su un campione di 21.549 individui di età variabile dai 18 anni in su in 20 mercati, commissionata da Symantec e realizzata dalla società di ricerche Reputation Leaders. Il margine di errore per il campione complessivo è di +/- .7%. Il campione italiano raccoglie le risposte di 1012 adulti a partire dai 18 anni di età. Il margine d'errore è del 3.1% per il totale del campione Italia. I dati sono stati raccolti tra il 5 e il 24 ottobre 2017 da Reputation Leaders.

La definizione di Symantec di crimine informatico

La definizione di crimine informatico continua a evolvere con l'aprirsi di nuove vie che consentono ai criminali informatici di accedere agli utenti in maniere nuove. Ogni anno effettuano una valutazione delle tendenze più recenti in materia di crimine informatico e aggiornano di conseguenza la metodologia da applicare al report. Nel Norton Cyber Security Insights Report 2017, un crimine informatico viene definito come – ma non si limita a – un numero di attività specifiche, ivi compresi il furto d'identità, la frode a carte di credito o la compromissione della password di un account. Per gli scopi del presente report, una vittima di crimine informatico è un partecipante alla ricerca che ha confermato di essere stato vittima di una o più di questi incidenti.