

Avviso USB: Mettere al sicuro i dati



Se da un lato, i drive USB hanno rivoluzionato il trasferimento dei dati, dall'altro hanno purtroppo dato spazio a gravi rischi per la sicurezza. Grazie alla loro estrema comodità di trasporto, i drive USB possono essere riposti ovunque, dalla tasca di una giacca al

ciondolo di un portachiavi, con gravi rischi per la sicurezza dei dati. È possibile gestire efficacemente i rischi connessi a questa enorme diffusione, senza dover arrivare a vietare del tutto l'uso dei drive USB e rinunciare così ai loro vantaggi?

Quali sono i rischi più diffusi?

I modi in cui i drive USB riescono a divenire un pericolo per i dati sono davvero tanti:

PERSI

Ogni anno, sono più di 22.000 i drive USB che finiscono inavvertitamente in lavanderia¹



TROVATI

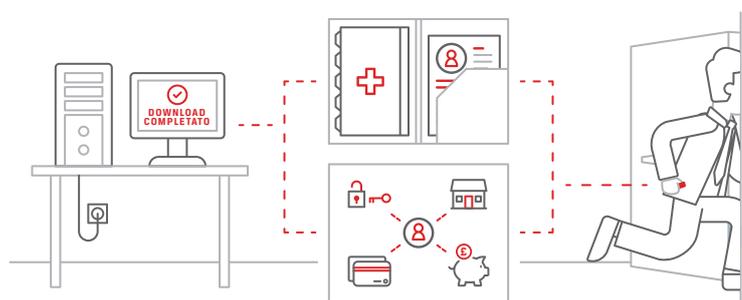
Il 48% delle persone che trovano un drive USB lo collegano e fanno clic almeno su un file⁴



RUBATI

Un drive USB contenente dati sensibili dei pazienti fu smarrito nel pronto soccorso di un ospedale²

Un dipendente infedele ha utilizzato un drive USB per rubare i dati bancari di circa 30.000 persone³



In che modo i professionisti dell'IT possono gestire la sicurezza dei drive USB?

Un sondaggio condotto da Spiceworks sui professionisti IT ha rilevato che sebbene siano tante le organizzazioni consapevoli dei rischi connessi alla sicurezza dei drive USB, ce ne sono altrettante che non hanno ancora messo a fuoco il problema⁵.



I drive USB con crittografia non rivelano mai i segreti che custodiscono.

I drive USB con crittografia possono rivelarsi strumenti molto efficaci nell'arginare questi problemi fin troppo comuni, assicurando così sicurezza e conformità a:



Protegete i vostri dati con Kingston.

I drive USB con crittografia IronKey di Kingston sono stati progettati per offrire protezione anche ai dati più riservati custoditi da agenzie governative, fornitori medici e istituzioni finanziarie, grazie all'impiego dei protocolli e degli standard più rigorosi oggi esistenti.

Fonti:

1. Steve Bush, "22,000 USB sticks go to the dry cleaners," ElectronicsWeekly.com, 14 gennaio, 2016. www.electronicweekly.com/news/business/information-technology/22000-usbs-sticks-go-to-the-dry-cleaners-2016-01/
2. Taya Flores, "IU Health Arnett reports missing patient info," JConline, 5 gennaio, 2016. www.jconline.com/story/news/2016/01/05/iu-health-arnett-reports-missing-patient-info/78300400/
3. Tom Brant, "Rapporto: FDIC Employees Caused Repeated Security Breaches," PC Magazine, 15 luglio, 2016. www.pcmag.com/news/346179/report-fdic-employees-caused-repeated-security-breaches
4. Elie Bursztein, "Concerns about USB security are real: 48% of people do plug-in USB drives found in parking lots," Elie.net, aprile 2016. www.elie.net/blog/security/concerns-about-usb-security-are-real-48-percent-of-people-do-plug-in-usb-drives-found-in-parking-lots
5. Spiceworks survey of 300 IT decision-makers in the US, Canada, and Europe, on behalf of Kingston, febbraio 2017.
6. Al fine di fornire soluzioni di gestione per i suoi drive USB, Kingston Digital ha stretto una partnership con DataLocker. www.kingston.com/us/usb/encrypted_security/management-solutions