

OUCH!

La newsletter mensile sulla Sensibilizzazione alla Sicurezza per te

# Pulizie di Primavera

## In sintesi

Molti di noi non vedono l'ora che arrivi la primavera! Il paesaggio inizia a cambiare, i fiori a sbocciare e, per molte persone, nasce anche il desiderio di fare le pulizie di primavera. E' facile comprendere il bisogno di ordinare le proprie cose, un po' meno quello di dover sistemare i nostri spazi digitali. Ecco alcuni suggerimenti per fare ordine nella tua vita digitale ed adottare nuove abitudini:



**BACKUPS:** Abbiamo messo questo passaggio al primo posto perché, nel lungo termine, è quello più importante da seguire, prima di considerare il resto. Non importa quanto tu sia attento alla sicurezza, prima o poi avrai probabilmente bisogno di un backup per recuperare i tuoi dati. I motivi possono essere un disco fisso che si rompe, la perdita di un dispositivo, o l'infezione di un malware o ransomware. Creare e programmare backup automatici ti garantisce la possibilità di recuperare i tuoi dati più importanti.



**CANCELLAZIONE:** Cancella ogni programma o app inutilizzati dai tuoi computer e dispositivi mobili. Alcune app richiedono grandi quantità di spazio, possono introdurre nuove vulnerabilità, e potrebbero anche causare rallentamenti. Meno app possiedi, maggiore sarà la sicurezza del tuo sistema e delle tue informazioni. Molti dispositivi possono mostrare da quanto tempo non usi una app specifica - se è passato più di qualche mese, probabilmente non hai bisogno di quell'app!



**AGGIORNAMENTI:** Aggiorna tutti i dispositivi e le app che possiedi, e abilita gli aggiornamenti automatici quando possibile. In questo modo le tue app e dispositivi rimarranno aggiornati, assicurandoti un funzionamento ottimale e rendendo più difficile per chiunque violarli.



**PASSWORD:** Controlla le tue password. Se stai usando la stessa password per diversi account, assicurati di cambiarle in modo da avere una password unica per ogni account. Non riesci a ricordare tutte le tue password? Potresti usare un gestore di password. Infine, abilita l'autenticazione a due fattori (2FA) quando possibile, specialmente per gli account email e di servizi finanziari.



**ACCOUNT SERVIZI FINANZIARI:** Assicurati che gli account della tua banca, carta di credito o piani pensionistici siano configurati per avvisarti ogni volta che viene effettuata un'operazione, specialmente in caso di acquisti importanti e trasferimenti di denaro. Prima individui l'attività fraudolenta, più facile sarà bloccarla. Se disponibile nel paese in cui vivi, il blocco della carta di credito può essere un modo efficace per proteggerti.



**BROWSER:** Controlla i plugin e componenti aggiuntivi installati nel tuo browser. Verifica le impostazioni delle autorizzazioni: I plugin hanno davvero bisogno di accedere alla tua posizione, password o elenchi di contatti? Se non usi più alcuni plugin, o hai dubbi sulla loro sicurezza, cancellali.



**SOCIAL MEDIA:** Prendi il controllo della tua presenza online. Controlla le impostazioni della privacy e cancella ogni foto o video che non siano più necessari. Puoi anche cercare te stesso su un motore di ricerca per vedere quali informazioni sono disponibili sulla tua persona. Ricorda che è meglio limitare la quantità di informazioni che condividi e anche il numero di persone che possono accedervi.



**SCRIVANIA:** Pulisci il cassetto della scrivania, cancella il contenuto dei vecchi dischi o unità USB, e magari elimina anche note e appunti con troppe informazioni. Se non ne hai già uno, potresti acquistare un distruggi documenti.



**EMAIL:** Fai pulizia nella tua posta elettronica, cancella quello che non ti serve e riorganizza il resto. Fai particolare attenzione a tutti i documenti sensibili, come quelli contenenti la tua data di nascita o altri dati personali, e spostali dalla casella della posta in arrivo!

Anche se può sembrare un lavoro arduo, in questo modo i tuoi dispositivi e informazioni saranno molto più protetti. Se non riesci a fare tutto insieme, puoi sempre decidere di completare un passaggio al giorno o alla settimana. Ogni passo può essere determinante per la tua protezione.

## Guest Editor

**Katie Nickels** ([@LiketheCoins](#)) è analista dell'intelligence presso Red Canary oltre che istruttrice SANS per il corso FOR578: Cyber Threat Intelligence. Ha lavorato per oltre un decennio nei sistemi di difesa, unità di crisi e intelligence per la prevenzione delle minacce informatiche.



## Risorse

Backups:

<http://www.sans.org/u/ZVr>

Creazione di password semplici:

<http://www.sans.org/u/ZVw>

Cerca te stesso online:

<http://www.sans.org/u/ZVB>

Eliminare i tuoi dispositivi mobili:

<http://www.sans.org/u/ZVG>

OUCH! è pubblicato da SANS Security Awareness e distribuito con licenza [Creative Commons BY-NC-ND 4.0](#). Puoi condividere o distribuire questa newsletter, a condizione che non venga modificata o usata per scopi commerciali. Redazione: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley