

4.

SALVAGUARDA I TUOI BENI VIRTUALI

Alle informazioni che conservi virtualmente dovresti dedicare la stessa cura che riservi agli oggetti di valore in casa tua: che siano i tuoi dati finanziari, la scansione del tuo passaporto o persino il tuo indirizzo o numero di telefono, vale la pena riflettere su dove conservi i tuoi dati personali di maggior valore e come puoi proteggerli.

Una **pulizia superficiale** va bene se vuoi apportare qualche veloce miglioramento mentre bevi un caffè. Cerca informazioni specifiche nella tua email o in altri account e cancellale: scansioni della tua carta d'identità, informazioni bancarie o sanitarie, giusto per citarne alcune. Se pensi ti serviranno in futuro, puoi sempre scaricarle o stamparle prima di cancellarle dal tuo indirizzo email.

Una **pulizia profonda** è più dettagliata, e dovresti farla una volta all'anno. Archivia tutto quel che hai nella tua email o nel tuo account sui social media, scaricalo sul tuo computer e cancella i contenuti online per ricominciare da zero.

Consiglio: Non basta cancellare. Dovresti anche svuotare il cestino e i file temporanei!

Decidi tu se fare il backup dei tuoi archivi e documenti su un cloud o se salvarli su un hard disk o una chiavetta USB esterna. A prescindere, assicurati di non perderli, che abbiano una buona password e che il backup abbia senso per te.

5.

PASSAPAROLA

Quando metti in sicurezza i tuoi account, rendi più sicure le tue password e ripulisci i tuoi dati, non ne benefici solo tu, ma **tutte le persone della tua rete sono un po' più al sicuro grazie al tuo impegno.**

Quando ripulisci la tua email o i profili social, considera cos'altro potresti scaricare e cancellare che potrebbe aiutare i tuoi amici o colleghi: i dati bancari di tua sorella, il codice per accedere al tuo ufficio o la fotocopia del passaporto di tuo figlio sono solo alcuni dei documenti che potrebbero creare problemi se finissero nelle mani sbagliate.

Passaparola! Migliorare la tua sicurezza digitale può essere facile quanto seguire alcuni semplici passi. Condividi questo Data Detox con amici, familiari e colleghi per aiutarli a cambiare le proprie abitudini, ognuno secondo le proprie esigenze.



D A T A
D E T O X
K I T

MODIFICA LE IMPOSTAZIONI

per proteggere i tuoi dati

Se internet fosse solo un posto in cui condividere foto di cani con costumi da dinosauro, le password non servirebbero a molto. Ma su internet paghi anche le bollette, prenoti visite mediche e potresti un giorno votare. Se rifletti sui "beni virtuali" che condividi su internet, e che conservi sui tuoi dispositivi, perché mai non dovresti tenerli al sicuro, esattamente come il portafoglio o le chiavi?

C'è un modo semplice per rendere più complicato per gli altri accedere ai tuoi beni virtuali: scegliere password difficili da indovinare. La maggior parte delle persone

non ha bisogno di abilità tecniche specifiche per entrare nei tuoi account, ma può accedervi cercando di indovinare la tua password oppure lanciando un programma automatico.

Una volta entrati su uno dei tuoi profili, malintenzionati possono provare a compromettere le password di altri tuoi account, raccogliere informazioni su di te e le tue abitudini, prendere il controllo di altri account o anche servirsi della tua identità digitale.

Seguendo questo Data Detox, imparerai misure concrete per migliorare la tua sicurezza online.

Cominciamo!

Un prodotto di

**TACTICAL
TECH**

Supportato da

Firefox

datadetoxkit.org
#datadetox

1.

CHIUDI A CHIAVE LA TUA PORTA DIGITALE

Avere un qualsiasi blocco sul telefono, tablet o computer ti offre maggiore protezione rispetto a non averne affatto. Ma così come i lucchetti che metti alle porte, anche **alcuni blocchi sono più sicuri di altri**.

Di tutti i blocchi esistenti, le password personalizzate e lunghe sono l'opzione più sicura. Significa che se sblocchi il tuo dispositivo con una password, questa dovrebbe includere lettere, numeri e caratteri speciali.

Assumiamo che al momento non usi nessun blocco per proteggere il tuo telefono. Con calma puoi aumentare la tua sicurezza impostando una password lunga. Se usi una sequenza, che ne diresti di renderla un poco più complessa? Se il tuo PIN attuale è 1234, perché non lanciare i dadi sette volte e memorizzare un PIN alternativo?

Un piccolo cambiamento può fare una grande differenza quando si tratta di mantenere il controllo dei tuoi dispositivi.

2.

ACCESSO NEGATO

Creare password sicure è facile. Devi solo seguire alcuni principi di base. Le tue password dovrebbero avere le seguenti caratteristiche.

Lunghe: **almeno otto caratteri. Ancora meglio? 16-20 caratteri.**

Uniche: **per ogni sito che usi dovresti impostare una password diversa.**

Casuali: **la tua password non dovrebbe seguire uno schema logico o essere facile da ricordare. Qui è dove entrano in gioco i password manager, i gestori di password.**

Le password migliori usano una combinazione di lettere, numeri e caratteri speciali. Questo ben noto consiglio rende le password più sicure e difficili da indovinare. Purtroppo alcuni sistemi non permettono di utilizzare caratteri speciali nelle password (come @\$%-+=), ma una combinazione sufficientemente lunga di lettere e numeri rimane meglio di una breve.

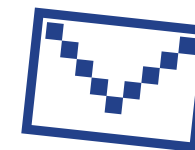
Idealmente, dovresti usare un **password manager dedicato** per generare e conservare le tue password. I password manager, come 1Password e KeePassXC per citarne alcuni consigliati dagli esperti di sicurezza, sono app il cui unico scopo è proteggere le tue credenziali di login e altri dati sensibili.

3.

UN LUCCHETTO NON BASTA

Impostare l'autenticazione a due fattori (2FA) o a più fattori (MFA) significa che, se anche qualcuno scoprisse la tua password, **non avrebbe comunque accesso all'elemento aggiuntivo necessario per accedere.**

Scorri le impostazioni di sicurezza dei siti e delle app che più utilizzi per verificare se puoi impostare questo passaggio extra. Comincia da quelli più importanti, come le app delle banche o dei servizi di posta elettronica che usi per recuperare le credenziali degli altri account.



Google:
Collegati a myaccount.google.com → Sicurezza → Verifica in due passaggi → Inizia

Facebook:
Menu → Impostazioni → Protezione e Accesso → Usa autenticazione a due fattori

Consiglio: Quando imposti il tuo secondo livello di verifica, dovrai selezionare un secondo modo per confermare la tua identità. Cerca di evitare di usare gli SMS (messaggi inviati al tuo numero di telefono) come secondo fattore, in caso perdessi il telefono. L'email in genere è un'opzione più affidabile.