

4.

BESKYTT DINE DIGITALE VERDISAKER

På samme måte som du beskytter verdisakene dine hjemme, bør du beskytte informasjon du lagrer digitalt – det være seg økonomisk informasjon, en skannet versjon av passet ditt eller til og med adresse og telefonnummer. Det lønner seg å tenke over hvor du lagrer dine mest verdifulle data, og hvordan du kan beskytte dem.

Om du vil gjøre noen raske grep i kaffepausen, er en «**flekkrens**» en god start. Søk opp bestemte typer informasjon du har liggende på e-post eller andre kontoer, og slett dem: for eksempel skanninger av ID-papirer, bankinformasjon eller forsikringsinformasjon. Finner du noe du har bruk for senere, kan du alltid laste det ned eller skrive det ut før du sletter det fra e-postkontoen.

En **dyprens** er grundigere og er kjekt å gjøre en gang i året. Lagre alt fra e-posten din eller kontoer på sosiale medier, last det ned til PC-en din, og slett det som ligger på nettet, så starter du på ny frisk.

Tips: Ikke bare trykk «slett» – tøm også søppelkurven og mellomlagrede filer!

Om du vil sikkerhetskopiere arkivene og dokumentene dine i skyen eller lagre dem på en ekstern harddisk eller minnepinne, er opp til deg. Uansett hvordan du lagrer det, må du passe på å ikke rote det bort, at passordet er sterkt, og at du velger en metode du synes er fornuftig.

5.

DEL MED ANDRE

Vi tenker ikke så ofte over det, men internett kalles et «nett» med god grunn. **Vi er alle knyttet sammen på nettet** i ulike nettverk, ikke bare som «venner» i sosiale medier, men også gjennom kontakter i e-posten og bildene vi legger ut.

Når du sikrer kontoene dine, styrker passordene og rydder i gamle data, trygger du ikke bare deg selv – **det gjør også alle du har koblinger til på nettet, litt tryggere.**

Rydder du opp i e-posten og på kontoer i sosiale medier, kan du ha i bakhodet hva annet du kan laste ned og slette som kan hjelpe venner og kollegaer: bankinformasjonen til søsteren din, inngangskoden til kontoret eller skanningen av passet til sønnen din. Dette er bare noen få eksempler på lagret informasjon som kan skape mye baluba om det kommer på avveier.

Del med andre! Å styrke din digitale sikkerhet kan være så enkelt som å følge noen enkle steg. Del denne datadetoxen med venner, familie eller kollegaer for å hjelpe dem med å endre vaner på en fornuftig måte.



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

BYTT INNSTILLINGER

for å holde dataene dine trygge

Hadde internett bare vært et sted der man deler bilder av hunder i dinosaurkostymer, hadde vi ikke hatt noe særlig behov for passord. Men det er på internett du betaler regninger, fornyer resepter og fyller ut skattemeldingen. Med tanke på alle dine «digitale verdisaker» du deler over internett – og lagrer på enhetene dine – **bør du ikke sikre dem slik du beskytter lommeboka eller nøkkelknippet?**

Med ett enkelt grep kan du gjøre det vanskeligere for andre å få tilgang til dine digitale verdisaker: Ikke gjør det lett for dem å gjette passordene dine. De fleste trenger ikke teknisk spisskompetanse for å få tilgang til kontoene dine – det kan de klare bare med noen få gjett på passordene dine eller ved å bruke et automatisert program.

Om har de først kommet seg inn på én konto, kan de prøve det samme passordet på andre kontoer, samle informasjon om deg og vanene dine, ta over kontoene dine eller attpåtil bruke din digitale identitet.

I denne datadetoxen lærer du praktiske grep for å styrke nettsikkerheten din.

Klar, ferdig, gå!

Et produkt av

**TACTICAL
TECH**

Støttet av

 **Firefox**

datadetoxkit.org
#datadetox

1.

HOLD DIGITALDØRA LÅST

Skjermlåser: Passordet, mønsteret, fingeravtrykket eller ansikts-ID-en du bruker til å låse opp enhetene dine, er det beste forsvaret du har mot at noen kommer seg inn på dem. Men det er mange låser å velge mellom der ute, og det kan være vanskelig å vite hvilken som er best for deg.

Å ha en form for lås på mobilen, nettbrettet eller PC-en gir deg mer beskyttelse enn om du ikke har det. **Og akkurat som med ulike typer låser du kan ha på ytterdøra di, er noen skjermlåser sikrere enn andre.**

Av alle låsetypene som finnes, er lange, unike passord de sterkeste. Det betyr at om du bruker et passord til å låse opp enheten din, bør det inneholde bokstaver, tall og spesialtegn.

La oss si at du i dag låser opp mobilen ved å sveipe med fingeren. Da kan du enkelt skjerpe sikkerheten ved å lage deg et langt passord. Eller bruker du et mønster for å låse opp? Hva med å gjøre mønsteret lengre? Er PIN-koden din 1234? Hva med å trille en terning sju ganger og heller pugge det som PIN-kode? **En liten endring kan gjøre god vei i vellinga for å få kontroll på enhetene dine.**

2.

LA DEN RETTE KOMME INN

Å lage førsteklasses passord er lett som en plett. Alt du trenger å gjøre, er å holde deg til noen enkle prinsipper. Passordet ditt bør være:

Langt: **Passord bør være minst åtte tegn lange. Enda bedre? 16–20 tegn.**

Unikt: **Hvert passord du bruker – på hvert nettsted – bør være forskjellig.**

Tilfeldig: **Passordet ditt bør ikke følge noe logisk mønster eller være lett å gjette. Her er passordadministratorer til stor hjelp.**

De sterkeste passordene inneholder en blanding av bokstaver, tall og spesialtegn.

Dette gode og gamle rådet gir deg stadig sterke passord som er vanskelige å gjette. Dessverre er det enkelte systemer som ikke lar deg bruke spesialtegn (som @#\$%-=+) når du lager passord, men en lang nok blanding av bokstaver og tall er bedre enn en kort en.

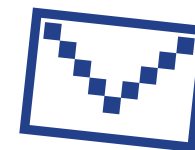
Helst bør du bruke en egen **passordadministrator** til å lage og lagre alle passordene dine. En passordadministrator – som 1Password og KeePassXC, som sikkerhetsekspertene ofte anbefaler – er enkelt og greit en app med ett bruksområde: å beskytte innloggingsinformasjonen din og annen sensitiv informasjon.

3.

BRUK EN EKSTRA LÅS

Å sette opp tofaktoraутентisering (2FA) eller flerfaktoraутентisering (MFA) betyr at selv om noen skulle finne ut av passordet ditt, **vil de sannsynligvis ikke ha den andre faktoren de trenger for å låse seg inn.**

Sjekk sikkerhetsinnstillingene på nettstedene og appene du bruker mest, og se om du kan sette på denne ekstra låsen. Begynn med de viktigste – nettbank-apper eller e-postkontoer du bruker til å gjenopprette de andre kontoene dine.



Google:
**Logg inn på myaccount.google.com →
Sikkerhet →
2-trinns bekreftelse →
Kom i gang**

Facebook:
**Meny →
Innstillinger →
Sikkerhet og innlogging →
Bruk totrinnsverifisering**

Tips: Når du setter opp et ekstra verifiseringstrinn, må du velge en metode for å bekrefte at du er deg. Prøv å unngå å bruke SMS (tekstmeldinger sendt til nummeret ditt) som det ekstra trinnet, i tilfelle du mister mobilen. E-post er vanligvis et tryggere valg.