4.

BESKYT DINE VIRTUELLE VÆRDIGENSTANDE

Du bør beskytte den information, du opbevarer online, på samme måde, som du beskytter værdigenstande i dit hjem. Uanset om det er dit regnskab, en scannet version af dit pas, eller endda din adresse og dit telefonnummer, er det værd at overveje **hvor** du opbevarer dine mest værdifulde personlige data, og **hvordan** de er beskyttet.

Pletrengøring kan være fint, hvis du laver småforbedringer i din kaffepause. Søg efter denne slags information og slet det fra din emailkonto - så er du godt i gang: Scanninger af dit kørekort og pas, bankoplysninger, forsikringsoplysninger og sygesikringsoplysninger. Hvis der er tale om information, du får brug for senere, kan du altid downloade det eller printe det ud, inden du sletter det fra din emailkonto.

En **hovedrengøring** er mere grundig, og bør foretages en gang om året. Arkiver alt i din emailkonto eller dine kontoer på sociale medier. Download det til din computer, og slet indholdet fra kontoerne for **en ny start**.

Tip: Det er ikke nok at slette - du skal også tømme skraldespande og slette midlertidige filer!

Det er op til dig om dine arkiver og dokumenter skal gemmes på et USB-drev, en ekstern harddisk eller et virtuelt drev i skyen. Uanset hvilken løsning, du vælger, skal du sikre dig, at du ikke mister den, at den har et stærkt kodeord, og at den giver mening for dig.

5.

GI' DET VIDERE

Selv om vi let glemmer det, kaldes internettet for "nettet" af en grund. **Vi er alle forbundet online** gennem netværk, ikke kun som "venner" på sociale medier, men også som kontakter i vores emailkontoer og gennem de billeder, vi deler online.

Når du sikrer dine kontoer, styrker dine kodeord og rydder op i dine data, er det ikke kun godt for dig - **alle du er forbundet med bliver sikret en smule bedre ved din indsats.**

Overvej hvad der ellers kan **hjælpe dine venner eller kolleger**, når du rydder op i din emailkonto og dine kontoer for sociale medier: Din søsters bankoplysninger, koden til kontoret, eller den scannede version af din søns pas er bare få eksempler på information, der kan skabe store problemer, hvis det havner i de forkerte hænder.

Gi' det videre! Din digitale sikkerhed kan øges ved at følge et par enkle trin. Del denne Data Detox med dine venner, familie og kolleger for at hjælpe dem ændre deres vaner på en måde, der giver mening for dem.

DATA DETOX KIT

SKIFT DINE INDSTILLINGER

for at sikre dine data

Hvis internettet udelukkende var et sted for billeddeling af **hunde iført dinosaurus-kostumer**, ville der ikke være brug for kodeord.

Men internettet er også stedet, hvor du betaler dine regninger, tilgår dine sundhedsdata, og er i kontakt med kommunen.

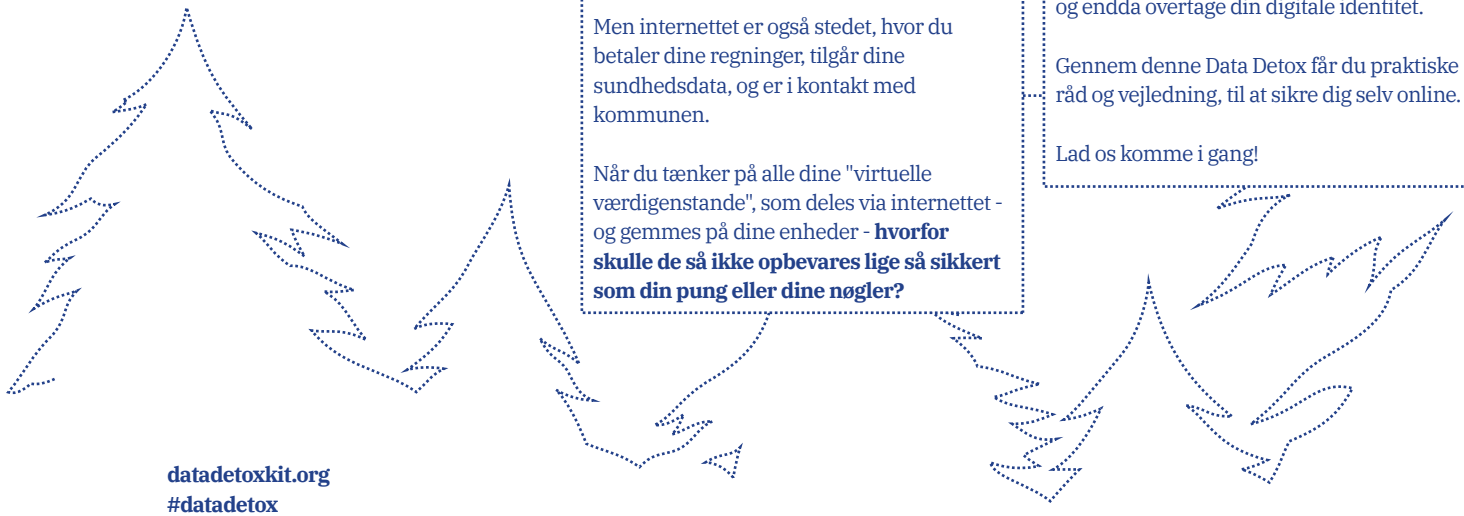
Når du tænker på alle dine "virtuelle værdigenstande", som deles via internettet - og gemmes på dine enheder - **hvorfor skulle de så ikke opbevares lige så sikkert som din pung eller dine nøgler?**

Der findes en enkel måde, hvorpå du kan gøre det svært for andre at få adgang til dine virtuelle værdigenstande: **Undgå at bruge kodeord, der let kan gættes.** Det kræver ikke særlige tekniske evner at få adgang til dine kontoer - det kan gøres ud fra få gæt på dine kodeord eller ved at afvikle et automatisk program.

Og når der først er adgang til dine kontoer, kan dit kompromitterede kodeord benyttes på andre kontoer, og til at samle information om dig og dine vaner, overtage dine kontoer, og endda overtage din digitale identitet.

Gennem denne Data Detox får du praktiske råd og vejledning, til at sikre dig selv online.

Lad os komme i gang!



A product of
TACTICAL TECH

Supported by
Firefox

datadetoxkit.org
#datadetox

1.

LÅS DIN DIGITALE DØR

Skærmlåse: Kodeord, mønstre, fingeraftryk eller face ID er nogle af **dine bedste forsvar** mod andre, som vil have adgang til din enhed. Men der er også andre muligheder, og det kan være svært at finde det bedst egnede for dig.

Enhver form for lås på din telefon, tablet eller computer er bedre end ingen lås. Og ligesom der findes forskellige dørlåse, er **nogle skærmlåse mere effektive end andre.**

Den mest effektive af alle låse, er lange unikke kodeord. Et effektivt kodeord består af både bogstaver, tal og specialtegn.

Hvis du låser din telefon op med et swipe, kan du øge din sikkerhed betragteligt ved at skifte til et langt kordord. Hvis du bruger låser din telefon op med et mønster, kan du øge sikkerheden ved at gøre mønstret længere. Bruger du 1234 som PIN-kode? Prøv at slå men en terning syv gange og brug de tal i stedet.

Der skal ikke så meget til for at sikre kontrollen med din enhed.

Du kan lære hvordan du skaber den mest effektive låseskærm under Styrk dine låste skærme.

2.

LUK DEN RETTE IND

Det er let at skabe stærke kodeord. Du skal bare følge nogle få enkle principper. Dine kodeord bør være:

Lange: **Kodeord består af mindst otte tegn. Endnu bedre? 16-20 tegn**

Unikke: **Hvert kodeord du bruger - for hver eneste side - bør være forskellig fra dine andre kodeord**

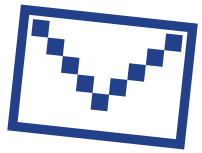
Random: **Dit kodeord bør ikke følge logiske mønstre eller være let at gætte. Det er her Password Managers kommer ind i billedet.**

De stærkeste kodeord indeholder en kombination af bogstaver, tal og specialtegn. Dette råd har bevist sit værd over tid, og sikrer dig fortsat kodeord, der er stærkere og sværere at gætte. Nogle systemer tillader ikke brugen af specialtegn (fx @#$%-=+), men en lang kombination at bogstaver og tal er stadig bedre end en kort en.

Ideelt bør du gøre brug af en **dedikeret Password Manager** til at generere og huske alle dine kodeord. En Password Manager - som eksempelvis 1Password og KeePassXC, der oftest anbefales af sikkerhedseksperter - er basalt set en app med det hovedformål at beskytte dine loginoplysninger og andre følsomme data.

3.

TILFØJ ENDNU EN NØGLE



Totrinsbekræftelse (2FA) eller multifaktorgodkendelse (MFA) gør det stort set umuligt for andre at komme ind, selv om de finder dit kodeord. Fordi **de med stor sandsynlighed ikke har adgang til den ekstra godkendelse.**

Kast et blik på sikkerhedsindstillingerne for dine mest benyttede hjemmesider og apps, og undersøg om du kan benytte en ekstra nøgle. **Læg ud med de vigtigste** - dine bank- og finansapps, eller services som email, som du også benytter til gendannelse af dine kontoer.

Google:
Log in på: myaccount.google.com →
Sikkerhed →
Totrinsbekræftelse →
Kom godt i gang

Facebook:
Menu →
Indstillinger →
Sikkerhed og login →
Brug totrinsgodkendelse

Tip: Når du tilføjer et ekstra sikkerhedslag, skal du vælge endnu en måde, hvorpå du kan bekræfte, at det er dig. Undgå at bruge SMS til dette (altså tekstbeskeder til din telefon), i tilfælde af du mister din telefon. Email er som regel den bedste løsning.