4.

BESCHERM JE VIRTUELE KOSTBAARHEDEN

Je geeft de waardevolle spullen in je huis een veilige plek en je zou hetzelfde moeten doen met de informatie die je virtueel bewaart – Of het nou om je financiële gegevens, scans van je paspoort of zelfs je adres of telefoonnummer gaat; het is geen overbodige luxe om na te denken over wáár en hóe je deze waardevolle persoon- lijke gegevens bewaart en beschermt.

Even **snel oppoetsen** is prima als je tijdens de koffie snel wat verbeteringen wilt doorvoeren. Zoek naar specifieke informatie in je e-mail of andere accounts en verwijder die: scans van je ID, bankgegevens of informatie over je zorgverzeke- ringen, om maar wat te noemen. Als het iets is wat je later weer nodig hebt kun je het altijd downloaden of printen voordat je het uit je e-mail account verwijdert.

Een **grote schoonmaak** gaat dieper en die zou je eens per jaar moeten doen. Archiveer alle gegevens in je e-mail of socialmedia-account, download die gegevens op je computer en verwij- der alle inhoud uit de accounts om weer met een schone lei te beginnen.

Tip: Als je het echt goed wilt doen, moet je niet alleen alles verwijderen, maar ook je prullenbak en tijdelijke bestanden leegmaken!

Je kunt zelf bepalen wat je het liefste doet: een back-up van je archieven en documenten in de cloud opslaan, of ze op een externe harde schijf of USB-stick bewaren. Hoe je de informatie ook opslaat, zorg ervoor dat je het niet kwijtraakt, dat je een sterk wachtwoord gebruikt en dat de methode bij je past.

Een product van
TACTICAL TECH

Ondersteund door
Firefox

5.

DOORGEVEN

Je zou het bijna vergeten, maar er is een reden dat we het internet het "web" noemen. **We zijn online allemaal met elkaar verbonden** door middel van verschillende netwerken, niet alleen als "vrienden" op social media, maar ook via de contacten in ons e-mailaccount en de foto's die we online delen. Als jij je accounts beveiligt, je wachtwoorden sterker maakt en je data opruimt ben jij niet de enige die daar baat bij heeft – **iedereen met wie je contact hebt, wordt zo een beetje veiliger door jouw inspanningen.**

Als je je e-mail en socialmedia-accounts opruimt bedenk dan wat je nog meer kunt downloaden en verwijderen om je vrienden en collega's te helpen: de bankgegevens van je zus, de toegangscode van het kantoor, de scan van het paspoort van je zoon zijn voorbeelden van gegevens die beslist niet in verkeerde handen mogen vallen.

Geef het door! Met een paar eenvoudige stappen kun je je digitale beveiliging verbeteren. Deel deze Data Detox met je vrienden, familie en collega's zodat ook zij hun gewoontes kunnen veranderen op een manier die bij hen past.

DATA DETOX KIT

VERANDER JE INSTELLINGEN

om je gegevens te beveiligen

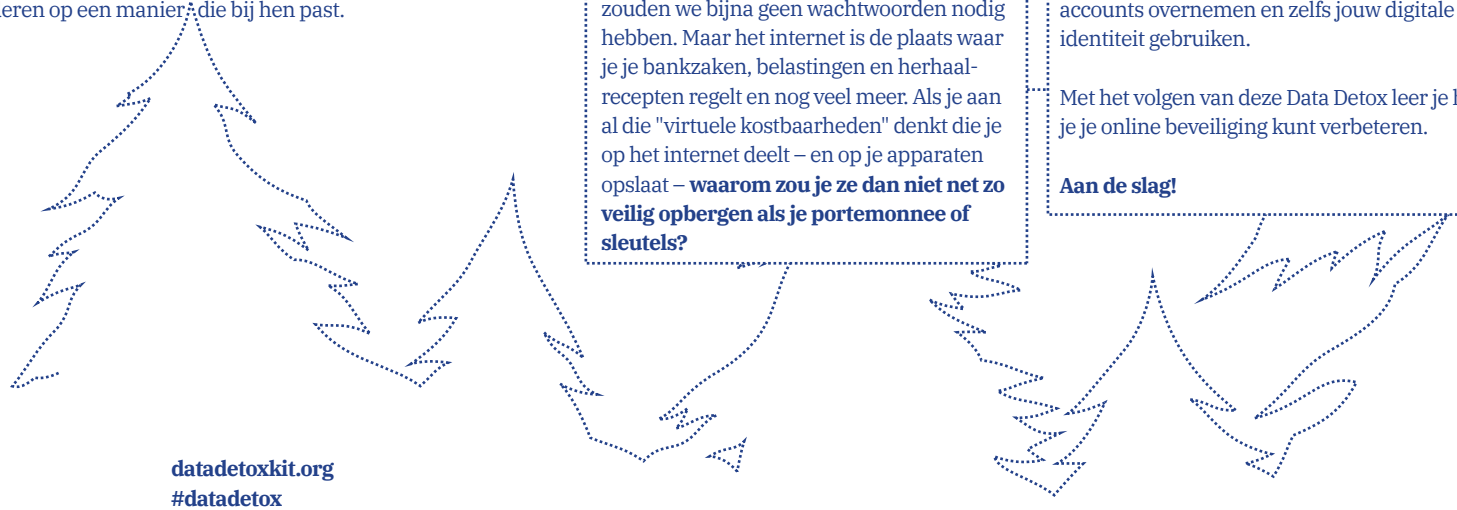
Als we op het internet alleen maar foto's van onze hond in rendierpak zouden delen, zouden we bijna geen wachtwoorden nodig hebben. Maar het internet is de plaats waar je je bankzaken, belastingen en herhaal- recepten regelt en nog veel meer. Als je aan al die "virtuele kostbaarheden" denkt die je op het internet deelt – en op je apparaten opslaat – **waarom zou je ze dan niet net zo veilig opbergen als je portemonnee of sleutels?**

Je kunt heel eenvoudig voorkomen dat anderen toegang krijgen tot jouw virtuele kostbaarheden: **zorg dat ze je wachtwoorden niet makkelijk kunnen raden**. Meestal hoeft iemand niet over gespecialiseerde technische vaardigheden te beschikken om in jouw account te komen – als ze goed kunnen raden, of een geautomatiseerd programma gebruiken, zijn ze zo binnen.

En als ze toegang hebben tot één account kunnen ze hetzelfde wachtwoord proberen voor je andere accounts; ze kunnen informatie verzamelen over jou en je gewoontes, je accounts overnemen en zelfs jouw digitale identiteit gebruiken.

Met het volgen van deze Data Detox leer je hoe je je online beveiliging kunt verbeteren.

Aan de slag!



datadetoxkit.org
#datadetox

1.

VERGRENDEL JE DIGITALE DEUR

Schermvergrendelingen: het wachtwoord, de vingerafdruk of gezichtsherkenning die je gebruikt om toegang te krijgen tot je apparaat zijn **prima verdedigingswerken** om te voorkomen dat iemand anders toegang krijgt tot je apparaat. Maar er zijn veel verschillende soorten vergrendelingen beschikbaar en het kan moeilijk zijn om te bepalen welke het beste werkt voor jou.

Iedere vorm van vergrendeling op je telefoon, tablet of computer geeft meer bescherming dan helemaal geen vergrendeling. En net als de verschillende soorten sloten die er voor deuren zijn, **zijn sommige schermver- grendelingen sterker dan andere.**

Van alle vergrendelingen die er bestaan zijn de lange, unieke wachtwoorden het sterkst. Dus als je je apparaat met een wachtwoord ontgrendelt, moet dat wachtwoord bestaan uit letters, cijfers en speciale tekens. Als je nu je telefoon opent door te vegen kun je de beveiliging verbeteren met het instellen van een lang wachtwoord. Gebruik je nu een bewegingspatroon? Dan zou je dat patroon langer kunnen maken. Gebruik je 1234 als pincode? Gooi eens zeven keer met een dobbelsteen en maak van die cijfers een pincode.

Met een kleine verandering kun je grotere controle krijgen over de beveiliging van je apparaten.

2.

EEN OPEN DEUR VOOR DE JUISTE PERSOON

Supergoede wachtwoorden maken is makkelijk. Je hoeft alleen maar wat basisprincipes te volgen. Kenmerken van een sterk wachtwoord:

Lang: **wachtwoorden moeten uit minimaal 8 tekens bestaan. Wil je het nog beter doen? 16 à 20 tekens.**

Uniek: **ieder wachtwoord voor iedere site moet anders zijn.**

Willekeurig: **je wachtwoord moet geen logisch patroon volgen of makkelijk te raden zijn. Wachtwoordmanagers kunnen je hierbij helpen.**

De sterkste wachtwoorden bestaan uit een combinatie van letters, cijfers en speciale tekens. Dit eeuwenoude advies is nog steeds van toepassing als het gaat om het maken van een sterk, moeilijk te raden wachtwoord. Helaas kun je in sommige wachtwoord- systemen geen gebruikmaken van speciale tekens (zoals @#$%-=+), maar een lange combinatie van letters en cijfers is nog altijd beter dan een korte.

Het is het beste als je een speciale wachtwoordmanager gebruikt om al je wachtwoorden te maken en bewaren. 1Password, LastPass en KeePassXC zijn wachtwoordmanagers die vaak worden aangeraden door beveiligingsexperts. Het zijn apps die je gebruikt om inloggegevens en andere gevoelige informatie te beschermen.

3.

MAAK EEN TWEEDE SLEUTEL

Als je tweestaps- of meervoudige verificatie instelt en iemand je wachtwoord ontdekt **beschikt die persoon waarschijnlijk niet over de extra informatie die nodig is om binnen te komen.**

Kijk eens naar de beveiligingsinstellingen van de sites en apps die je het meest gebruikt om te zien of je zo'n extra stap kunt instellen. Begin met de belangrijkste – bank-apps, of diensten zoals e-mail die je gebruikt als back-up wanneer je geen toegang krijgt tot je andere accounts.

Google:
Log in op: myaccount.google.com →
Beveiliging →
2-stapsverificatie →
Aan de slag

Facebook:
Menu →
Instellingen →
Beveiliging en aanmelding →
Tweestapsverificatie gebruiken

Tip: als je een tweede verificatiestap wilt instellen moet je een manier kiezen om te bevestigen dat jij het bent. Kies liever niet voor sms als tweede stap, want daar heb je niets aan als je je telefoon bent verloren. E-mail is een betere optie.