4.

MINSKA DINA SPÅR

Webbläsaren på din telefon sparar mycket information om dig – din plats, vad du söker efter, vilka hemsidor du använder – och kan ge bort den informationen. Du kan ta tillbaka kontrollen över en del av den informationen genom att göra några ändringar.

Telefoner, surfplattor och datorer har ofta förinstallerade webbläsare som inte prioriterar din integritet: Du kan istället **ladda ner och använda en webbläsare** som håller din aktivitet på nätet **mer privat från början** och skyddar dig från spårare.

För ytterligare lite bättre integritetsskydd kan du installera extrafunktioner, eller ”tillägg” (dessa är lättinstallerade miniprogram till din webbläsare som kan **göra din aktivitet på nätet mer privat**).

För att blockera spionerande reklam och osynliga spårare, installera **uBlock Origin** (för Chrome, Safari och Firefox) eller **Privacy Badger** (för Chrome, Firefox och Opera).

För att försäkra dig om att din anslutning till hemsidor alltid är säker när så är möjligt, installera **HTTPS Everywhere**: ett webbläsartillägg som ser till att din kommunikation med många stora sidor är krypterad och skyddad. Om du använder Safari och vill ha denna funktion, använd en sökmotor som inte är Google, till exempel DuckDuckGo, som automatiskt hänvisar dig till krypterade anslutningar.

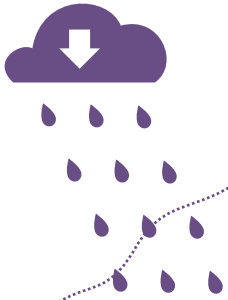
5.

AVTAGGA DIG SJÄLV OCH DINA VÄNNER

Har du bidragit till datainsamling av dina vänner genom att tagga dem i foton och inlägg?

Minska deras datamängd (och ditt samvete på köpet) genom att **avtagga dem** i så många foton och inlägg som möjligt.

Sprid budskapet! Uppmuntra dina vänner, din familj och dina kollegor att delta i kampen mot oskyddad data. Om vi jobbar tillsammans för att ta kontroll över våra dataspår så kan vi hjälpa varandra att detoxa.



TA KONTROLL ÖVER DIN SMARTPHONE-DATA

Förbättra din integritet på nätet

DATA DETOX KIT

När du tänker på vad din data berättar för andra om dig så kanske det inte verkar som en så stor grej: vem bryr sig om att du gillar countrymusik, att köpa fler skor än du behöver eller att du behöver planera dina semestrar ett år i förväg?

Problemet är vad som händer med din data. Över tid så kan man urskilja **intima digitala mönster**: dina vanor, rörelser, relationer, preferenser, åsikter och hemligheter avslöjas för dem som **analyserar och tjänar pengar** på dem, såsom företag och datamäklare.

Genom att följa denna Data Detox får du en inblick i hur och varför detta händer och du får en chans att ta praktiska steg för att **ta kontroll över den data du lämnar efter dig på nätet**.

Nu kör vi!

En produkt från
TACTICAL TECH

Med stöd av
Firefox

datadetoxkit.org
#datadetox

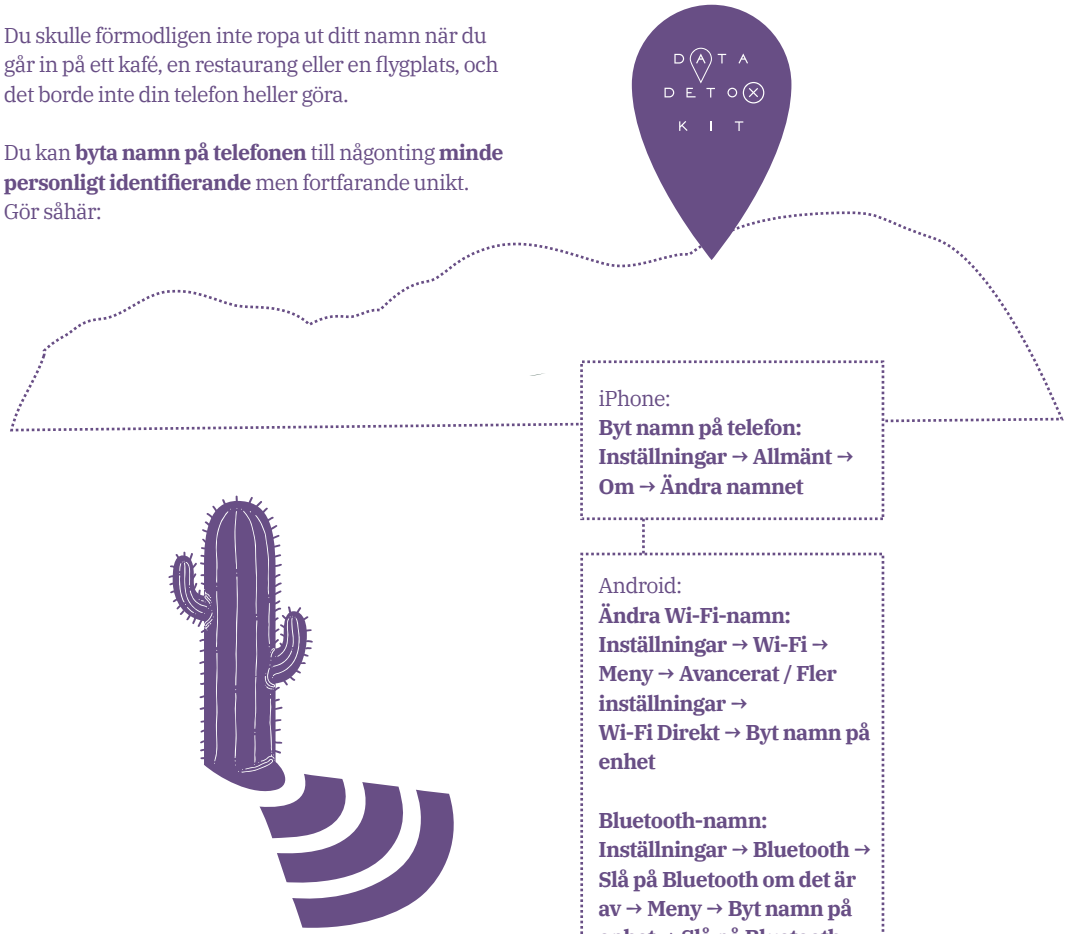
1.

BYT ENHETSNAMN

Du kanske någon gång har ”döpt” din telefon för Wi-Fi, Bluetooth eller båda två. Eller så har namnet kanske valts automatiskt när du installerade enheten. Det betyder at “Alex Chungs Telefon” är vad som syns för ägaren av Wi-Fi-nätverket och, om din Bluetooth är påslagen, för alla i närheten som också har sin Bluetooth påslagen.

Du skulle förmodligen inte ropa ut ditt namn när du går in på ett kafé, en restaurang eller en flygplats, och det borde inte din telefon heller göra.

Du kan **byta namn på telefonen** till någonting **minde personligt identifierande** men fortfarande unikt. Gör såhär:



iPhone:
Byt namn på telefon:
Inställningar → Allmänt → Om → Ändra namnet

Android:
Ändra Wi-Fi-namn:
Inställningar → Wi-Fi → Meny → Avancerat / Fler inställningar → Wi-Fi Direkt → Byt namn på enhet

Bluetooth-namn:
Inställningar → Bluetooth → Slå på Bluetooth om det är av → Meny → Byt namn på enhet → Slå på Bluetooth

2.

RENSA DINA GEOGRAFISKA FOTSPÅR

Det kan verka som att din platsdata bara är **slumpmässiga bitar** data, men om man lägger ihop dem så kan de avslöja **viktiga detaljer om dig** och dina vanor, var du bor, var du arbetar och var du gillar att umgås med vänner. Det är det som gör det så eftertraktat bland företag och datamäklare.

Du kan **gå igenom varje apps inställningar** och **slå av platstjänster**. Håll utkik efter appar där du egentligen inte behöver tjänsten (behöver det där spelet verkligen veta var du befinner dig?) och för appar som du inte vill dela din plats med:

Android:
Inställningar → Appar → Hantera platstillgång på en app i taget.

iPhone:
Inställningar → Integritetsskydd → Platstjänster → Hantera platstillgångar på en app i taget.

3.

STÄDA BLAND DINA APPAR

Dina sociala medie-appar, spel och väderappar är intresserade av din data ... och de kan samla in en hel del.

Att göra dig av med de apparna som du aldrig använder på din telefon kan vara ett effektivt sätt att ge ditt digitala jag en detox

Att städa bland apparna kan också **frigöra mer utrymme** på telefonen, minska dataanvändningen och **öka batteritiden**. Det kan till och med förbättra telefonens prestanda, beroende på vilken app du raderar.

Android:
Inställningar → Appar → Välj appen du vill avinstallera → Avinstallera

iPhone:
Tryck och håll kvar fingret på en app tills de alla börjar skaka och små kryss dyker upp i övre vänstra hörnet på varje app.

För att ta bort en app, tryck på det lilla krysset.

För att återgå till vanligt läge, tryck på hemknappen.

4.

SKYDDA DINA VIRTUELLA VÄRDESAKER

På samma sätt som du skyddar dina värdesaker i hemmet bör du skydda värdefull information som du sparar digitalt – vare sig det gäller bankinformation, en inskannad bild av ditt pass, eller till och med din adress och ditt telefonnummer, så är det värt att tänka på **var** du sparar din mest värdefulla personliga information och **hur** du kan skydda den.

En **punktrengöring** är toppen om du vill göra några snabba förbättringar över en kopp kaffe. Sök efter specifik information i din e-post eller andra konton och ta bort den: **skannade bilder av ditt ID, bankinformation eller försäkringsuppgifter** med mera. Om det är något du kan behöva senare så kan du alltid ladda ner det eller skriva ut det innan du tar bort det från ditt e-postkonto.

En **djup rengöring** är mer grundlig och är lämplig att göra en gång om året. Arkivera allt i din e-post och dina sociala medie-konton, ladda ner det till din dator och ta bort allt innehåll på kontot för att **få en nystart**.

Tips: Ta inte bara bort saker, töm också papperskorgen och ta bort tillfälliga filer!

Det är upp till dig om du vill göra säkerhetskopior av dina arkiv och dokument i molnet eller spara dem på en extern hårddisk eller USB-sticka. Oavsett hur du sparar filerna, se till att du inte tappar bort dem, att du har ett starkt lösenord och att det passar dig.

5.

VI HJÄLPER VARANDRA

Det är lätt att glömma att nätet kallas för ett ”nät” av en anledning. **Vi kopplas alla samman** via olika nätverk, inte bara som ”vänner” på sociala medier, utan även genom kontakterna i våra e-postkonton och de foton vi delar på nätet. När du säkrar dina konton, förstärker dina lösenord och städar upp bland din data så är det inte bara dig själv du hjälper – **alla du är ihopkopplade med blir lite säkrare tack vare dig**.

När du städar din e-post och dina sociala medie-konton, tänk på vad du mer skulle kunna ladda ner och ta bort som skulle kunna **hjälpa dina vänner och kollegor**: din systers bankinformation, portkoden till kontoret, eller din sons inskannade lösenord är bara några exempel på dokument som skulle skapa problem om de hamnade i fel händer.

Vi hjälper varandra! Du kan förbättra din digitala säkerhet genom att följa några få enkla steg. Dela denna Datadetox med dina vänner, din familj, eller dina kollegor för att hjälpa dem ändra sina vanor på sätt som passar dem.

DATA DETOX KIT

ÄNDRA DINA INSTÄLLNINGAR

för att säkra din data

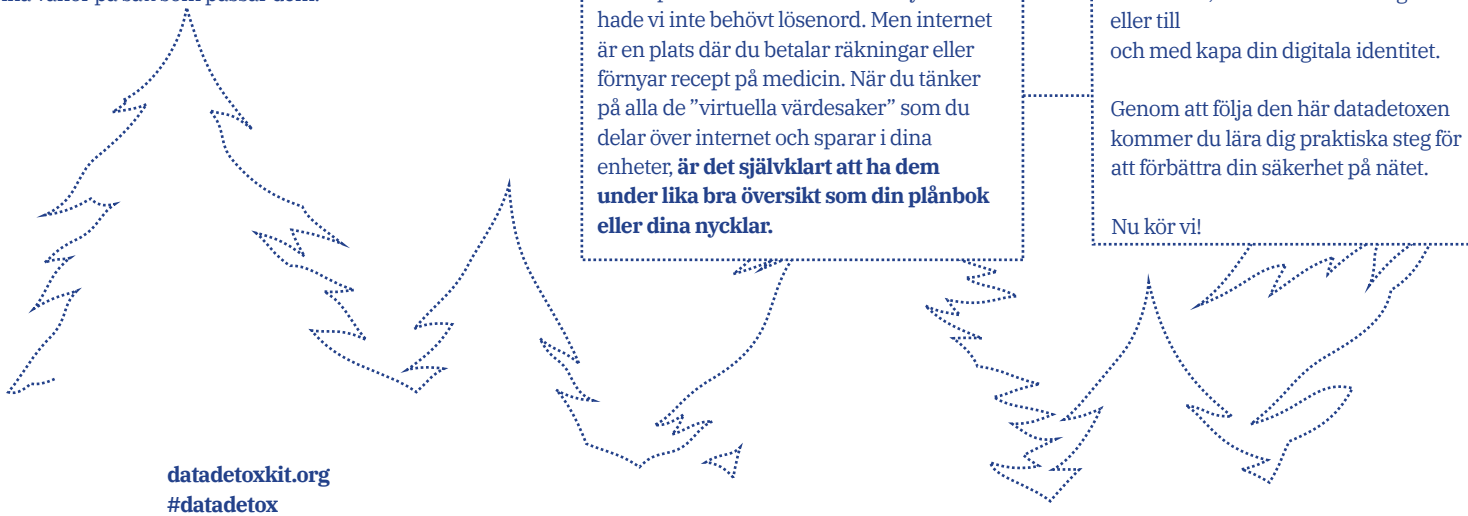
Om internet bara var en plats för att dela bilder på hundar i dinosauriekostymer så hade vi inte behövt lösenord. Men internet är en plats där du betalar räkningar eller förnyar recept på medicin. När du tänker på alla de ”virtuella värdesaker” som du delar över internet och sparar i dina enheter, **är det självklart att ha dem under lika bra översikt som din plånbok eller dina nycklar.**

Det finns ett enkelt sätt att göra det svårare för andra att få tillgång till dina virtuella värdesaker: **gör det inte lätt för dem att gissa ditt lösenord**. De flesta behöver inga speciellt tekniska kunskaper för att ta sig in i dina konton, de behöver bara försöka gissa ditt lösenord eller köra ett automatiskt program för att göra det.

Och när de väl tagit sin in i ett konto kan de testa det lösenordet på andra konton, samla information om dig och dina vanor, ta över konton du äger eller till
och med kapa din digitala identitet.

Genom att följa den här datadetoxen kommer du lära dig praktiska steg för att förbättra din säkerhet på nätet.

Nu kör vi!



En produkt från
TACTICAL TECH

Med stöd av
Firefox

datadetoxkit.org
#datadetox

1.

LÅS DIN DIGITALA DÖRR

Skärmlås: lösenordet, mönstret, fingeravtrycket, eller ansikts-ID:et du använder för att få tillgång till din enhet är några av **dina bästa försvar** mot personer som vill ta sig in i dina enheter. Men det finns många olika metoder och det kan vara svårt att veta vilket som passar dig bäst.

Att ha något slags lås på din telefon, platta eller dator ger dig mer skydd än inget lås alls. Och precis som de olika typerna av lås du kan ha på en dörr är **vissa skärmlås är starkare än andra**.

Det starkaste låset av alla är ett långt, unikt lösenord. Det innebär att om du låser upp enheten med ett lösenord så bör det innehålla bokstäver, siffror och specialtecken.

Säg att du använder en enkel svepgest för att öppna din telefon. Du kan sakta öka din säkerhet genom att skapa ett långt lösenord. Har du redan idag ett system för att skapa och komma ihåg lösenord? Vad sägs om att göra det längre? Är din PIN 1234? Vad sägs om att slå en tärning sju gånger och memorera resultatet som en PIN istället?

En liten förändring kan räcka långt för att få kontroll över dina enheter

2.

LÅT DEN RÄTTE KOMMA IN

Att skapa jättebra lösenord är enkelt. Allt du behöver göra är att följa några enkla principer. Ditt lösenord bör vara:

Långt: lösenord borde vara minst åtta tecken. Ännu bättre är 16-20 tecken.

Unikt: alla dina lösenord – för alla sidor du använder – bör vara olika

Slumpmässigt: ditt lösenord borde inte följa ett logiskt mönster eller vara enkelt att gissa. Det är här som lösenordshanterare kan vara väldigt användbara.

De starkaste lösenorden använder en kombination av bokstäver, siffror och specialtecken. Det ger starkare, mer svårgissade lösenord. Tyvärr tillåter vissa system inte specialtecken (som @#$%-=+), men en tillräckligt lång kombination av bokstäver och siffror är fortfarande bättre än en kort.

Det allra bästa är att använda en **lösenordshanterare** för att skapa och spara alla dina lösenord. Lösenordshanterare – som 1Password och KeePassXC som båda ofta rekommenderas av säkerhetsexperter – är appar vars enda syfte är att skydda dina inloggningsuppgifter och andra viktiga data.

3.

LÄGG TILL EN NYCKEL TILL

Att skapa en tvåfaktorauktorisering (2FA) eller multifaktorauktorisering (MFA) innebär att även om någon får tag på ditt lösenord så har de **förmodligen inte den extrafaktor de behöver för att komma in**.

Titta på säkerhetsinställningarna på dina mest använda appar och se om de tillåter en sådan extranyckel. **Börja med de viktigaste apparna** – ekonomiappar eller tjänster som t.ex. e-post som du använder för att återskapa lösenord för andra konton.

DATA DETOX KIT

Google:
Logga in på **myaccount.google.com** →
Säkerhet →
Tvåstegsverifiering →
Kom igång

Facebook:
= meny →
Inställningar →
Säkerhet och inloggning →
Använd tvåfaktorsautentisering

Tips: När du lägger till ett verifieringslager behöver du ytterligare ett sätt att bekräfta att det är du som loggar in. Undvik gärna SMS utifall att du blir av med din telefon. E-post är oftast mer pålitligt.

4.

GÖR DIG SJÄLV HÖRD

Om du inte är nöjd med den vanebildande eller oärliga design och desinformation du möter på olika hemsidor eller i appar du använder så kan du e-posta, skriva på Twitter och tala om för företagen att du inte gillar deras beteenden. När ett företag pressas av dess mest värdefulla tillgång – användarna – så finns det en chans till faktisk förändring.

Om du inte känner att din åsikt blir hörd så finns det något väldigt effektivt som du kan göra: **använda en annan hemsida eller app**. Om du har förklarat att du är missnöjd med något som en sida eller app gör och sedan faktiskt slutar använda sidan eller avinstallerar appen, och tillräckligt många gör detsamma, **så märks det**.

5.

SPRID BUDSKAPET

Sprid budskapet! Det här är ett enkelt knep, men det kan ha stor effekt. Berätta för dina vänner, din släkt och dina kollegor om sakerna du märker. Du kan uppmana dem att ta den här detoxen med dig! Alla kämpar med att hantera sina telefonvanor. Det viktiga är att du hittar ett sätt som känns rätt för dig och som passar just din livsstil. Testa dig fram tills du hittar vad som känns rätt, och uppdatera dina vanor när dina behov ändras över tid. Det finns ingen lösning som passar för alla.

Och slutligen, dela dina val med personer omkring dig. Låt oss säga att du inte kommer vara tillgänglig på Messenger efter klockan 20 varje kväll eftersom det är då du börjar din skrämfria tid: berätta det för din släkt och dina vänner så att de kan ringa dig istället. Håll igång en dialog och ställ frågor, så att du kan leva ett balanserat uppkopplat liv som passar dig.

DATA DETOX KIT

UNDVIK STANDARDINSTÄLLNINGAR

för att öka ditt digitala välmående

När ”drog du ur kontakten” senast och lät bli att röra någon teknikpryl på en hel dag, eller ens på en hel timme?Du är inte ensam om att alltid vara uppkopplad. Den genomsnittliga personen pekar, klickar och sveper på sin telefon mer än 2600 gånger om dagen. Om du gör någonting så ofta så vill du väl ändå känna att det är värt det? Hur kan du se till att din tid med din enhet blir kvalitetstid?

Det börjar med insikten att det där suget efter teknik inte är ditt fel! Tro det eller ej, dina favoritappar och hemsidor är designade så att varje funktion, färg och ljud ”optimerats” för att hålla dig fast, såld och se till att du kommer tillbaka gång efter annan.

Vill du hitta en hälsosammare balans mellan ditt uppkopplade och ditt nedkopplade liv? Det är vad den här delen av Datadetoxen handlar om.
Nu kör vi!

En produkt från
TACTICAL TECH

Med stöd av
Firefox

datadetoxkit.org
#datadetox

1.

VAR NÄRVARANDE I NUET

Det här tipset är svårare än det låter. Att stanna kvar i nuet kräver daglig träning. Det är som en muskel i din hjärna som du måste träna regelbundet. Du kan börja med att lägga märke till din relation till tekniken du använder.

Hur mycket tid spenderar du på din telefon?

Om du inte är nöjd med svaret så finns det inställningar och strategier som du kan använda för att få kontroll över den teknik du använder.

Om ditt mål är att spendera mindre tid på Facebook, Instagram eller Snapchat, ändra då inställningar och åtkomst för dessa appar för att få dem att fungera bättre för dig.

Vissa appar, t.ex. Instagram, har till och med en inställning där appen diskret påminner dig när du nått din dagliga tidsgräns för användning.

Instagram:
Profil → meny →
Inställningar → Konto →
Din Aktivitet →
Sätt Daglig Påminnselse

Om du märker att telefonen stör dina konversationer i verkliga livet med ringsignaler, surrande och blinkande så kan du **tillfälligt tysta den**, lägg den med skärmen nedåt eller lägga undan den i fickan eller din väska så att den inte är i blickfånget.

2.

KÄNN IGEN DESIGNTRICKEN

Övertalande design, även känd som ”mörka mönster” är designmönster baserade på mänsklig psykologi med målet att få dig att skriva upp dig på någonting, köpa någonting, eller ge bort mer personlig information än du förstått eller tänkt dig.

Vanliga designknep är att använda vissa färger, knapplaceringar, tvetydig text, eller inkomplett information. Ibland är knepen uppenbara, men ibland är de svårare att se. Du har kanske redan känt igen vissa när du skrivit upp dig på en prenumeration eller handlat på nätet. Anledningen till att du ser dessa knep överallt är att de fungerar – de får oss att klicka, prenumerera, köpa oftare och de får oss att komma tillbaka. Ju mer medveten du är om de diskreta små knepen och manipulationerna som är inbäddade i hemsidorna du använder, desto bättre rustad och informerad blir du.

Det finns flera saker du kan göra för att överlista dina appar.

Känn igen när du blir påverkad: Det första du kan göra är att helt enkelt bli medveten om när de här teknikerna används mot dig. Läs mer om de olika typerna här och följ Twitterkontot eller hashtaggen för att hålla koll på nya övertalningstekniker.

Ta och dela skärmdumpar: Ta skärmdumpar när du stöter på den här typen av designmönster på nätet och dela dem med dina vänner (men kom ihåg att utelämna personinformation som kan identifiera dig först!). Du kan också be företagen att ändra sina metoder.

Var lugn: Om det finns en nedräkningsklocka på en köpsida, fråga dig själv ”Är det verkligen bråttom?” Om du märker att du klickar på en knapp som du inte riktigt ville klicka på, lägg märke till knappens färg eller hur tjänsten formulerat sin text. Om du känner dig förvirrad – anta inte direkt att det är ditt fel – titta på orden som sidan eller appen använder; de kan mycket väl vara oklara.

3.

VAR MEDIEKRITISK

På samma sätt som du kan lära dig att överlista funktioner och design som försöker få dig att fortsätta scrolla och klicka så kan du lära dig att känna igen nyhetsartiklar och inlägg som försöker lura dig.

Du har vid det här laget säkert hört talas om problemen med ”desinformation” och ”fake news”. Du kan känna igen desinformation om du har som vana att ställa kritiska frågor kring nyheter du konsumerar, speciellt om nyheterna verkar överraskande, otroliga, eller för bra för att vara sanna.

Vilken sida är nyheten från?
Vem skrev nyheten (och när)?
Vad säger artikeln som helhet, utöver rubriken?
Vilka källor hänvisar de till?

I slutändan vill du kunna avgöra vilka nyheter som är sanna och vilka som är falska – speciellt om du tänker dela dem med släkt eller vänner.

Om du tror att det är desinformation och vill stoppa dess spridning så har de flesta plattformar en funktion för att rapportera inlägget. Du kanske också vill ta en funderare huruvida du vill fortsätta följa kontot i fråga eller inte.

5.

SÖK SANNINGEN PÅ INTERNET

Termen “fake news” används för en bred samling felaktig eller vilseledande information, inklusive satir, dåligt researchad eller obekräftat innehåll och bluffar. Fake news sprids inte alltid med dåligt uppsåt, men oavsett varför det delas så är resultatet oftast detsamma: mottagarna tror att något felaktigt är korrekt, eller att någonting som inte hänt har hänt.

I bästa fall kanske det är en humoristisk meme, i värsta fall kan det vara felaktig hälsoinformation eller falsk politisk information.

Trots dina bästa försök att undersöka och fråga kritiska frågor kring artiklar du läser så kan du fortfarande bli förvirrad. Men: du är inte ensam!

Alle man på däck
Bara för att en hemsida inte erkänner några misstag innebär det inte att man inte gör dem. De mest pålitliga publikationerna är de som är extra försiktiga med sanningen och anställer personer eller hela avdelningar för faktakoll.

Håll utkik efter transparenta källor, det vill säga de som publicerar rättelser när de haft fel. Ännu bättre är när uppdateringen sammanfattas längst upp i artikeln och delas på sociala medier, så du inte behöver leta efter den.

6.

SPRÄCK DIN FILTERBUBBLA

Efter att hemsidor och appar byggt en profil över vad dina intressen är kan du helt plötsligt befinna dig i en **filterbubbla**. Det innebär att tjänster matar dig med historier som liknar de du redan blivit engagerad av. Hur begränsar eller ändrar det vad du hör talas om?

Filterbubblor kan göra att folk ser helt olika historier, nyhetsrubriker, artiklar och annonser, vilket kan göra att de har tillgång till helt olika uppsättningar med information som inte har någonting gemensamt. En illustration av detta finns i den interaktiva artikeln **Blue Feed, Red Feed** (graphics.wsj.com/blue-feed-red-feed).

Om du vet att du ser algoritmiskt kurerat innehåll i en filterbubbla som sträcker sig över dina appar och hemsidor så blir frågan: vad kan du göra för att ta dig ur filterbubblan?

Ändra vindriktningen och blanda nyheterna
Ett bra sätt att spräcka filterbubblan är att prenumerera på tjänster som samlar in nyheter och information från ett brett utbud av **källor och perspektiv**. RSS-flöden, forum och mailinglistor med en bred samling åsikter och teman kan hjälpa dig att komma ut ur din bubbla. **Global Voices** och **The Syllabus** är utmärkta startpunkter.

DATA DETOX KIT

6 TIPS FÖR ATT UNDVIKA DESINFORMATION PÅ NÄTET

Appar, hemsidor och nätmedia kan vara toppen för att hitta nyheter, knep i vardagen och underhållning. Men bland allt detta innehåll kan det vara svårt att navigera bland allt som distraherar och hitta det du verkligen letar efter.

Det kan dessutom vara svårt att se skillnad mellan dikt och verklighet när du ser en video, bild, eller artikel på nätet. Från personlighetstest som bygger en profil av dig till chockerande rubriker och förvanskade foton och videor som kan övertyga dig om en helt annan verklighet, så är allt du ser på nätet inte nödvändigtvis som det verkar.

I den här Datadetoxen kommer du att få utforska desinformationsrelaterade ämnen och termer, och få råd om hur du navigerar genom all information där ute.

Nu kör vi!

datadetoxkit.org **#datadetox**

En produkt från
TACTICAL TECH

Projektpartners
Save the Children 100 ANNI
IFLA

Finansierat av Europeiska unionen

1.

INSE DIN MÖJLIGHET ATT GÖR AVTRYCK

Att gilla, dela, retweeta och reposta – alla dessa handlingar innebär att interagera med saker du ser på nätet och dina interaktioner spelar stor roll. När tillräckligt många personer interagerar med en bild, video eller inlägg så sprids det snabbt och blir, per definition, ”viralt”.

Stanna upp ett ögonblick och fråga dig själv **”Hur påverkar jag andra på nätet?”** När såg du senast en chockerande eller rolig artikel, rubrik, video eller bild som du några sekunder senare hade vidarebefordrat till dina vänner? **Forskare har konstaterat** att de historier och bilder som oftast blir virala är de som gör dig rädd, äcklad, imponerad, arg eller orolig. Om detta är något som hände dig senast i morse så var inte ledsen för det!

Att dela spelar roll
Delande är en form av deltagande. När du delar någonting, vad som helst, så deltar du i att potentiellt göra det viralt. Om det du delar till exempel visar sig vara falskt, vill du då verkligen associeras med det? Innan du delar en länk, tänk på att du kanske delar något som inte är sant, som är destruktivt eller osunt.

2.

TÄNK EFTER INNAN DU TAR DET DÄR PERSONLIGHETSTESTET

När såg du senast ett test (i text eller som fotofilter) med ett namn i stil med:

- Vilket årtionde är du?
- Vad är ditt kraftdjur?
- Vad är din drömsemster?
- … listan kan göras lång!

Även om det kan vara frågan om ett roligt test som är gjort för att underhålla dig, så kan frågorna lika gärna vara utformade för att samla in information om dig och **kategorisera din personlighet** utifrån så kallade **psykometriska mönster**.

Dina svar på ett test som “Vilken Simpsons-karaktär är du?” tillsammans med dina andra vanor som kan övervakas av din webbläsare, app, eller länkade saker så som kundkort kan ge dataanalytiker en fingervisning om vilken slags person du är, vad du bryr dig om och hur man kan få dig att köpa ett par skor (till exempel), eller till och med bygga en profil av dig för att försöka påverka hur du röstar i nästa val.

Ha fler hemligheter
När du tänker på privat information är det kanske dina lösenord, ID-nummer och bankkontonummer det första du kommer att tänka på. Men detaljer såsom vad som skrämmer dig, vad som irriterar dig och vad dina ambitioner är precis lika personliga. Dessa detaljer är värdefulla för dataanalytiker och berättar vad som motiverar dig som person. Tänk efter en extra gång innan du ger bort den typen av information i en undersökning eller ett test.

3.

NAPPA INTE PÅ BETET

Klickbete (Click bait på engelska) är en term som används för att beskriva överdrivna, oärliga eller påhittade rubriker som är avsedda att få folk att klicka på en rubrik eller länk. Ju fler interaktioner en artikel, video eller bild får, desto mer pengar kommer den förmodligen att tjäna. Det gör att det finns en drivkraft att säga vad som helst för att få dig att klicka på och dela ett företags innehåll.

Utifrån personlighetsprofiler som byggs av de plattformar du använder (t.ex. Facebook och Instagram) kan du få skräddarsydda rubriker s om har skapats **för att anspela på dina känslor** på ett sätt som får dig att klicka.

Klickbete kan hittas tillsammans med desinformation, men inte alltid. När du väl börjat känna igen klickbetesrubriker kommer du märka dem överallt på Youtube, bloggar och

Hitta källan
Stanna inte vid rubriken när du står inför klickbete. Om det ser ut som en säker länk, klicka på artikeln och läs den från början till slut. Ta reda på vem som skrivit artikeln, när den publicerades och vilka dess källor är. Inuti artikeln kanske det står att den är en betald annons eller att det är en opinionstext. Dessa detaljer kan hjälpa dig att avgöra

4.

SE UPP FÖR FÖRFALSKNINGAR

Deep fakes är video, ljudklipp eller bilder som digitalt manipulerats, vanligtvis för att ersätta någons ansikte eller rörelser, eller för att ändra orden de säger. Även om ”deep fakes” är en rätt ny term så har de funnits i en eller annan form i evigheter. Det är ännu enklare att skapa så kallade **cheap fakes** – vilseledande innehåll som inte kräver sofistikerad teknologi men som istället kan skapas genom att bara sätta fel rubrik på ett foto eller en video, eller genom att använda gamla bilder och filmer för att illustrera nya händelser.

Det kan verka omöjligt att bekämpa falskt innehåll, men det finns något du kan göra… förbli grundad.

Ha fötterna på jorden och utforska
Precis som när du har att göra med klickbete så är det viktigt att **inte okritiskt acceptera något så som det presenteras**. Om en video eller ett foto verkar överraskande eller otroligt – notera då den känslan och överväg om det finns mer här än det du kan se med blotta ögat. Om du ser samma bild dyka upp på många platser i ditt flöde eller om den delats många gånger, notera det som en anledning att söka upp den ursprungliga källan.

Det är då du behöver **ställa följdfrågor**: vem publicerade informationen. Om det är en bild så kan du göra om omvänd bildsökning på TinEye och i vilka andra sammanhang bilden dyker upp.

Kolla med andra trovärdiga nyhetskällor innan du bestämmer dig för att informationen är sann och innan du delar den med släkt och vänner.