

4.

НАМАЛЕТЕ ГИ ТРАГИТЕ ШТО ГИ ОСТАВАТЕ

Прелистувачот за интернет на вашиот телефон чува многу податоци за вас – вашата локација, што пребарувате, кои веб-страници ги користите – и може да ги издава тие податоци.

Со неколку мали промени можете да ја одржите контролата над вашите податоци.

Телефоните, таблетите и компјутерите имаат однапред инсталирани прелистувачи на кои вашата приватност не им е приоритет.

Наместо тоа, може да преземете и да користите прелистувач што веќе им дава поголема приватност на вашите активности на интернет и ве заштитува од програми за следење.

За дополнително зајакнување на приватноста, може да инсталирате и додатоци (add-ons) и екстензии (extensions) (ова се мини програми што се лесни за инсталирање и може да ви помогнат активностите на интернет да ви бидат позаштитени).

5.

ОТСТРАНЕТЕ ГИ ОЗНАЧУВАЊАТА/ТАГОВИТЕ ЗА ВАС И ЗА ДРУГИТЕ

Дали во минатото сте придонесувале кон собирањето податоци за вашите пријатели означувајќи ги во фотографии и објави?

Редуцирајте ги достапните податоци на интернет за вашите пријатели со отстранување на ознаките за нив во што е можно повеќе фотографии и објави.

Пренесете ја пораката! Поттикнете ги вашите пријатели, семејство и соработници да ви се приклучат во оваа мисија за контролирање на споделените податоци. Ако ги здружиме силите во контрола на трагите од податоци, ќе си помогнеме едни на други во процесот на „детоксикација“.

Подготвено од

TACTICAL
TECH

Поддржано од



datadetoxkit.org
#datadetox



Со цел да ги блокирате шпионските огласи и невидливите програми за следење, инсталирајте uBlock Origin (за Chrome, Safari и Firefox) или Privacy Badger (за Chrome, Firefox и Opera).

Со цел да се осигурите дека вашиот пристап до веб-страниците е безбеден, инсталирајте HTTPS Everywhere: екстензија за прелистувач за да сте сигурни дека вашата комуникација на различни интернет-страници е енкриптирана и заштитена при поврзувањето. Доколку користите Safari и сакате да ја користите оваа опција, тогаш за ваш главен пребарувач изберете продукт што не е на Google, како на пример DuckDuckGo, што автоматски ви овозможува енкриптирано пребарување.



УПРАВУВАЈТЕ СО ПОДАТОЦИТЕ НА ВАШИОТ ПАМЕТЕН ТЕЛЕФОН

за поголема заштита на приватноста на интернет

Доколку си поставите прашање што кажуваат вашите податоци за вас, можеби тоа не изгледа како нешто страшно: кому му е од интерес дали сакате кантри музика, дали сакате да купувате повеќе чевли отколку што ви е потребно или, пак, го планирате следниот одмор една година однапред?

Проблемот е во тоа што се случува со вашите податоци. Со текот на времето се креираат интимни дигитални обрасци: вашите навикни, движења, врски, вкусови, ставови и тајни им се откриваат на оние што ги анализираат и профитираат од нив, како бизнисите и посредниците за податоци.

Следејќи го ова Упатство за детоксикација од податоци, ќе дознаете како и зошто се случува сево ова, како и кои конкретни чекори да ги преземете за да ги контролирате трагите што ги оставате на интернет.

Да започнеме!

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

1. ПРОМЕНЕТЕ ГО ИМЕТО НА ВАШИОТ УРЕД

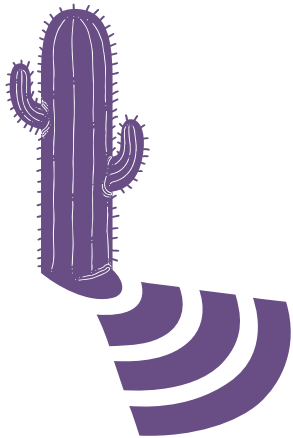
Веројатно во некој момент сте му дале име на вашиот уред за безжично поврзување (Wi-Fi), или преку блутут (Bluetooth), или можеби името автоматски се генерирало при нагодувањата.

Значи, „телефонот на Алекс Чунг“ (Alex Chung's Phone) е она што е видливо за сопственикот на мрежата на која сте безжично поврзани или, доколку ви е вклучена опцијата за блутут, за сите кои во околината ја имаат вклучено оваа опција.

Сигурно не би влегле во кафе-бар, ресторан или аеродром и на глас да го кажете сопственото име; според тоа, не би требало тоа да го прави ни вашиот телефон.

Може да го промените името на вашиот телефон во нешто помалку лично, но сепак уникатно за вас.

Еве како:



iPhone:
Промена на име на телефон:
Нагодувања → Општи нагодувања → За уредот → Променете го името

Андроид:
Променете име на мрежата за безжично поврзување
Нагодувања → Безжично поврзување → Мени → Напредно/Повеќе можности → Wi-Fi Direct → Преименувај го уредот
Промена на името за блутут поврзување:
Нагодувања → Блутут → Вклучете блутут доколку е исклучен → Мени → Преименувај го уредот → Исклучи блутут

2. ИЗБРИШЕТЕ ГИ ТРАГИТЕ ЗА ВАШИТЕ ЛОКАЦИИ

Иако можеби се чини дека податоците за вашите локации се само неповрзани информации, доколку се погледнат заедно, можат да откријат многу важни детали за вас и вашите навики, на пример каде живеете, каде работите и каде сакате да се дружите со пријателите.

Затоа и многу бизниси и посредници за податоци се исклучително заинтересирани за нив.

Може да ги прегледате апликациите на кои сте им дале согласност да ја следат вашата локација и да ја исклучите таа опција. Побарајте ги апликациите што немаат потреба од користење на вашата локација за да работат (на пример: дали одредена игра мора навистина да знае каде сте?) и исклучете ја опцијата за сите апликации кои не сакате да имаат пристап до вашата локација:

3. СРЕДЕТЕ ГИ ВАШИТЕ АПЛИКАЦИИ

Апликациите на социјалните мрежи, игри и апликации за временска прогноза се заинтересирани за вашите податоци... и може да собираат многу од нив.

Бришењето на тие случајни апликации што никогаш не ги користите е моќен начин за прочистување на вашата дигитална личност, вашето дигитално „јас“.

Дополнително, расчистувањето може да ослободи простор на вашиот телефон, да ја намалите употребата на податоците и да го продолжите времетраењето на батеријата.

Андроид:
Нагодувања → Апликации → Контролирајте го пристапот до локација во зависност од апликацијата

iPhone:
Нагодувања → Приватност → Услуги за локација → Контролирајте го пристапот до локација во зависност од апликацијата

Андроид:
Нагодувања → Апликации → Изберете ја апликацијата којашто сакате да ја деинсталирате → Деинсталирај

iPhone:
Изберете една апликација додека не почнат сите да се движат и на горниот лев агол на секоја апликација ќе се појават крвчиња.

За да ја избришете апликацијата, допрете го крвчето на таа апликација.

За да се вратите во нормална состојба, изберете го копчето за главното мени.

4. ЗАШТИТЕТЕ ГИ ВАШИТЕ ВИРТУЕЛНИ ВРЕДНИ РАБОТИ

На истиот начин како што се грижите за вредните работи во вашиот дом треба да постапувате и со информациите што ги чувате виртуелно – без разлика дали станува збор за вашата финансиска евиденција, за скенираните страници од пасошот или, пак, за вашата адреса или телефонски број. Важно е да размислите каде ги зачувувате **вашиите највредни лични податоци** и како може да ги заштитите.

Зачистување (spot clean) е добра опција доколку сакате набрзина, додека пиете кафе, да направите неколку подобрувања. Побарајте одредени податоци што се наоѓаат во вашата електронска пошта или на други профили и избришете ги: скенирани копии од вашата лична карта, банкарски податоци, информации за здравствено осигурување и друго. Доколку подоцна нешто од тоа ви е потребно, секогаш може да го преземете или да го отпечатите пред да го избришете од електронската адреса.

Длабинското чистење (deep clean) е подетално и добро е да се прави барем еднаш годишно. Архивирајте сè во вашата електронска пошта или од профилот на социјалните мрежи, преземете го на вашиот компјутер и избришете ја содржината на профилите за да почнете одново.

Совет: Немојте само да бришете – испразнете го и фолдерот со избришани податоци и привремените датотеки.

Ваше е дали ќе сакате од архивирани податоци и документи да направите резервна копија (back up) на облак (cloud) или, пак, ќе ги зачувате на надворешен хардиск или USB. Без разлика како ќе ги зачувате своите податоци, внимавајте да не ги изгубите и да бидат заштитени со силна лозинка која може да ја запамтите.

5. ПРОСЛЕДЕТЕ ПОНАТАМУ

Честопати и лесно се заборава дека интернетот со причина има назив „мрежа“ (World Wide Web заб. прев.). Сите сме поврзани на интернет преку различни мрежи, не само како „пријатели“ на социјалните медиуми, туку и преку контактите во нашите електронски адреси и фотографиите што ги споделуваме на интернет. Кога ги обезбедувате вашите профили, зајакнете ги лозинките и исчистете ги податоците. Придобивката не е само ваша – туку сите со кои сте поврзани со тој чекор ќе станат побезбедни.

Кога ги чистите електронската пошта и профилите на социјалните мрежи, размислете што друго може да преземете и да избришете, а што може да им помогне на вашите пријатели или соработници: банкарските податоци на вашата сестра, клучот со код од вашата канцеларија или скенираната копија на пасошот на вашиот син се само некои од податоците што може да ви предизвикаат главоболка доколку паднат во погрешни раце.

Проследете понатаму! Зајакнувањето на вашата дигитална безбедност може да е едноставно доколку следите неколку основни чекори. Споделете го ова Упатство за детоксикација од податоци со вашите пријатели, семејство или соработници, помогнете им да ги променат навиките на начин што ќе им одговара.



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

ПРОМЕНЕТЕ ГИ НАГОДУВАЊАТА

за да ги заштитите вашите податоци

Кога интернетот би бил само место на кое се споделуваат слики од кучиња што носат костими на диносауруси, нема да има многу потреба од лозинки. Но, интернетот е место на кое плаќате сметки, ги обновувате рецептите и се регистрирате за гласање на избори. Кога ќе размислите за сите свои виртуелни вредни нешта што се споделуваат преку интернет – и нивното зачувување на вашите уреди – зошто не би ги чувале безбедно исто како вашиот паричник или клучеви?

Постои еден едноставен начин да го отежните пристапот на другите до вашите вредни виртуелни нешта: да не дозволите вашите лозинки да се пробијат лесно. На повеќето луѓе не им се потребни специјални технички вештини за да ги пробијат вашите профили – можат да влезат само со неколку погоднувања на вашата лозинка или преку некоја автоматизирана програма.

Откако ќе влезат на вашиот профил, може да ја испробаат компромитираната лозинка на други профили, да соберат информации за вас и за вашите навики, да ги преземат профилите што ги имате, па дури и да го искористат вашиот дигитален идентитет.

Следејќи го ова Упатство за детоксикација од податоци, ќе научите практични чекори околу зајакнувањето на вашата безбедност на интернет.

Да започнеме!

Подготвено од

TACTICAL
TECH

Поддржано од

Firefox

datadetoxkit.org
#datadetox

1. ЗАКЛУЧЕТЕ ЈА ВАШАТА ДИГИТАЛНА ВРАТА

Заклучување на екранот: лозинка, шема, отпечаток или идентификација со лицето за пристап до вашиот уред се најдобрата одбрана против некој што би сакал да влезе во уредот. Но, постојат различни видови на заштита и може ќе биде тешко да утврдите кој е најдобар за вас.

Доколку го заклучувате вашиот телефон, таблет, или компјутер, тоа ви дава повеќе заштита отколку кога тоа не го правите. Но, исто како различните брави што би ги ставиле на врата, некои заклучувања на екранот се посигурни од другите.

Од сите заштити кои се достапни, уникатните лозинки се најјаките. Тоа значи дека, доколку го заклучувате вашиот уред со лозинка, таа треба да содржи букви, броеви и посебни знаци.

Да речеме дека користите основна шема за отклучување на вашиот телефон. Можете полесно да ја зголемите заштитата преку поставување долга лозинка. Дали користите посебна шема за заклучување? Дали мислите дека таа шема не треба да е толку едноставна? Дали користите 1234 како PIN? Дали можете, наместо ова, седум пати да фрлите коцка и да го запомнете тој број како PIN?

Со мала промена може да направите голем придонес за да ја задржите контролата над вашите уреди.

2. ПУШТЕТЕ ГИ ВИСТИНСКИТЕ

Создавањето врвни лозинки е едноставно. Сè што треба да направите е да следите неколку основни принципи.

Долги: **лозинките треба да содржат минимум осум знаци. Што е подобро? 16-20 знаци.**

Единствени: **секоја шифра што ја користите – за секоја страница – треба да биде различна.**

Случаен избор: **вашата лозинка не треба да има логичен образец или да може лесно да се погоди. Тука може да ви бидат од помош алатките за управување со лозинки (password managers).**

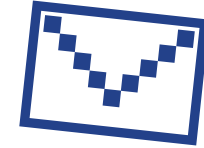
Најјаките лозинки содржат комбинација од букви, бројки и посебни симболи. Овој проверен совет сè уште помага за создавање силна лозинка која е тешко да се погоди. Некои системи за лозинки, за жал, не ви дозволуваат да користите посебни симболи (како на пример @ # \$% - = +), но доволно долга комбинација од букви и бројки е сепак подобра отколку кратка.

Во идеален случај, би требало да користите алатка за управување со лозинки за да ги генерирате и да ги чувате сите ваши лозинки. Алатките за управување со лозинките, како на пример – 1Password и KeePassXC, кои безбедносните експерти честопати ги препорачуваат – се во основа апликации чија единствена цел е да ги заштитат вашите податоци за најава и другите чувствителни податоци.

3. ДОДАЈТЕ ВТОР КЛУЧ

Поставувањето двостепена автентикација (2FA) или повеќестепена идентификација (MFA) значи дека дури и некој да ја открие вашата лозинка, најверојатно, нема да го има дополнителниот фактор којшто им е потребен за влез.

Прегледајте ги безбедносните наредувања за страниците и апликациите кои најчесто ги користите и видете дали може да додадете уште еден клуч. Почнете со најважните – апликации поврзани со финансии или сервисии како електронска пошта која ја користите за поврат на останатите профили.



Гугл:
Пријавете се на: myaccount.google.com → Безбедност → Потврда во два чекори → Почнете

Фејсбук:
Мени → Наредувања → Безбедност и пријава → Употребете двостепена автентикација

Совет: Кога го поставувате следното ниво за верификација, ќе треба да изберете и втор начин да потврдите дека сте вие. Избегнувајте да користите испраќање СМС-пораки како ваш втор фактор, во случај да го изгубите телефонот. Вообичаено електронската пошта е посигурна опција.

4. НЕКА СЕ СЛУШНЕ И ВАШИОТ ГЛАС

Доколку содржините на веб-страниците или апликациите што често ги користите ви изгледаат дека се неверодостојни или содржат погрешни информации, можете да испратите електронска пошта, да напишете твитови и јасно да им укажете на компаниите дека не се согласувате со нивниот начин на работа. Кога компаниите се притиснати од оние кои им се најважни – нивните корисници – постои голема веројатност навистина да се коригираат.

Доколку сметате дека не се слушаат вашите критики, имате уште една моќна алатка на располагање: користете друга веб-страница или апликација. Доколку сте ги информирале дека не сте задоволни со нешто што го прави одредена веб-страница или апликација и потоа сте престанале да ја користите или сте ја избришале од вашиот уред – и доколку доволен број луѓе го направат истото – тогаш компаниите **ќе забележат**.

5. ПРОШИРЕТЕ ЈА ВЕСТА

Пренесете понатаму! Едноставен совет што лесно се заборава, но може да има значителен ефект. Известете ги вашите пријатели, семејство и соработници за работите што ги забележувате и побарајте од нив да ви се приклучат во дигиталната детоксикација! Сите сме соочени со предизвици додека ги користиме нашите телефони. Најважно е да најдете начин што ви одговара вам и на вашиот начин на живот.

Експериментирајте додека не најдете соодветни решенија, потоа приспособувајте ги своите навики како што ви се менуваат потребите. Не постои универзално решение за сите корисници.

И, на крај, споделете информации за вашите технолошки избори и решенија со луѓето околу вас. На пример, да речеме дека ќе бидете недостапни на апликациите за комуницирање преку пораки секој ден по 20.00 часот затоа што сте одлучиле дека после тоа време едноставно нема да користите дигитални уреди: кажете им на вашето семејство и пријатели дека наместо со порака, може да ви се јават. Бидете отворени за дијалог, прашувајте и ќе живеете урамнотежен онлајн живот којшто ви одговара.

НАПУШТЕТЕ ГИ
ФАБРИЧКИТЕ
НАГОДУВАЊА
за да ја подобрите вашата
дигитална добросостојба

Кога последен пат се „исклучивте“ и не користевте технологија цел ден или барем еден час? Ако сте постојано онлајн/на интернет, тогаш не сте сами. Како може да проверите дали времето поминато на вашиот уред е квалитетно потрошено време?

Сè започнува со сознанието дека неодоливата привлечност кон технологијата не е ваша вина! Верувале или не, вашите омилен апликации и веб-страница се дизајнирани така што секоја карактеристика, боја и звук се „оптимизирани“ за да го задржат вашето внимание, да ве направат зависни и да имате потреба повторно да се навраќате на нив.

Дали сакате да поставите рамнотежа помеѓу вашиот живот онлајн и реалниот свет (офлајн)? За тоа зборуваме во овој дел на Упатството за детоксикација од податоци.

Да започнеме!

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

1. БИДЕТЕ ПРИСУТНИ ВО МОМЕНТОТ

Практикувањето на овој совет е потешко отколку што изгледа. За да се биде присутен во моментот, потребно е секојдневно вежбање. Тоа е како мускул во вашиот мозок што треба постојано да го вежбате за да го зајакнете. Може да започнете со тоа што прво ќе станете свесни за вашата релација со технологијата што ја користите.

Колку време поминувате на вашиот телефон?

Доколку не сте задоволни од одговорот, постојат наредувања и стратегии што може да ги следите за да стекнете контрола над технологијата што ја користите.



Доколку вашата цел е да го намалите времето што го поминувате на Фејсбук, на Инстаграм или на Снепчет, променете ги наредувањата и дозволите за тие апликации, со цел повеќе да работат во ваш интерес.

Некои апликации, како, на пример, Инстаграм, дури имаат и опција за апликацијата да ве потсети кога сте го надминале дневното ограничување.

Инстаграм:

Профил → Мени → Наредувања → Профил → Вашата активност → Поставете дневен потсетник

Доколку утврдите дека вашиот телефон ви пречи додека разговарате во живо со некого, бидејќи свони, вибрира или светка, може привремено да го ставите на тивок режим, да го свртите со екранот надолу или да го ставите в џеб или чанта, за да не ви се наоѓа пред очи.

2. ВООЧЕТЕ ГИ ТРИКОВИТЕ ВО ДИЗАЈНОТ

Привлечните дизајни, познати и како „темен модел“/„неодолив модел“ (dark patterns), се дизајни што се засноваат врз човековата психологија, коишто се користат да ве натераат да се претплатите или да купите нешто, да дадете лични податоци, повеќе отколку што сте мислеле или сте имале намера.

Вообичаените трикови во дизајнот може да се состојат во специфичните бои, поставеноста на копчињата, нејасните текстови или делумни информации. Понекогаш овие трикови се очигледни, но некогаш е тешко да се забележат. Можеби веќе сте забележале некои од овие трикови кога сте се претплатиле или сте купувале нешто на интернет.

Причината зошто ги гледате овие дизајнерски трикови насекаде е затоа што функционираат – нè тераат да кликнеме, да се претплатиме, почесто да купуваме и да се враќаме повторно. Колку повеќе сте свесни за суптилните поттикнувачки и манипулативни елементи вградени во веб-страниците што ги користите, толку подобро ќе ги препознавате и ќе ги избегнувате.

Постојат неколку работи што може да ги направите за да ги надмудрите вашите апликации.

Препознајте кога апликациите ве “наведуваат” да направите нешто : Прво што може да направите е едноставно да сте свесни за употребата на овие техники.

Сликајте и споделете: Направете слика на екранот (screenshot) кога ќе најдете на таков дизајн на интернет и споделете ја со вашите пријатели (без да споделувате лични детали по коишто може да ве идентификуваат – приватноста на прво место!) Може да побарате од компаниите да ги променат своите практики.

Останете смирени: Доколку на страницата за купување има часовник што одбројува, поставете си прашање: Дали е ова навистина итно? Доколку се затекнете како кликате на копчето, а не сте сакале, размислете за текстот на копчињата или боите што ги користи оваа услуга. Доколку се чувствувате збунето, немојте веднаш да претпоставите дека е тоа ваша вина – размислете за зборовите што ги користи оваа веб-страница или апликација, затоа што и тие може да бидат нејасни.

3. БИДЕТЕ МУДРИ СО МЕДИУМИТЕ

Исто како што може да научите да ги надмудрите карактеристиките и дизајните што имаат за цел да ве задржат на страницата, така може да бидете паметни и да научите како да забележите вести или објави кои се наведувачки.

Досега сигурно сте чуле за проблемите со погрешните информации и „лажните вести.“ Воочувањето на погрешните информации може да ви стане нешто вообичаено доколку поставувате критички прашања за секоја вест што ја примате, особено доколку звучи изненадувачка, претерана или предобра за да биде вистинита.

На крај ќе сакате и да проверите која вест е вистинита или лажна – особено доколку планирате да ја споделите со семејството или со пријателите.

На каква веб-страница е објавена оваа содржина? Кој го напишал (и кога)? За што зборува целиот напис, покрај насловот? На кои извори се повикуваат?



Доколку сметате дека информацијата е погрешна и сакате да спречите да се шири, повеќето платформи имаат место каде што може да ја пријавите објавата. Дополнително, може да одлучите дали ќе продолжите да го следите профилот што ја објавил веста.



5. БАРАЈТЕ ЈА ВИСТИНАТА НА ИНТЕРНЕТ

Терминот „лажни вести“ се користи за широк спектар од неточни или наведувачки информации, вклучително и сатира, слабо истражени или непроверени содржини, шеги и лаги. Лажните вести не се шират секогаш со лоша намера, но без разлика на причината поради која што се споделуваат, резултатот е речиси секогаш ист: лицата кои ја примаат информацијата веруваат дека нешто погрешно е всушност точно или дека се случило нешто што никогаш не се случило.

Во најдобар случај, може да е смешно меме. Во најлош случај, може да се неточни здравствени совети или лажни политички информации.

Дури и да вложите напор дополнително да истражите и да поставите критички прашања за написите што ги читате, може сепак да се збуните. Но знајте го ова: не сте сами!

Со сите сили

Само затоа што некоја интернет-страница не ги признава своите грешки, не значи дека не ги прави. Всушност, најверодостојни публикации се тие коишто се исклучително внимателни со вистината и вработуваат луѓе или цели оддели чијашто единствена работна обврска е да проверуваат факти.

Барајте извори што објавуваат исправки кога ќе згрешат. Дури и подобро е кога ажурираните информации се сумирани на почетокот на написот и се објавени на социјалните медиуми, па не мора дополнително да ги пребарувате.

datadetoxkit.org #datadetox

Подготвено од

TACTICAL
TECH

Партнери на проектот



МАКЕДОНСКИ
ИНСТИТУТ
ЗА МЕДИУМИ



Финансирано од
Европската Унија

6. ИЗЛЕЗЕТЕ ОД ЗАТВОРЕНИОТ КРУГ НА ИНФОРМИРАЊЕ (ИНФОРМАЦИСКИОТ МЕУР)

Откако интернет-страниците и апликациите ќе ве профилираат според вашите интереси, може да се најдете во затворен круг на информирање/информациски меур. Ова се случува кога сервисот ви нуди повеќе содржини слични на оние кои веќе ги читате. Како на овој начин се ограничува или се менува нивото на нашата информираност?

Затворениот круг на информирање/информацискиот меур може да доведе до тоа луѓето да гледаат сосема различни верзии на стории, наслови на вести, написи и реклами, како што е прикажано во интерактивниот напис Blue Feed, Red Feed (graphics.wsj.com/blue-feed-red-feed/).

Доколку знаете дека гледате содржина која алгоритамот избрал да ви ја прикаже на различните апликации и интернет-страници што ги користите, се поставува прашањето: како да излезете од тој затворен круг на информирање/информациски меур?

Променете ја насоката и измешајте ги своите вести

Добар начин за да го прекинете информацискиот меур е да се претплатите на услуги што собираат вести и информации од различни извори со разновидни гледишта. RSS канали, форуми и листи за испраќање пошта коишто овозможуваат широк спектар на мислења и теми може да ви помогнат да излезете од затворениот круг на информирање. Global Voices (globalvoices.org) и The Syllabus (the-syllabus.com) се одлични опции за почеток.

Апликациите, интернет-страниците и онлајн медиумите може да се неопходни за пристап до вести, совети за подобар живот и забава. Но, меѓу мноштвото содржини, може да ви биде тешко да се снајдете и да дојдете до она што ви треба.

Кога ќе најдете на некое видео, слика или напис онлајн некогаш дури може и да ви биде тешко да ја утврдите разликата меѓу фактите и фикцијата.

Од тестови на личноста кои се обидуваат да ве профилираат, до шокантни наслови и изменети фотографии и видеа што може да ве убедат во целосно различна реалност - она што го гледате на интернет не е секогаш она што се чини.

Во ова Упатство за детоксикација од податоци ќе најдете теми и популарни зборови поврзани со погрешните информации, почнувајќи од тоа како да ја препознаете вашата одговорност, а завршувајќи со истражување на пошироката слика. Пригоа, ќе добиете и совети како да се снајдете низ сето она што ве опкружува.

Да започнеме!

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

6 СОВЕТИ ЗА ИЗБЕГНУВАЊЕ НА ПОГРЕШНИТЕ ИНФОРМАЦИИ НА ИНТЕРНЕТ

1. РАЗБЕРЕТЕ ЈА ВАШАТА МОЌ ЗА БРАНУВАЊЕ

Допаѓање, споделување, ретвит, повторна објава – сите овие активности опишуваат на кој начин комуницирате со она што го гледате на интернет – и вашите интеракции прават голема разлика. Кога доволен број на луѓе реагираат на некоја слика, видео-запис или објава, тие брзо се шират и, по дефиниција, стануваат „вирални“.

Застанете за момент и поставете си прашање: Какво е моето влијание на интернет? Кога последен пат сте виделе шокантен или смешен напис, наслов, видео или слика и веќе за неколку секунди сте им го испратиле на вашите пријатели? Истражувачите утврдиле дека написите и сликите коишто најчесто стануваат вирални се оние кои што предизвикуваат страв, одвратност, зачуденост, бес или анксиозност. Доколку вакво нешто сторивте утрово, не чувствувајте се лошо!



Важноста на споделувањето

Споделувањето е форма на учество. Кога споделувате нешто (што било), постои можност тоа што сте го презеле да стане вирално. На пример, доколку излезе дека некоја објава е лага, дали сакате вашето име и углед да се поврзани со неа? Пред да споделите некоја содржина, размислете дали ширите нешто невистинито, деструктивно или токсично.

2. РАЗМИСЛЕТЕ УШТЕ ЕДНАШ ПРЕД ДА ГО НАПРАВИТЕ ТЕСТОТ НА ЛИЧНОСТА

Кога последен пат видовте квиз (дали текстуален или преку фотографија) со наслов како на пример:

- Во која деценија од животот сте?
- Кое е вашето духовно животно?
- Кој е вашиот совршен одмор?
- ...списокот продолжува

Иако постои можност овој забавен квиз да бил осмислен за едноставно да ви го привлече вниманието, истовремено постои можност прашањата да биле внимателно смислени со цел да соберат податоци и да направат категоризација на вашата личност, врз основа на таканаречениот психометриски модел.

Вашите одговори на квиз како „Кој лик од Симпсонови си?“ заедно со другите навики што можеби ги следи вашиот прелистувач, апликација или поврзаните работи како картичките за лојалност, може да им дадат претстава на аналитичарите на податоци за тоа каква личност сте, за што се грижите и како да влијаат врз вас за да си купите пар чевли (на пример)... или да направат ваш профил за да утврдат како да влијаат врз вас при гласање за следните избори.

Чувајте повеќе тајни

Кога помислувате за лични податоци, можеби прво напамет ви паѓаат податоци за лозинки, матичен број, сметка во банка. Но, деталите за вас, како на пример што е она што ве плаши, што ве иритира и вашите амбиции, се исто така лични информации. Аналитичарите на податоци може да ги сметаат овие податоци како многу важни, утврдувајќи што е она што ве определува како личност. Добро размислете пред да дадете такви информации во некоја анкета или квиз.

3. НЕ ЗАГРИЗУВАЈТЕ НА МАМКАТА

„Кликбејт“ е термин што се користи за да се опишат сензационалистички, нечесни или измислени наслови што се користат со намера да се наведат луѓето да кликнат на насловот или на линкот. Колку повеќе внимание добива одреден напис, видео или слика, толку поголеми можности има за заработка. Ова значи дека креаторите на содржини имаат мотив да кажат што било само за да ве натераат да кликнете или да ги споделите нивните содржини.

Врз основа на профилот на личноста која за вас ја прават платформите што ги користите (како, на пример, Фејсбук и Инстаграм), може да добиете приспособени наслови создадени да ви предизвикаат емоции, со што ќе ве наведат да кликнете.

„Кликбејт“ најчесто се поврзува со погрешни информации, но тоа не мора да биде случај секогаш. Штом еднаш ќе научите да ги препознавате „кликбејт“ насловите, ќе почнете да ги забележувате и на Јутјуб, на блогите и во таблоидите.



Проверете го изворот

Кога ќе налетате на „кликбејт“, не застанувајте кај насловот. Доколку изгледа како безбеден линк, кликнете на написот и дознајте кој е авторот, кога е објавено и на кои извори се повикува. Постои можност во самиот напис да има забелешка дека станува збор за платена содржина или реклама или, пак, е категоризиран како мислење. Ваквите детали ќе ви помогнат да утврдите дали вреди да го читате написот.

4. ВНИМАВАЈТЕ НА ЛАГИТЕ

„Дипфејкови“ се видеозаписи, аудиоисечеци или слики што се дигитално изменети, вообичаено за да се измени нечие лице или движење или за да се променат нивните зборови. Иако „дипфејкот“ е понов израз, тој постоел во друг облик подолго време. Дури е и полесно да се креираат евтини „дипфејкови“ – наведувачки содржини за коишто не е потребна софистицирана технологија, туку може да се направат со вметнување погрешен наслов на фотографија или видео или со користење застарена содржина со цел да се илустрира настан од сегашноста.

Може да изгледа невозможно вистински да се бориме против ваквите манипулации, но има нешто важно што може да го направите ...

Останете цврсто на нозе и истражувајте

Исто како кога се справувате со „кликбејт“ содржини, не прифаќајте ништо од прва. Доколку некое видео или фотографија ви изгледаат изненадувачки или неверојатни, земете го тоа предвид и размислете дали има нешто повеќе од она што е видливо на прв поглед.

Доколку забележите дека една иста слика почесто се јавува во вашите вести или повекепати е споделена со вас, сфатете го ова како можна причина да го проверите вистинскиот извор.

Тогаш треба да поставите повеќе прашања: кој го објавил (која интернет-страница, кој бил авторот)? Кога е објавена? Доколку е слика, направете хронолошко пребарување на пребарувачи за фотографии како што е Тинај (TinEye, tineye.com) и проверете каде сè може да ја најдете.

Проверете други веродостојни извори на вести пред да поверувате дека се вистинити и пред да ги споделите со вашите пријатели и семејство.