

4.

ZMANJŠAJTE SVOJE SLEDI

Brskalnik na telefonu skladišči veliko informacij o vas – vašo lokacijo, zgodovino brskanja, katere strani obiskujete – in te podatke morda posreduje naprej. Z nekaj majhnimi spremembami lahko pridobite nadzor nad nekaterimi informacijami.

Telefoni, tablice in računalniki imajo prednastavljen brskalnik, katerega glavna naloga ni skrb za vašo zasebnost. Namesto tega lahko **naložite in uporabite brskalnik, ki že samodejno skrbi za zasebnost** spletne aktivnosti in vas tako ščiti pred sledilci.

Če bi želeli okrepiti svojo zasebnost, lahko namestite dodatke, poznane kot »razširitve in dodatki« (to so enostavno namestljivi mini programi za vaš brskalnik, ki **skrbijo za dodatno zasebnost vaše spletne aktivnosti**).

5.

ODSTRANITE OZNAKE SEBE IN OSTALIH

Ste prispevali k zbiranju podatkov o svojih prijateljih, tako da ste jih v preteklosti označili v objavi ali na fotografiji?

Zmanjšajte količino njihovih podatkov, ki so bili naloženi, (poleg tega pa očistite svojo vest) in jih odznačite na čim več fotografijah in objavah.

Povejte naprej! Spodbudite svoje prijatelje, družinske članke in sodelavce, da se vam pridružijo pri nadzoru podatkov, ki jih nezavedno delimo. Uspešni bomo šele takrat, ko bomo prav vsi delali skupaj in si prizadevali za nadzor svojih digitalnih sledi.

Ustvaril

TACTICAL
TECH

Podpora

Firefox

datadetoxkit.org
#datadetox



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

Če želite blokirati vohunske aplikacije in nevidne sledilce, namestite uBlock Origin (za Chrome, Safari in Firefox) ali Privacy Badger (za Chrome, Firefox in Opero).

Če želite, da bodo vaše povezave do spletnih mest varne, namestite HTTPS Everywhere: tj. razširitev brskalnika, ki zagotavlja šifriranje in zaščito vaše komunikacije z večino pomembnejših spletnih mest. V kolikor uporabljate Safari, se izogibajte rabi privzetih brskalnikov, ki so del Googla, in raje uporabite denimo DuckDuckGo, ki samodejno šifrira uporabnikovo identiteto.

NADZORUJTE PODATKE SVOJEGA PAMETNEGA TELEFONA

in tako izboljšajte svojo spletno zasebnost

Če pomislite na to, kaj s svojimi podatki sporočate drugim, se vam morda ne bo zdelo nič posebnega: komu je mar, ali ste ljubitelj country glasbe, da nakupujete več čevljev, kot jih potrebujete, ali da načrtujete svoje potovanje že leto vnaprej?

Težava se skriva v tem, kaj se dogaja z vašimi podatki. Sčasoma ti tvorijo intimne digitalne vzorce: vaše navade, gibanje, odnosi, izbire, prepričanja in skrivnosti se razkrijejo tistim, ki jih analizirajo in z njimi služijo. To so razna podjetja in posredniki podatkov.

Ko boste sledili orodju za podatkovno razstrupljanje, se boste seznanili s tem, kako in zakaj se vse to dogaja. Hkrati vam orodje ponuja praktične nasvete za nadzor vaših podatkovnih sledi na spletu.

Pa začnimo!

1.

SPREMENITE IME SVOJE NAPRAVE

V nekem trenutku boste morda svoj telefon "poimenovali" za potrebe WiFi-ja, Bluetootha ali obojega – ali pa je bilo ime med nastavitvijo samodejno ustvarjeno. To pomeni, da je »telefon Janeza Novaka« viden lastniku omrežja WiFi in če je vaš Bluetooth vklopljen, je viden tudi vsem v vaši okolici, ki imajo prav tako vklopljen Bluetooth.

Ob vstopu v kavarno, restavracijo ali letališče svojega imena gotovo ne bi najavili, prav tako pa ne bi smeli najaviti svojega telefona.

Ime svojega telefona lahko spremenite v nekaj, kar vas manj osebno identificira, vendar vas še vedno uspešno predstavlja. To naredite tako:



2.

POČISTITE SLEDI O SVOJI LOKACIJI

Čeprav se vam zdi, da so podatki o vaši lokaciji samo naključni delčki informacij, pa lahko skupek letih razkrije pomembne podrobnosti o vas in vaših navadah, na primer kje živite, delate in kje se najraje družite s prijatelji. Prav zato so to v mnogih podjetjih in pri mnogih posrednikih podatkov zelo iskane informacije.

Lahko pregledujete dovoljenja posamezne aplikacije in izklopite lokacijske storitve. Poiščite aplikacije, ki informacije o vaši lokaciji dejansko ne potrebujejo za svojo storitev (ali mora neka računalniška igrice resnično vedeti, kje se nahajate?) in tiste, katerim ne želite podati teh informacij:

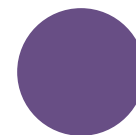
3.

UREDITE SVOJE APLIKACIJE

Aplikacijam za družabna omrežja, igre in vremensko napoved so vaši podatki pomembni ... in morda jih v veliko meri tudi zbirajo.

Brisanje naključnih aplikacij v telefonu, ki jih nikoli ne uporabljate, je lahko učinkovit način za razstrupljanje svoje digitalne identitete.

Poleg tega lahko čiščenje sprosti prostor v telefonu, zmanjša porabo podatkov in podaljša življenjsko dobo baterije. To lahko, odvisno od aplikacije, celo poveča splošno učinkovitost in delovanje naprave.



Android:
Nastavitve → Aplikacije →
Upravlja z dovoljenji za lokacijo
pri posameznih aplikacijah

iPhone:
Nastavitve → Zasebnost →
Dovoljenja za lokacijo →
Upravlja z dovoljenji za lokacijo
pri posameznih aplikacijah

Android:
Nastavitve → Biometrični
podatki in varnost / Lokacija
→ Izklopite lokacijo

iPhone:
Nastavitve → Zasebnost →
Dovoljenja za lokacijo →
Izklopite jih

4.

ZAŠČITITE SVOJE VIRTUALNE DRAGOCENOSTI

Tako kot skrbite za svoje dragocenosti doma, bi morali poskrbeti tudi za informacije, ki jih hranite virtualno – naj gre za vašo finančna poročila, optično prebrane osebne dokumente, domači naslov ali telefonsko številko, vredno je premisliti o tem, **kje** lahko hranite svoje najpomembnejše osebne podatke in **kako** jih zaščititi.

Čiščenje pomnilnika je odlično, če želite ob kavi narediti nekaj hitrih izboljšav. Poiščite specifične informacije, ki se nahajajo na vašem elektronskem naslovu ali drugih računih, in jih izbrišite: **optično prebrani osebni dokumenti, bančni izpiski ali podatki o zdravstvenem zavarovanju**, če jih navedemo le nekaj. Če gre za stvari, ki jih boste še potrebovali, jih lahko vedno naložite ali natisnete, preden jih izbrišete iz vašega elektronskega naslova.

Globinsko čiščenje je bolj temeljito in ga je priporočljivo opraviti vsaj enkrat letno. Arhivirajte zadeve na svojem elektronskem naslovu ali družbenih omrežjih, prenesite jih na računalnik in izbrišite vso vsebino na računu za **svjež začetek**.

Nasvet: Brisanje ni dovolj – izpraznite tudi koš inčasne datoteke!

Od vas je odvisno, ali boste varnostno kopiranje arhiva in dokumentov shranili v oblak, na zunanji trdi disk ali USB-ključ. Ne glede na način shranjevanja, ki ga boste izbrali, poskrbite, da podatkov ne izgubite in nastavite močno geslo.

5.

PREDAJTE NAPREJ

Čeprav to večkrat pozabimo, poimenovanje "splet" ni zgolj naključno. **Vsi smo povezani na spletu** prek različnih omrežij in to ne samo kot "prijatelji" na družbenih omrežjih, temveč nas povezujejo tudi stiki na naših elektronskih naslovih in fotografijah, ki jih delimo. Ko zaščitite svoj račun, okrepite gesla in počistite svoje podatke, s tem ne pridobite samo vi – **vsi, ki so povezani z vami, so zaradi vaših prizadevanj malo bolj varni**.

Ko počistite svoj elektronski naslov in račune na družbenih omrežjih, premislite, kaj bi še lahko naložili ali izbrisali in tako **pomagali prijateljem ali sodelavcem**: sestrični bančni izpiski, kodirna gesla za vstop v poslovne prostore ali optično prebrani dokumenti, kot je sinov potni list, so le nekateri izmed dokumentov, ki bi vam, če bi pristali v napačnih rokah, znali povzročiti glavobol.

Predajte naprej! Z upoštevanjem nekaterih osnovnih korakov lahko izboljšate svojo digitalno varnost. Delite Orodje za podatkovno razstrupljanje s svojimi prijatelji, družinskimi člani in sodelavci ter jim t **ako pomagajte spremeniti njihove navade na način, ki jim bo ustrezal**.



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

SPREMENITE NASTAVITVE

da zaščitite svoje podatke

Če bi bil splet namenjen zgolj deljenju fotografij psov, **oblečenih v kostum dinozavra**, ne bi bilo večje potrebe po geslih. Pa vendar temu ni tako – splet uporabljamo za plačevanje položnic, naročevanje na zdravstvene preglede in v volilne namene. Zakaj ne bi tudi "virtualnih dragocenosti", ki jih delite na spletu – in hranite na vaših napravah – **zavarovali tako dobro, kot varujete svojo denarnico ali ključče?**

Obstaja preprost način, kako ostalim otežiti dostop do vaših virtualnih dragocenosti: **ne omogočite jim, da zlahka ugotovijo vaša gesla**. Večina ljudi za dostop do vašega računa ne potrebuje specializiranega tehničnega znanja – to lahko storijo le s par poskusi ugibanja ali z uporabo avtomatskega programa.

In ko enkrat vstopijo v vaš račun, bodo morda poskusili z istim geslom dostopati tudi do vaših drugih računov, zbrati informacije o vas in vaših navadah, prevzeti vaš račun ali celo uporabiti vašo digitalno identiteto.

V nadaljevanju Podatkovne razstrupitve se boste naučili praktičnih korakov za izboljšanje varnosti na spletu.

Pa začnimo!

Ustvaril

TACTICAL
TECH

Podpora

Firefox

datadetoxkit.org
#datadetox

1.

ZAKLENITE SVOJA DIGITALNA VRATA

Zaklepanje zaslona: geslo, vzorec, prstni odtis ali prepoznavanje obraza, ki jih uporabljate za odklepanje naprave, so **vaša najboljša obramba** proti morebitnim vsiljivcem. A teh možnosti je še veliko in včasih se je težko odločiti za pravo.

Kakršna koli zaščita na telefonu, tabličnem računalniku ali računalniku je boljša od tiste, ki je ni. In prav tako, kot se razlikuje kakovost ključavnic, ki jih lahko namestite na vhodna vrata, **so nekateri načini zaklepanja zaslona varnejši od drugih.**

Najboljši način za zaščito so dolga in unikatna gesla. Če odklepate svoj zaslon z geslom, naj bo to sestavljeno iz črk, števil in posebnih znakov.

Če za odklepanje telefona uporabljate preprost način, kot je denimo vlečenje, lahko varnost postopno povečujete z nastavitvijo dolgega gesla. Ali se trenutno za odklepanje poslužujete vzorca? Kaj pa, če vzorec podaljšate? Ali uporabljate za geslo 1234? Kaj pa, če raje sedemkrat vržete igralno kocko in si zapomnite nastalo kombinacijo ter to uporabite za novo geslo? **Majhne spremembe lahko pomembno pripomorejo k nadzoru nad vašo napravo.**

2.

IZBERITE PRAVO

Ustvariti vrhunsko geslo je enostavno. Vse, kar morate storiti, je samo to, da sledite nekaj osnovnim vodilom.

Vaše geslo naj bo:

Dolgo: **geslo naj bo sestavljeno iz najmanj osmih znakov. Ali še bolje 16–20 znakov**

Izvirno: **vsako geslo, ki ga uporabljate za vsako spletno stran naj bo različno**

Naključno: **geslo naj ne bo logično ali enostavno za uganiti. Pri tem so zelo uporabni upravljavci gesel**

Najmočnejša gesla so sestavljena iz kombinacije črk, števil in posebnih znakov.

To je trenutno vodilni nasvet za oblikovanje varnejših gesel, ki jih je še težje razvozlati. Nekateri sistemi varnostnih gesel pa žal ne omogočajo posebnih znakov (kot npr. @#%*-+=), a je dovolj dolga kombinacija črk in števil še vedno boljše kot kratko geslo.

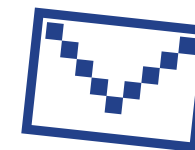
V idealnem primeru bi morali uporabljati **namenski upravljavec gesel**, s katerim ustvarite in shranite vsa gesla. Upravljavec gesel – denimo 1Password ali KeePassXC, tista, ki ju strokovnjaki s področja varnosti največkrat priporočajo – so dejansko aplikacije, katerih edini namen je zaščititi vaše prijavnice in ostale občutljive podatke.

3.

DODAJTE DRUGI KLJUČ

Nastavitev dvostopenjskega potrjevanja (2FA) ali večstopenjskega potrjevanja (MFA) pomeni, da četudi nekdo ugotovi vaše geslo, **najbrž ne bo imel vsega potrebnega za vstop.**

Oglejte si varnostne nastavitve spletnih strani in aplikacij, ki jih najpogosteje uporabljate, da ugotovite, če lahko namestite dodatni ključ. **Začnite z najpomembnejšimi** – aplikacije s področja financ ali storitve, kot je elektronski naslov, ki ga uporabljate za zaščito drugih računov.



Google:
Prijavite se v: myaccount.google.com
→Varnost →
Dvostopenjsko potrjevanje →
Začni

Facebook:
Menu →
Nastavitve →
Varnost in prijava →
Uporabi dvostopenjsko potrjevanje

Nasvet: Ko nastavite naslednji sloj preverjanja, boste morali izbrati drug način za potrjevanje identitete. Izogibajte se uporabi SMS sporočil (sporočil, ki so poslana na vašo telefonsko številko), da ostanete zaščiteni tudi v primeru izgube telefona. Bolj zanesljiva možnost je elektronski naslov.

4.

SPOROČITE SVOJE MNENJE

Če niste zadovoljni z zasvajajočimi in prepričljivi dizajni ali zavajajočimi informacijami na spletnih straneh ali aplikacijah, ki jih uporabljate, lahko pošljete elektronsko sporočilo ali čivknete na Twitterju in tako sporočite podjetjem, da se ne strinjate z njihovim početjem. Ko so podjetja podvržena pritiskom, ki prihaja od njihovih najpomembnejših dobrin – njihovih uporabnikov – obstaja možnost za spremembo.

Če imate občutek, da vaše povratne informacije niso bile slišane, obstaja zelo učinkovit način: uporabite različne spletne strani ali aplikacije. Če ste sporočili svoje nezadovoljstvo nad početjem neke spletne strani ali aplikacije in jo potem nehali uporabljati ali izbrisali – in je to poleg vas storilo dovolj ljudi – **bodite prepričani, da bo to opaženo.**



5.

RAZŠIRITE GLAS

Predajte naprej! Na ta nasvet zlahka pozabimo, čeprav lahko doseže velik vpliv. Povejte svojim prijateljem, družinskim članom in sodelavcem o svojih opažanjih in jih povabite, da se vam pridružijo v tej podatkovni razstrupitvi! Vsi se spopadamo z vprašanjem, kako uspešno upravljati svoje mobilne navade. Pomembno je, da najdete način, ki vam bo odgovarjal in bo ustrezal vašemu načinu življenja. Preizkušajte, dokler ne najdete pravega, potem pa sčasoma spremenite svoje navade in potrebe. Ne obstaja namreč samo en način, ki bi zadovoljil vse.

Ne pozabite sporočiti svojih odločitev ljudem okoli sebe. Recimo da se boste vsak dan po 20. uri odklopili od zaslonov vaših pametnih naprav in boste zato neodzivni na sporočila: povejte prijateljem in družinskim članom, da vas pokličejo, če karkoli potrebujejo. Pustite odprto pot dialogu in bodite kritični, kar vam bo pomagalo doseči uravnoteženo življenje, ki vam bo ustrezalo.



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

IZOGNITE SE PRIVZETIM NASTAVITVAM

da bi izboljšali svoje počutje na spletu

Kdaj ste se nazadnje “odklopili” od tehnologije in se je niste dotaknili cel dan? Ali vsaj eno uro? Če ste neprestano na spletu, niste edini. Kako se prepričati, da je čas, ki ga preživimo na pametnih napravah, kakovosten?

Vse se začne z zavedanjem, da neukrotljiva želja po tehnologiji ni vaša krivda! Verjeli ali ne, vaše najljubše aplikacije in spletne strani so oblikovane tako, da so vsaka posebnost, barva ali zvok namensko optimizirani, da bi zadržali vašo pozornost, vas prepričali v nakup in povraten obisk.

Želite poiskati zdrav in uravnotežen odnos med vašim spletnim in realnim življenjem? Prav o tem govori podatkovna razstrupitev.

Pa začnimo!

Ustvaril

TACTICAL
TECH

Podpora

 Firefox

datadetoxkit.org
#datadetox



1.

BODITE PRISOTNI IN SLEDITE TRENUTNEMU DOGAJANJU

Nasvet je težje upoštevati, kot se sprva zdi. Osredotočenost na trenutno dogajanje zahteva dnevno vadbo. Je kot mišica v vaših možganih, s katero morate pridno vaditi, da bi jo okrepili. Začnete lahko tako, da opazujete vaš odnos s tehnologijo, ki jo uporabljate.

Koliko časa preživite na telefonu?

Če z odgovorom niste zadovoljni, obstajajo nastavitve in strategije, s katerimi lahko pridobite nadzor nad uporabo tehnologije.



Če je vaš cilj preživeti manj časa na Facebooku, Instagramu ali Snapchatu, spremenite nastavitve in dovoljenja teh aplikacij, da vam bodo bolje služile.

Nekatere aplikacije, denimo Instagram, ponujajo celo možnost subtilnega opozorila, ko presežete svoj dnevni limit.

Instagram:
Profile → **Menu** →
Nastavitve → **Account** →
Your Activity →
Set Daily Reminder

Če ugotovite, da vaš telefon z vibriranjem, zvonjenjem ali svetlobnimi opozorili ovira pogovore v resničnem življenju, ga lahko začasno utišate, obrnete narobe ali celo pospravite v žep ali torbico ter ga tako odstranite iz svojega vidnega polja.

2.

PREPOZNAJTE OBLIKOVALSKE ZVIJAČE

Vplivajško oblikovanje, poznano tudi kot "dark patterns", je oblikovanje, ki temelji na psihologiji človeka, njegov namen pa je prepričati vas v prijavo na obvestila, nakup ali pa razkritje več osebnih podatkov, kot ste sprva mislili ali nameravali.

Oblikovalske zvijače pogosto vključujejo določene barve, postavitev ikon, nejasna besedila ali nepopolne informacije. Včasih so precej očitne, spet drugič jih je zelo težko opaziti. Mogoče ste na nekatere že naleteli med spletnim nakupovanjem ali naročanjem na obveščanje. Zaradi visoke učinkovitosti lahko tovrstne dizajne najdemo povsod – pripravijo nas do klika, naročanja na obveščanje, pogostejšega nakupovanja in povratnega obiska. Bolj kot se zavedate subtilnih spodbud in manipulacij, ki so vgrajene v spletne strani, bolj spretni in informirani postajate.

Obstajajo številni načini, s katerimi lahko postanete pametnejši od aplikacij, ki jih uporabljate.

Prepoznajte zvijače: Dober začetek je že to, da se zavedate uporabe tovrstnih tehnik. Več o različnih vrstah si lahko preberete na spletu.

Posnetek zaslona in deljenje: Ko naletite na prepričljive spletne dizajne, naredite posnetek zaslona in ga delite s prijatelji (izpustite kateri koli podatek, ki razkriva identiteto – zasebnost je na prvem mestu). Podjetja lahko tudi prosite, da spremenijo svojo prakso.

Ostanite mirni: Če je na spletni strani, namenjeni nakupovanju, odštevalna ura, se vprašajte: "Je to res nujno?" Če pritisnete na gumb, čeprav tega dejansko niste želeli, pomislite na napis na gumbu ali na barve, ki jih uporablja servis. Če ste zmedeni, ne prevalite krivde nase – preučite besede na spletni strani ali aplikaciji, saj so morda nejasne.

3.

OSTANITE MEDIJSKO SPRETNI

Tako kot se lahko naučimo biti pametnejši od oblikovnih značilnosti in lastnosti, katerih namen je spodbuditi skrolanje in klikanje, se lahko naučimo prepoznavati tudi zavajajoče novice, objave in izdelke.

Gotovo ste do zdaj že slišali za problem zavajajočih informacij in lažnih novic. Te lahko prepoznate in premagate – naj vam zastavljanje kritičnih vprašanj o prebranih novicah pride v navado, predvsem če so presenetljive, škandalozne ali predobre, da bi bile resnične.

Konec koncev želite biti prepričani, ali je novica resnična ali lažna – predvsem če jo nameravate deliti s prijatelji ali družinskimi člani.

Na kateri spletni strani je prispevek objavljen?
Kdo ga je napisal (in kdaj)?
Kaj piše v celotnem prispevku, torej pod naslovom?
Na katere vire informacij se naslanja?



Če menite, da gre za zavajajočo informacije in želite preprečiti njeno širjenje, vam večina platform ponuja možnost, da lažno objavo prijavite. Premislite tudi o tem, če želite še vedno slediti računu, ki je informacijo objavil.



5.

IŠČITE RESNICO NA INTERNETU

Izraz “lažne novice” se nanaša na širok spekter neresničnih ali zavajajočih informacij, vključujoč satire, slabo raziskane ali nepreverjene vsebine, prevare in goljufije. Lažne novice niso vedno deljene z namenom škodoželjnosti, a ne glede na razloge, je rezultat isti: prejemniki verjamejo, da je nekaj lažnega resnično, ali da se je nekaj zgodilo, čeprav se dejansko ni.

V najboljšem primeru gre lahko za smešen meme, v najslabšem pa za lažne informacije s področja zdravstva ali politike.

Kljub vložnemu trudu v preiskovanje in spraševanje kritičnih vprašanj o prebranem članku, je lahko končno rezultat še vedno isti, tj. občutek zmedenosti. Nikar ne pozabite: niste edini!

Nasvet: položite vse karte na mizo

Čeprav vse spletne strani ne priznajo svojih napak, to še ne pomeni, da jih ne naredijo. Najbolj zanesljive publikacije so še posebej previdne pri raziskovanju resnice, zato tudi ne preseneča, da zaposlujejo ljudi ali oddelke, ki se ukvarjajo izključno s preverjanjem dejstev.

Poiščite transparentne vire, ki izpostavijo tudi lastne napake. Še bolje je, če so posodobitve dobro vidne recimo na vrhu članka in deljene prek socialnih omrežij. Obstajajo spletna orodja, s katerimi si lahko pomagata.

datadetoxkit.org #datadetox

A product of
**TACTICAL
TECH**

Project partners
 **Save the Children**
100 ANNI



 Funded by
the European Union

6.

RAZBLINITE SVOJ MEHURČEK FILTRIRANJA

Ko spletne strani in aplikacije ustvarijo profil vaših interesov, se lahko znajdete v mehurčku filtriranja. To je, ko vam strežnik postreže z zgodbami, podobnimi tistim, po katerih ste že poizvedovali. Kako to omejuje ali spreminja prejete informacije?

Mehurčki filtriranja lahko povzročijo, da so ljudem prikazane povsem drugačne zgodbe, novinarske naslove, članke in reklame, kar lahko pomeni, da imajo dostop do informacij, ki nimajo nič skupnega, kot je bilo demonstrirano v interaktivnem članku Blue Feed, Red Feed. graphics.wsj.com/blue-feed-red-feed.

Nasvet: prevetrite vsebino in premešajte novice

Dober način je razbliniti mehurček filtriranja z odjavo od servisov, ki agregirajo novice in informacije z različnih virov in perspektiv. RSS novice, forumi in elektronske liste, ki spodbujajo različna mnenja in tematike, vam lahko pomagajo zapustiti mehurček. Global Voices (globalvoices.org) in The Syllabus (the-syllabus.com) sta odlični možnosti za začetek.

Aplikacije, spletne strani in druga spletna omrežja so lahko odličen način za pridobivanje novic, življenjskih nasvetov in zabave. Med vsemi ponujenimi vsebinami pa moramo znati spretno krmariti, da bi našli informacije, ki jih resnično potrebujemo.

Še več – ko naletimo na videoposnetek, fotografijo ali spletni članek, je pogosto težko

razlikovati med resničnimi dejstvi in izmišljotinami. Različni testi osebnosti, ki vas skušajo profilirati, šokantni naslovi in predelane fotografije ter videoposnetki, ki prikazujejo povsem drugačno resničnost, so dokaz, da na spletu stvari niso takšne, kot so videti na prvi pogled.

V nadaljevanju “podatkovne razstrupitve” boste raziskovali področja, povezana z lažnimi informacijami, in pridobili nasvete za prepoznavanje le-teh.

Pa začnimo!

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

ŠEST NASVETOV, KAKO SE IZOGNITI INTERNETNIM LAŽNIM INFORMACIJAM

1.

ZAVEDAJTE SE SVOJE MOČI VPLIVA

Všečkanje, deljenje in posredovanje objav ter tvitov – ta dejanja opisujejo, kako procesirate informacije, ki jih pridobite na spletu. Ko se dovolj ljudi odzove na neko fotografijo, videoposnetek ali objavo, se ta hitro širi in postane viralna.

Vzemite si trenutek in se vprašajte: “Kakšen je moj vpliv na internetu?” Kdaj ste nazadnje videli šokanten ali zabaven naslov, članek, videoposnetek ali fotografijo in jo nemudoma posredovali vašim prijateljem? Znanstveniki so raziskali, da so največkrat deljene vsebine tiste, ki v človeku prebujajo strah, zgroženost, strahospoštovanje, jezo ali tesnobo. Če ste nekaj takega doživeli danes zjutraj, se nikar ne počutite krive!



Nasvet: z deljenjem pokažemo, da nam je mar

Deljenje je oblika sodelovanja. Ko nekaj delimo (karkoli), sodelujemo pri tem, da objava postane viralna. Kaj pa, če se izkaže za lažno? Bi še vedno želeli, da je kakorkoli povezana z vašim imenom in ugledom? Preden delite povezavo, dobro premislite, če obstaja možnost, da gre za nekaj neresničnega, destruktivnega ali škodljivega.

2.

DVAKRAT PREMISLITE, PREDEN OPRAVITE TEST OSEBNOSTI

Kdaj ste nazadnje opazili kviz (tekstkovni ali slikovni) z naslovom, kot je denimo:

- V katero desetletje spadate?
- Katera je vaša spiritualna žival?
- Kako izgleda vaš sanjski oddih?
- itd.

Obstaja sicer možnost, da je namen kviza zabavati uporabnika. Večja verjetost pa je, da so bila vprašanja skrbno oblikovana tako, da pridobijo čim več podatkov o vaši osebnosti s tako imenovanimi psihometričnimi testiranj. Najpogostejši način za ustvarjanje psihološkega profila je ocenitev vaše osebnosti glede na 5 značilnosti: odprtost, vestnost, ekstravertnost, sprejemljivost in nevroticizem (v angleščini poznano pod kratico OCEAN), ki služijo za boljše doseganje ljudi.

Vaši odgovori na kviz, kot je “Kateri lik iz Simpsonov vam je najbolj podoben?”, lahko v kombinaciji z ostalimi navadami, ki se beležijo ob uporabi spletnega iskalnika, aplikacij in raznih kartic zvestobe, podajo analitiko podatke o vašem tipu osebnosti in zanimanjih. To jim omogoča oblikovanje strategij za doseganje vpliva na vaše odločitve – vse od nakupovanje, pa do volitev.

Nasvet: obdržite več zasebnosti

Osebnostne informacije najpogosteje povezujemo z gesli, identifikacijsko številko in bančnim računom. A so podrobnosti o vas, kot so vaši strahovi, ambicije, stvari, ki vas strašijo, prav tako zasebne. Prav te informacije so koristne za analitike podatkov, saj jim omogočajo profiliranje vaše osebnosti. Dobro premislite, preden delite tovrstne podatke v kvizu ali anketi.

3.

NE ZAGRIZITE V VABO

Vaba za klik je izraz, ki označuje pretirano kričeče (senzacionalistične), zavajajoče ali izmišljene naslovnice, ki provokativno napeljuje bralca na klik. Večji odziv v povezavi s člankom, videoposnetkom ali fotografijo prinaša tudi večji zaslužek. To pomeni, da so avtorji močno motivirani, da naredijo karkoli je potrebno, da kliknete oz. delite neko vsebino.

Glede na osebnostni profil, zgrajen na podlagi vaše aktivnosti na platformah, kot sta Facebook in Instagram, lahko prejmete personalizirane objave, ki so oblikovane tako, da se dotaknejo vaših čustev na način, da povečajo možnost vašega odziva.

Vabo za klik lahko najdete med lažnimi informacijami, ni pa nujno. Ko se enkrat naučite prepoznavati tovrstne strategije, jih boste opazili povsod na Youtubu, blogih ali v tabloidih.



Nasvet: najдите izvor

Ko naletite na vabo na klik, se nikar ne ustavite pri naslovu. Če povezava izgleda varna, kliknite na članek in ga v celoti preberite. Bodite pozorni na to, kdo ga je napisal, kdaj je bil izdan in kakšne reference navaja. Lahko se zgodi, da je znotraj članka zaznamek, ki je dejansko plačljiv oglas ali pa avtor trdi, da gre za njegovo osebno mnenje. Tovrstni podatki vam povedo, če je nadaljnje branje vredno vaše energije.

4.

BODITE POZORNI NA LAŽNE INFORMACIJE

Globoki ponaredki so videoposnetki, zvočni posnetki ali fotografije, ki so bili digitalno prilagojeni, tako da nadomestijo obraz, gibanje ali besede. Čeprav je izraz “globoki ponaredek” relativno nov, pojav v različnih oblikah poznamo že desetletja (npr. slike Cottingley fairies iz leta 1917 ali film Forrester Gumb iz leta 1994). Še lažje je ustvariti t. i. poceni ponaredke – zavajajoča vsebina, ki ne zahteva prefinjene tehnologije, temveč se jo zlahka ustvari z neustreznimi naslovi, fotografijami ali videoposnetki. Možna je tudi uporaba že zastarele vsebine, ki opisuje aktualne dogodke.

Nasvet: ostanite zasidrani in raziskujte

Podobno kot pri vabi za klik, nikar na sprejmete ničesar, brez da bi to preverili. Če ogledan videoposnetek ali fotografija izgledata škandalozno, upoštevajte svoje občutke in premislite o tem, kaj se dogaja v ozadju. V kolikor opazite, da se fotografija pogosto pojavlja v ospredju oz. je bila večkrat deljena, poskusite priti do pravega vira.

Takrat si boste postavili več vprašanj: kdo je izdajatelj (katera spletna stran, kdo je avtor)? Kdaj je bila izdana? Če gre za fotografijo, uporabite sistem za iskanje fotografij TinEye in poglejte, kje vse jo lahko najdete.

Raziščite in preverite tudi druge vire informacij, preden informacijo sprejmete kot resnično in jo delite z vašimi prijatelji in družinskimi člani.