4.

UMANJITE SVOJE TRAGOVE

Internetski preglednik na vašem telefonu pohranjuje puno podataka o vama - vašu lokaciju, ono što tražite, koja web mjesta koristite - i te podatke može proslijediti trećoj strani. Pomoću sitnih izmjena možete vratiti kontrolu nad nekim od tih podataka.

Telefoni, tableti i računala uglavnom dolaze s unaprijed instaliranim preglednicima koji ne daju prednost vašoj privatnosti. Umjesto toga, možete **preuzeti i koristiti preglednik** koji već čini vašu web aktivnost prema zadanim postavkama privatnom, štiteći vas od programa za praćenje.

A za neke dodatne pojačivače privatnosti možete instalirati dodatke poznate kao „dodaci i proširenja“ (ovo su mini programi za vaš preglednik koji se lako mogu instalirati i koji vašu mrežnu aktivnost mogu učiniti privatnijom).

5.

UKLONITE OZNAKE SA SEBE I DRUGIH

Jeste li aktivno doprinijeli prikupljanju podataka o svojim prijateljima tako što ste ih u prošlosti označili na fotografijama i objavama?

Smanjite tok njihovih podataka tako što ćete **ukloniti oznake** na što više fotografija i postova.

Prenesite dalje! Potaknite svoje prijatelje, obitelj i suradnike da vam se pridruže u kontroli dijeljenja podataka. Ako svi zajedno radimo na kontroli naših tragova podataka, možemo bolje pomoći jedni drugima i u detoksikaciji.

Proizvod

TACTICAL TECH

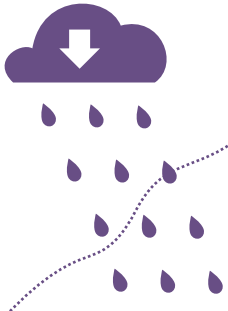
Podržan od

Firefox

datadetoxkit.org
#datadetox

Kako biste blokirali špijunske oglase i nevidljive tragače, instalirajte uBlock Origin (za Chrome, Safari i Firefox) ili Privacy Badger (za Chrome, Firefox i Opera).

Kako biste bili sigurni da su vaše veze s web mjestima sigurne tamo gdje je to moguće, instalirajte HTTPS Everywhere: proširenje preglednika koje osigurava šifriranje i zaštitu tranzita vaše komunikacije s mnogim glavnim web mjestima. Ako ste korisnik Safarija i željeli biste koristiti ovu značajku, postavite zadanu tražilicu na proizvod koji nije Google, poput DuckDuckGo, koji vas automatski preusmjerava na šifrirane veze.



DATA DETOX KIT

UPRAVLJANJE PODACIMA O PAMETNOM TELEFONU

kako biste povećali vašu privatnost na mreži

Ako se zapitate što vaši podaci drugima govore o vama, možda se na prvu stvar ne čini tako važnom: koga zanima što ste ljubitelj country glazbe, volite kupiti više cipela nego što vam je potrebno ili svoj godišnji odmor planirate godinu dana unaprijed?

Problem leži u onome što se događa s vašim podacima. S vremenom povezani pojavljuju se intimni digitalni obrasci: vaše navike, kretanja, odnosi, sklonosti, stavovi i tajne otkrivaju se onima koji ih analiziraju i od njih profitiraju, poput tvrtki i posrednika podataka.

Slijedeći ovaj Komplet, uvidjet ćete kako i zašto se sve to događa te ćete moći poduzeti praktične korake za kontrolu tragova podataka koje ostavljate diljem interneta.

Započnimo!

1.

PROMIJENITE NAZIV UREĐAJA

Vjerojatno ste u nekom trenutku imenovali svoj telefon za spajanje putem opcije Wi-Fi, Bluetooth ili za oboje - ili je možda ime automatski generirano tijekom postavljanja.

To znači da je "Telefon Alexa Chunga" ono što je vidljivo vlasniku Wi-Fi mreže, a ako je vaš Bluetooth uključen, i svima koji u tom području također imaju uključen Bluetooth.

Zasigurno ne biste ulazeći u kafić, restoran ili zračnu luku, svima na glas objavili svoje ime i prezime, pa to isto ne bi trebao činiti ni vaš telefon.

Možete promijeniti ime svog telefona u nešto manje osobno, ali još uvijek jedinstveno za vas. Evo kako:

iPhone:
Vaihda puhelimen nimi:
Asetukset → Yleiset →
Tietoja → Vaihda nimi

Android:
Promjena Wi-Fi naziva:
Postavke →
Wi-Fi → izbornik →
Napredno / Više značajki →
Wi-Fi Direct →
Preimenuj uređaj
Promjena Bluetooth imena:
Postavke → Bluetooth →
Uključite Bluetooth ako je isključen → izbornik →
Preimenuj uređaj →
Isključite Bluetooth

2.

OČISTITE OTISKE SVOJE LOKACIJE

Iako se možda čini da su podaci o vašoj lokaciji samo slučajni fragmenti informacija, kada ih se sagleda kao cjelinu, mogli bi otkriti važne detalje o vama i vašim navikama, poput: mjesta gdje živite, gdje radite i gdje se volite družiti s prijateljima. To je razlog zbog čega su mnoge tvrtke i posrednici podataka izuzetno zainteresirani za njih.

Možete pregledati dozvole svake aplikacije i isključiti usluge lokacije. Potražite aplikacije koje zapravo ne trebaju taj podatak za davanje usluge (mora li ta igra zaista znati gdje se nalazite?) te isključite opciju i za aplikacije kojima ne želite dati pristup toj informaciji:

Android:
Postavke → Apps →
Upravljajte pristupom lokaciji prema aplikaciji

iPhone:
Postavke → Privatnost →
Lokacijske usluge →
Upravljajte pristupom lokaciji prema aplikaciji

3.

UREDITE SVOJE APLIKACIJE

Vaše aplikacije na društvenim mrežama, igre i prognoza vremena koriste vaše podatke ... i velika je vjerojatnost da ih prikupljaju u većim količinama.

Uklanjanje aplikacija koje nikada ne upotrebljavate s telefona može biti moćan način detoksikacije vaše digitalne osobnosti.

Osim toga, čišćenje također može osloboditi prostor na vašem telefonu, smanjiti upotrebu podataka i produžiti vijek trajanja baterije. Ovisno o aplikaciji, čišćenje ujedno može i poboljšati ukupna svojstva uređaja.

Android:
Postavke → Apps →
Odaberite aplikaciju koju želite deinstalirati →
Deinstaliraj

iPhone:
Pritisnite jednu aplikaciju dok se sve ne počnu kretati i dok se u gornjem lijevom kutu svake aplikacije ne pojave mali križići.

Da biste izbrisali aplikaciju, dodirnite mali križić te aplikacije.

Da biste se vratili u normalno stanje, pritisnite gumb početnog zaslona.

4.

ZAŠTITITE SVOJE VIRTUALNE VRIJEDNOSTI

Baš kao što brinete o vrijednim predmetima u svom domu, tako biste trebali postupiti i s podacima koje virtualno pohranjujete - bilo da se radi o vašoj financijskoj evidenciji, skeniranju putovnice ili čak adresi ili telefonskom broju, važno je gdje pohranjujete svoje najcjenjenije osobne podatke i kako ih možete zaštititi.

Spot clean izvrstan je ako želite napraviti nekoliko brzih poboljšanja uz kavu. Potražite određene podatke koji se nalaze u vašoj e-pošti ili na drugim računima i izbrišite ih: skenove osobne iskaznice, bankovnih podataka ili podataka o zdravstvenom osiguranju, da nabrojimo samo neke. Ako vam kasnije zatreba nešto od spomenutog, uvijek isto možete ponovno preuzeti ili isprintati prije brisanja s računa e-pošte.

Dubinsko čišćenje temeljitije je i dobro ga je raditi jednom godišnje. Arhivirajte sve na svom računu e-pošte ili na društvenim mrežama, preuzmite podatke na računalo i izbrišite sadržaj računa da biste započeli iznova.

Savjet: Nemojte samo brisati - također ispraznite kantu za smeće i privremene datoteke!

Na vama je želite li sigurnosnu kopiju arhiva i dokumenata napraviti u oblaku ili ih spremiti na vanjski tvrdi disk ili USB. Bez obzira na to kako čuvate svoje podatke, pripazite da ih ne izgubite te da ih čuva snažna lozinka koja za vas ima smisla.

5.

PROSLIJEDI DALJE

Često se i lako zaboravlja da se web s razlogom naziva "mreža". **Svi smo povezani na mreži** putem različitih mreža, ne samo kao „prijatelji“ na društvenim mrežama, već i putem kontakata na našim računima e-pošte i fotografija koje dijelimo na mreži. Kada osigurate svoje račune, ojačate lozinke i očistite podatke, niste samo vi u prednosti - **svi s kojima ste povezani pomalo su sigurniji upravo zbog vašeg truda.**

Kada čistite račune e-pošte i društvenih mreža, razmislite što još možete preuzeti i izbrisati što bi moglo pomoći vašim prijateljima ili suradnicima: bankovni podaci vaše sestre, ključni kôd vašeg ureda ili sken putovnice vašeg sina samo su neke od evidencija koje bi vam mogle izazvati glavobolju ukoliko dođu u pogrešne ruke.

Prenesite dalje! Povećavanje vaše digitalne sigurnosti može biti jednostavno kroz slijeđenje nekoliko osnovnih koraka. Podijelite ovaj Komplet sa svojim prijateljima, obitelji ili suradnicima kako biste im pomogli u promijeni navika na načine koji za njih imaju smisla.

DATA DETOX KIT

POMAKNITE POSTAVKE

za zaštitu podataka

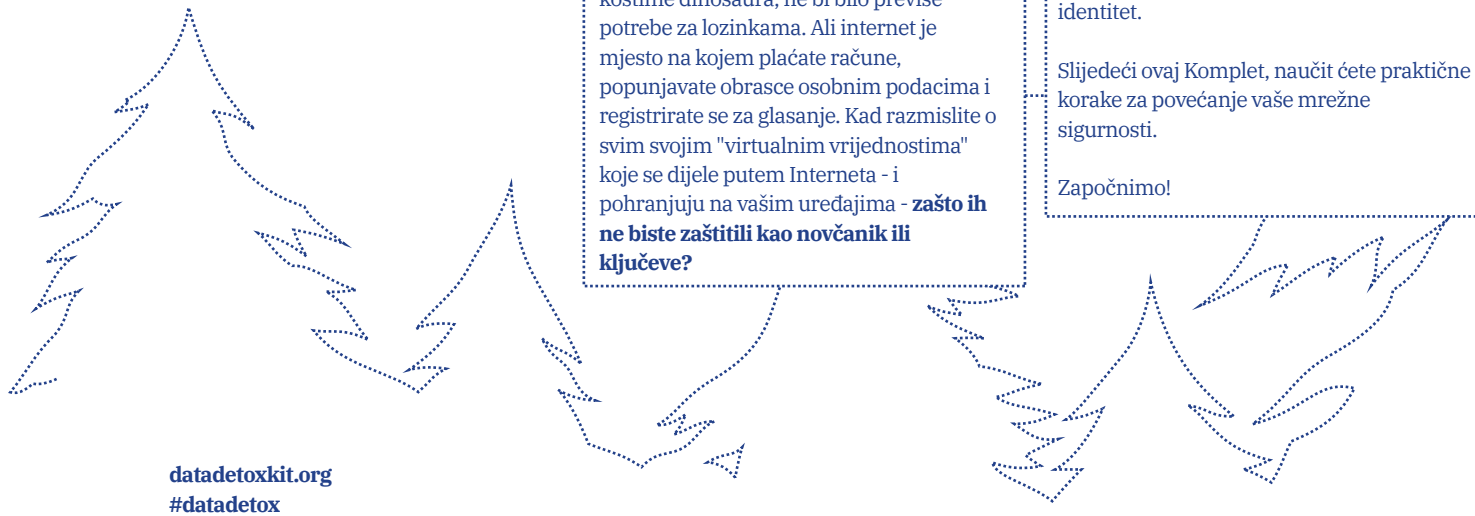
Kad bi internet bio samo mjesto na kojem se razmjenjuju slika pasa koji nose kostime dinosaura, ne bi bilo previše potrebe za lozinkama. Ali internet je mjesto na kojem plaćate račune, popunjavate obrasce osobnim podacima i registrirate se za glasanje. Kad razmislite o svim svojim "virtualnim vrijednostima" koje se dijele putem Interneta - i pohranjuju na vašim uređajima - **zašto ih ne biste zaštitili kao novčanik ili ključeve?**

Postoji jedan jednostavan način da drugima otežate pristup vašim virtualnim vrijednostima: **nemojte im olakšati pogađanje vaših lozinki.** Većini ljudi nisu potrebne posebne tehničke vještine da bi ušli na vaše račune - to mogu učiniti samo nagađanjem lozinki ili pokretanjem automatiziranog programa.

A nakon što uđu na jedan račun, mogu isprobati tu kompromitiranu lozinku na drugim računima, prikupiti podatke o vama i vašim navikama, preuzeti račune u vašem vlasništvu ili čak koristiti vaš digitalni identitet.

Slijedeći ovaj Komplet, naučit ćete praktične korake za povećanje vaše mrežne sigurnosti.

Započnimo!



Proizvod
TACTICAL TECH

Podržan od
Firefox

datadetoxkit.org
#datadetox

1.

ZAKLJUČAJ SVOJA DIGITALNA VRATA

Zaključavanje zaslona: lozinka, uzorak, otisak prsta ili ID lica koji upotrebljavate za pristup uređaju neke su od **najboljih obrana** protiv nekoga tko bi možda želio ući u vaš uređaj. Ali postoji puno različitih vrsta zaštite i možda će biti teško znati koja je prava za vas.

Ukoliko imate bilo kakvu bravu na telefonu, tabletu ili računalu, ona vam pruža veću zaštitu nego da nemate nikakvu bravu. I baš kao i različite vrste brava koje biste mogli staviti na vrata, **neke su brave zaslona jače od drugih.**

Od svih brava koje postoje, duge, jedinstvene lozinke su najjače. To znači da ako otključavate uređaj lozinkom, ona bi trebala sadržavati slova, brojeve i posebne znakove.

Recimo da koristite osnovni potez za otvaranje telefona. Možete polako povećati svoju sigurnost postavljanjem duge lozinke. Ili sada koristite zaključavanje uzorkom? Što kažete na to da svoj uzorak učinite dužim? Upotrebljavate 1234 kao svoj PIN? Što kažete na to da umjesto ove kombinacije, sedam puta bacite kockice i zapamtite taj PIN? **Mala promjena može uvelike doprinijeti zadržavanju kontrole nad vašim uređajima.**

2.

PUSTITE ONOG PRAVOG

Stvaranje vrhunskih lozinki je jednostavno. Sve što trebate je slijediti nekoliko osnovnih principa. Vaše lozinke trebaju biti:

Dugačke: **lozinke trebaju imati najmanje osam znakova. Još bolje? 16-20 znakova**

Jedinstvene: **svaka lozinka koju upotrebljavate - za svaku web stranicu - treba biti različita**

Nasumične: **vaša lozinka ne bi trebala slijediti logičan obrazac niti bi je trebalo lako moći pogoditi. Tu upravitelji lozinki postaju vrlo korisni.**

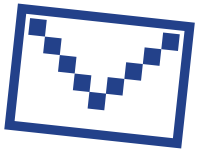
Najjače lozinke koriste kombinaciju slova, brojeva i posebnih simbola. Ovaj provjereni savjet čini jaču lozinku koju je teže pogoditi. Neki sustavi lozinki nažalost ne dopuštaju upotrebu posebnih simbola (poput @ # $% - = +), ali dovoljno duga kombinacija slova i brojeva ipak je bolja od kratke.

U idealnom slučaju, trebali biste koristiti namjenski upravitelj lozinki za generiranje i spremanje svih lozinki. Upravitelj lozinki - poput 1Password i KeePassXC, koje često preporučuju sigurnosni stručnjaci - u osnovi je aplikacija čija je jedina svrha zaštititi vaše vjerodajnice za prijavu i druge osjetljive podatke.

3.

DODAJ DRUGI KLJUČ

Postavljanje dvofaktorske autentifikacije (2FA) ili više faktorske autentifikacije (MFA) znači da čak i ako netko pronađe vašu lozinku, **vjerojatno neće imati dodatni faktor koji treba za ulaz.**



Pregledajte sigurnosne postavke svojih najčešće korištenih web lokacija i aplikacija da biste vidjeli možete li postaviti ovaj dodatni ključ. Započnite s najvažnijim - bilo kojim financijskim aplikacijama ili uslugama poput e-pošte koje upotrebljavate za oporavak ostalih računa.

Google:
Prijavite se na myaccount.google.com → Sigurnost → Potvrda u 2 koraka → Započnite

Facebook:
izbornik → Postavke → Sigurnost i prijava → Upotrijebi dvofaktorsku autentifikaciju

Savjet: Kada postavljate sljedeći sloj provjere, morat ćete odabrati drugi način potvrde da ste to vi. Pokušajte izbjegavati korištenje SMS-a (tekstualnih poruka poslanih na vaš telefonski broj) kao drugog čimbenika, samo u slučaju da izgubite telefon. E-pošta je obično pouzdanija opcija.

4.

NEKA SE ČUJE I TVOJ GLAS

Ukoliko ste nezadovoljni dizajnom web lokacije ili aplikacije koju često posjećujete i koristite ili pak se na njima objavljuju pogrešne informacije uvijek ih možete kontaktirati. Tvrtkama možete slati e-poštu, pisati tweetove i tako im jasno dati do znanja da se ne slažete s njihovom praksom i poslovanjem. Kad najvrjednija imovina tvrtke - njihovi korisnici vrše pritisak da se poduzmu određene mjere - postoji velika šansa da do promjena doista i dođe.

Ako vam se čini da vaše kritike ne dopiru do davatelja usluga, možete učiniti nešto doista moćno: koristite drugo web mjesto ili aplikaciju. Ako dovoljan broj ljudi prenese svoje nezadovoljstvo web mjestom ili aplikacijom stvaratelju iste, te prestane koristiti njihovu uslugu deinstalacijom aplikacije- **tvrtka će to itekako primijetiti.**

5.

ŠIRITE VIJEST

Šalji dalje! Ovo je jednostavan savjet kojeg ljudi često zaborave, i zbog toga može uzrokovati ozbiljne posljedice. Obavijestite svoje prijatelje, obitelj i suradnike o stvarima koje primjećujete, čak ih i zamolite da vam se pridruže u ovoj detoksikaciji!

Svatko se bori s kontroliranjem svojih navika u korištenju telefona. Najvažnije je pronaći način korištenja koji odgovara vama i vašem načinu života. Eksperimentirajte dok ne pronađete odgovarajuća rješenja. Zatim ažurirajte svoje navike sukladno novim potrebama. Ne postoji univerzalno rješenje za sve korisnike.

I na kraju, komunicirajte o svojim tehničkim izborima i rješenjima s ljudima oko vas. Recimo, Informirajte obitelj i prijatelje da ćete biti nedostupni u svojoj aplikaciji za razmjenu poruka svakoga dana nakon 20:00 sati jer ćete tada započeti rutinu bez zaslona: recite im neka vas umjesto toga nazovu.

Držite dijalog otvorenim, postavljajte pitanja i možete živjeti uravnoteženim mrežnim životom koji vama odgovara.

DATA DETOX KIT

BIJEG OD ZADANIH POSTAVKI

za poboljšanje vaše digitalne dobrobiti

Kada ste se zadnji put "isključili" i niste dodirnuli tehnologiju cijeli dan, ili čak samo sat vremena? Ako ste stalno na mreži, niste sami. Sve čemu posvetite toliko vremena mora biti vrijedno vaše pažnje. Kako možete provjeriti je li vrijeme provedeno na vašem uređaju kvalitetno utrošeno?

Sve započinje saznanjem da neodoljiva privlačnost prema tehnologiji nije vaša krivnja! Vjerovali ili ne, vaše omiljene aplikacije i web stranice dizajnirane su na taj način da svaka značajka, boja i zvuk služi i 'optimizirana' je da vas drži priključenima, zaokupljenima i da se uvijek vraćate po još.

Želite pronaći zdraviju ravnotežu između vašeg mrežnog i izvanmrežnog života? O tome pričamo u ovom dijelu Kompleta.

Započnimo!

Proizvod
TACTICAL TECH

Podržan od
Firefox

datadetoxkit.org
#datadetox

1.

BUDITE PRISUTNI U TRENUTKU

Ostvarivanje ovog savjeta je teže nego što se čini. Ostajanje u trenutku zahtijeva svakodnevnu praksu. Ono je poput mišića u vašem mozgu kojeg trebate redovito trenirati kako bi izgradio svoju snagu. Možete početi tako što ćete si osvijestiti svoj odnos s tehnologijom koju koristite.

Koliko vremena provodite na telefonu?

Ako ste nezadovoljni odgovorom, postoje postavke i strategije koje možete slijediti kako biste stekli kontrolu nad upotrebom vaše tehnologije.

Ako vam je cilj provesti manje vremena na Facebooku, Instagramu ili Snapchatu, promijenite postavke i dopuštenja tih aplikacija kako bi radile u vašem interesu. Neke aplikacije poput Instagrama čak imaju opciju kada vas aplikacija blago podsjeća kad ste dosegli dnevno ograničenje.

Instagram:
Profil → izbornik → Postavke → Račun → Vaša aktivnost → Postavi dnevni podsjetnik

Postoje i aplikacije koje vam pomažu u mjerenju vremena korištenja. Android i iPhone sada mog provjeravati navike korištenja pomoću Googleove digitalne dobrobiti i najnovijeg iOS ažuriranja). Usluge vas informiraju koliko često provjeravate telefon i predlažu postavke kojima možete dodatno upravljati.

2.

UOČITE TRIKOVE U DIZAJNU

Uvjerljivi dizajn, poznat i kao "tamni uzorak", temelji se na na ljudskoj psihologiji koja se koristi da vas isprovocira da se pretplatite ili kupite nešto te odate više osobnih podataka nego što ste mislili ili namjeravali.

Uobičajeni trikovi dizajna mogu uključivati upotrebu određenih boja, nejasnih tekstova ili nepotpunih podataka te ciljano postavljanje gumba. Ove dizajnerske trikove vidite svugdje zbog toga jer su učinkoviti - natjeraju nas da češće kliknemo, pretplaćujemo se, kupujemo te se iznova vraćamo.

Što ste svjesniji ugrađenih suptilnih poticaja i manipulacija na web mjestima koja upotrebljavate, to postajete pametniji i informiraniji.

Postoji nekoliko stvari koje možete učiniti kako biste nadmudrili svoje aplikacije.

Prepoznajte kad vas guraju: Prvo što možete učiniti je da jednostavno osvijestite upotrebe ovih tehnika.

Snimka zaslona i dijeljenje: Snimite zaslon kad god naiđete na uvjerljiv dizajn na mreži i podijelite ga prijateljima (izostavljajući bilo koji detalji pomoću kojeg vas je moguće osobno identificirati - privatnost prije svega!). Možete sugerirati i tvrtkama da promijene svoju praksu.

Ostanite mirni: Ako na stranici za kupnju postoji odbrojavanje, zapitajte se , "Je li ovo stvarno hitno?" Ako se zateknete kako ste kliknuli na gumb koji zapravo niste htjeli, razmislite o natpisu na gumbu ili boji koju usluga koristi. Ako se osjećate zbunjeno, nemojte odmah pretpostaviti da ste vi krivi - razmotrite riječi koje koristi web mjesto ili aplikacija, jer mogu biti nejasne.

3.

BUDITE MUDRI S MEDIJIMA

Baš kao što možete naučiti nadmudriti značajke i dizajn čiji je cilj zadržati vas na stranici, također možete biti pametni i naučiti uočavati vijesti ili postove čija je funkcija zavarati vas.

Do sada ste već čuli za probleme 'dezinformacija' i 'lažnih vijesti'. Uočavanje pogrešnih informacija vam može uobičajeno ako se naviknete postavljati kritična pitanja o bilo kojoj vijesti koju konzumirate, pogotovo ako je izgleda iznenađujuće, nečuveno ili predobra da bi bilo istinita.

Na kraju ćete htjeti i provjeriti koje su vijesti stvarne ili lažne, pogotovo ako ih planirate podijeliti s obitelji ili prijateljima.

S kojeg je web mjesta ovo?
Tko ga je napisao (i kada)?
O čemu govori cijeli članak, izvan naslova?
Na koje se izvore pozivaju?

Ako uočite pogrešne informacije i želite spriječiti njihovo širenje, većina platformi ima mjesto gdje možete prijaviti tave objave. Možete također odlučiti želite li i dalje pratiti račun koji je te netočne informacije objavio.

5.

TRAŽITE ISTINU NA INTERNETU

Izraz "lažne vijesti" koristi se za širok raspon netočnih ili obmanjujućih informacija, uključujući satiru, slabo istražene ili neprovjerene sadržaje, podvale, šale i prevare. Lažne vijesti se ne šire uvijek zlonamjerno, ali bez obzira na razlog zbog kojeg se dijele, rezultat je općenito isti: ljudi na prijemnoj strani tih informacija vjeruju u nešto što je zapravo netočno ili se nikada nije dogodilo.

U najboljem slučaju, to može biti šaljivi meme. U najgorem slučaju, to mogu biti netočni zdravstveni savjeti ili lažne političke informacije.

Čak ako istražujete i postavljate kritička pitanja o informacijama iz članaka koje ste pročitali, oni vas svejedno mogu zbuniti. Ali znajte ovo: niste sami!

Sve ruke na palubu
Samo zato što web stranica ne priznaje svoje pogreške, ne znači da ih nema. Zapravo su najpouzdanije publikacije one koje su vrlo oprezne s istinom i zapošljavaju ljude ili čitave odjele čiji je jedini posao provjera činjenica.

Potražite izvore koji izdaju ispravke kada su u krivu. Još je bolje kada je ažuriranje sažeto na vrhu članka i podijeljeno na društvenim mrežama, tako da ga ne morate pretjerano tražiti .

6.

PUKNITE SVOJ MJEHURIĆ S FILTROM

Nakon što web stranice i aplikacije izgrade profil vaših interesa, mogli biste se naći u mjehuriću s filtrom. Ovo stanje se javlja kada vas usluge „hrane“ sa sve više priča sličnih onima na koje ste već kliknuli. Kako to možete ograničiti ili promijeniti teme o kojima čitate?

Biti zarobljen u mjehuriću filtra znači da će različiti ljudi vidjeti potpuno drugačije priče, naslove vijesti, članke i oglase o sličnim temama, kao što je prikazano u interaktivnom članku Blue Feed, Red Feed (graphics.wsj.com/blue-feed-red-feed).

Ako znate da gledate posebno za vas dizajnirani algoritamski uređen sadržaj u vašim aplikacijama i web lokacijama, pitanje je: Kako izaći izvan tog oblačića s filtrom?

Promijenite smjer vjetra i promiješajte svoje vijesti
Dobar način da puknete oblačić filtra je pretplatiti se na usluge koje prikupljaju vijesti i informacije iz različitih izvora i s raznolikim perspektivama. RSS feedovi, forumi i popisi za slanje pošte koji imaju široki spektar mišljenja i tema mogu vam pomoći da vidite izvan svog oblačića. Global Voices (globalvoices.org) i The Syllabus (the-syllabus.com) izvrsne su mogućnosti za početak.

DATA DETOX KIT

6 SAVJETA ZA IZBJEGAVANJE ZABLUDA NA MREŽI

Aplikacije, web stranice i internetski mediji mogu biti presudni za pristup vijestima, savjetima za bolji život i zabavi. Pronalaženje željenih informacija može biti otežano zbog velike količine sadržaj i distrakcija koje nas okružuju u virtualnom svijetu.

Štoviše, ponekad je teško utvrditi razliku između činjenica i fikcije kada na mreži naiđete na video, sliku ili članak. Od upitnika ličnosti koji vas pokušavaju profilirati, šokantnih naslova i izmijenjenih fotografija ili videozapisa koji vas mogu uvjeriti u potpuno drugačiju stvarnost, ono što vidite na mreži nije uvijek ono što se čini.

U ovom Detoksu podataka istražit ćete teme povezane s dezinformacijama i modernim rječnikom, počevši od pogleda izbliza na vašu odgovornost, a zatim proširujući sliku, istovremeno dobivajući savjete kako pronaći svoj put kroz ono što nas okružuje.

Idemo!

datadetoxkit.org **#datadetox**

Proizvod
TACTICAL TECH

Podržan od
Save the Children 100 ANNI
IFLA
Financira Europska unija

1.

SHVATITE SVOJU MOĆ STVARANJA VALOVA

Sviđanje, dijeljenje, ponovno objavljivanje - sve ove radnje opisuju na koji način komunicirate s onim što vidite na mreži - i vaše interakcije čine veliku razliku. Kad se dovoljno ljudi bavi slikom, videozapisom ili objavom oni po definiciji postaju "viralni" jer se brzo šire po mreži ili platformi.

Odvojite trenutak i zapitajte se: **„Kakav je moj utjecaj na mreži?“** Kada ste zadnji put vidjeli šokantan ili smiješan članak, naslov, video ili sliku, te ga za nekoliko sekundi već proslijedili svojim prijateljima? Istraživači su pronašli da su priče i slike koje će vjerojatno postati viralne one zbog kojih osjećate strah, zgroženost, strahopoštovanje, ljutnju ili tjeskobu. Ako ste ovo učinili jutros, ne osjećajte se loše!

2.

RAZMISLITE DVAPUT PRIJE NEGO ŠTO ISPUNITE TAJ UPITNIK OSOBNOSTI

Kada ste zadnji put vidjeli kviz (bilo u tekstualnim ili foto filtrima)koji se zove poput:

- Koje ste desetljeće?
- Koja je tvoja duhovna životinja?
- ... popis se nastavlja!

Iako postoji šansa, da je ovo doista bio zabavni kviz osmišljen kako bi vas primamio na rješavanje i angažman, moguće je i da su pitanja bila pažljivo izrađena za prikupljanje podataka i kategorizaciju vaše osobnosti, na temelju tzv. psiho metrijskih obrazaca.

Svoje odgovore na kviz poput "Koji ste lik iz Simpsona?" s ostalim navikama koje možda nadgleda vaš preglednik, aplikacija ili povezane stavke poput kartica vjernosti, analitičarima podataka mogu dati jasnu sliku kakva ste osoba, do čega vam je stalo i kako mogu na vas utjecati da kupite par cipela (na primjer) ... ili kako bi uz pomoć profiliranja odredili najbolju metodu putem koje bi pokušali utjecati na to da na sljedećim izborima glasate na određeni način.

3.

NE GRIZITE MAMAC

Klik - mamac pojam je koji se koristi za opisivanje senzacionalističkih, nepoštenih ili izmišljenih naslova koji se koriste s namjerom da navedu ljude da kliknu na naslov ili poveznicu. Što publika više pažnje posveti članku, videozapisu ili slici, putem klikanja to će više novaca vjerojatno zaraditi. To znači su kreatori motivirani da kažu sve što je potrebno kako bi vas naveli da kliknete ili podijelite njihov sadržaj.

Na osnovu profila osobnosti koji o vama grade platforme koje koristite (poput Facebooka i Instagrama), možda ćete dobiti prilagođene naslove koji stvoreni su da pokrenu vaše osjećaje na način koji je najvjerojatniji da biste kliknuli.

Klik-mamac se često povezuje uz pogrešne informacije, ali to ne mora uvijek biti slučaj. Jednom kada naučite prepoznati naslove klik - mamaca, primijetit ćete ih posvuda po YouTubeu, blogovima i tabloidima.

4.

PAZITE NA LAŽI

Deep fakes su videozapisi, audio isječci ili slike koji su već bili snimljeni digitalno izmijenjeni, obično za zamjenu nečijeg lica ili pokreta ili kako bi promijenili njihove riječi. Iako je "duboka krivotvorina" novi izraz, zapravo je postojao u drugom obliku desetljećima. Još je lakše stvoriti takozvani jeftini lažnjak - obmanjujući sadržaj za nastanak kojeg nije potrebna sofisticirana tehnologija, ali umjesto toga može se stvoriti jednostavnim stavljanjem pogrešnog naslova na fotografiju ili videozapisu ili upotrijebiti zastarjeli sadržaj kako bi se ilustrirao trenutni događaj.

Možda se čini nemogućim istinski se boriti protiv krivotvorina, ali postoji nešto što je ključno i što možeš učiniti... ostani čvrsto na tlu.

Ostanite uzemljeni i istražujte
Baš kao kad imate posla s klik-mamcem, nemojte stati na naslovu. Ako se videozapis ili fotografija koju ste vidjeli čini iznenađujućim ili nečuvenim, prepoznajte taj osjećaj i uzmite u obzir da se možda iza naslova krije više od onoga što je vidljivo na prvi pogled. Također, ako primijetite da se ista slika javlja u vašim novostima ili je više puta podijeljena s vama, shvatite to kao poticaj da ju istražite podrobnije i otkrijete njen pravi izvor.

Tada ćete poželjeti postaviti više pitanja: tko ju je objavio (koja web stranica, tko je autor)? Kada je objavljena? Ako je riječ o slici, pokrenite obrnuto pretraživanje prema slici na TinEye i pogledajte gdje je još možete pronaći.

Provjerite druge vjerodostojne izvore vijesti prije nego što povjerujete u njezinu istinitost i vjerodostojnost te prije nego što je podijelite s prijateljima i obitelji.

Dijeljenje je znak brižnosti
Dijeljenje je oblik sudjelovanja. Kada nešto podijelite (bilo što), postoji šansa da to što ste podijelili postane viralno. Ako se, na primjer, ispostavi da je objava lažna, doista želite da se uz nju veže vaše ime i ugled? Prije nego što podijelite vezu, razmislite širite li možda nešto neistinito, destruktivno ili otrovno.

Čuvaj više tajni
Kad pomislite na privatne podatke, možda su vam prve stvari koje vam padnu na pamet vaše lozinke, identifikacijski broj i broj bankovnog računa. Ali detalji o vama, poput onoga što vas plaši, što vas živcira i vaše ambicije, jednako su osobni. Analitičari podataka ove podatke mogu smatrati vrijednima, rasvjetljavajući ono što vas tjera da budete osoba. Dobro razmislite prije nego što date takve informacije u anketi ili kvizu.

Idi na izvor
Kad se suočite s klik-mamcem, nemojte se zaustaviti na naslovu. Ako se poveznica doima sigurnom, kliknite na članak i saznajte tko je autor, kada je objavljen i na koje se izvore poziva. Postoji mogućnost da u članku postoji napomena da se radi o plaćenom sadržaju ili oglasu ili je možda kategoriziran kao mišljenje. Ovi detalji mogu vam pomoći da odlučite vrijedi li ga čitati.