4.

SAMAZINI SAVAS PĒDAS

Tālruņa pārlūks glabā daudz informācijas par jums – jūsu atrašanās vietu, to, ko jūs meklējat, jūsu izmantotās tīmekļa vietnes – un var nodot šo informāciju tālāk. Jūs varat atgūt kontroli pār šo informāciju, veicot dažas izmaiņas.

Tālruņos, planšetdatoros un datoros parasti ir iepriekš uzstādītas pārlūkprogrammas, kurām jūsu konfidencialitāte nav prioritāte. Tā vietā jūs varat lejupielādēt un izmantot pārlūkprogrammu, kas jau pēc noklusējuma padara jūsu tīmekļa darbību privātu, pasargājot jūs no izsekotājiem.

Turklāt dažiem papildu privātuma uzlabotājiem varat instalēt ekstras, ko sauc par "pievienojumprogrammām un paplašinājumiem" (tās ir viegli instalējamas mazās programmas jūsu pārlūkprogrammai, kas var padarīt jūsu tiešsaistes darbību privātāku).

5.

DZĒS SAVUS UN CITU TAGUS

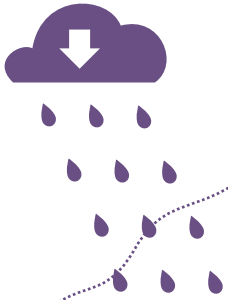
Vai iepriekš esat palielinājis savu draugu datu apjomu, atzīmējot viņus fotoattēlos un publikācijās?

Maziniet datu daudzumu (un reizē arī nomieriniet savu sirdsapziņu), dzēšot tagus pēc iespējas lielākā skaitā fotoattēlu un publikāciju.

Pastāstiet citiem! Mudiniet draugus, ģimeni un kolēģus pievienoties jums šajā viegli pieejamo datu kontrolēšanas akcijā. Ja mēs visi strādājam kopā, lai kontrolētu pašu atstātās datu pēdas, mēs varam viens otram labāk palīdzēt atbrīvoties no visa liekā.

Autors

TACTICAL TECH



DATA DETOX KIT

Lai bloķētu spiegošanas reklāmas un neredzamos izsekotājus, instalējiet uBlock Origin (Chrome, Safari un Firefox) vai Privacy Badger (Chrome, Firefox un Opera).

Lai nodrošinātu, ka savienojumi ar tīmekļa vietnēm ir droši, kur vien iespējams, instalējiet HTTPS Everywhere: tas ir pārlūkprogrammas paplašinājums, kas nodrošina, ka jūsu saziņa ar daudzām lielākajām tīmekļa vietnēm tiek šifrēta un aizsargāta tranzītā. Ja lietojat Safari un vēlaties izmantot šo funkciju, iestatiet noklusējuma meklētājprogrammu uz produktu, kas nav Google produkts, piemēram, DuckDuckGo, kas automātiski novirza jūs uz šifrētiem savienojumiem.

KONTROLĒ SAVA VIEDTĀLRUŅA DATUS,

lai uzlabotu savu privātumu tiešsaistē

Ja domājat par to, ko jūsu dati stāsta par jums citiem, var šķist, ka tas nav nekas īpašs, jo kuru gan interesē, ka jūs esat kantrimūzikas fans, ka jums patīk iegādāties vairāk apavu, nekā nepieciešams, vai ka savu nākamo atvaļinājumu jūs sākat plānot jau gadu iepriekš.

Problēma slēpjas tajā, kas notiek ar jūsu datiem. Laika gaitā kopā ņemot, rodas dziļi personiski digitāli modeļi: jūsu paradumi, pārvietošanās, attiecības, vēlmes, uzskati un noslēpumi tiek atklāti tiem, kas tos analizē un gūst peļņu, piemēram, uzņēmumiem un datu brokeriem.

Šīs datu detoksikācijas laikā jūs gūsiet ieskatu tajā, kā un kāpēc tas viss notiek, un veiksiet praktiskas darbības, lai kontrolētu datu pēdas internetā.

Ķersimies pie darba!

datadetoxkit.org
#datadetox

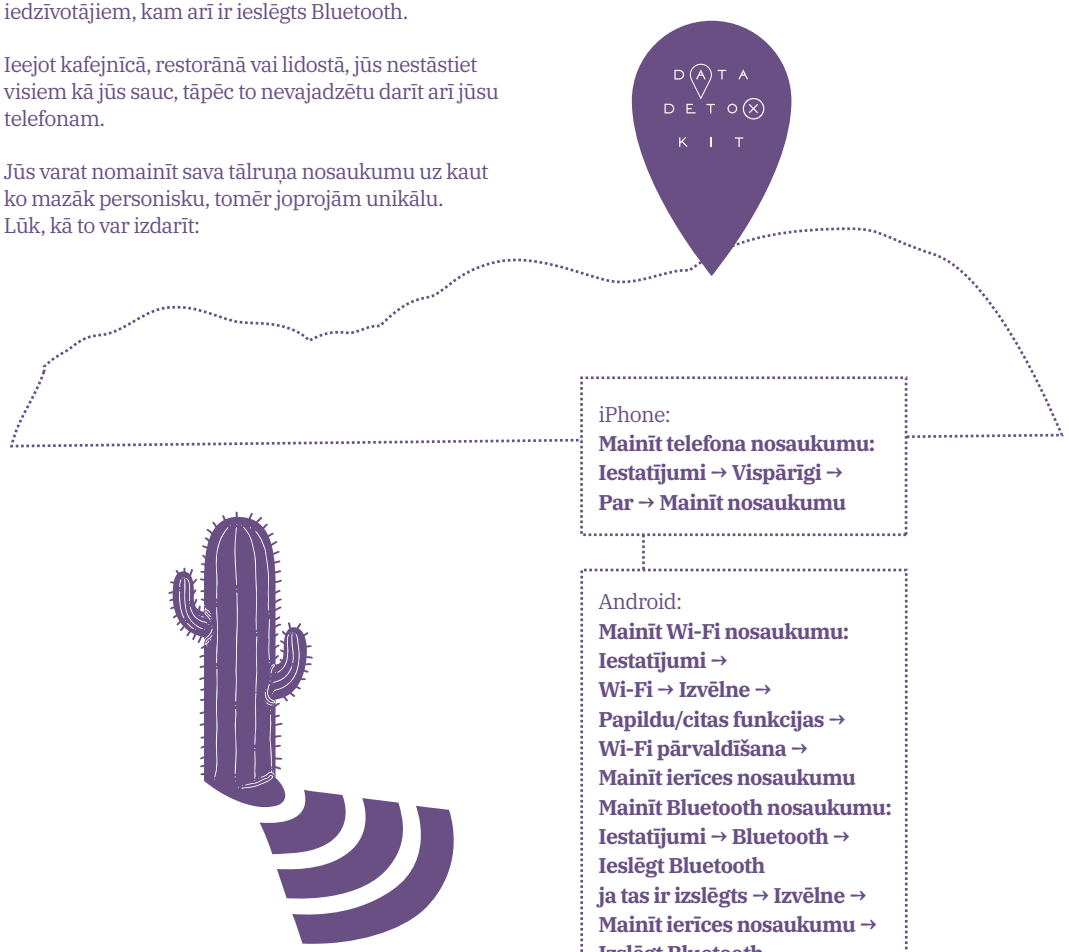
1.

NOMAINI SAVAS IERĪCES NOSAUKUMU

Iespējams, ka kādā brīdī savam telefonam esat "iedevis vārdu" savienojumam ar Wi-Fi, Bluetooth vai abiem, vai arī uzstādīšanas laikā nosaukums tika ģenerēts automātiski. Tas nozīmē, ka "Aleksa Čuna telefons" ir tas, kas ir redzams Wi-Fi tīkla īpašniekam un, ja ir ieslēgts Bluetooth, visiem rajona iedzīvotājiem, kam arī ir ieslēgts Bluetooth.

Ieejot kafejnīcā, restorānā vai lidostā, jūs nestāstiet visiem kā jūs sauc, tāpēc to nevajadzētu darīt arī jūsu telefonam.

Jūs varat nomainīt sava tālruņa nosaukumu uz kaut ko mazāk personisku, tomēr joprojām unikālu. Lūk, kā to var izdarīt:



iPhone:
Mainīt telefona nosaukumu:
Iestatījumi → Vispārīgi →
Par → Mainīt nosaukumu

Android:
Mainīt Wi-Fi nosaukumu:
Iestatījumi →
Wi-Fi → Izvēlne →
Papildu/citas funkcijas →
Wi-Fi pārvaldīšana →
Mainīt ierīces nosaukumu
Mainīt Bluetooth nosaukumu:
Iestatījumi → Bluetooth →
Ieslēgt Bluetooth
ja tas ir izslēgts → Izvēlne →
Mainīt ierīces nosaukumu →
Izslēgt Bluetooth

2.

NOTĪRI SAVAS ATRAŠANĀS VIETAS PĒDAS

Lai gan var šķist, ka jūsu atrašanās vietas dati ir tikai nejauši informācijas fragmenti, tie, kad ir redzami visi kopā, var atklāt svarīgas detaļas par jums un jūsu paradumiem, piemēram, kur jūs dzīvojat, kur strādājat un kur jums patīk pavadīt laiku kopā ar draugiem. Tieši tāpēc šī informācija ir ārkārtīgi svarīga daudziem uzņēmumiem un datu brokeriem.

Jūs varat izskatīt katras lietotnes atļaujas un izslēgt atrašanās vietas noteikšanas pakalpojumu. Pārbaudiet lietotnes, kurām šis pakalpojums patiesībā nav nepieciešams (vai tiešām tai spēlei ir jāzina, kur jūs atrodaties?), un tām, kurām negribat izpaust šo informāciju, iestatiet:

Android:
Iestatījumi → Lietotnes →
Pārvaldīt piekļuve atrašanās vietai katrā lietotnē

iPhone:
Iestatījumi → Konfidencialitāte → Atrašanās vietas pakalpojumi → Pārvaldīt piekļuvi atrašanās vietai katrā lietotnē

3.

SAKĀRTO SAVAS LIETOTNES

Jūsu sabiedrisko mediju lietotnes, spēles un laika ziņu lietotnes interesējas par jūsu datiem, un tās, iespējams, savāc diezgan daudz ziņu par jums.

Atbrīvošanās no nejaušajām lietotnēm tālrunī, kuras jūs nekad neizmantojat, var būt efektīvs veids, kā attīrīt savu digitālo "es".

Turklāt lietotņu sakārtošana var atbrīvot vietu tālrunī, samazināt datu izmantošanu un palielināt akumulatora darbības laiku.

Android:
Iestatījumi → Lietotnes →
Izvēlieties lietotni, kuru jūs gribat atinstalēt → Atinstalēt

iPhone:
Spiediet uz vienas lietotnes, līdz tās visas sāk šūpoties un katras lietotnes augšējā kreisajā stūrī parādās mazs krustiņš.

Lai izdzēstu lietotni, pieskarieties tās mazajam krustiņam.

Lai atgrieztos normālā režīmā, nospiediet sākuma pogu.

4.

AIZSARGĀ SAVAS VIRTUĀLĀS VĒRTSLIETAS

Tāpat kā jūs rūpējaties par vērtīgajām mantām savās mājās, to vajadzētu darīt arī ar informāciju, kuru jūs glabājat virtuāli – neatkarīgi no tā, vai tie ir jūsu finanšu pārskati, pases skenējumi vai pat jūsu adrese vai tālruņa numurs, ir vērts padomāt par to, kur jūs glabājat **vērtīgākos personas datus** un kā jūs varat tos pasargāt.

Atsevišķu **datu dzēšana** ir lielisks vieds, kā veikt dažus ātrus uzlabojumus pie kafijas tases. Meklējiet konkrētu informāciju, kas atrodas jūsu e-pastā vai citos kontos, un izdzēsiet to: jūsu ID skenējumus, bankas datus vai veselības apdrošināšanas informāciju – un tie ir tikai daži no sensitīvo datu veidiem. Ja jums tie būs nepieciešami vēlāk, jūs vienmēr varat tos lejupielādēt vai izdrukāt, pirms izdzēšat no sava e-pasta konta.

Ģeneraltīrīšana ir rūpīgāks darbs, un to ir vēlams veikt reizi gadā. Arhivējiet visu, kas atrodas jūsu e-pastā vai sociālo tīklu kontā, lejupielādējiet to datorā un izdzēsiet konta saturu, lai sāktu visu no jauna.

Padoms: Ar izdēšanu vien nepietiek – iztukšojiet arī miskasti un dzēsiet pagaidu failus!

Tas, vai arhivētos dokumentus vēlaties dublēt mākonī vai saglabāt ārējā cietajā diskā vai USB spraudnī, ir jūsu ziņā. Neatkarīgi no tā, kā jūs tos saglabājat, pārliecinieties, ka jūs tos nezaudēsit, tiem ir stipra parole, un tie jums ir lietderīgi.

Autors

TACTICAL TECH

5.

PASTĀSTI CITIEM

Lai gan to var viegli aizmirst, tīmekli sauc par "tīmekli" zināmu iemeslu dēļ. Mēs visi esam savienoti tiešsaistē, izmantojot dažādus tīklus, ne tikai kā "draugi" sociālajos tīklos, bet arī izmantojot kontaktpersonas mūsu e-pasta kontos un fotogrāfijas, ko kopīgojam tiešsaistē. Kad jūs aizsargājat savus kontus, izvēlieties spēcīgas paroles un iztīriet datus, ieguvējs esat ne tikai jūs – pateicoties jums, visi, ar kuriem esat izveidojis savienojumu, iegūst nedaudz vairāk drošības.

Tīrot e-pasta un sociālo tīklu kontus, apsveriet, ko vēl jūs varat lejupielādēt un dzēst, lai potenciāli palīdzētu draugiem vai kolēģiem: māsas bankas rekvizīti, biroja durvju kods vai dēla pases skenējums ir tikai daži no ierakstiem, kas varētu radīt galvassāpes, ja tie nonāktu nepareizās rokās.

Pastāstiet citiem! Palielināt digitālo drošību ir pavisam vienkārši, un to var izdarīt, veicot vien dažas pamatdarbības. Pastāstiet par šo datu detoksikācijas iespēju draugiem, ģimenei vai kolēģiem, lai palīdzētu viņiem apzināti mainīt savus paradumus.

DATA DETOX KIT

MAINI IESTATĪJUMUS,

lai pasargātu savus datus

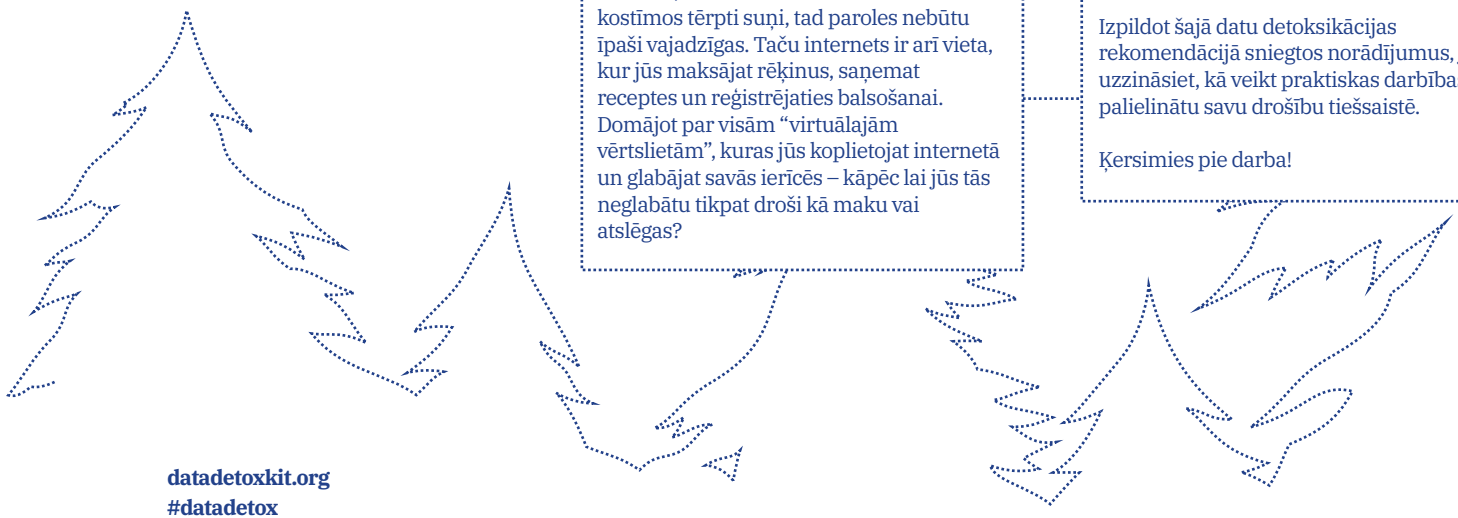
Ja internets būtu tikai vieta, kur dalīties ar attēliem, kuros ir redzami dinozauru kostīmos tērpti suņi, tad paroles nebūtu īpaši vajadzīgas. Taču internets ir arī vieta, kur jūs maksājat rēķinus, saņemat receptes un reģistrējaties balsošanai. Domājot par visām "virtuālajām vērtslietām", kuras jūs koplietojat internetā un glabājat savās ierīcēs – kāpēc lai jūs tās neglabātu tikpat droši kā maku vai atslēgas?

Ir viens vienkāršs veids, kā citiem apgrūtināt piekļuvi jūsu virtuālajām vērtslietām: nepadariet viņiem jūsu paroļu atminēšanu pārāk vieglu. Lielākajai daļai cilvēku nav nepieciešamas specializētas tehniskās iemaņas, lai iekļūtu jūsu kontos – viņi to var izdarīt, izmēģinot vien dažas jūsu paroļu iespējamās versijas vai iedarbinot automatizētu programmu.

Un, kad viņi ir iekļuvuši vienā kontā, viņi šo kompromitēto paroli var izmēģināt citos kontos, apkopot informāciju par jums un jūsu paradumiem, pārņemt jūsu kontus vai pat izmantot jūsu digitālo identitāti.

Izpildot šajā datu detoksikācijas rekomendācijā sniegtos norādījumus, jūs uzzināsiet, kā veikt praktiskas darbības, lai palielinātu savu drošību tiešsaistē.

Ķersimies pie darba!



datadetoxkit.org
#datadetox

1.

AIZSLĒDZ SAVAS DIGITĀLĀS DURVIS

Ekrāna slēdzenes: parole, zīmējums, pirksta nospiedums vai sejas ID, ko izmantojat, lai piekļūtu ierīcei, ir daži no labākajiem aizsardzības līdzekļiem, lai novērstu nevēlamu piekļuvi jūsu ierīcei. Bet to var darīt daudzos un dažādos veidos, un varētu būt grūti saprast, kurš no tiem ir piemērots tieši jums.

Nobloķēts tālrunis, planšetdators vai dators nodrošina lielāku aizsardzību nekā nekāda aizsardzība. Tāpat kā ir pieejamas dažāda veida slēdzenes durvīm, arī dažas ekrāna slēdzenes ir izturīgākas par citām.

No visām pieejamajām slēdzenēm visstiprākās ir garas, unikālas paroles. Tas nozīmē, ka, atbloķējot ierīci ar paroli, tajā jābūt **burtiem, ciparim un speciālajām rakstzīmēm.**

Pieņemsim, ka tālruņa atvēršanai izmantojat vienkāršu pirksta kustību. Iestatot garu paroli, jūs varat lēnām uzlabot savu drošību. Vai arī jūs šobrīd izmantojat zīmējuma slēdzeni? Varbūt jums vajadzētu izveidot šo zīmējumu garāku? Vai jūs kā savu PIN kodu izmantojat 1234? Kā būtu, ja tā vietā jūs septiņas reizes uzmestu kauliņus un iegaumētu šādi izveidoto PIN? **Nelielas izmaiņas var ievērojami palīdzēt saglabāt kontroli pār ierīcēm.**

2.

IELAID IEKŠĀ ĪSTO

Augsta drošības līmeņa paroļu izveidošana ir vienkārša. Atliek tikai ievērot dažus pamatprincipus. Jūsu parolēm vajadzētu būt:

Garām: **parolēm ir jābūt veidotām no vismaz astoņām rakstzīmēm. Kas būtu vēl labāk? 16–20 zīmes.**

Unikālai: **katrai parolei, ko izmantojat – katrai vietnei – ir jābūt atšķirīgai.**

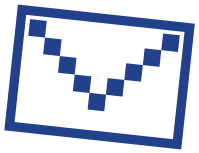
Nejaušai: **parolei nevajadzētu sekot loģiskam modelim vai būt viegli uzminamai. Šeit ļoti noder paroļu pārvaldnieki.**

Spēcīgākajās parolēs tiek izmantota burtu, ciparu un speciālo simbolu kombinācija. Šis gadu gaitā sevi pierādījušais padoms joprojām mudina izveidot stiprāku, grūtāk uzminamu paroli. Dažas paroļu sistēmas diemžēl neļauj izmantot īpašus simbolus (piemēram, @ # $% - = +), taču pietiekami gara burtu un ciparu kombinācija joprojām ir labāka par īsu.

Ideālā gadījumā, lai ģenerētu un saglabātu visas paroles, izmantojiet **īpašu paroļu pārvaldnieku**. Paroļu pārvaldnieks, piemēram, 1Password un KeePassXC, ko bieži iesaka drošības speciālisti, būtībā ir lietotne, kuras vienīgais mērķis ir aizsargāt jūsu autorizēšanās un citus sensitīvus datus.

3.

PIEVIENO OTRU ATSLĒGU



Divfaktoru autentifikācijas (2FA) vai daudzfaktoru autentifikācijas (MFA) iestatīšana nozīmē, ka pat tad, ja kāds atrod jūsu paroli, viņam, iespējams, nebūs papildu faktora, kas nepieciešams, lai iekļūtu iekšā.

Izpētiet jūsu visbiežāk izmantoto vietņu un lietotņu drošības iestatījumus, lai noskaidrotu, vai varat **iestatīt šo papildu atslēgu**. Sāciet ar vissvarīgākajām – jebkurām finanšu lietotnēm vai pakalpojumiem, piemēram, e-pastu, ko izmantojat, lai atgūtu citus jūsu kontus.

Google:
Pierakstieties:
myaccount.google.com →
Drošība → 2 soļu verifikācija →
Sākt

Facebook:
Izvēlne →
Iestatījumi →
Drošība un pieteikšanās →
Izmantot divu faktoru utentifikāciju

Padoms: Uzstādot nākamo verifikācijas slāni, kā apstiprinātāju izvēlieties sevi. Centieties neizmantot īsziņas (ziņas, kas tiek nosūtītas uz jūsu tālruņa numuru) kā otro faktoru gadījumam, ja pazaudēsit tālruni. E-pasts parasti ir drošāka izvēle.

4.

LIEC SEVI SADZIRDĒT

Ja neesat apmierināts ar atkarību veidojošu vai lēmumu ietekmējošu dizainu vai dezinformāciju tīmekļa vietnēs vai biežāk lietotajās programmās, varat nosūtīt e-pasta ziņojumus, rakstīt tvītus un informēt uzņēmumus, ka nepiekrītat viņu praksei. Ja uzņēmumus spiež rīkoties to vērtīgākais aktīvs – lietotāji – pastāv iespēja, ka tie varētu mainīties.

Ja jums šķiet, ka jūsu atsauksmes netiek uzklausītas, ir viens patiešām ietekmīgs veids, kā rīkoties: izmantojiet citu tīmekļa vietni vai lietotni. Ja esat paziņojis, ka neesat apmierināts ar kaut ko, ko dara tīmekļa vietne vai lietotne, un pēc tam faktiski pārstājat to lietot vai atinstalējat, un to dara pietiekami daudz cilvēku, **tas tiks pamanīts.**

5.

RUNĀ PAR UZZINĀTO

Pastāstiet citiem! Šo padomu ir viegli aizmirst, taču tas var būt ļoti efektīvs. Pastāstiet draugiem, ģimenei un kolēģiem par to, ko jūs pamanāt, kā arī palūdziet, lai viņi pievienojas jums šajā detoksikācijas akcijā! Katram ir grūtības ar saviem telefona lietošanas paradumiem. Svarīgi ir atrast sev un dzīvesveidam piemērotu telefona lietošanas veidu. Eksperimentējiet, līdz atrodat pareizāko pieeju, pēc tam atjauniniet savus paradumus, atbilstoši tam, kā laika gaitā mainās jūsu vajadzības. Nav tāda risinājuma, kas būtu vienādi labs visiem.

Un, visbeidzot, dariet apkārtējiem zināmu savu izvēli tehnoloģiju jomā. Pieņemsim, ka Messenger lietotnē pēc plkst. 20.00 jūs ikdienā nebūsiet sasniedzams, jo tieši tad sāksiet savu dienas daļu bez ekrāna: pastāstiet ģimenei un draugiem, lai rakstīšanas vietā viņi varētu jums piezvanīt. Uzturiet dialogu atvērtu, uzdodiet jautājumus un dzīvojiet līdzsvarotu tiešsaistes dzīvi, kas ir piemērota tieši jums.

DATA DETOX KIT

IZVAIRIES NO NOKLUSĒJUMIEM,

lai uzlabotu savu digitālo labklājību

Kad jūs pēdējo reizi "atslēdzāties" un nepieskārāties tehnoloģijām visas dienas garumā, pat ne uz stundu? Ja jūs visu laiku esat tiešsaistē, jūs neesat viens. Kā pārliecināties, ka ierīcē pavadītais laiks ir kvalitatīvs laiks?

Tas sākas ar apzināšanos, ka neatvairāmā tieksme pēc savas ierīces nav jūsu vaina! Ticiet vai nē, bet jūsu iecienītākās lietotnes un tīmekļa vietnes ir izstrādātas tā, lai ikviena iezīme, krāsa un skaņa būtu "optimizēta", lai uzķertu jūs uz āķa un liktu jums pirkt un atgriezties.

Vai vēlaties atrast veselīgāku līdzsvaru starp dzīvi tiešsaistē un dzīvi bezsaistē? Tieši tam ir veltīta šī datu detoksikācijas akcijas daļa.

Ķersimies pie darba!

Autors

TACTICAL TECH

datadetoxkit.org
#datadetox

1.

ESI KLĀTESOŠS

Sekot šim padomam ir grūtāk nekā šķiet. Prasme būt "šeit un tagad" ir jāpraktizē katru dienu. Tā ir kā muskulis smadzenēs, kas regulāri jātrenē, lai padarītu to spēcīgāku. Varat sākt ar to, ka piefiksējat savas attiecības ar tehnoloģijām, kuras lietojat.

Cik daudz laika jūs pavadāt pie tālruņa?

Ja neesat apmierināts ar atbildi, ir iestatījumi un stratēģijas, kurām varat sekot, lai iegūtu kontroli pār to, kā jūs izmantojat tehnoloģijas.

Ja jūsu mērķis ir veltīt mazāk laika Facebook, Instagram vai Snapchat, mainiet šo lietotņu iestatījumus un atļaujas, lai tās darbotos jūsu interesēs.

Dažām lietotnēm, piemēram, Instagram, pat ir opcija, ar kuras palīdzību lietotne saudzīgi atgādina, kad esat sasniedzis savu dienas laika limitu.

Instagram:
Profils → Izvēlne → Iestatījumi → Konts → Jūsu aktivitāte → Iestatīt ikdienas atgādinājumu

Ja konstatējat, ka tālrunis ar zvaniem, dūkoņu vai ekrāna izgaismošanos traucē jūsu sarunām reālajā dzīvē, varat to uz laiku apklusināt, nolikt ar ekrānu uz leju vai pat ielikt kabatā vai somā, lai tas būtu ārpus jūsu redzesloka.

2.

PAMANI DIZAINA TRIKUS

Ietekmējošais dizains, pazīstams arī kā "maldinošie modeļi", ir cilvēka psiholoģijā balstīts dizains, kas tiek izmantots, lai provocētu jūs kaut kur pierakstīties, kaut ko iegādāties vai sniegt vairāk personiskās informācijas, nekā bijāt domājis vai plānojis.

Izplatītākie dizaina uzvedinātāji var būt noteiktu krāsu izmantošana, pogu izvietojums, neskaidri teksti vai nepilnīga informācija. Reizēm šie triki ir acīmredzami, bet citreiz tos ir grūtāk pamanīt. Iespējams, dažus no tiem jūs jau esat pamanījis, reģistrējoties abonementam vai iepērkoties tiešsaistē. Iemesls, kāpēc visur redzat šos dizaina trikus, ir tas, ka tie darbojas – liek mums klikšķināt, abonēt, pirkt biežāk un turpināt atgriezties. Jo vairāk apzināsities smalkās uzvednes un manipulācijas, kas iekļautas jūsu izmantotajās vietnēs, jo zinošāks un informētāks kļūsit.

Ir vairākas iespējas, kā pārspēt lietotnes.

Atpazīstiet mēģinājumus jūs uz kaut ko uzvedināt. Pirmais, ko var darīt, ir vienkārši apzināties, ka šie paņēmieni tiek izmantoti.

Uzņemiet ekrānuzņēmumu un dalieties ar to. Uzņemiet ekrānuzņēmumus jebkurā brīdī, kad tiešsaistē ieraugāt ietekmējošu dizainu, un nosūtiet tos draugiem (noklusējot jebkādas personu identificējošas detaļas – konfidencialitāte pirmajā vietā!). Varat arī aicināt uzņēmumus mainīt savu praksi.

Saglabājiet mieru. Ja pirkuma lapā ir laika atskaites pulkstenis, pajautājiet sev: "Vai tas tiešām ir steidzami?" Ja konstatējat, ka noklikšķināt uz pogas, kad īsti to nemaz negribējāt darīt, padomājiet par formulējumu uz pogas vai pakalpojuma sniedzēja izmantotajām krāsām. Ja jūtaties apjucis, nevainojiet uzreiz sevi – apsveriet tīmekļa vietnes vai lietotnes izmantotos vārdus, jo tie varētu būt neskaidri.

3.

IESI TAUPĪGS, LIETOJOT MEDIJUS

Tāpat kā jūs varat iemācīties atpazīt pazīmes un noformējumus, kas paredzēti, lai jūs turpinātu ritināt un klikšķināt, jūs varat apgūt arī to, kā pamanīt jaunumus vai ziņas, kas domātas, lai jūs maldinātu.

Jūs droši vien jau esat dzirdējis par dezinformācijas un viltus ziņu problēmām. Ar maldinošu informāciju var tikt galā gudri, ja izstrādā ieradumu uzdot kritiskus jautājumus par jebkuru izlasīto ziņu, īpaši, ja tā šķiet pārsteidzoša, ārkārtīga vai pārāk laba, lai būtu patiesa.

Galu galā, kā pārliecināties, vai ziņas ir īstas vai viltotas – īpaši, ja plānojat ar tām dalīties ar ģimeni vai draugiem.

Kas tā ir par vietni?
Kurš to rakstīja (un kad)?
Kas ir teikts visā rakstā, ne tikai virsrakstā?
Uz kādiem avotiem ir dota atsauce?

Ja uzskatāt, ka tā ir maldinoša informācija, un vēlaties apturēt tās izplatīšanos, lielākajai daļai platformu ir vieta, kur var ziņot par publikāciju. Iespējams, jūs arī apdomāsiet, vai turpināt sekot kontam, kas publicēja šo ziņu.

5.

MEKLĒ PATIESĪBU INTERNETĀ

Termins “viltus ziņas” tiek lietots, lai apzīmētu visdažādāko neprecīzu vai maldinošu informāciju, tostarp satīru, slikti izpētītu vai nepārbaudītu saturu, mānīšanos un blēdības. Viltus ziņas ne vienmēr izplatās ļaunprātīgi, bet neatkarīgi no to kopīgošanas iemesla rezultāts kopumā ir viens un tas pats: saņēmēji uzskata, ka patiesībā kaut kas nav kārtībā vai ka ir noticis kaut kas tāds, kas patiesībā nav noticis. Labākajā gadījumā tā varētu būt smieklīga mēme. Sliktākajā gadījumā tā var būt neprecīza informācija par veselību vai nepatiesa politiskā informācija.

Pat pēc pamatīgas izpētes un izlasīto rakstu kritiskas iztirzāšanas jūs tomēr varat justies apjucis. Taču atcerieties – jūs šajā situācijā neesat viens!

6.

IZKĀP NO SAVA FILTRA BURBUĻA

Kad tīmekļa vietnes un lietotnes būs izveidojušas jūsu interešu profilu, iespējams, nonāksiet filtra burbulī. Šajā gadījumā pakalpojumi piedāvā vairāk stāstu, kas ir līdzīgi tiem, uz kuriem jau klikšķināt. Kā tas ierobežo vai maina to, ko jūs uzzināt?

Atrašanās filtra burbulī var likt cilvēkiem redzēt pilnīgi atšķirīgus stāstus, ziņu virsrakstus, rakstus un reklāmas, kā to demonstrē interaktīvais raksts “Zilās ziņas, sarkanās ziņas” (graphics.wsj.com/blue-feed-red-feed).

Ja jūs zināt, ka visās lietotnēs un tīmekļa vietnēs skatāt algoritmiski ierobežotu tieši jums paredzētu saturu, jautājums ir šāds: kā tikt ārā no filtra burbuļa?

DATA DETOX KIT

6 PADOMI, KĀ IZVAIRĪTIES NO MALDINOŠAS INFORMĀCIJAS TIEŠSAISTĒ

Bez malā stāvētājiem
Tikai tas, ka tīmekļa vietnes savas kļūdas neatzīst, nenozīmē, ka tās šīs kļūdas nepieļauj. Visuzticamākās publikācijas ir tās, kas pievērš īpašu uzmanību patiesumam un nodarbina cilvēkus vai veselas nodaļas, kuru vienīgais uzdevums ir faktu pārbaude.

Meklējiet avotus, kas veic labojumus, ja ir kļūdījušies. Vēl labāk ir tad, ja atjauninājumi ir apkopoti pašā raksta sākumā un tiek kopīgoti sociālajos tīklos, tā aiztaupot lasītājam to meklēšanu.

Maini debespuses un miksē saņemtās ziņas
Labs veids, kā izlauzties no filtra burbuļa, ir abonēt pakalpojumus, kas apkopo ziņas un informāciju no dažādiem avotiem un ar daudzveidīgu perspektīvu kopumu. RSS plūsmas, forumi un adresātu saraksti, kas izmanto plašu viedokļu un tēmu klāstu, var palīdzēt palūkoties ārpus jūsu burbuļa. Global Voices (globalvoices.org) un The Syllabus (the-syllabus.com) ir lieliskas vietnes, ar ko sākt.

Lietotnes, tīmekļa vietnes un tiešsaistes mediji var būt pamats ziņu, padomu un izklaides piekļuvei. Bet visā daudzveidīgajā saturā var būt grūti izvairīties no neskaitāmajiem uzmanības novērsējiem, kamēr cenšaties atrast to, ko patiesībā meklējat.

Turklāt, uzejot video, attēlu vai rakstu tiešsaistē, var būt grūti noteikt atšķirību starp faktu un fikciju.

Sākot ar personības noteikšanas testiem, kas cenšas izveidot jūsu profilu, un beidzot ar šokējošiem virsrakstiem un izmainītiem fotoattēliem vai video, var pārliecināt jūs par pavisam citu realitāti – tas, ko redzat tiešsaistē, ne vienmēr ir tas, pēc tā tas izskatās.

Šajā datu detoksikācijas akcijā jūs izpētīsiet ar maldinošu informāciju saistītas tēmas un liekvārdus, skatot tuvplānā savu atbildību, pakāpeniski saskatot lielāku kopainu un vienlaikus saņemot padomus par ceļu šajā informācijas pasaulē.

Aiziet!

datadetoxkit.org **#datadetox**

Autors
TACTICAL TECH

Projekta partneri
Save the Children 100 ANNI
IFLA

Finansē Eiropas Savienība

Tulkojums
GOETHE INSTITUT

1.

APZINIES, KA SPĒJ RADĪT PĀRMAIŅAS

Tīkšķi, dalīšanās, ziņu pārsūtīšana un pārpublicēšana – tas viss raksturo to, kā jūs mijiedarbojaties ar tiešsaistē redzamo, un jūsu mijiedarbībai ir liela nozīme. Kad uz attēlu, video vai ziņu reaģē pietiekami daudz cilvēku, tā strauji izplatās, kļūst "virāla".

Šis ir īstais brīdis, lai pajautāju sev: "Kāda ir mana ietekme tiešsaistē?" Kad jūs pēdējo reizi redzējāt šokējošu vai jocīgu rakstu, virsrakstu, video vai attēlu un dažu sekunžu laikā to jau nosūtījāt draugiem? Pētnieki ir noskaidrojuši, ka vislielākā iespēja kļūt "virāliem" ir stāstiem un attēliem, kas rada bailes, riebumu, bijību, dusmas vai satraukumu. Ja tieši to jūs izdarījāt vēl šorīt, nejūtieties slikti!

Dalīšanās – tās ir rūpes
Dalīšanās ir līdzdalības veids. Daloties ar kaut ko (jebko), jūs ietekmējat tā iespēju kļūt "virālam". Ja izrādīsies, ka tas, piemēram, ir viltojums, vai tiešām vēlaties, lai tas saistītos ar jūsu vārdu un reputāciju? Pirms kopīgojat saiti, apsveriet, vai neizplatāt kaut ko nepatiesu, destruktīvu vai toksisku.

2.

PADOMĀ DIVREIZ, PIRMS VEIC ŠO PERSONĪBAS TESTU

Kad pēdējo reizi redzējāt testu (teksta vai foto filtros) ar šādu vai līdzīgu nosaukumu:

- Kāds ir tavs patiesais vecums?
- Kas ir tavs totēma dzīvnieks?
- Kāds ir tavs ideālais atvaļinājums?
- ... saraksts ir bezgalīgs!

Lai gan pastāv iespēja, ka šis bija jautrs tests, lai piesaistītu jūsu uzmanību, ir arī pilnīgi iespējams, ka jautājumi tika rūpīgi izstrādāti, lai apkopotu datus par jūsu atbilstību tā sauktajiem psihometriskajiem modeļiem.

Jūsu atbildes uz testa jautājumiem, piemēram, "Kurš Simpsonu tēls jūs esat?", kopā ar citiem jūsu ieradumiem, kurus varētu pārraudzīt jūsu pārlūkprogramma, lietotne vai savienotie vienumi, piemēram, lojalitātes kartes, datu analītiķiem var sniegt priekšstatu par to, kāds cilvēks jūs esat, kas jūs interesē un kā jūs pamudināt uz jauna apavu pāra iegādi (piemēram)... jeb izveidot jūsu profilu, lai saprastu, kā jūs ietekmēt, lai panāktu noteiktu jūsu balsojumu nākamajās vēlēšanās.

Pēc iespējas vairāk paturi noslēpumā
Domājot par privātu informāciju, pirmās lietas, kas ienāk prātā, varētu būt jūsu paroles, personas kods un bankas konta numurs. Taču tikpat personiska ir arī informācija par to, kas jūs biedē vai kaitina un kādas ir jūsu ambīcijas. Šīs ziņas var būt vērtīgas datu analītiķiem, ļaujot saprast, kas varētu uzrunāt jūs kā personību. Padomājiet divreiz, pirms sniedzat šāda veida informāciju aptaujā vai testā.

3.

NEUZĶERIES UZ ĒSMAS

Klikšķu ēsma ir termins, ko lieto, lai aprakstītu sensacionālus, negodīgus vai izdomātus virsrakstus, kurus izmanto ar nolūku provocēt cilvēkus noklikšķināt uz virsraksta vai saites. Jo vairāk uzmanības saņem raksts, video vai attēls, jo vairāk naudas tas, visticamāk, nopelnīs. Tas nozīmē, ka veidotāji ir motivēti teikt visu nepieciešamo, lai jūs noklikšķinātu uz viņu satura vai dalītos ar to.

Pamatojoties uz personības profilu, ko par jums izveidojušas jūsu izmantotās platformas (piemēram, Facebook un Instagram), jūs varat saņemt pielāgotus virsrakstus, kas emocionāli mudinās jūs klikšķināt.

Klikšķu ēsma var būt blakus maldinošai informācijai, bet ne vienmēr. Kad sāksiet atpazīt klikšķu ēsmas virsrakstus, jūs tos pamanīsit visur – platformās, blogos un tabloīdos.

Atrodi avotu
Uzdrošties klikšķu ēsmai, neapstājieties pie virsraksta. Ja tā izskatās pēc drošas saites, noklikšķiniet uz raksta un noskaidrojiet, kas ir raksta autors, kad tas tika publicēts un uz kādiem avotiem tas atsaucas. Iespējams, ka rakstā ir piezīme, ka tas ir maksas saturs vai reklāma, vai varbūt tas ir kategorizēts kā viedokļa raksts. Šie sīkumi var palīdzēt izlemt, vai tas ir jūsu laika un enerģijas vērts.

4.

UZMANIES NO VILTOJUMIEM

Dziļie viltojumi ir video, audioklipi vai attēli, kas ir digitāli pārveidoti, parasti, lai aizstātu kāda seju vai kustības vai mainītu kāda teikto. Lai gan "dziļie viltojumi" ir salīdzinoši jauns termins, tie patiesībā tādā vai citādā formā ir pastāvējuši jau gadiem ilgi. Vēl vieglāk ir radīt tā dēvētos **lētos viltojumus** – maldinošu saturu, ko bez izsmalcinātas tehnoloģijas var radīt ar nepareizu virsrakstu fotogrāfijai vai videosižetam, vai ar novecojušu saturu ilustrējot aktuālu notikumu.

Var šķist neiespējami pilnībā apkarot viltojumus, bet vienu jūs varat darīt vienmēr – palieciet nesatricināms.

Paliec nesatricināms un veic izpēti
Tāpat kā ar klikšķu ēsmu, neko nepieņemiet kā pašsaprotamu. Ja redzētais video vai foto šķiet pārsteidzošs vai satriecošs, atpazīstiet šo sajūtu un rēķinieties, ka tur varētu būt kas vairāk, nekā izskatās. Savukārt, ja pamanāt, ka jūsu plūsmā parādās viens un tas pats attēls vai tas ir kopīgots ar jums jau vairākas reizes, atpazīstiet to kā iemeslu sameklēt īsto avotu.

Tieši tad jūs gribēsies uzdot vēl citus jautājumus: kurš to publicēja (kura mājaslapa, kurš bija autors)? Kad tas tika publicēts? Ja tas ir attēls, veiciet reverso attēla meklēšanu vietnē TinEye (tineye.com) un pārbaudiet, kur vēl to atrodat.

Pirms pieņemat kaut ko kā patiesu un kopīgojat to ar draugiem un ģimeni, pārbaudiet citus uzticamus ziņu avotus.