

Vitālijs Rakstiņš
**DIGITĀLĀ
DETOKSIKĀCIJA**



**DIARIES OF THE
INFORMATION WAR**



VITALIJS RAKSTINS



Saīsinātā versija

**PRETOŠANĀS
ROKASGRĀMATA**

Gatavība apdraudējuma situācijām hibrīda kara laikā digitālajā un informatīvajā vidē

Vitālijs Rakstiņš



Neviens viedais produkts nevar būt 100% drošs.

Visiem (!) viedajiem produktiem ir ievainojamības, par kurām mēs vēl nezinām (slēptās ievainojamības).

Produkti nevar būt droši vienreiz un uz visiem laikiem: laicīga drošības atjauninājumu izvietošana ir galvenais, lai uzlabotu produktu digitālo drošību.



Kā varu aizsargāt savu telefonu?



Telefons, planšete un lietotnes, ko izmanto, ir aprīkotas ar aizsardzību. Tā ir kā mūris, kas neielaiž vīrusus. Laiku pa laikam tiek atklāti “caurumi” aizsardzības mūros. Tos var novērst ar atjauninājumiem (update). Katrs no tiem ir kā papildus ķieģelis mūra stiprināšanai, tādēļ nekavējies tos instalēt.

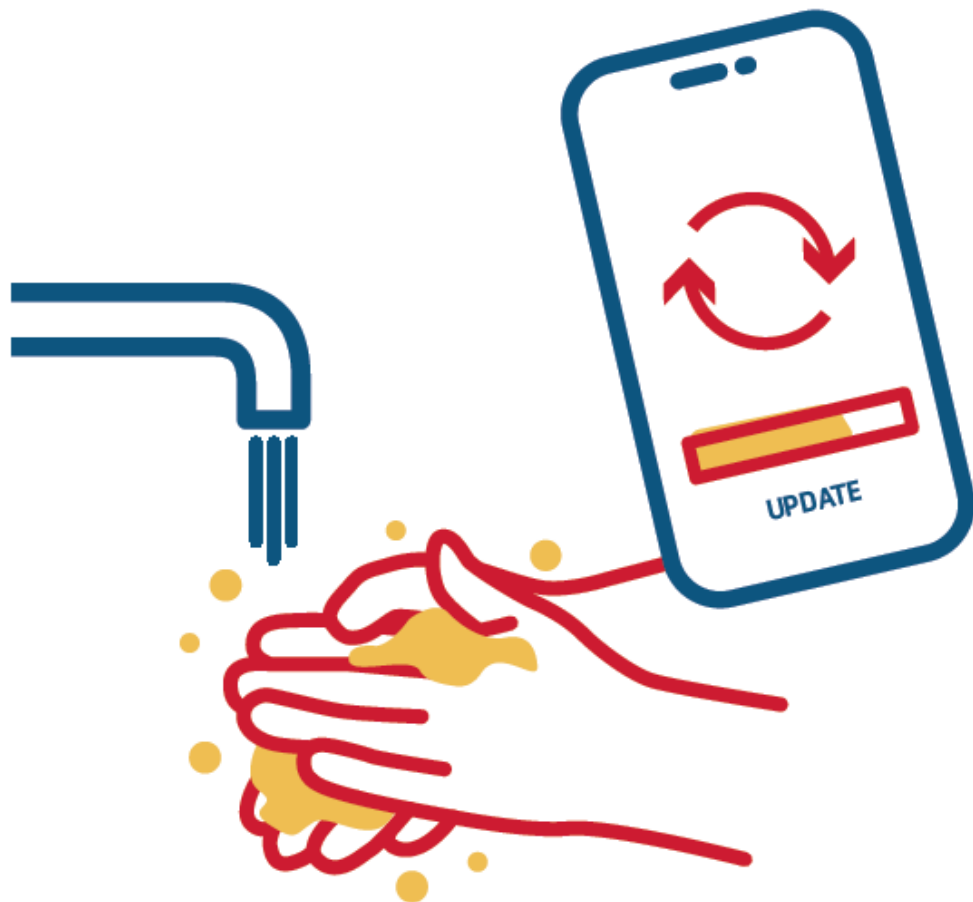




Cik bieži jāatjauno programmas?



Telefona drošība ir ikdienas uzdevums. Līdzīgi kā mazgājam rokas vai tīrām zobus, arī par digitālo higiēnu ir jādomā ik dienu. Viena kļūda un esi briesmās!



Kā varu zināt, vai mans telefons ir pasargāts?



Pavaicā pieaugušajiem, vai Tavā telefonā ir jaunākās un drošākās programmu versijas.





DRAUDU VEKTORI UN POTENCIĀLĀS IEVAINOJAMĪBAS VAR TIKT ATTIECINĀMAS PRET DAŽĀDĀM VIENĪBĀM, KĀ:

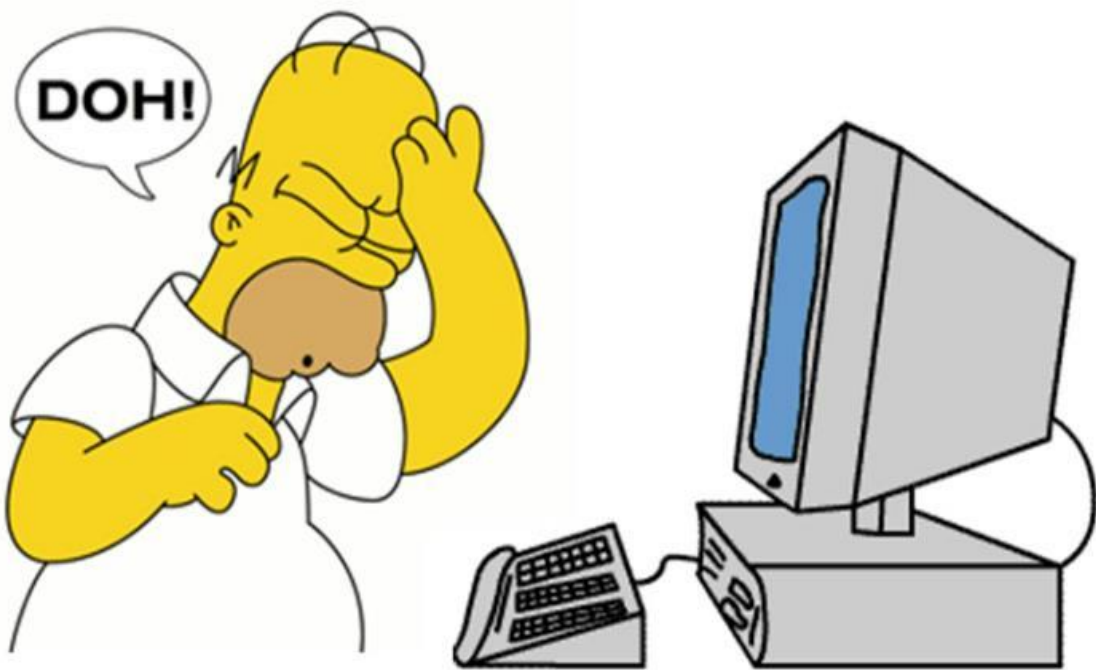
- Galapunkts: datori, planšetdatori, mobilie tālruņi, viedās ierīces utt.
- Savienojamība: internets, Wi-Fi, Bluetooth utt.
- Tīkla ierīce: maršrutētāji, Wi-Fi piekļuves punkti.
- Lietojumprogramma: dators un mobilā ierīce.
- Paroles: vienkāršība un atkārtota izmantošana.
- Komunikācija: ikdienas sociālie tīkli, ziņojumapmaiņa, e-pasti.
- Fiziskā drošība: piekļuve galapunktiem, ierīcēm, tīklam utt.

Kiberdrošības riskus **var pārvaldīt un samazināt** līdz pieņemamam risku līmenim!



KĀ PAMATS LABAI KIBERHIGIĒNAI IR IEVĒROT ŠOS PRIEKŠNOTEIKUMUS:

- Pārziniet savus digitālos aktīvus.
- Regulāri atjauniniet savu programmatūru – iekārtas, sistēmas un aplikācijas.
- Aizsargājiet savu galapunktu savienojumus ar internetu.
- Izmantojiet stipras paroles un iespējojiet MFA (daudzpakāpju verifikāciju), kur tas ir iespējams.
- Pārdomātā veidā kopīgojiet jebkādu informāciju.
- Komunicējiet drošā veidā.



Biežākie veiksmīgu uzbrukumu cēloņi bija:

- atteikšanās no drošības par labu ērtībai, izvēloties vienkāršas paroles vai arī vienu paroli vairākiem resursiem;
- nezināšanas dēļ vai ērtības labad resursu papildu aizsardzībai netika izmantota divu faktoru autentifikācija, kas būtu pasargājusi no konta pārņemšanas, pat ja uzbrucējs būtu ieguvis paroli;
- apstākļi, kuri paaugstina kļūdīšanās iespējamību - steiga, nogurums, neparasta situācija, procedūru neesamība vai to nepārzināšana, mazs ekrāns - mazināja analītisku pieeju situācijai un palielināja iespējamību, ka uzbrukums netiks atpazīts.



Kā tas var notikt?



Never vaļā datnes, kas izskatās aizdomīgi, jo nevar zināt, kas tur ir iekšā.

Ja saņem ziņu no nepazīstama telefona numura vai e-pasta, nespied uz tajā iekļauto saiti.

Nekad nelieto nezināmas lietotnes, kas nav no Google Play vai Apple Store veikala.



Nekad nelieto nezināmās lietotnes, kas nav Google Play vai Apple Store veikalā.



- pārbaudām e-pasta sūtītāju un adresātu
- **neatveram šaubīgas saites e-pastā**
- **neatveram šaubīgus e-pasta pielikumus**



Neuzmanības vai kļūdas dēļ vari **pats nejauši ielaist** vīrusus savā telefonā.



Never vaļā datnes, kas izskatās aizdomīgi, jo nevar zināt, kas tur ir iekšā.

Pikšķerēšana



- Pikšķerēšana, jeb tā sauktais fišings (angļu: phishing) ir uzbrukuma veids, kurā mēģina ar viltu iegūt no interneta lietotāja konfidenciālo informāciju, piemēram, lietotāju vārdus, paroles, kredītkaršu numurus.
- Pikšķerēšana ir vispopulārākais uzbrukuma veids pret lietotāju.
- Visizplatītākais veids, kā ielauzties iestādēs un jūsu datoros ir mērķēti "pikšķerēšanas" e-pasti.
- Pikšķerēšanai līdzvērtīga krāpniecība, bet izmantojot rīkus, kā piemēram, telefona zvanus un sms, kuru tehniskais nosaukums ir višings un smišings.



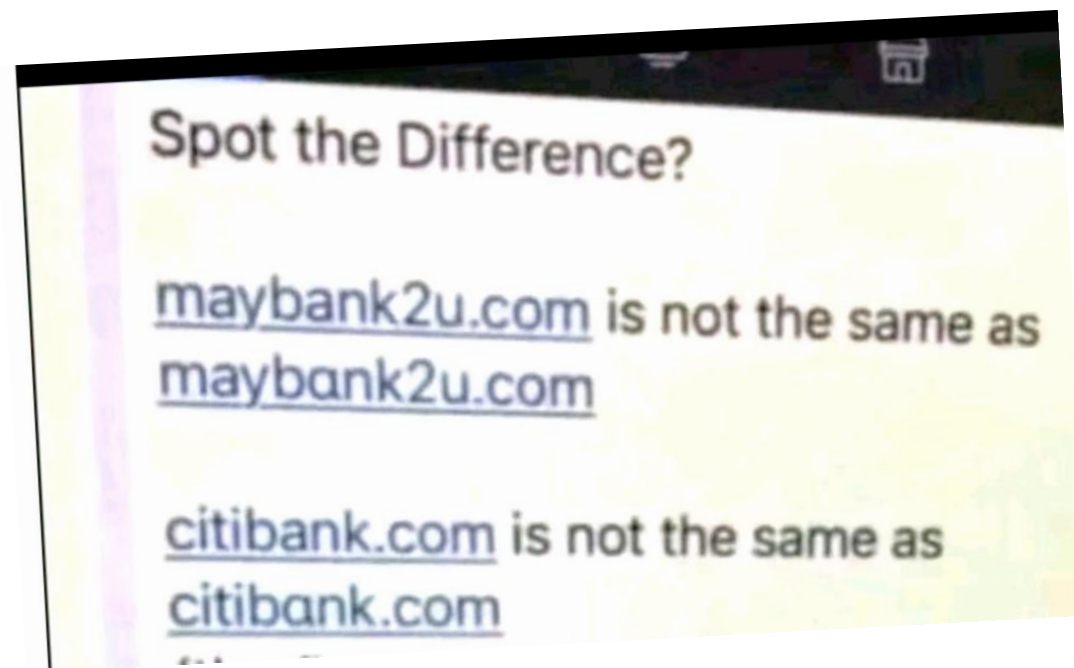
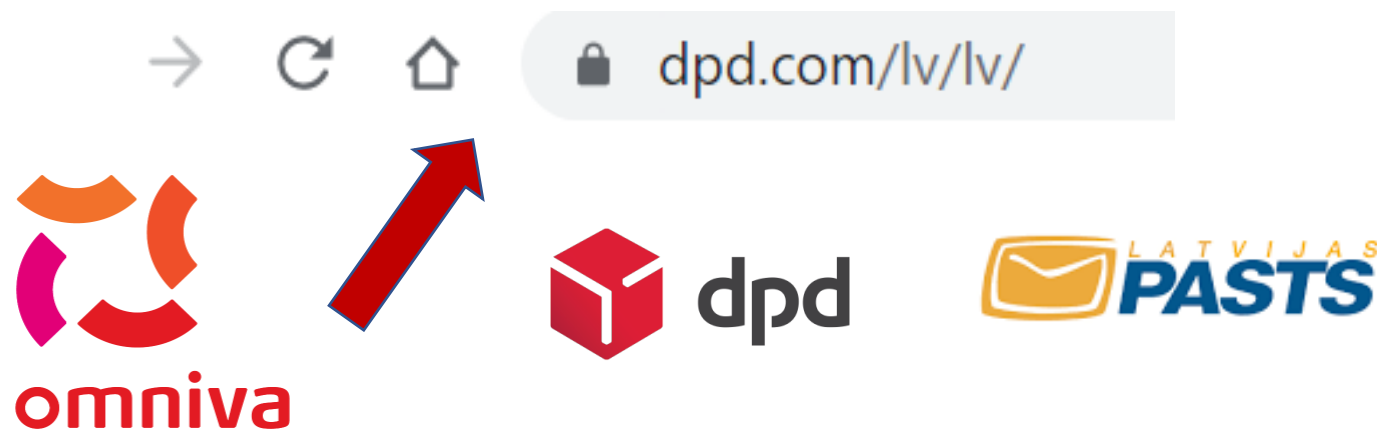
Kā varu zināt, kuras saites ir drošas?



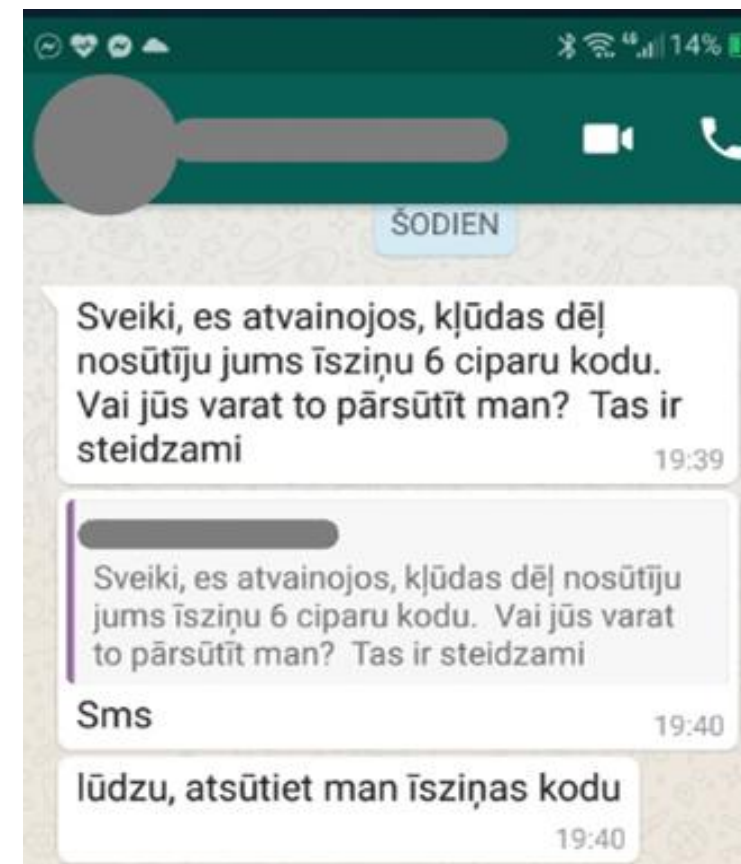
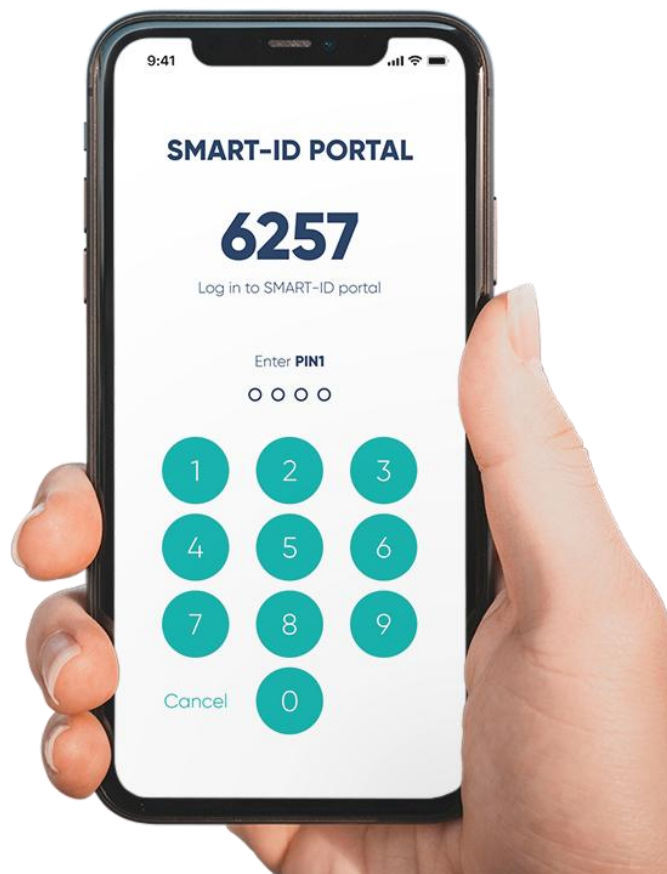
Pievērs uzmanību tīmekļa vietnes adresei (piemēram, e-klasse.lv), jo ļaundari var apmullot Tevi norādot līdzīgu, bet tomēr viltus adresi, kas Tevi aizvedīs uz viltus vietni.



Vizuāli atdarina pazīstamos zīmolus



Darbības (biznesa) procesu nepārzināšana



Paroles

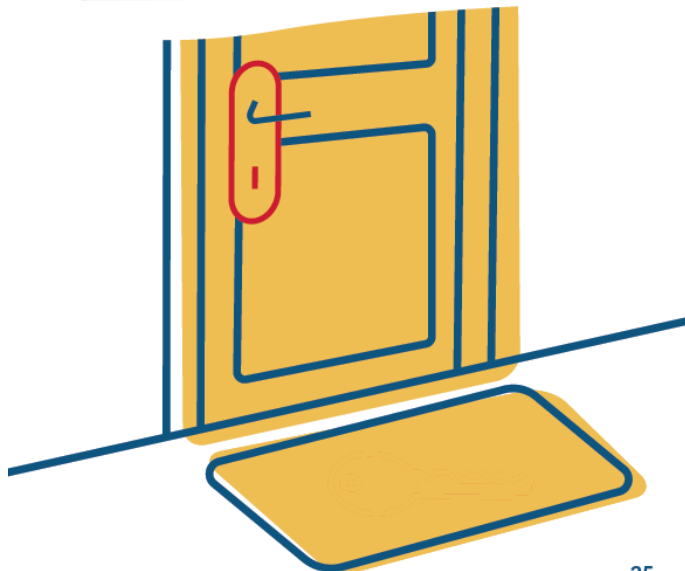
 Un ja nu kāds uzmin manu paroli vai to ierauga?

 Papildus parolei izmanto arī citus rīkus (sejas atpazīšana, saņemtais kods, SMS u.tml.).
Katrs šāds rīks ir kā papildus slēdzene ārdurvīm.



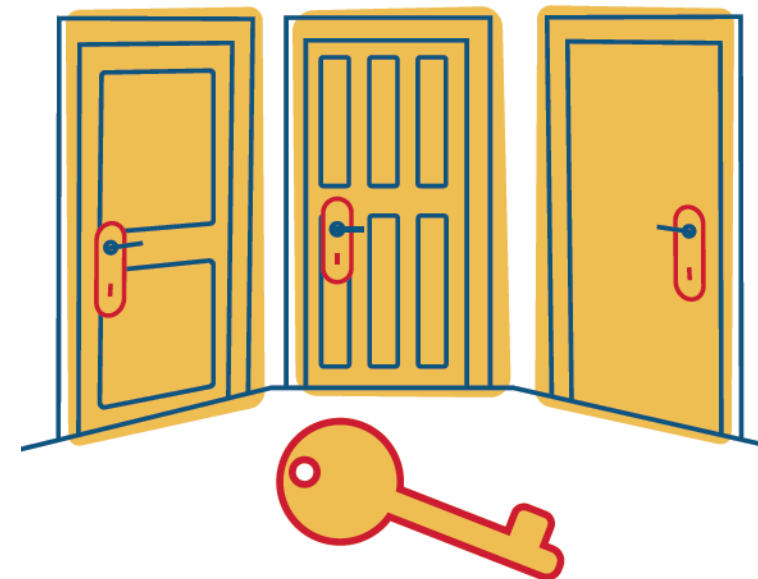
 Kā varu zināt, vai mana parole nav pārāk vienkārša?

 Neizmanto parolē savu vārdu, piemēram, "Toms123".
12345 vai Tavs vārds un dzimšanas dienas datums nav droša parole!
Vienkāršas paroles ir kā durvju atslēgas slēpšana zem paklāja pie durvīm.



 Vai varu izmantot vienu paroli visam?

 Katrā tīmekļa vietnē, portālā, spēlē, lietotnē jāizmanto atšķirīga parole, kas nekur citur neatkārtojas.
Visām durvīm nedrīkst būt viena atslēga!



[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate](#)  

';--have i been pwned?

Check if your email or phone is in a data breach

pwned?

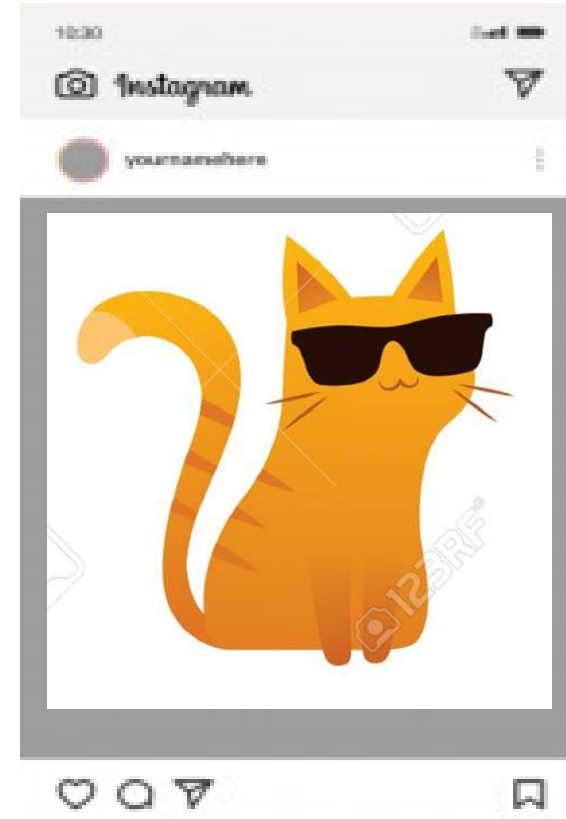
Slepenais jautājums ?



Geni
A MyHeritage Company

Bērziņa (Liepiņa)

**Mātes meitas /
pirmslaulību uzvārds?**



Mājdzīvnieka vārds

Neizmanto publisko Wi-Fi interneta tīklu, jo to var pārvaldīt ļaundaris [!]



Ja iespējams, tad labāk izmanto mobilo internetu no sava mobilo sakaru operatora.



PUBLISKAIS BEZVADU TĪKLS NAV DROŠS, JO TAS RADA AUGSTU RISKU, KA PERSONAS AR SPECIALIZĒTIEM RĪKIEM VAR:

- Pārtvert savienojumus, iegūstot sensitīvus datus kā paroles un bankas datus.
- Iegūt informāciju par to, kādas aplikācijas un/vai saites tiek apmeklētas.
- Attālināti uzstādīt ļaunatūru.
- Izmantot sistēmu nepilnības – konfigurācijas vai ievainojamības.

Neatstāt telefonu bez uzraudzības



Vai kaut kas apdraud manu telefonu, ja neesmu pieslēdzies internetam?



Vīrusi uzbrūk internetā, bet arī klātienē jābūt piesardzīgam! Neatstāj savu telefonu bez uzraudzības (pat nobloķētu ar paroli vai izslēgtu), jo to var “uzlauzt” un piekļūt Taviem datiem!





Kā es uzzināšu, ja mans telefons būs inficēts?



Ja Tavs mobilais telefons vai planšete uzvedas “jocīgi”, iespējams, tas ir “saslimis” jeb inficēts ar datorvīrusiem.



Ja telefons pats atslēdzas, vai tas var būt inficēts?



Jā, tas ir iespējams. Ja telefons “uzkarst” vai darbojas ļoti lēni, tas var būt inficēts.



Pazīmes, ka telefons varētu būt inficēts:

- telefons pats izslēdzas / ieslēdzas
- Ir paradušas lietotnes, ko neesiet instalējis
- Telefons ātri izlādējas
- Telefons ievērojami uzkarst
- Ir palielinājies interneta trafiks (pateriņš)
- Sarunu laikā problēmas ar sakariem / traucējumi.



Internetā es labprāt dalos ar savām bildēm un video! Mani draugi seko līdzīgi maniem piedzīvojumiem!



Ir jauki internetā sazināties ar draugiem, bet pirms ko publicē internetā, izvērtē, vai šis saturs nerada draudus Tev un Tavai ģimenei!



Gribu būt populārs internetā, tāpēc manu sociālo tīklu kontu saturam var sekot ikviens!



Publisks, visiem atvērts un pieejams konts sociālajos tīklos ir kā visiem apskatāmas gleznas muzejā. Pārrunā ar vecākiem, vai tas ir droši un Tev nepieciešams!



Kā pasargāties no svešiniekiem?



Vecāki vai citi pieaugušie var palīdzēt uzstādīt privātuma iestatījumus sociālajos tīklos.

Tad Tavu darbību internetā, Tavas bildes un ziņas neredzēs sveši, ar Tevi nesaistīti cilvēki!





Ko vēl nevaru publicēt?



Es ieteiktu Tev npublicēt:

- ✗ Bilde, kur redzama Tavas ģimenes ikdiena.
- ✗ Tava mājas adrese.
- ✗ Tavi ikdienas pārvietošanās maršruti.
- ✗ Neatzīmē sociālajos tīklos savu atrašanās vietu.

Pārrunā ar vecākiem:

- ✓ Kādas bildes no savas ikdienas gaitām vai mājas Tu drīksti publicēt.
- ✓ Ar kuriem draugiem un kurās lietotnēs vari dalīties ar savu atrašanās vietu.
- ⊘ Nekad neatzīmē sociālajos tīklos savu atrašanās vietu.



Atceries! Tu nedzīvo akvārijā. Tev nav jāizrāda citiem viss, ko dari!



Kas var notikt, ja kāds zina, kur atrodos?



Ja Tu atzīmē, kur atrodies, Tevi var izsekot.

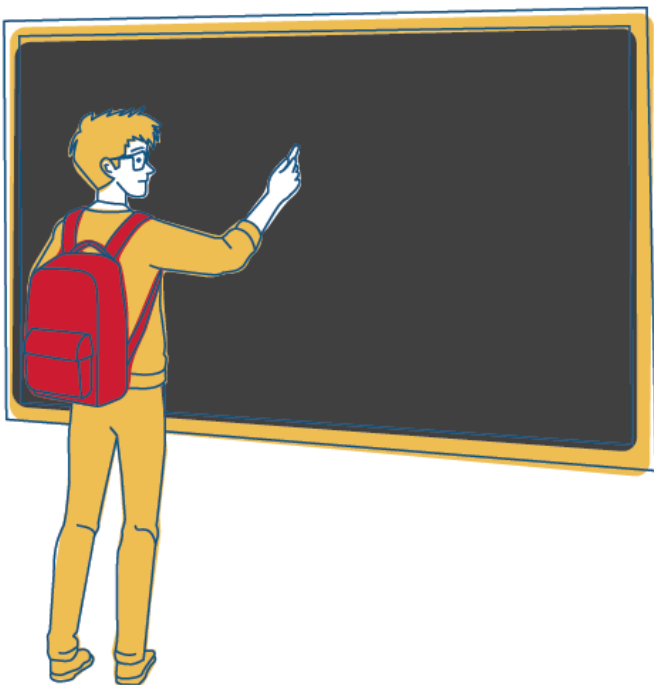
Ja atzīmēsi, ka kopā ar ģimeni esi kaut kur devies, Tu svešiniekus informēsi, ka mājās šobrīd neviena nav.



 Nekad neraksti internetā to, ko pēc tam vari nožēlot.

 Kāpēc?

 Iedomājies, ka raksti komentāru nevis internetā vai mesendžerī, bet klases priekšā uz tāfeles. Vai Tu būtu gatavs uz tāfeles uzrakstīt to pašu tekstu, ko internetā?



 Ja man vairs nepatīk savas bildes, es tās dzēšu no interneta.

 Publicēto internetā nekad nevarēsi izdzēst. Tas paliks uz visiem laikiem.



Publicēto internetā nevarēsi nekad izdzēst.



Tas paliks uz visiem laikiem.

Visu, ko publicēsi internetā
varēs redzēt arī sveši cilvēki!



Tevi var nofotografēt vai
nofilmēt, Tev pat to nezinot



Jebkuru sarunu var ierakstīt
un pēc tam pārsūtīt tālāk vai
publicēt interentā.

Ja kādam sūti savas bildes vai
pārdomas, atceries, ka to var
nofotografēt ar ekrānšāviņu
un pārsūtīt tālāk citiem.



Interneta satura kontroles aizsardzības līmeņi



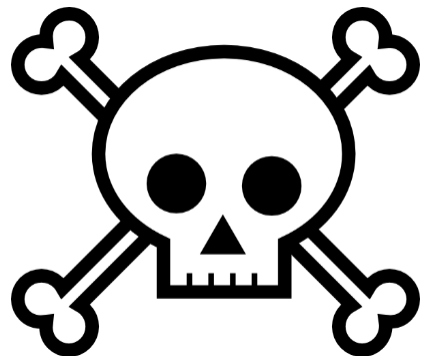
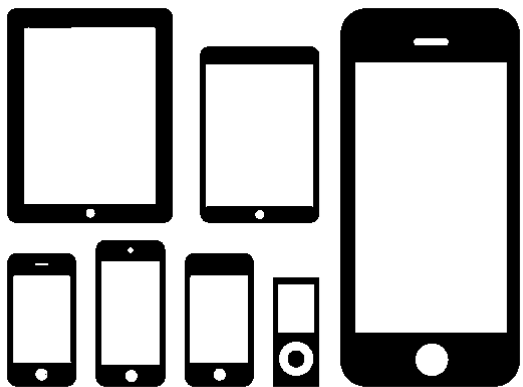
Valstu un BigTech filtri



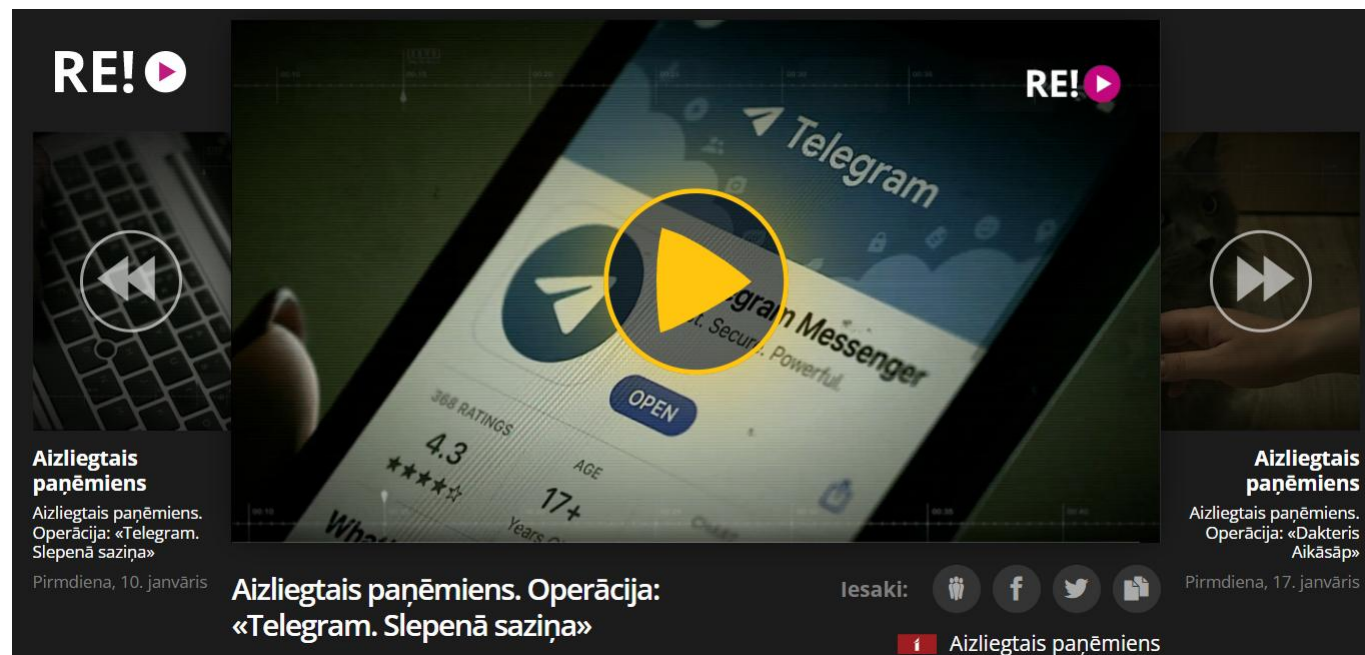
Drošības iestatījumi



Bērniem domātie kanāli / platformas



— Design by All-free-download.com —



Ko tik "Telegram" nevarot nopirkt! Var recepšu medikamentus, var, protams, arī alkoholu nakts laikā dabūt. Var nopirkt koplietošanas auto kontus, proti, ja kādam nav autovadītāja apliecība vai tā ir atņemta, vai vēl par agru, lai pie tās tiktu, tad var dabūt citas un uz citu tiesību vārda pievienot savu konta numuru. Un braukt uz nebēdu.

Sliktas atzīmes

Problēmas ar uzvedību

Konflikti skolā / izolācija

Jauns paziņu loks (ar līdzīgiem mārķeriem)

Jaunās intereses: specifiskā literatūra,
filmas;

Nervozitāte

Neadekvātas emocionālās reakcijas

Fiziskās izmaiņas

Vizuālie un lingvistiskie mārķeri

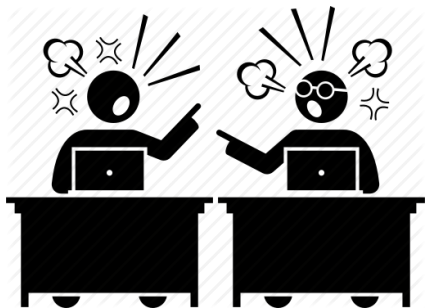
Pīrsings, rētas, tetovējumi u.tml.

Pēkšņa interese par ieročiem, cīņas veidiem

Parādās nauda / prasa ekstra līdzekļus

Destruktīvā uzvedība

Vairs nestrādā ietekmes rīki



Par pretlikumīgām darbībām,
internetā - sods būs **reāls!**



- Par **fizisku vai emocionālu vardarbību pret bērnu** piemēro brīdinājumu vai naudas sodu
- Par **neslavas celšanu** vainīgo personu soda ar piespiedu darbu vai ar naudas sodu
- Par **cieņas un goda aizskaršanu**,
- Par **nelikumīgām darbībām ar fiziskās personas datiem**, ja ar to radīts būtisks kaitējums
- Par **draudiem izdarīt slepkavību vai nodarīt smagu miesas bojājumu**
- Par **vairākkārtēju vai ilgstošu citas personas izsekošanu, novērošanu, draudu izteikšanu šai personai vai nevēlamu saziņu ar šo personu**,
- Par **vardarbīgu materiālu izplatīšanu**
- Par **16 gadu vecumu nenasniegušas personas pamudināšanu iesaistīties seksuālās darbībās** Par rasismu un naida kurināšanu internetā
- Par **autortiesību vai blakustiesību pārkāpšanu**,
- Par patvaļīgu (bez attiecīgas atļaujas vai izmantojot citai personai piešķirtas tiesības) **pieklūšanu automatizētai datu apstrādes sistēmai** vai tās daļai,
- Par Latvijas valsts ģerboņa vai Latvijas valsts karoga noraušanu, saplēšanu, salaušanu, iznīcināšanu vai par citādu šo **valsts simbolu zaimošanu**, kā arī par Latvijas valsts himnas publisku zaimošanu -



Es internetā varu rakstīt anonīmi!



Katra Tava darbība internetā atstāj digitālas pēdas, pēc kurām Tevi var atrast “reālajā” dzīvē.



Viss ko Tu dari internetā ir izsekojams un Tevi varēs atrast “reālajā” dzīvē.



Unikālais
lietotņu un
programmu
saraksts



Biežāk apskatīto /
meklēto tēmu saraksts



Bluetooth signatūra:
ierīces ar kurām Jūs bieži
savienojāties



Purchase History



Meklēšanas signatūra



Ierīces identifikātori



Unikālais draugu loks



Ģeogrāfiskā signatūra:
regulārie maršruti u.tml.

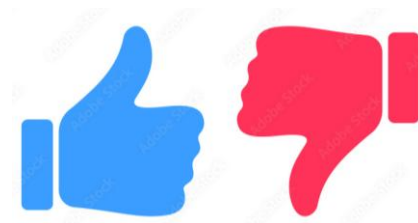
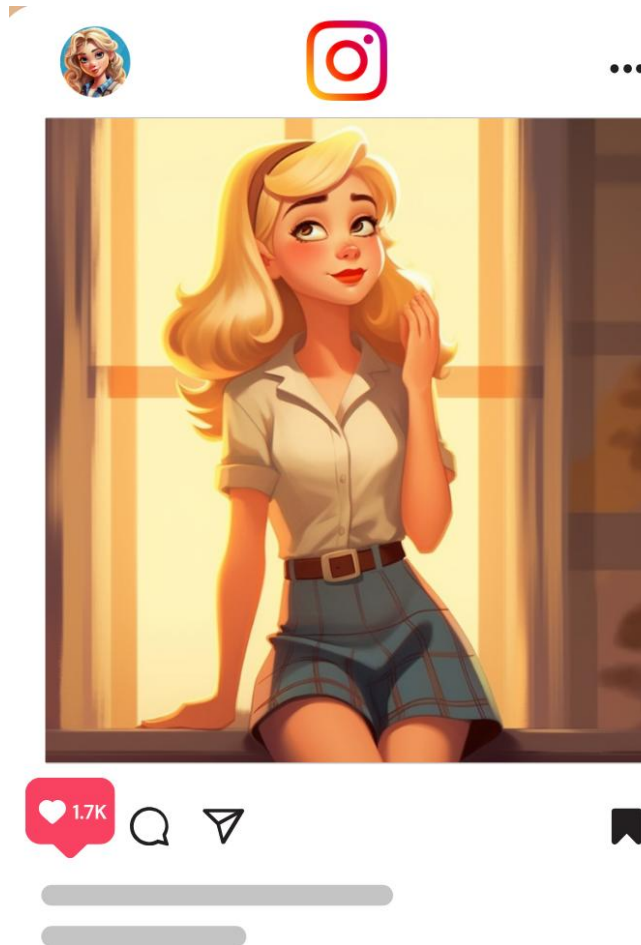


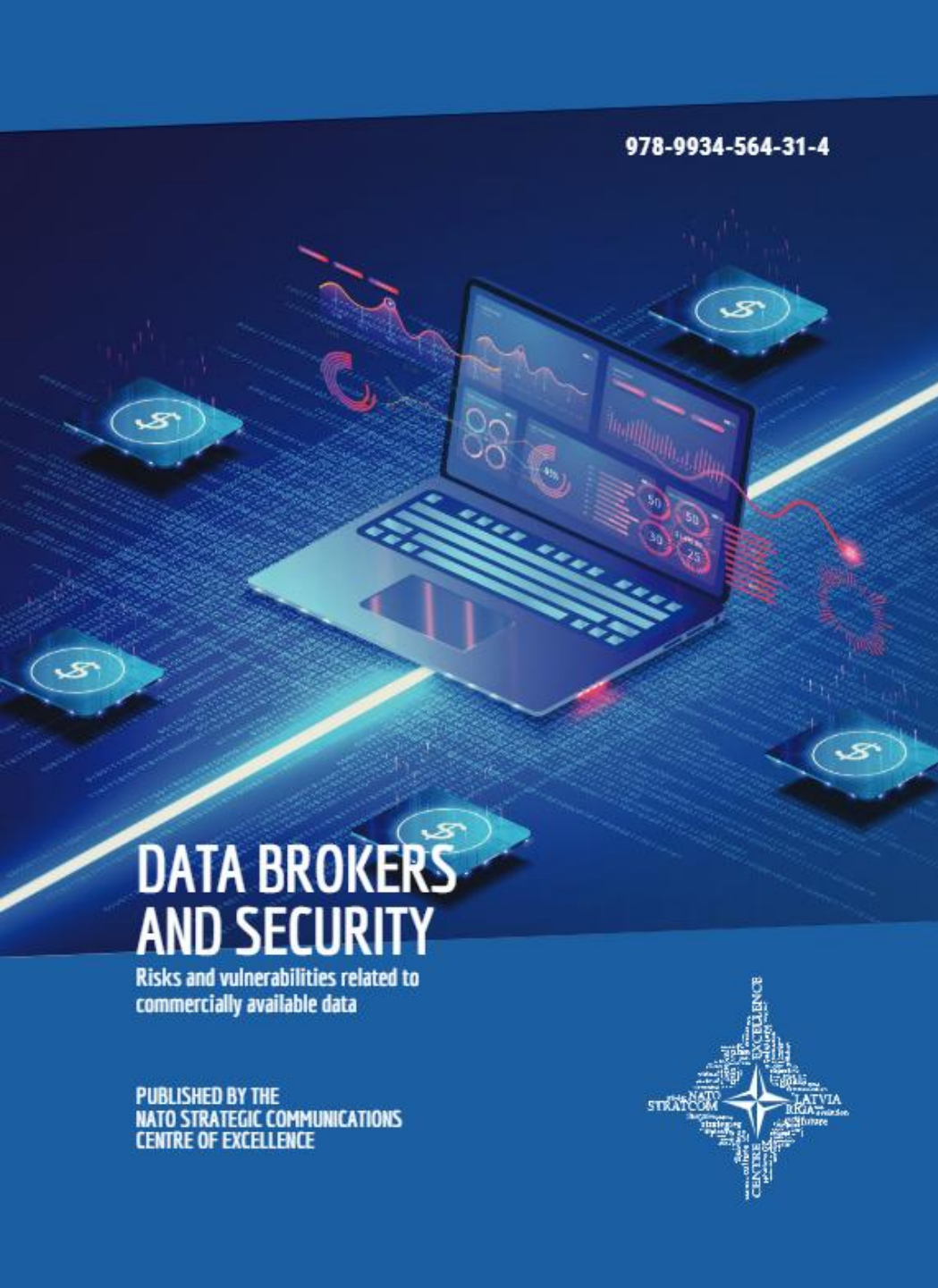
Leksikas signatūra / balss signatūra



Wi-Fi signatūra: Wi fi tīkli
Jums apkārt

Visvairāk interesējošie dati





978-9934-564-31-4

DATA BROKERS AND SECURITY

Risks and vulnerabilities related to
commercially available data

PUBLISHED BY THE
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE



Dzīve bez privātuma. Eksperimentā izdodas nopirkt datus par 100 000 Rīgas un Pierīgas iedzīvotājiem



Klausīties audio formātā ^①

SABIEDRĪBA

2021. gada 23. janvārī 07:40



Edvīns
Rakickis

Jauns.lv

NATO Stratēģiskās komunikācijas izcilības centra ("Stratcom") pētījumā par datu brokeriem jeb kompānijām, kas vāc un tālāk pārdod informāciju par personām, ar eksperimenta palīdzību noskaidrots, ka par salīdzinoši nelielu samaksu var iegūt detalizētu informāciju par Latvijas iedzīvotājiem.

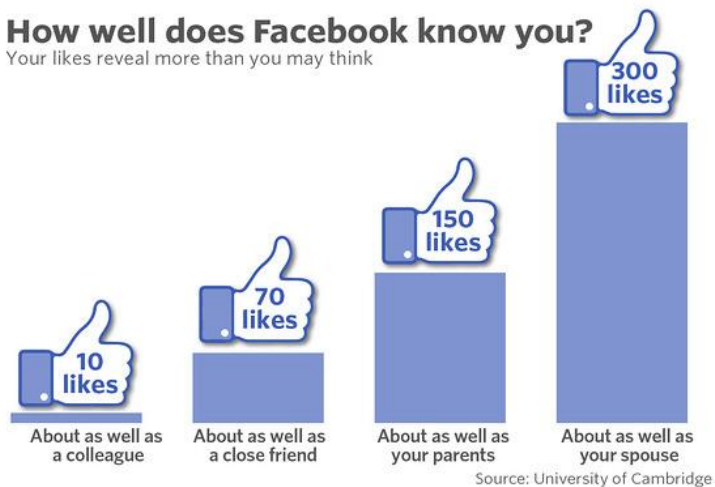
Iegādātā datu analīze pētniekiem deva iespēju tikt pie detalizētas informācijas par mērķauditorijas demogrāfiju (vecums, dzimums, ģimenes stāvoklis utt.) un uzvedību (viedierīču, aplikāciju, interneta banku, dažādu kuponu, lietošanās paradumi, kā arī iepirkšanās, ceļošanas un aktivitāšu piekopšana).

Īsāk sakot – šī informācija ļauj izdarīt secinājumus par to, kur konkrēta mērķauditorija iepērkas, kuros bāros bauda dzērienus, kuras kafejnīcas un izklaides vietas apmeklē.



How well does Facebook know you?

Your likes reveal more than you may think



Fiziskie dati: dzimums, vecums u.tml.

Veselība: ir/ nav brilles, ir/nav lieks svars u.tml.

Apģērbs: jaunas /modernas drēbes; kāds stils, kādas krāsas u.tml.

Cilvēki apkārt: ģimene, bērni, draugi u.tml.

Ienākumi: mašīna, mājas interjers, aksesuāri, ceļojumi u.tml.

Ieradumi: sports; smēķēšanā; alkohols u.tml.

Vietas, kas tiek apmeklētas: teātri, sporta klubi, nakts klubi u.tml.

Semantiskie un politiskie dati: viedokļi, komentāri, kam seko / ko lasa; reliģiskie / ezoteriski uzskati u.tml.

Izglītība: gramatika, vārdu krājums u.tml.

Aktivitāte: cik bieži tiešsaistē, cik aktīvi komentē, kādos laikos

Intereses: māksla, mūzika, literatūra u.tml.

Uzvedība: pieklājība, pozitīvs/negatīvs; lieto lamus vārdus; u.tml.

Ietekmējamība: cik bieži iesaistās strīdos; kā reaģē; cik aktīvs masu akcijās u.tml.

Pirktspēja (scoring)

Delete My Account

If you do not think you will use Facebook again and would like your account deleted, we can take care of this for you. Keep in mind that you will not be able to reactivate your account or retrieve any of the content or information you have added.

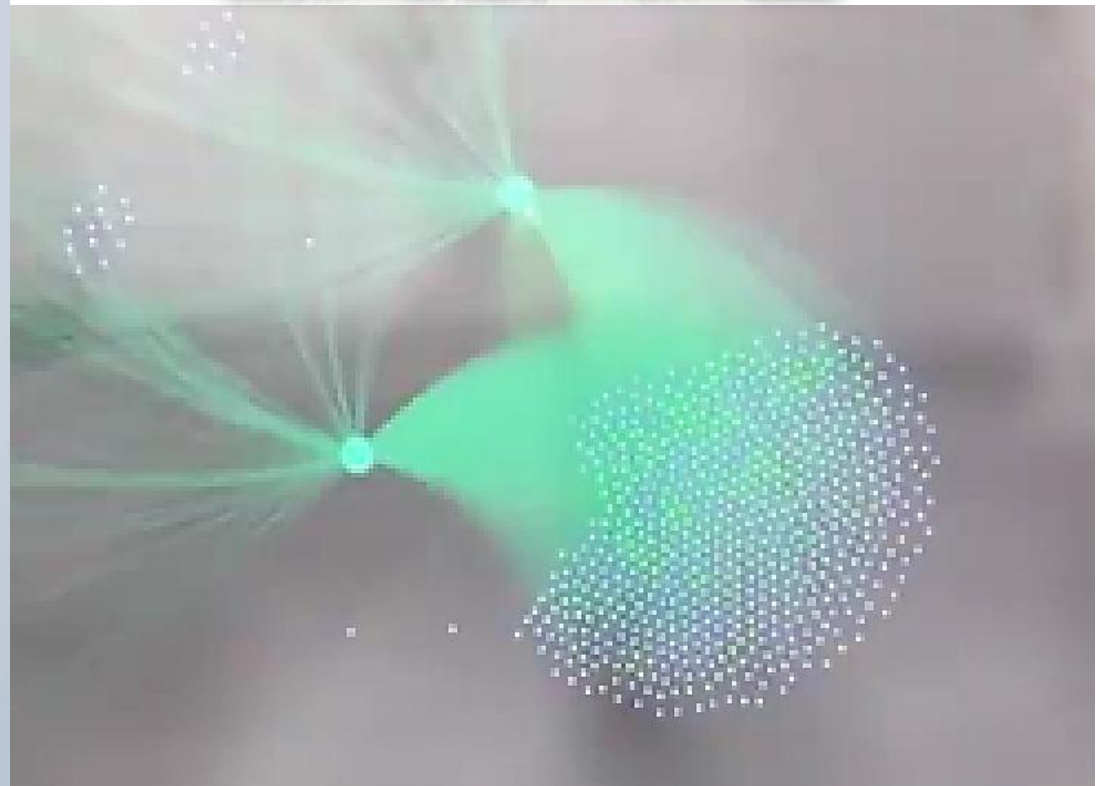
If you would still like your account deleted, click "Delete My Account".

[Learn more about account deletion](#)

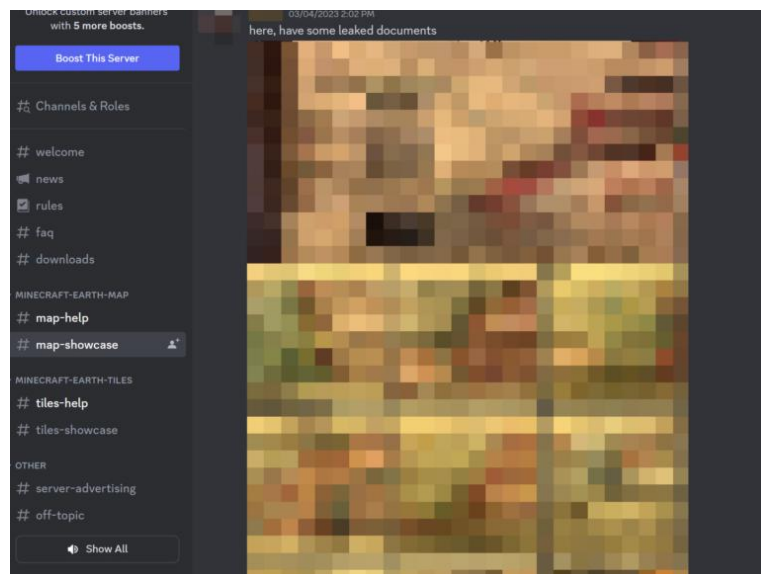
Delete My Account

Cancel





Nekontrolētā vide



Spēļu tīrsetāvas



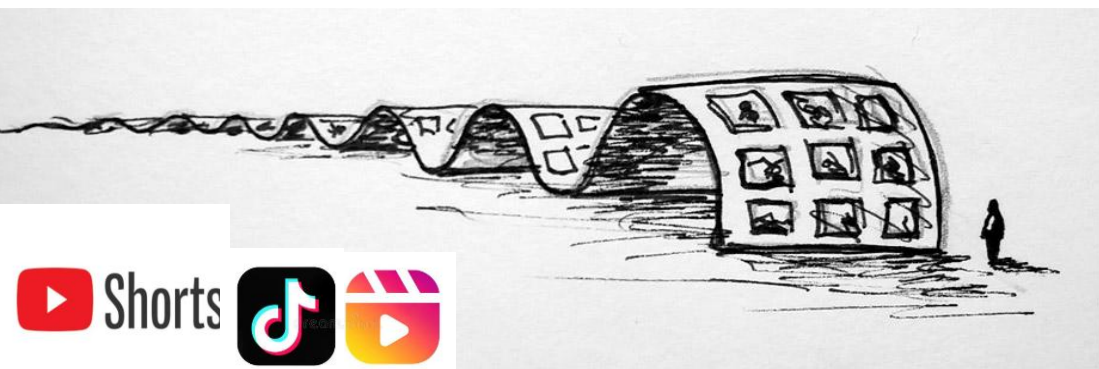
Reklāmas un propaganda



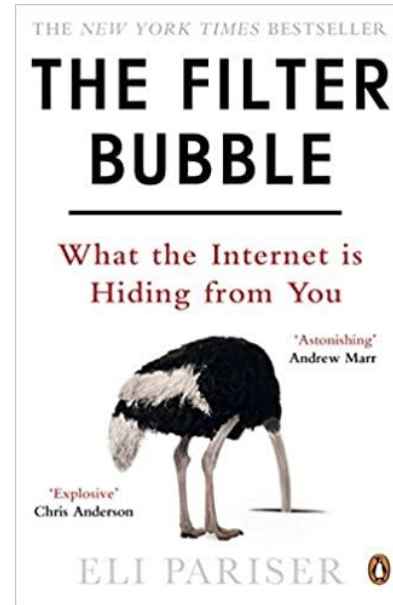
Informācijas patēriņa modelis (media consumption pattern)



Cilvēku vidējais uzmanības ilgums samazinās



Informācijas patēriņa modelis (media consumption pattern)



YouTube, the Great Radicalizer



By Zeynep Tufekci

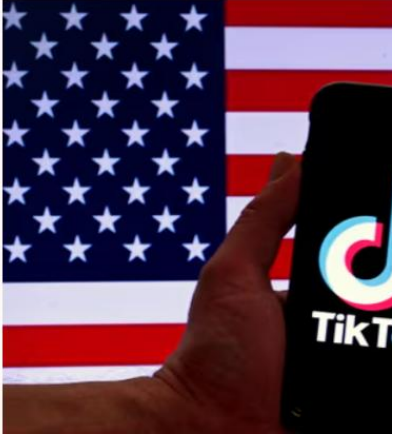
March 10, 2018



TikTok is part of China's cognitive warfare campaign

Nita Farahany

Militaries are racing to develop weapons that can directly assault or disable human minds in the context of our peril



TikTok shows less 'anti-China' content than other rival networks: Study

TikTok has faced intense scrutiny from US concerned about the Chinese government's influence



NBC NEWS

TikTok says it's not spreading Chinese propaganda. The U.S. says there's a real risk. What's the truth?

Ken Dilanian

Updated Mon, September 16, 2024 at 8:31 PM GMT+3 · 8 min read

US TikTok users who search for terms like “Tiananmen,” “Tibet,” and “Uyghur” — words commonly used in Chinese Communist Party propaganda — see less “anti-China” content than those same searches produce on Instagram and YouTube.



Publiskie forumi

Slēgtas grupas

Grupas,
klani



Delfi

ARKĒMES

RUS



20.02.2023 13:47:09

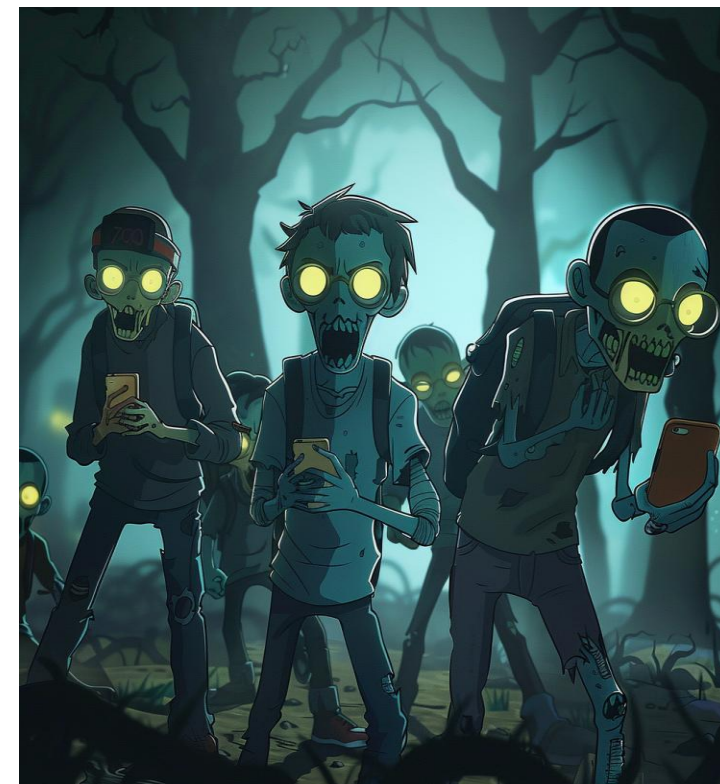
Upurus meklē videospēļu platformās: "Eiropols" brīdina par kultu draudiem jauniešiem

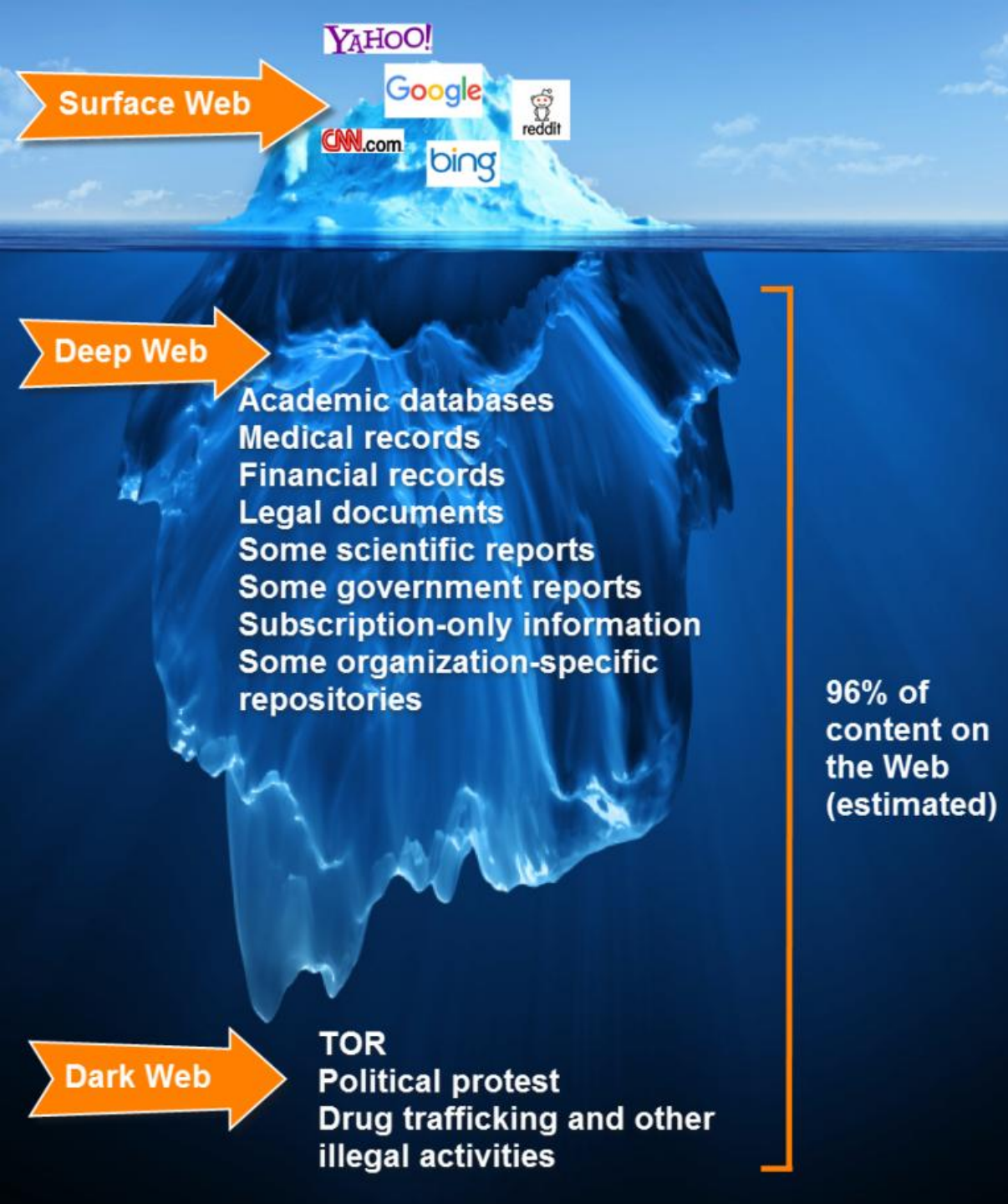
LETA



Foto: Shutterstock

Eiropas Savienības (ES) policijas aģentūra "Eiropols" ceturtdien izdevusi brīdinājumu par vardarbīgiem noziedzīgiem grupējumiem, kas internetā vervē nepilngadīgos, lai pamudinātu viņus pastrādāt vardarbības un terora aktus.





Depresija
(par neīsto dzīvi, IG)



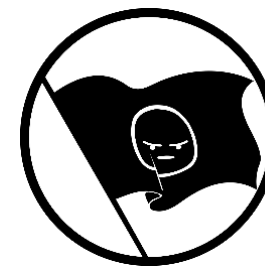
Bullying (iebiedēšana, apsmiešana, šantāža)



Suicidālās grupas



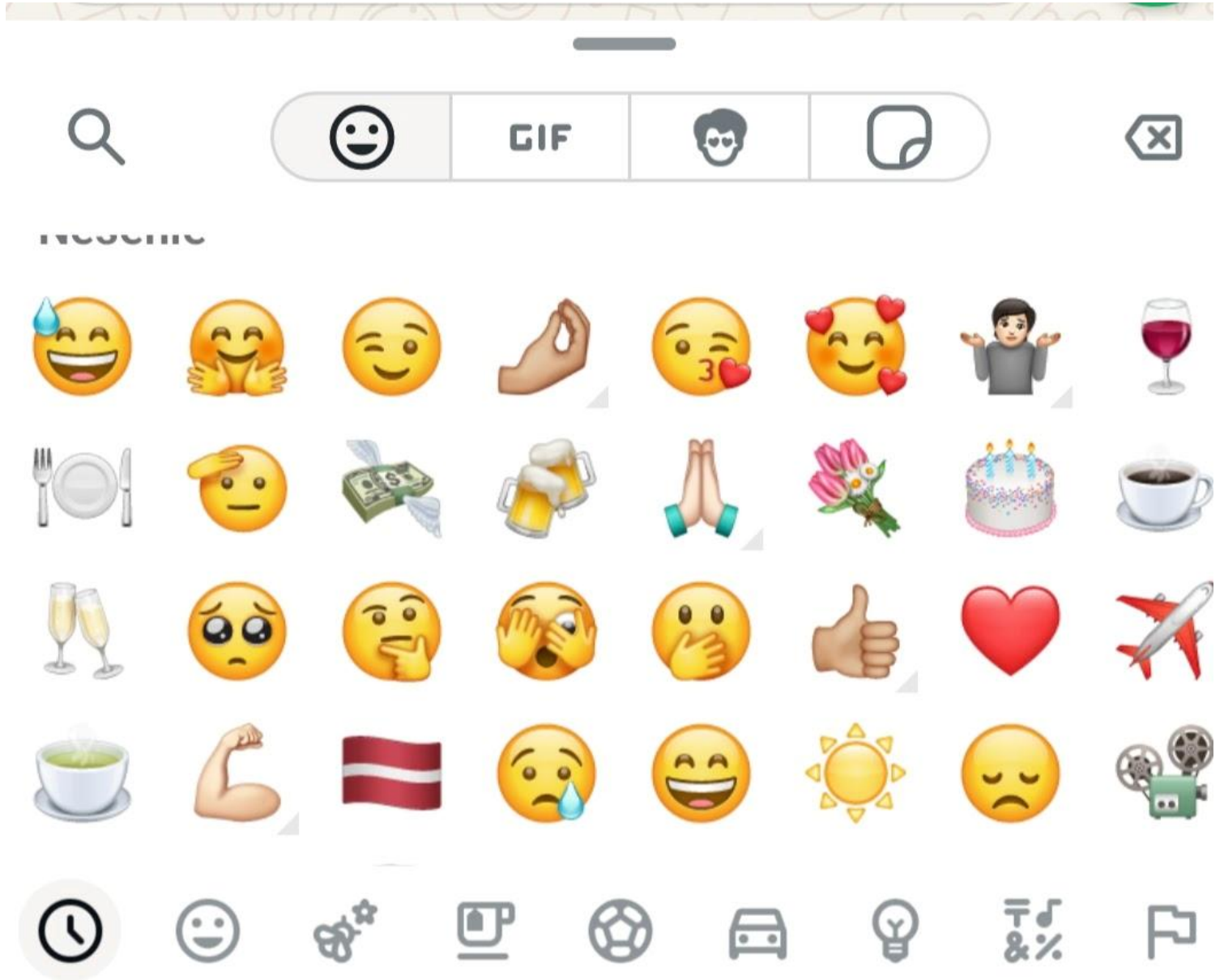
Bīstamas spēles



Radikalizācija



Delikventais dzīves stils.



Self-harm:

	Razor – self-harming by cutting
	Scissors – self-harming by cutting
	Sword – self-harming by cutting
	Blood drop – hurting or bleeding
	Fire – burning self
	Crying face – feeling depressed and sad
	Black heart – feeling emotionless or sad
	Cloud with rain – feeling down

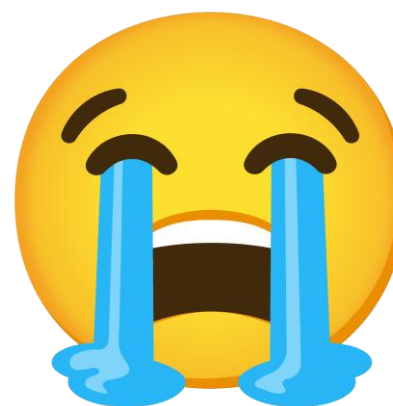
   
expressing violence

   
feeling trapped, sad,
and cutting to cope

   
feeling down, emotionally
hurting, wanting to die

This emoji could mean your suicide risk is high, according to AI

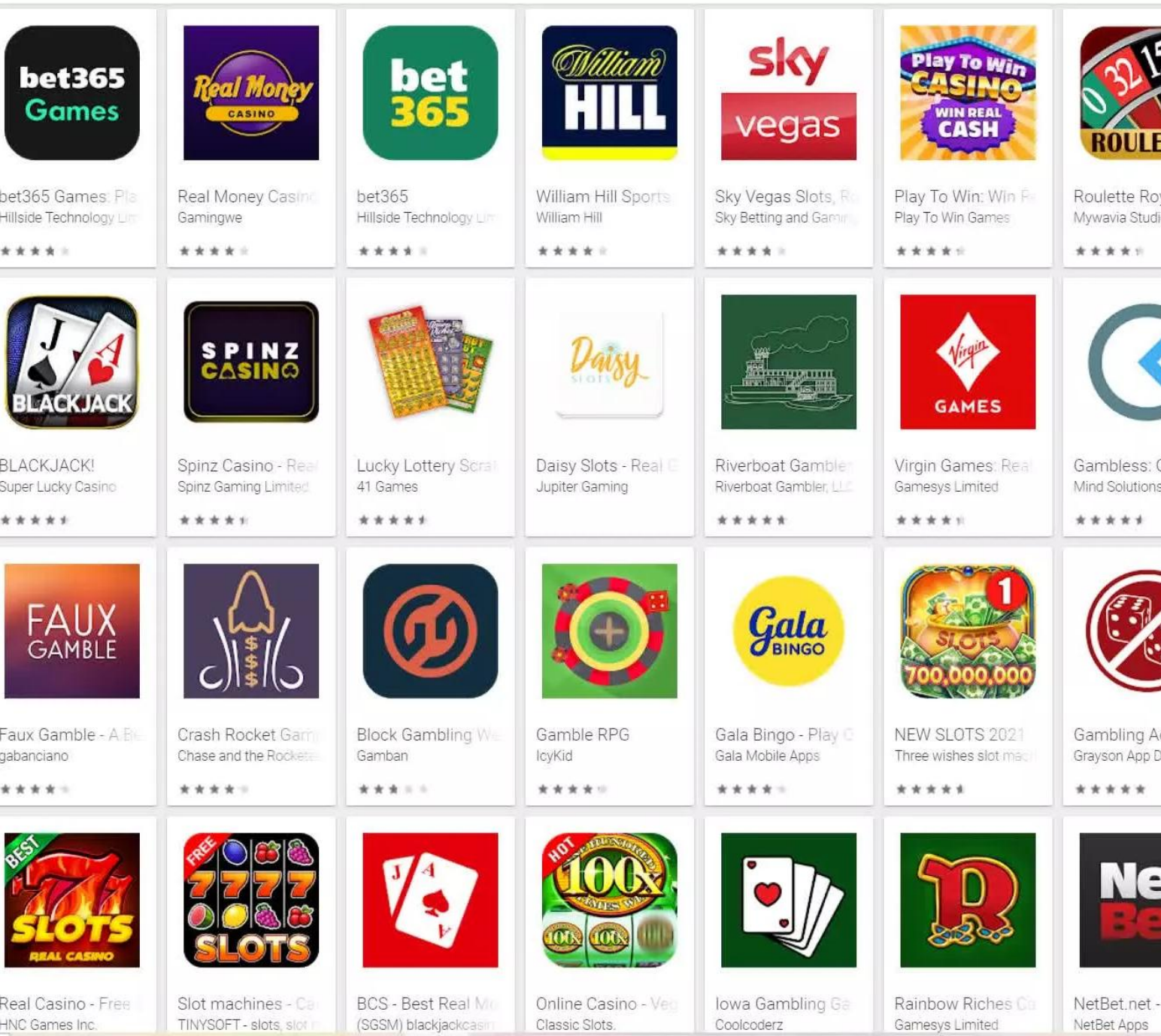
Crisis Text Line used artificial intelligence to pinpoint the things people text when they're thinking of suicide.



Based on its [analysis](#) of 129 million messages processed between 2013 and the end of 2019, the nonprofit found that the pill emoji, or 💊, was 4.4 times more likely to end in a life-threatening situation than the word suicide.

Other words that indicate imminent danger include 800mg, acetaminophen, excedrin, and antifreeze; those are two to three times more likely than the word suicide to involve an active rescue of the texter. The loudly crying emoji face, or 😭, is similarly high-risk. In general, the words that trigger the greatest alarm suggest the texter has a method or plan to attempt suicide or may be in the process of taking their own life.







Binance: Pērc BTC un Kripto

Binance Inc.

Līdzīgas lietotnes



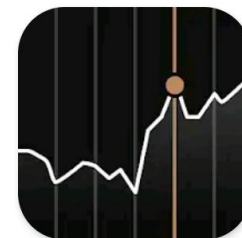
eToro: Trade.
Invest. Connect.



XTrend Speed
Trading App



Tiešsaist. tirdzn.
Capital.com



Binance TH: Bitcoin and Cryptocurrency
Gulf Binance • Finances
4,7 ★ 500 tūkst.+



Trust: Crypto & Bitcoin Wallet
DApps Platform, Inc. • Finances
4,5 ★ 50 milj.+



OKX: Buy Bitcoin BTC & Cryptocurrency
OKX • Finances • Kriptovalūta
4,4 ★ 10 milj.+



Bybit: Bitcoin, Crypto Exchange
Bybit • Finances • Kriptovalūta
4,6 ★ 10 milj.+



Bitget - Buy & Sell Cryptocurrency
BG LIMITED • Finances
4,2 ★ 10 milj.+



Bitcoin Wallet
Bitcoin Wallet development... • Finances
4,3 ★ 10 milj.+



Tor Browser

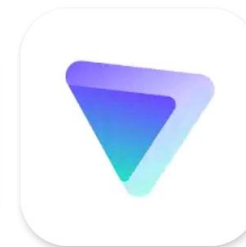
The Tor Project



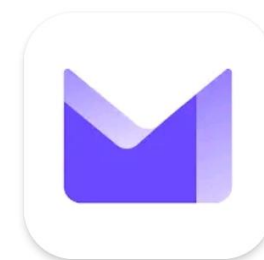
DuckDuckGo
Private Browser
4,7 ★



Tor Browser
(Alpha)
4,2 ★



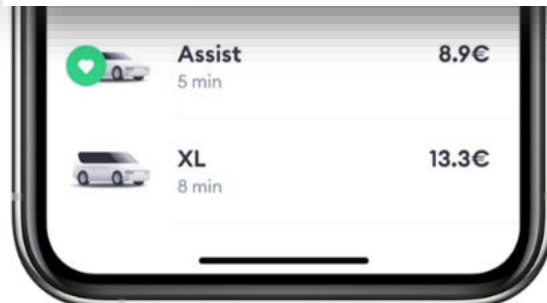
VPN Proton: Fast
& Secure VPN
4,5 ★



Proton Mail:
Encrypted Email
4,5 ★



Friday 22:00
From Home to Center



Friday 23:49
From Center to
different address

Ride-Share Apps: A National Security Risk?

Elisabeth Braw
Senior Fellow, American Enterprise Institute

Uber accused of charging more to customers with low phone battery in Belgium

Newspaper investigation in Brussels finds price increase of 6 per cent for devices running out of charge



34

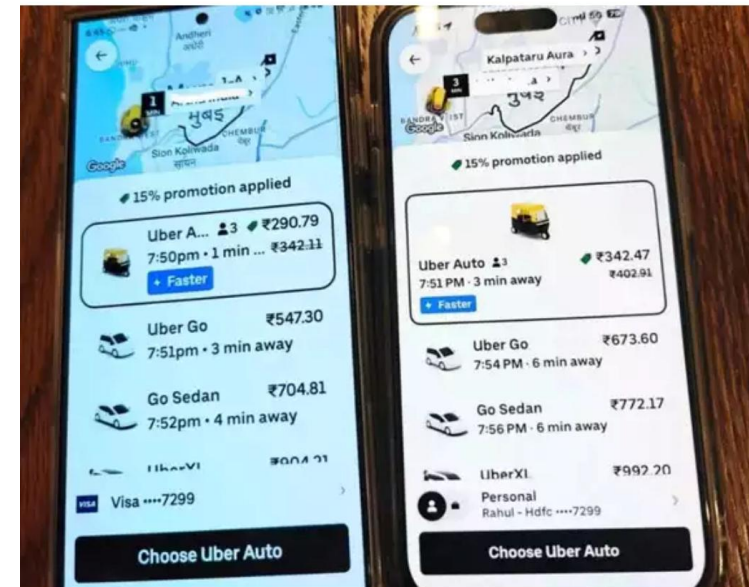


Gift this article free



Popular ride-hailing app Uber has been accused of charging customers in Belgium more if their phone battery is low Credit: ANDREW CABALLERO-REYNOLDS/AFP/Getty Images

'Low phone battery, higher Uber fares': Delhi entrepreneur's shocking discovery sparks debate over fare manipulation



Uber Fares

Synopsis

Rishabh Singh's investigation reveals Uber's pricing can change based on device platform and battery level. He found discrepancies between Android and iOS fares, and noted higher fares on low battery devices. Singh urges for transparency, suggesting users deserve to know if their data is used to manipulate prices. His findings sparked discussion online.

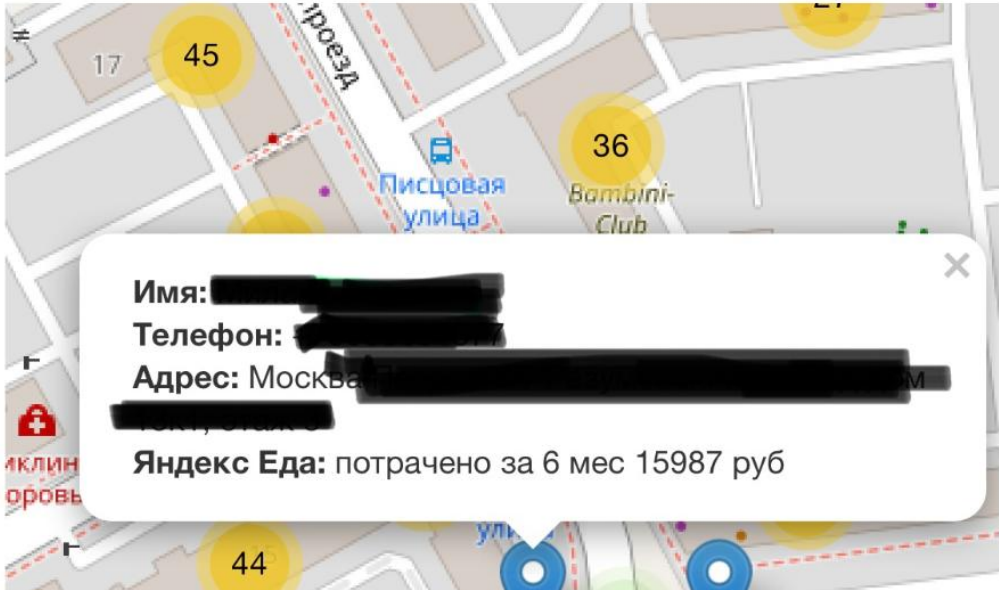
Data leak from Russian delivery app shows dining habits of the secret police / The leak exposed names, delivery addresses, phone numbers, and delivery instructions

By **EMMA ROTH**
Apr 3, 2022, 7:21 PM GMT+1 | 0 Comments / 0 New



A map with personal data of Yandex.Food users (even the amount of orders) was leaked to the network. Yandex is investigating the situation

March 22, 2022



Food Delivery Leak Unmasks Russian Security Agents

April 1, 2022 Russia Tech Team

Russian tech giant Yandex has blamed one of its employees for the hacking and subsequent leak of data from Yandex Food, a popular food delivery service in Russia.

Among the many users affected are serving agents of Russia's security services and military, who in several cases even ordered food to their places of work using their official email addresses.

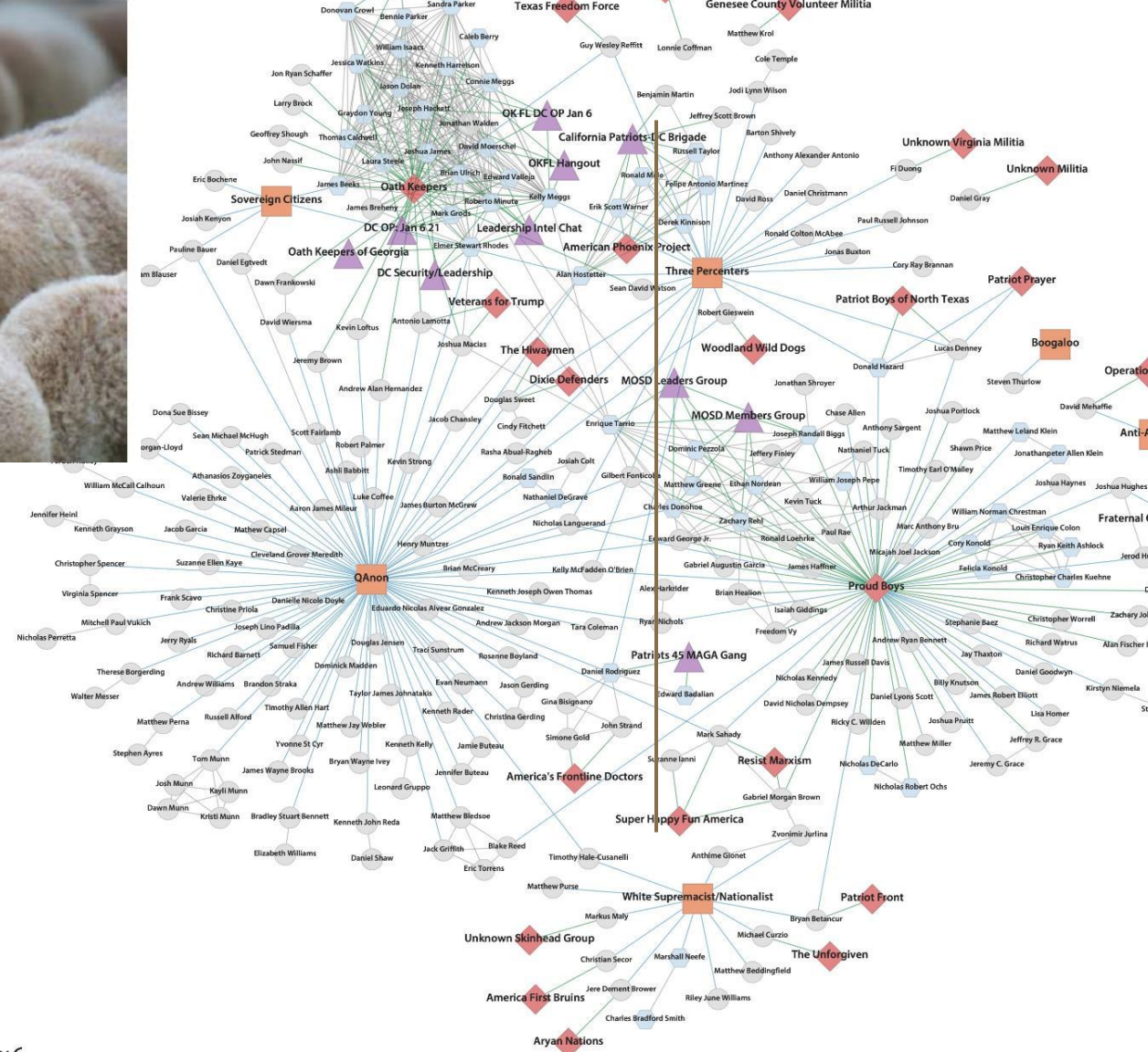
This leak includes user emails, a large number of phone numbers, addresses, and orders made on the platform. Russia's state media watchdog Roskomnadzor has strongly



A close-up photograph of a German Shepherd dog sitting in a field of sheep. The dog is looking directly at the camera with a happy expression, its mouth open and tongue hanging out. It has dark fur with tan markings on its face and chest. The sheep are white and fluffy, filling the background and foreground.

Ohio State Regular Militia

American Patriots



 *Group*

 *Movements*

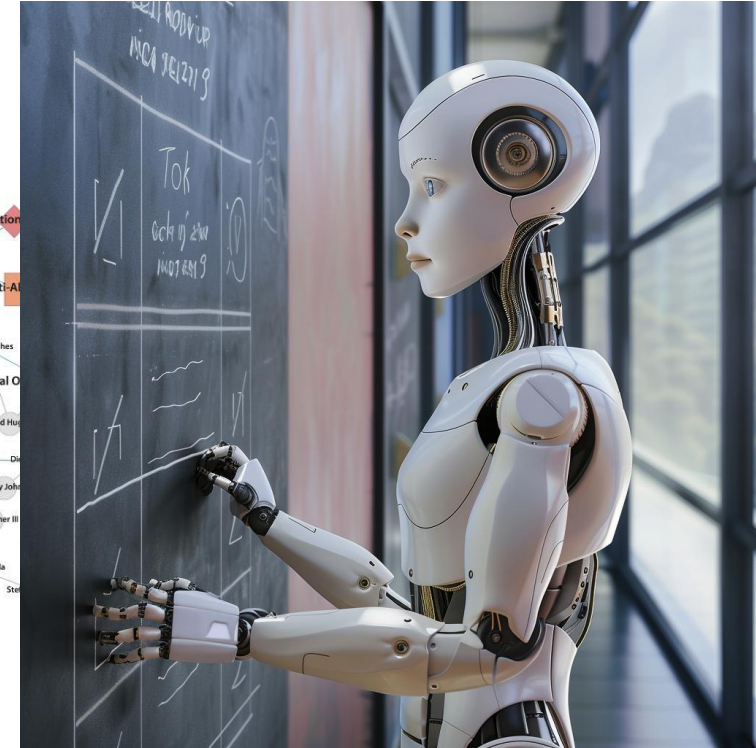
 *Communication Netw*

 *Charged with Conspiracy*

Member

— *Self-Affili*

—— Relationship Prior to January





Google Play

Games

Apps

Movies

Books

GeoGuessr

GeoGuessr

In-app purchases

4.1★

12.2K reviews

1M+

Downloads



PEGI 3

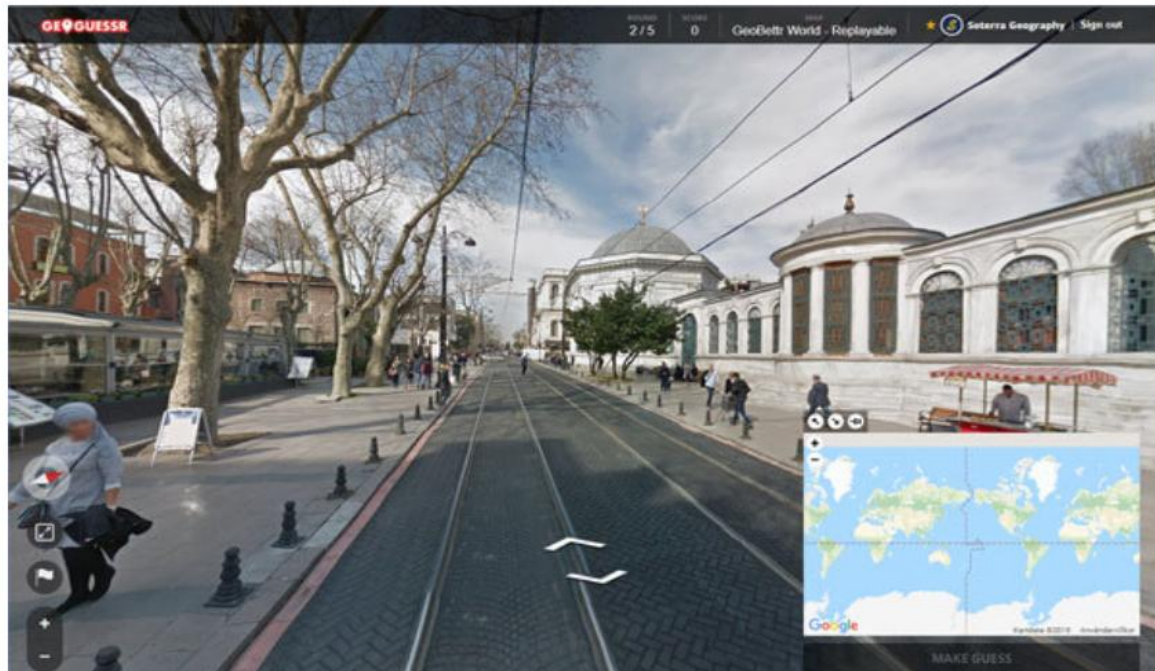


Install



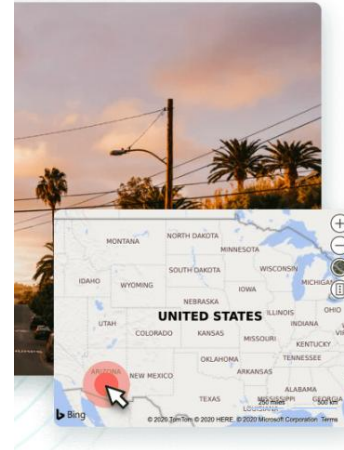
Add to wishlist

The game is so much fun because it places you somewhere in the world, with the only clue about your location being a Google Maps Street View. It's your job to figure out where you are, and then drop a pin to lock in your guess.



Where in the world are we?

GeoGuessr is a geography game, in which you are dropped somewhere in the world in a street view panorama and your mission is to find clues and guess your location on the world map.



What is Get Lost?

Get Lost is a geographic discovery game that uses randomized Streetside maps.



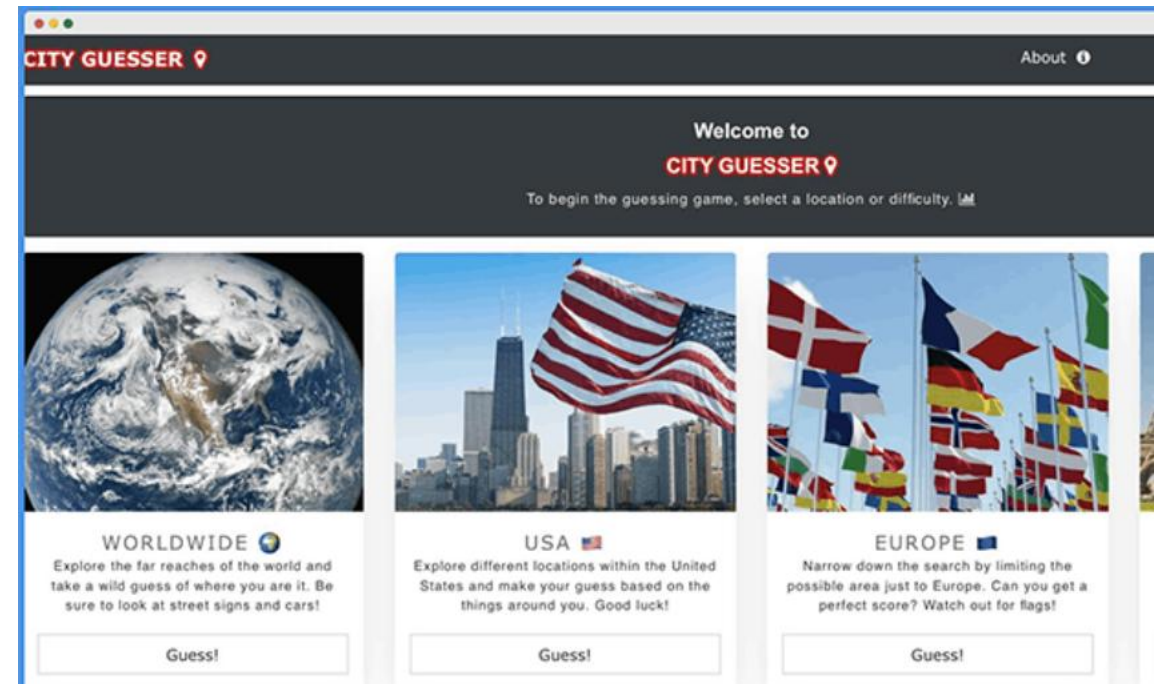
Investigate

Try to figure out your location from clues in the streetside images.



Make a Guess

Click the map wherever you think you are to make a guess. You have five rounds.



Pentagon to review security after Strava reveals sensitive information

Strava broadcast patterns of movement of US personnel at American military facilities around the world, including in war zones

Reuters

Mon 29 Jan 2018 18.35 GMT



The Pentagon said on Monday it was reviewing whether it needed to bolster its security protocols after fitness tracking devices broadcast patterns of movement of US personnel at American military facilities around the world, including in war zones.



IRAQ



SYRIA



AFGHANISTAN

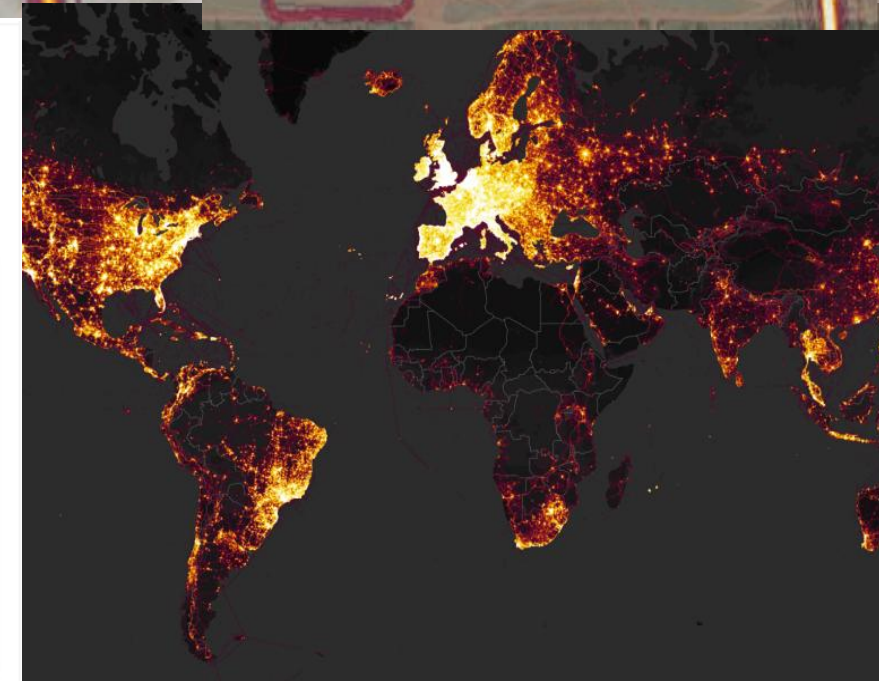
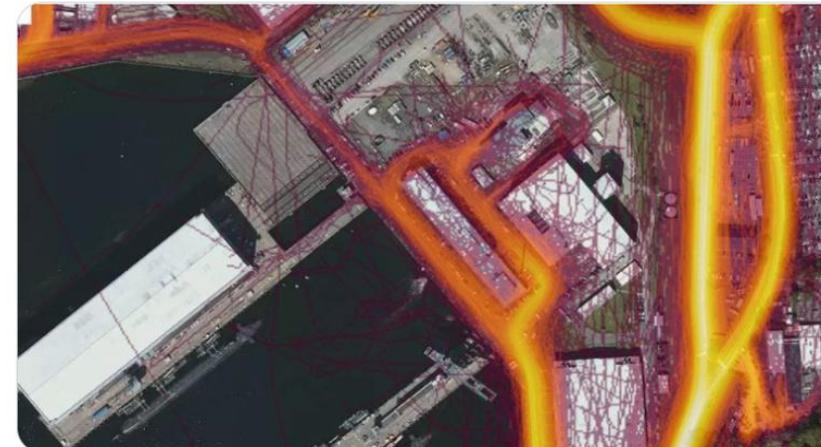


DJIBOUTI



Mustafa Al-Bassam @musalbas · Jan 29, 2018

This is Strava fitness tracker data at HMNB Clyde, a military base where Britain's nuclear weapons are stored. How are the security checks so bad in these places, that employees are allowed to bring arbitrary electronic devices in close proximity to nukes? labs.strava.com/heatmap/#16.77...





Military And Intelligence Personnel Can Be Tracked With The Untappd Beer App

May 18, 2020 Privacy Untappd

Surprise! The beer-rating app Untappd can be used to track the location history of military personnel. The social network has over eight million mostly European and North American users, and its features allow researchers to uncover sensitive information about said users at military and intelligence locations around the world.





Chief Intelligence Directorate names details of commanders whose soldiers are firing cruise missiles at Ukrainians

SUNDAY, 14 AUGUST 2022, 11:49



ДОХОДЫ ФИЗИЦ 2004		ДОХОДЫ ФЗ 2010	
Имя	ОБУХОВ ПАВЕЛ БОРИСОВИЧ	ФИО:	НАУМОВ ВЛАДИМИР ВЛАДИМИРОВИЧ
Дата рождения	7.2.1983	День рождения:	18.03.1982
Телефон	2983507	Адрес:	г. Москва, м. Мещеряковская, д. 19, кв. 19
Дата актуальности	24.03.2004	Паспорт:	46 081 19
Работодатель	ВА РВСН ИМЕНИ ПЕТРА ВЕЛИКОГО	Годовой доход:	8829.6
ИНН юл	77050	Год:	2001
Адрес	„77„ КИТАЙГОРОДСКИЙ ПРОЕЗД, 9, 5,	Работа:	ВА РВСН ИМЕНИ ПЕТРА ВЕЛИКОГО
Сумма годового дохода	25396.80		
Телефон: 7926569		Телефон: 7926279	
Страна: Россия		Страна: Россия	
Регион: г. Москва и Московская область		Регион: г. Москва и Московская область	
Оператор: ПАО "МегаФон"		Оператор: ПАО "МегаФон"	
В базах: Обухов Павел Борисович		В телефонных книгах: ГВЦ Дежурная Смена, Наумов Владимир ГВЦ	
В телефонных книгах: Павел Гвц М-р, Павел Обухов ГВЦ, Паша Обухов			
ВОДИТЕЛИ МОСКВА 2017 06		ВОДИТЕЛИ МОСКВА 12 2018	
Имя	ОБУХОВ ПАВЕЛ БОРИСОВИЧ	ФИО:	Наумов Владимир Владимирович
Дата рождения	7.2.1983	День рождения:	18.03.1982
Паспорт	46081	Адрес:	Знаменка - 19
Телефон	792656	Возраст:	40 лет
Адрес места работы	119019, г. Москва, ул. Знаменка, д. 19		

DRUG BOSS DOWNFALL Drug cartel kingpin arrested in UK after his wife gave away key details in glam holiday picture posts online

One picture showed Grijalba and his wife in front of the Eiffel Tower

Nick Parker, Foreign Editor
Published: 14:17 ET, Jan 24 2025 | Updated: 5:50 ET, Jan 25 2025



Latvijas Gaisa spēku bāzes izspiegošana un provokācijas

Īsumā par personām



Martins Griķis un Sergejs Hodonovičs

- Latvijas Republikas pilsoņi;
- abiem jauniešiem, no kuriem vienam ir 20, bet otram 23 gadi, nav augstākās izglītības vai profesionālu prasmju;
- jaunieši bija atvērti piepelnīšanās iespējām internetā;
- spiegoja un veica citas darbības Krievijas spēcienesta labā.



Aizturēšana:

VDD sadarbībā ar MIDD personas aizturēja 2023. gada 24. aprīlī.

Par noziedzīgu nodarījumu

- M. Griķis (pirmajā attēlā) veidoja informācijas avotu tīklu ziņu iegūšanai par Latvijas valsts aizsardzības resoru. M. Griķis, izmantojot saziņas lietotni "Telegram", piesaistīja S. Hodonoviču, kurš ieguva izlūkziņas par NBS Gaisa spēku bāzi, kā arī karavīru un militārās tehnikas pārvietošanos tās apkārtnē – Lielvārdes un Rembates pagastos.
- S. Hodonovičs papildus tika izmantots arī provokāciju īstenošanai. Viņš pilsētvidē veica huligāniskas darbības, zīmējot grafiti, kas rada

iespaidu par sabiedrībā šķietami valdošu atbalstu Krievijas agresijai.

Izmeklēšanas rezultāts

Abi jaunieši par vainīgiem atzīti gan pirmās, gan otrās instances tiesā. Otrās instances tiesa 2024. gada 30. janvārī M. Griķim piesprieda brīvības atņemšanu uz trīs gadiem, savukārt S. Hodonovičam – uz diviem gadiem un astoņiem mēnešiem. Papildus M. Griķim piesprieda probācijas uzraudzību uz diviem gadiem un sešiem mēnešiem, savukārt S. Hodonovičam – uz diviem gadiem un četriem mēnešiem. Spriedums vēl nav stājies spēkā.

Ko vēsta šis gadījums:

- Ņemot vērā kopš Krievijas iebrukuma Ukrainā VDD un MIDD pastiprināto pretizlūkošanas režīmu un sabiedrības modrību pret aizdomīgām aktivitātēm, Krievijas spēcienestiem ir kļuvusi sarežģītāk īstenot izlūkdarbības Latvijas teritorijā. Šā iemesla dēļ Krievijas spēcienesti Latvijas valstspiederīgo vervēšanai, kā arī informācijas apmaiņai aizvien biežāk izmanto interneta vidi.
- Satura kontroles trūkuma dēļ ziņojumapmaiņas platforma "Telegram" ir kļuvusi par vienu no visbiežāk izmantotajiem saziņas rīkiem dažādu noziedzīgu darbību veikšanai, tajā skaitā personu vervēšanai, spiegošanas organizēšanai un izlūkinformācijas ieguvei.
- Krievijas spēcienesti ir gatavi savās interesēs izmantot arī personas bez izglītības, pastāvīgiem ienākumiem un nākotnes perspektīvām. Devianti jaunieši Krievijas spēcienestiem ir parocīgs vervēšanas mērķis, jo ir ieinteresēti vieglā peļņā un prot lietot informācijas tehnoloģijas.



Ja kaut kur redzi šādu zīmi, šo objektu nedrīkst fotografēt!



Ja kāds internetā Tevi lūdz veikt šādu objektu fotografēšanu vai filmēšanu, nedari to! Reizēm šāds aicinājums var būt kā izaicinājums vai daļa no spēles, tomēr šādi vari iedzīvoties nepatīkšanās.



child | data | citizen



How Tech Companies
Are Profiling Us
from before Birth

Veronica Barassi



Forbes

Subscribe

Subscribe now

Feb 16, 2012, 11:02am EST

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did



Kashmir Hill Former Staff

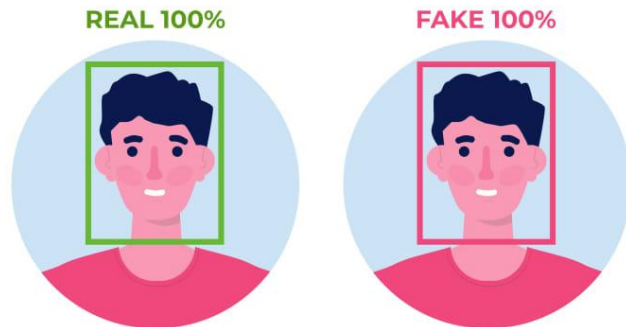
Tech

Welcome to The Not-So Private Parts where technology & privacy collide

Follow

«Mežonīgie rietumi» digitālajā vidē

Mērķis: līdz sistēma sakārtosies (eventuāli **3-5 gadi**) atstāt minimālas digitālās pēdas / minimālo informāciju par sevi.



Tehnoloģijas apsteidz regulējumu / aizsardzības pasākumus, jeb **paļauties var tikai uz kritisko domāšanu**

Nepieciešams izskaidrot ilgtermiņa sekas



Ja kaut kas publicēts, tas var nokļūt visu cilvēku redzeslokā.



Nevar nodzēst

Ko darīt?



Soli pa solim!



Jaunu interešu un paziņu loku veidošana.

Vecākam jārāda piemērs: ja samazināt interneta lietošanu, tad visiem ☺

Jautājumi diskusijai?

1. Kādas tēmas, jūsuprāt, būtu visnoderīgāk iekļaut mācību stundās, lai skolēni zinātu kā pareizi rīkoties moderno apdraudējumu situācijās?
2. Kādas praktiskās aktivitātes vai mācību uzdevumi, pēc jūsu domām, palīdzētu skolēniem labāk apgūt šādas prasmes apdraudējuma gadījumos?
3. Kuru mācību priekšmetu ietvaros, jūsuprāt, būtu vispiemērotāk iekļaut šādu apmācību par rīcību apdraudējumu situācijās?