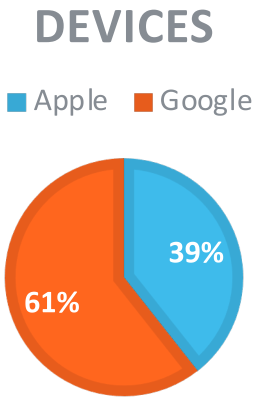
Real-time evidence

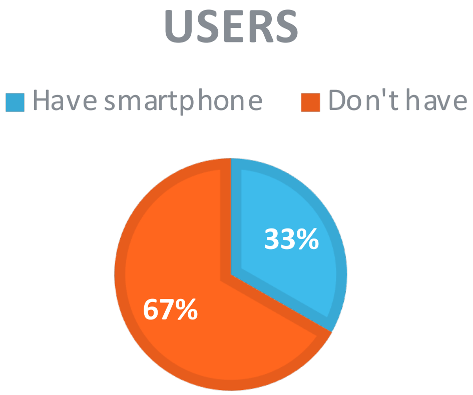
Using Apple iCloud and Google to track users in real time

Smartphone usage over the world

Apple: 2 billion iOS devices sold, 500 million active iOS devices (2018)

Google: 2.5 billion active Android devices (May 2019)





What’s inside a smartphone?

- Contacts & calendars
- Call logs and text messages
- Emails and chats
- **Account and application passwords**
- **Web and Wi-Fi passwords**
- Documents, settings and databases
- Web history & searches
- Pictures and videos
- Location history, routes and places
- Third-party app data
- Cached internet data
- System and application logs
- Social network activities

What's in the Cloud?

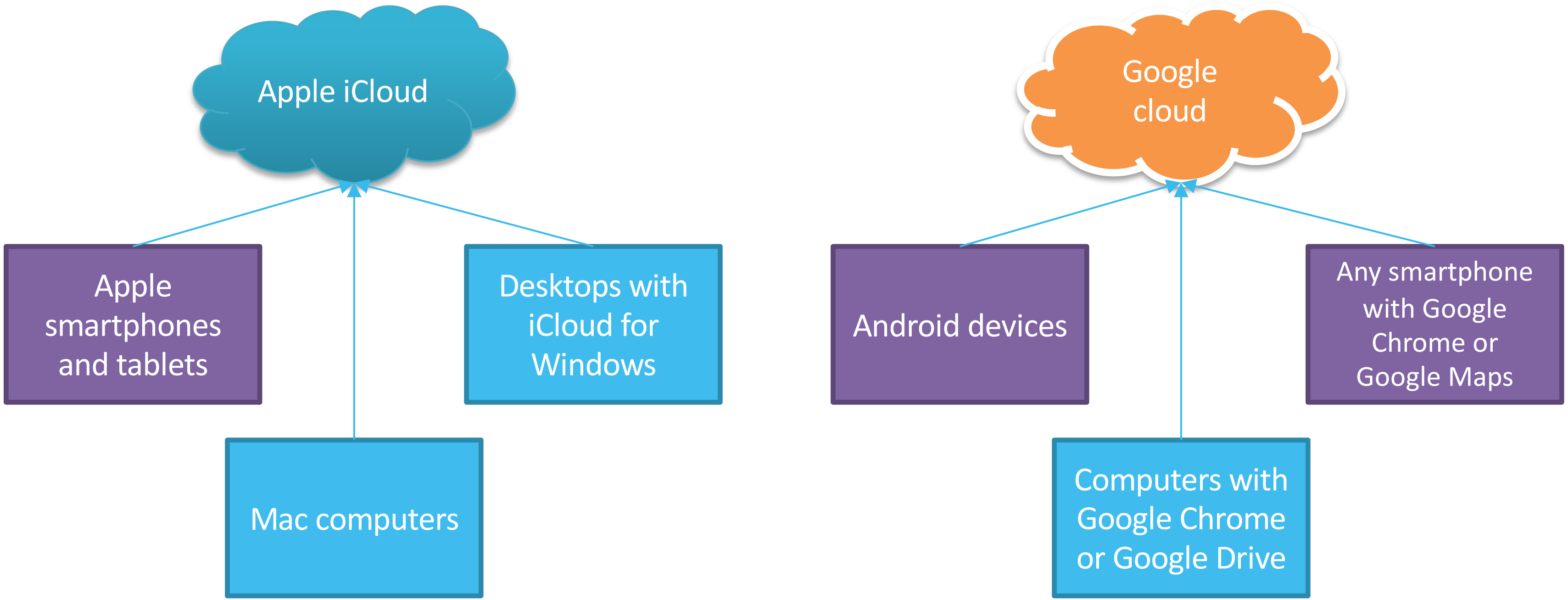
Apple

- iOS device backups: 2 snapshots of each device
- Synchronized data
- File/document storage

Google

- Synchronized data
- Android device backups
- File/document storage

Cloud data: not just smartphones


Apple iCloud
Apple smartphones and tablets
Mac computers
Desktops with iCloud for Windows
Google cloud
Android devices
Computers with Google Chrome or Google Drive
Any smartphone with Google Chrome or Google Maps

What data is synced?

Apple iOS: iCloud

- Account info
- Calendars, Contacts, Notes
- Call logs (phone, FaceTime, *sometimes* other apps)
- iOS 11 and newer: Apple Health
- iOS 11.4 and newer: iMessage/SMS
- iOS 12: voice memos
- Safari history, bookmarks, opened tabs
- Home, News, Books
- Apple Maps: searches, favorites
- Wi-Fi networks
- iCloud Photo Library
- Screen Time (usage and restrictions)
- **iCloud Keychain (passwords)**
- **FileVault2 recovery token**
- ***Some deleted data***

Google Account

- Dashboard: devices, stats and personal data
- Location and POI-based mapping data
- Google search history
- Mail, calendars, notes
- Calls
- SMS messages
- Chrome history, bookmarks, auto-fill, **passwords**
- Wi-Fi networks
- Photo library
- Google Fit (health) data
- Digital Wellbeing (usage data)

Synced data by platform

	Apple	Google
Contacts/calendars/tasks	+	+
Call log	+	7.0+
Notes	+	+
Messages	iOS 11.4 + 2FA	8.0+
Mail	iCloud mail	Gmail
Internet	Safari	Chrome
Media	iCloud Photo Library	Google Photos
Documents	iCloud Drive	Google Docs
Location	Current/last	Current, history
Usage statistics and restrictions	Screen Time	Digital Wellbeing (some devices)
Third-party app data	iCloud Drive	Google Drive
Other	Health, Wallet, Maps etc	Dashboard, Google Fit etc

Secrets stored in the cloud

	Apple	Google
Wi-Fi passwords	+	+
Web site passwords	+	+
Credit cards (autofill)	CVC/CVV is not stored	CVC/CVV is not stored
Credit cards (payment systems)	*Apple Pay (Wallet): last 4 digits only*	*Google Pay (?)*
App-specific	*It depends*	*Sometimes (Android 8+)*
Authentication tokens	+	+
Encryption keys	+	-
Certificates	+	-
Autocomplete	+	+

Synced data vs backups

Real-time synchronization, data appears in the cloud in minutes

Backups are huge, difficult to access, contain a lot of useless information

Apple detects backup downloads by third-party apps and may lock accounts

Some types of synced data not included in iCloud backups if sync is enabled:

- Photos (if iCloud Photo Library is enabled)
- Text messages and iMessages (iOS 11.4 and newer, if synced)
- Health & Home: not in iCloud backups (regardless the settings)

Advantages of obtaining synced data

- Usually enabled by default
- Little known, rarely disabled
  - **Challenge**: try making your iPhone to NOT sync call logs via cloud
- **Real-time data and real-time availability**
- Deleted data is available for many categories (documents, call logs, pictures: up to 30 days)
- Weaker protection compared to cloud backups
- Current location

iCloud Keychain

Synchronized over all connected devices

Requires Two-Factor Authentication and device passcode

Contains:

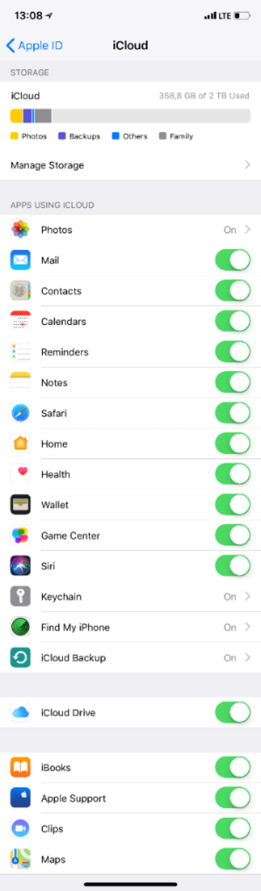
- Apple IDs with passwords
- Wi-Fi passwords
- E-Mail account passwords
- Passwords stored in Safari
- Credit cards (no CVC/CVV)
- Authentication tokens (e.g. for social networks)

Apple Health Evidence

- Steps, floors climbed using iPhone hardware (dedicated low-power co-processor)
- Other physical activity data recorded with HealthKit devices (iPhone, Apple Watch, compatible fitness trackers etc.)
- Data collected with third-party apps (Nike+, Strava, Workouts++)
- Apple Watch: heart rate, GPS data (if workout is detected), AW4: ECG

Apple Health and Cloud

- Native Apple Health data is synced with iCloud to all registered devices
- Third-party apps operate through HealthKit
- Some third-party app data is not shared with Apple Health
- Certain apps use proprietary cloud sync (Strava, Endomondo)
- **Medical ID** data is unique per device and **does not sync**
- **CDA records** do not sync (to the best of our knowledge)
- **ECG** do not sync



13:08 LTE

Apple ID — iCloud

STORAGE

iCloud 358,8 GB of 2 TB Used

🟨 Photos 🟪 Backups 🟦 Others ⬜ Family

Manage Storage >

APPS USING ICLOUD

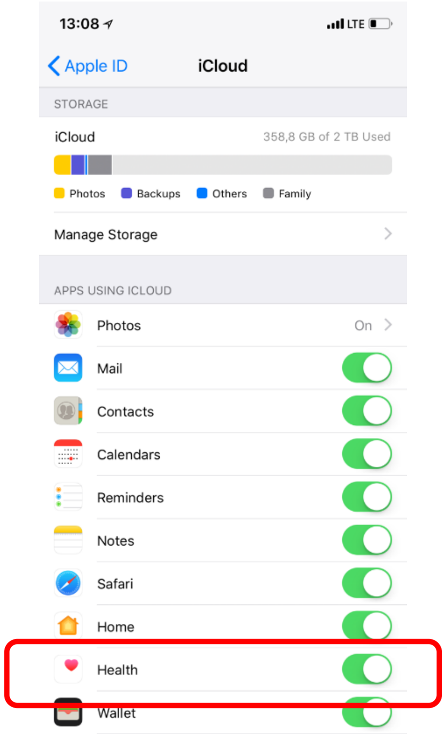
Photos On >
Mail ●
Contacts ●
Calendars ●
Reminders ●
Notes ●
Safari ●
Home ●
Health ●
Wallet ●
Game Center ●
Siri ●
Keychain On >
Find My iPhone On >
iCloud Backup On >

iCloud Drive ●

iBooks ●
Apple Support ●
Clips ●
Maps ●

Apple Health and iCloud

- Apple Health data **can** be obtained from iCloud
- May contain significantly more information compared to what is available on device
- Technically, Apple Health belongs to “synced data” as opposed to “cloud backups”
  - This results in significantly more reliable extraction
  - Loose expiration rules of iCloud tokens compared to backups



13:08 LTE

Apple ID iCloud

STORAGE

iCloud 358,8 GB of 2 TB Used

🟨 Photos 🟪 Backups 🟦 Others ◼ Family

Manage Storage

APPS USING ICLOUD

Photos On

Mail

Contacts

Calendars

Reminders

Notes

Safari

Home

Health

Wallet

Apple Health Sync and Protection Mechanisms

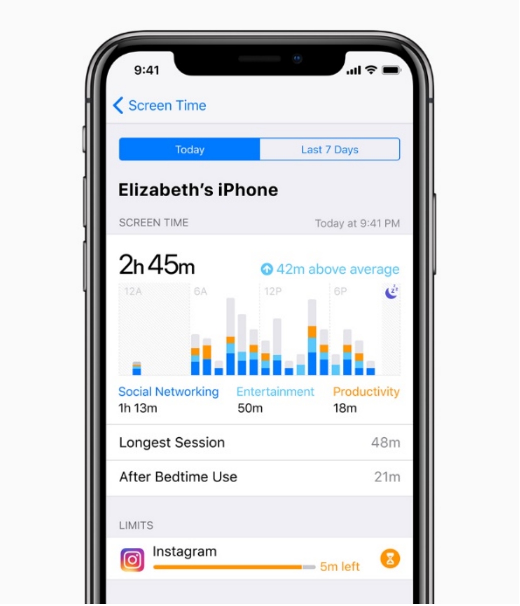
- Regular syncing: scheduled, after device reboot, on account change
- Data is stored in iCloud Drive (in chunks)
- **iOS 11**: unlike iCloud Keychain or Messages, iCloud Health data has no additional protection
  - No need to enter device passcode, no additional encryption
- **iOS 12**: iCloud Health encrypted with a key stored in iCloud Keychain
  - Accessing iCloud Health data requires device passcode or system password from an already enrolled device

blog.elcomsoft.com/2019/01/securing-and-extracting-health-data-apple-health-vs-google-fit/

Apple Screen Time

- Comprehensive usage statistics (incl. Safari history)
- Usage restrictions remotely enforceable
- Collected from all devices sharing the same Apple ID

    + from child acconts
- iCloud sync requires Two-Factor Authentication
- Screen Time data is additionally protected
- Passcode or system password required to access Screen Time data
- Screen Time password is stored in the iCloud



Elizabeth's iPhone

SCREEN TIME Today at 9:41 PM

2h 45m 42m above average

Social Networking 1h 13m
Entertainment 50m
Productivity 18m

Longest Session 48m

After Bedtime Use 21m

LIMITS

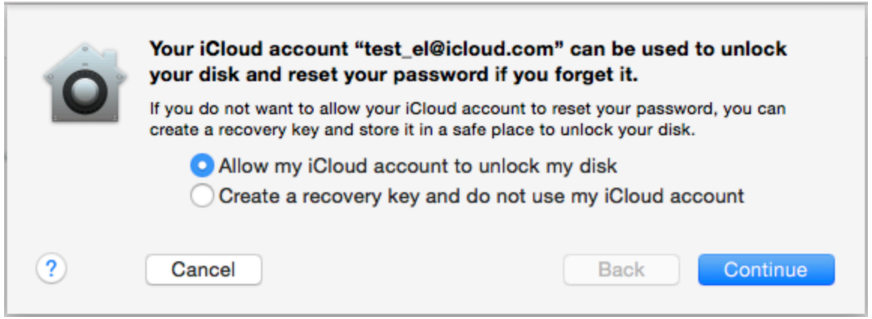
Instagram 5m left

Apple FileVault 2 key in iCloud

FileVault 2 is a disk encryption feature introduced in OS X 10.7

Several methods to access encrypted volumes

- Password
- Recovery passphrase
- Recovery certificate
- **Recovery key stored in iCloud**
- HFS+: disk image can be decrypted
- APFS: will be able to decrypt soon



Your iCloud account "test_el@icloud.com" can be used to unlock your disk and reset your password if you forget it.

If you do not want to allow your iCloud account to reset your password, you can create a recovery key and store it in a safe place to unlock your disk.

● Allow my iCloud account to unlock my disk

○ Create a recovery key and do not use my iCloud account

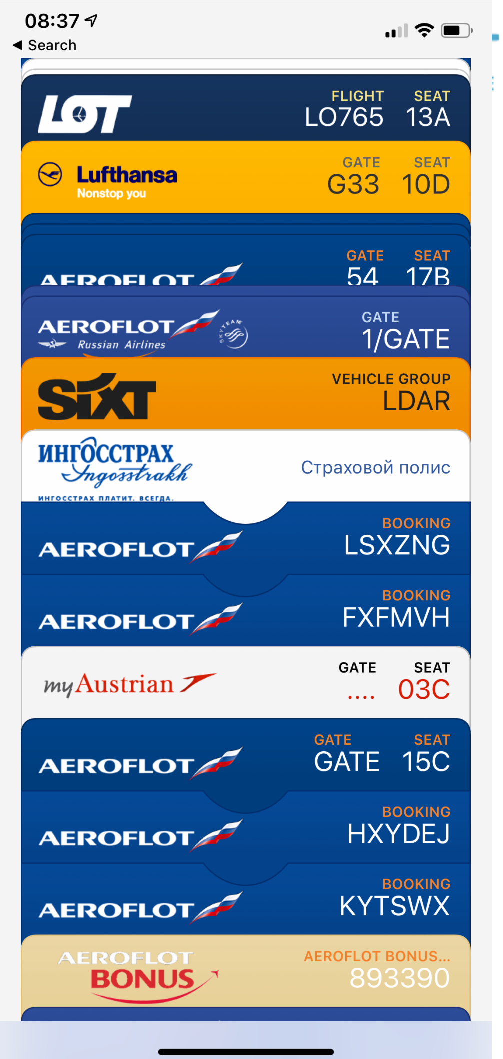
Apple Wallet

Stored in iCloud

Synchronized between devices in real-time

Contains:

- Discount cards and coupons
- Event and transport tickets
- Frequent flyer cards
- Boarding passes
- Insurance, car rentals
- Apple Pay cards (not synced)



08:37

◀ Search

LOT — FLIGHT LO765 — SEAT 13A

Lufthansa Nonstop you — GATE G33 — SEAT 10D

AEROFLOT — GATE 54 — SEAT 17B

AEROFLOT Russian Airlines — GATE 1/GATE

SIXT — VEHICLE GROUP LDAR

ИНГОССТРАХ Ingosstrakh ИНГОССТРАХ ПЛАТИТ. ВСЕГДА. — Страховой полис

AEROFLOT — BOOKING LSXZNG

AEROFLOT — BOOKING FXFMVH

myAustrian — GATE .... — SEAT 03C

AEROFLOT — GATE GATE — SEAT 15C

AEROFLOT — BOOKING HXYDEJ

AEROFLOT — BOOKING KYTSWX

AEROFLOT BONUS — AEROFLOT BONUS... 893390

Apple iCloud: authentication tokens

Tokens are binary files

Do not contain account password or password hash

Saved to desktop computers to sync with iCloud

Saved on iOS and tvOS devices

Some tokens are “pinned” to the device

Allow users to bypass entering login & password

Allow investigators to bypass 2FA

Apple iCloud: Anisette data

- Anisette data is a set of binary data stored on PC or Mac
- Generated/updated in real time
- Required for accounts that use 2FA
- It’s random data generated by iOS/macOS kernel (using hardware ID)
- Cannot be easily generated ion Windows computers
- Required to access iCloud backups
- Required to access specific synced data (keychain, messages, Health)
- When we have Anisette data, we can enter into the “circle of trust”
- We still need login and password

iCloud backups vs. iCloud sync: Data

	Backups	Synced data
Photos	If no iCloud Photos	If iCloud Photos enabled
Health	No	Yes
Messages	If no iCloud Messages	If iCloud Messages enabled
Browser history, tabs	Yes	Yes
Passwords	No (this device only)	Yes, if iCloud Keychain enabled

iCloud backups vs. iCloud sync: Availability

	Backups	Synced data
Maintenance	Once a day, when charging & connected	Nearly real-time sync
Accessible with	Login & password (and second factor); no 2FA: with tokens	Login & password (&2FA); authentication tokens
Risk of temp. account lock	The risk exists	No risk
Access to deleted data	Some (old backups, SQLite)	Some, for several categories (usually 30 days)
Availability	Often no backups (5GB iCloud limit, disabled by the user)	Almost always available

Apple: requirements to access evidence

- Synchronized data (general) including iCloud Photos, Safari history, contacts etc.
  - Apple ID and password; second factor if 2FA is enabled, or
  - Non-expired iCloud authentication token
- Synchronized data (secure) including iCloud Keychain, Health, Messages, Screen Time
  - Apple ID, password, 2FA and device passcode or system password of an already enrolled device; anisette data for some categories
- iCloud backups
  - Apple ID and password; second factor if 2FA is enabled; anisette data

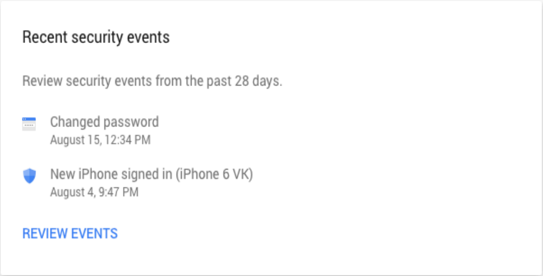
Apple: risks when accessing online evidence

- Synchronized data (general):
  - No known risks
- Synchronized data (secure) including iCloud Keychain, Health, Messages, Screen Time
  - 10 wrong passcode attempts <u>will</u> wipe secure sync data (not a configurable setting but fixed iCloud behavior); number of failed attempts can be obtained
- iCloud backups
  - Apple may temporarily lock iCloud account, may require password reset (usually the next day, but not on weekends)

- *Apple constantly monitor iCloud activities and check for multiple accounts access from the same IP*

Google: collecting data from multiple sources

- Multiple devices
  - Mac
  - Windows
  - iPhone
  - iPad
  - ...and Android
- Apps
  - Dropbox
  - Auth
  - Chrome
  - Remote desktop
  - Many more



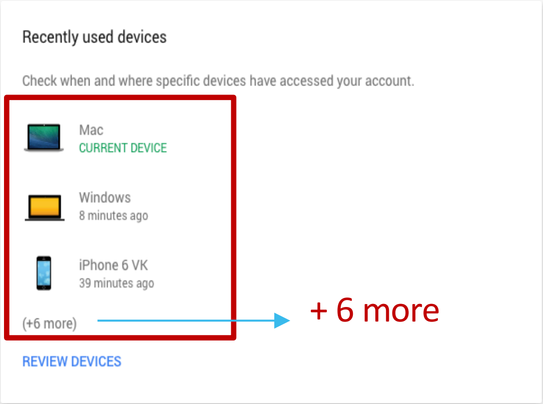
Recent security events

Review security events from the past 28 days.

Changed password
August 15, 12:34 PM

New iPhone signed in (iPhone 6 VK)
August 4, 9:47 PM

REVIEW EVENTS



Recently used devices

Check when and where specific devices have accessed your account.

Mac
CURRENT DEVICE

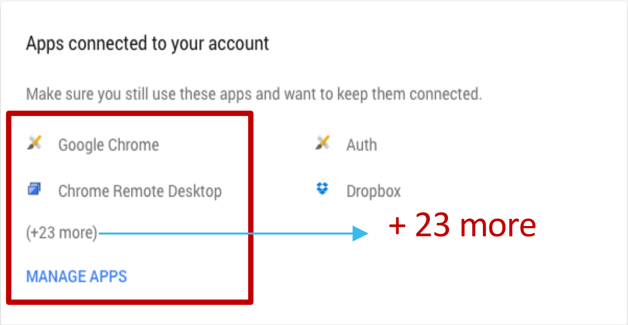
Windows
8 minutes ago

iPhone 6 VK
39 minutes ago

(+6 more)

+ 6 more

REVIEW DEVICES



Apps connected to your account

Make sure you still use these apps and want to keep them connected.

Google Chrome

Auth

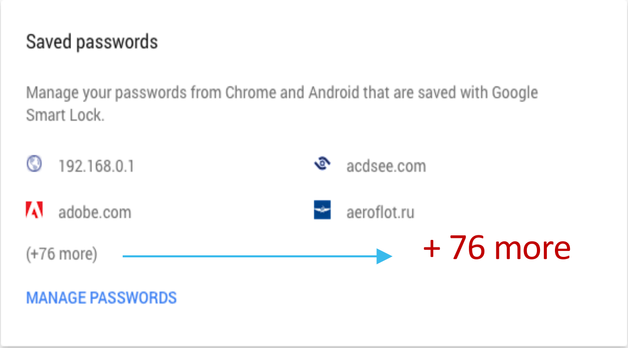
Chrome Remote Desktop

Dropbox

(+23 more)

+ 23 more

MANAGE APPS



Saved passwords

Manage your passwords from Chrome and Android that are saved with Google Smart Lock.

192.168.0.1

acdsee.com

adobe.com

aeroflot.ru

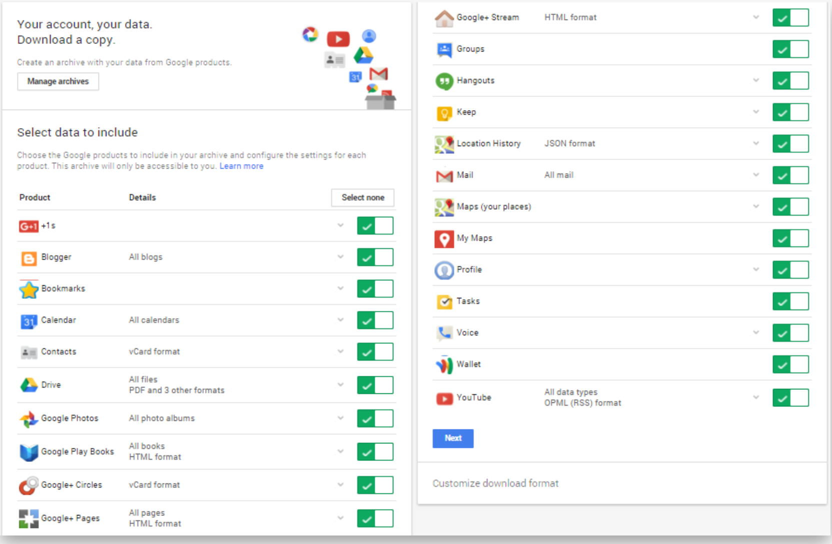
(+76 more)

+ 76 more

MANAGE PASSWORDS

Google Takeout

- Leaves many traces
- Not everything is exported
- Limited flexibility
- Numerous awkward formats
- User alerted via email



Your account, your data.
Download a copy.

Create an archive with your data from Google products.

Select data to include

Choose the Google products to include in your archive and configure the settings for each product. This archive will only be accessible to you. Learn more

Product	Details	Select none
+1s		✓
Blogger	All blogs	✓
Bookmarks		✓
Calendar	All calendars	✓
Contacts	vCard format	✓
Drive	All files PDF and 3 other formats	✓
Google Photos	All photo albums	✓
Google Play Books	All books HTML format	✓
Google+ Circles	vCard format	✓
Google+ Pages	All pages HTML format	✓
Google+ Stream	HTML format	✓
Groups		✓
Hangouts		✓
Keep		✓
Location History	JSON format	✓
Mail	All mail	✓
Maps (your places)		✓
My Maps		✓
Profile		✓
Tasks		✓
Voice		✓
Wallet		✓
YouTube	All data types OPML (RSS) format	✓

Customize download format

Google Dashboard – not available in Google Takeout

Account
- email
- number of Google API clients (sites and apps)
- account time: personal, work, both
- Activities in last 28 days
  - browsers and OSs that had access
  - locations
  - new apps and sites

YouTube
- number of videos and playlists loaded
- user name
- sex
- last video rating (+video name and date)
- activities for last 28 days
  - number of views, by day
  - total views
  - searches
  - likes and dislikes

Search history (query + date)
- last Web search
- last image search
- last news search
- last video search
- last maps search
- last books search
- activities for last 28 days
  - top 10 searches
  - percentage of searches by category (web, image etc.)
  - activity (by day)

Google Sync. (non-Android devices)
- number of bookmarks
- last sync date
- number of passwords
- number of Chrome extensions

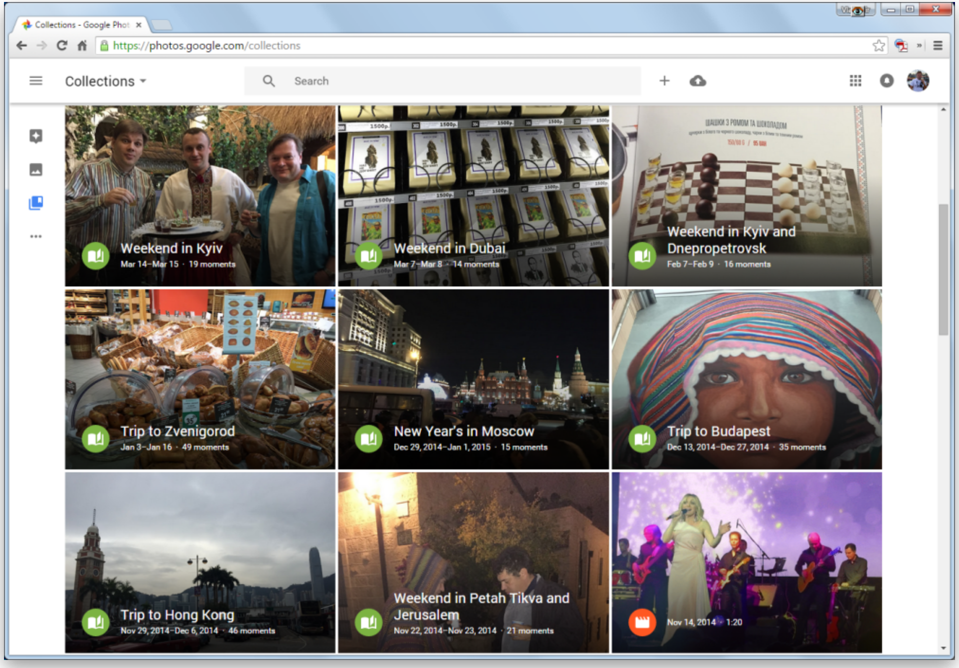
Profile info
- Google+ name
- profile URL
- number of phone numbers
- number of "+1"

Gmail
- number of mail threads
- last thread subject
- number of messages in inbox
- last incoming message subject
- number of sent mails
- last sent mail subject

Android
- make, model
- first auth date/time
- last activity date/time
- apps that backup their data (name, date, size)

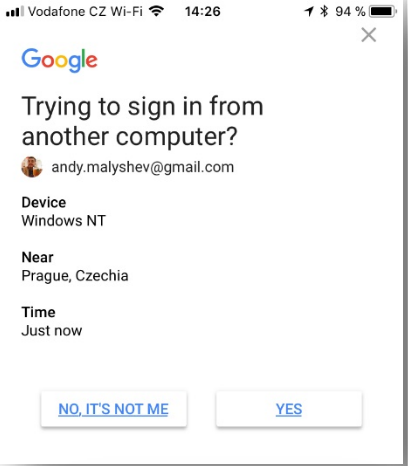
Google Photos

- Albums/events
- Comments
- EXIF
- Geo tags
- Subscriptions
- View counters
- People


Collections - Google Phot
https://photos.google.com/collections
Collections
Search
Weekend in Kyiv
Mar 14–Mar 15 · 19 moments
Weekend in Dubai
Mar 7–Mar 8 · 14 moments
Weekend in Kyiv and Dnepropetrovsk
Feb 7–Feb 9 · 16 moments
Trip to Zvenigorod
Jan 3–Jan 16 · 49 moments
New Year's in Moscow
Dec 29, 2014–Jan 1, 2015 · 15 moments
Trip to Budapest
Dec 13, 2014–Dec 27, 2014 · 35 moments
Trip to Hong Kong
Nov 29, 2014–Dec 6, 2014 · 46 moments
Weekend in Petah Tikva and Jerusalem
Nov 22, 2014–Nov 23, 2014 · 21 moments
Nov 14, 2014 · 1:20

Google account: many different types of 2FA

- Google prompt: application on mobile device
- Authenticator app: time limited codes
- Single-use backup codes
- SMS codes
- FIDO hardware security key (Yubico etc)
- **All 2FA types can be bypassed using authentication tokens from Google Chrome or Google Drive**



Vodafone CZ Wi-Fi 14:26 94 %

Google

Trying to sign in from another computer?

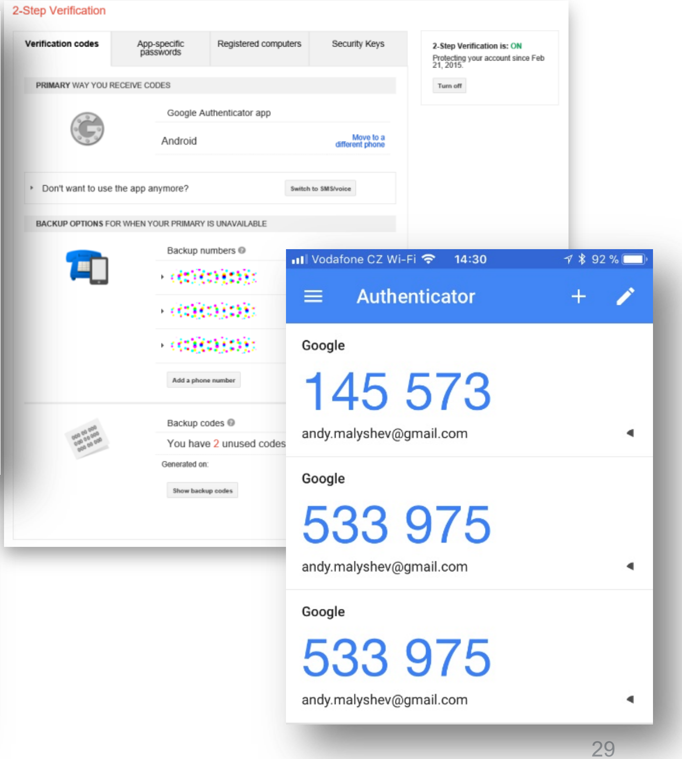
andy.malyshev@gmail.com

Device
Windows NT

Near
Prague, Czechia

Time
Just now

NO, IT'S NOT ME | YES



2-Step Verification

Verification codes | App-specific passwords | Registered computers | Security Keys

2-Step Verification is: ON
Protecting your account since Feb 21, 2015.
Turn off

PRIMARY WAY YOU RECEIVE CODES

Google Authenticator app
Android — Move to a different phone

Don't want to use the app anymore? — Switch to SMS/voice

BACKUP OPTIONS FOR WHEN YOUR PRIMARY IS UNAVAILABLE

Backup numbers
[redacted]
Add a phone number

Backup codes
You have 2 unused codes
Generated on:
Show backup codes

Vodafone CZ Wi-Fi 14:30 92 %

Authenticator

Google
145 573
andy.malyshev@gmail.com

Google
533 975
andy.malyshev@gmail.com

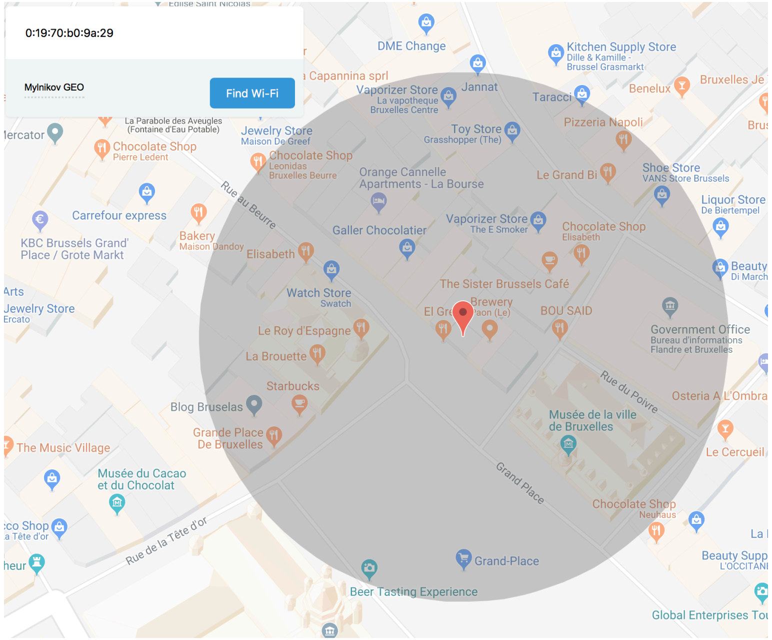
Google
533 975
andy.malyshev@gmail.com

Locations by devices and applications

Source	On device	Apple iCloud	Google cloud
Apple device: last location	+	+	-
Apple device: location history	+	-	-
Apple Maps: searches and favorites	+	+	-
Apple: significant locations	+	-	-
Apple Health (only if workout is detected)	+	+	-
Photos: iOS (EXIF, if location enabled)	+	+	app req-d
Google Maps: Android devices	+	-	+
Google Maps: iOS and WM devices	+	-	+
Google Fit	+	-	+
Photos: Android	+	-	+
Uber	+	Backups	-

Wi-Fi hotspots: getting locations

- Both Google and Apple clouds store wi-fi hotspot BSSID
- BSSID can be used to reverse-lookup hotspot location
- Databases of hotspot locations:
    - Google
    - Mylnikov GEO
    - Wigle.net
    - openBMAP



0:19:70:b0:9a:29

Mylnikov GEO

Google Fit Evidence

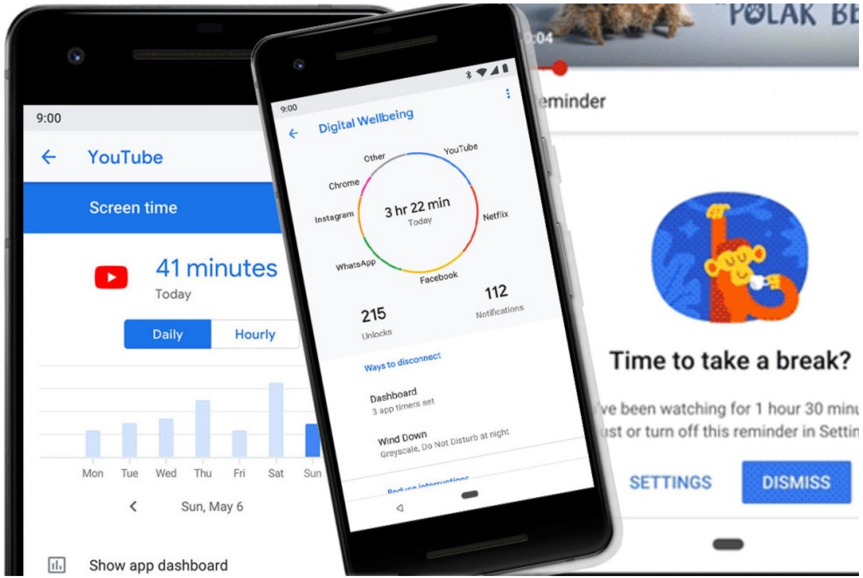
- Collects information from the phone
- Relies heavily on **Location History**
- Makes use of AI to approximate number of steps walked
- Stores user’s location (updates in background)
- May use data collected by compatible third-party apps and trackers
- Most third-party apps and trackers (other than WearOS) won’t submit any data to Google Fit

Extracting Google Fit Evidence

- Google Fit data is synced with Google Account
- Absolutely no additional protection
- Straightforward extraction, no passcode required
- Analysis may be more difficult than Apple: third-party data may be stored without proper standardization
- blog.elcomsoft.com/2019/01/securing-and-extracting-health-data-apple-health-vs-google-fit/

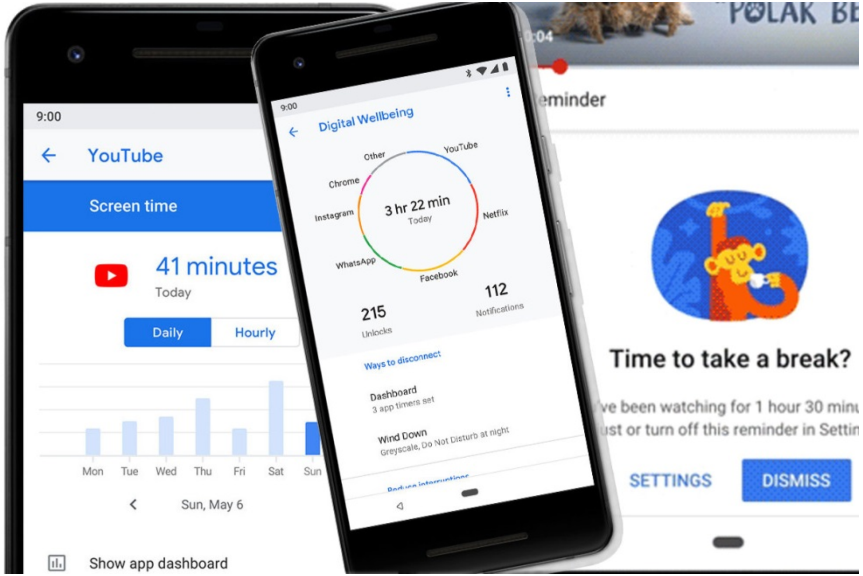
Digital Wellbeing

- Appeared in Android 9
- Google alternative to Apple Screen Time
- Available in counted few devices
- As of 2019, availability and usage of Digital Wellbeing is extremely limited



Digital Wellbeing

- General stats on app usage (per app stats)
- Restrictions on local device
- Collected information is similar (in a lesser way) to Google Dashboard
- Obtaining Google Dashboard data from Google Account supersedes Digital Wellbeing data



Google: requirements to access evidence

- All information:
  - Google Account login and password; second factor if 2FA is enabled
- Google Drive:
  - Google Account login and password; second factor if 2FA is enabled, or
  - Google Drive app token
- Synced data:
  - Google Account login and password; 2FA if enabled, or
  - Authentication token (but works for a limited set of data)

Google: risks when accessing online evidence

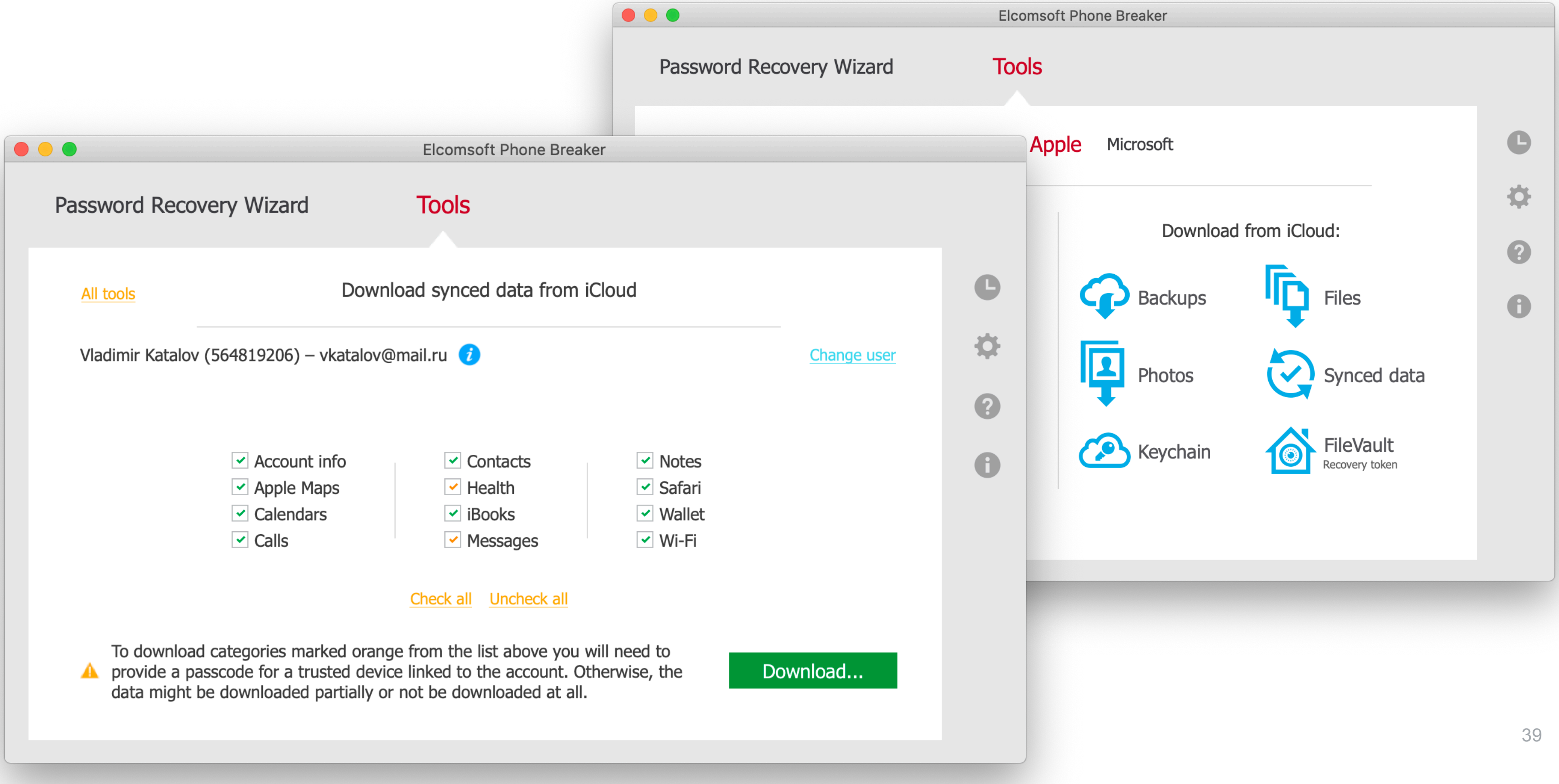
- All data, Google accounts with 2FA:
  - No known risks

- All data, Google accounts without 2FA:
  - When accessing data from another location (e.g. a different country), Google may trigger security alert, require additional authentication
  - Google may temporarily lock user’s account, require changing password

Google account access leaves notable traces on the account

Synchronized data: conclusion

- Apple and Google collect as much data as possible (and increasing)
- Most data is synchronized in real-time, sometimes once a day
- Both Apple and Google use 2FA to secure cloud access
- Apple has additional protection (device-specific anisette data)
- Apple may stop making local (iTunes) backups one day and stay with iCloud backups only
- In certain cases 2FA can be bypassed using authentication tokens
- Always collect passwords and token from desktops even if you are investigating the smartphone only
- Not all the cloud data can be provided by Apple/Google by LE requests
- Cloud acquisition can help to get data from multiple devices (including locked or damaged)
- Cloud access protocols are undocumented and frequently updated

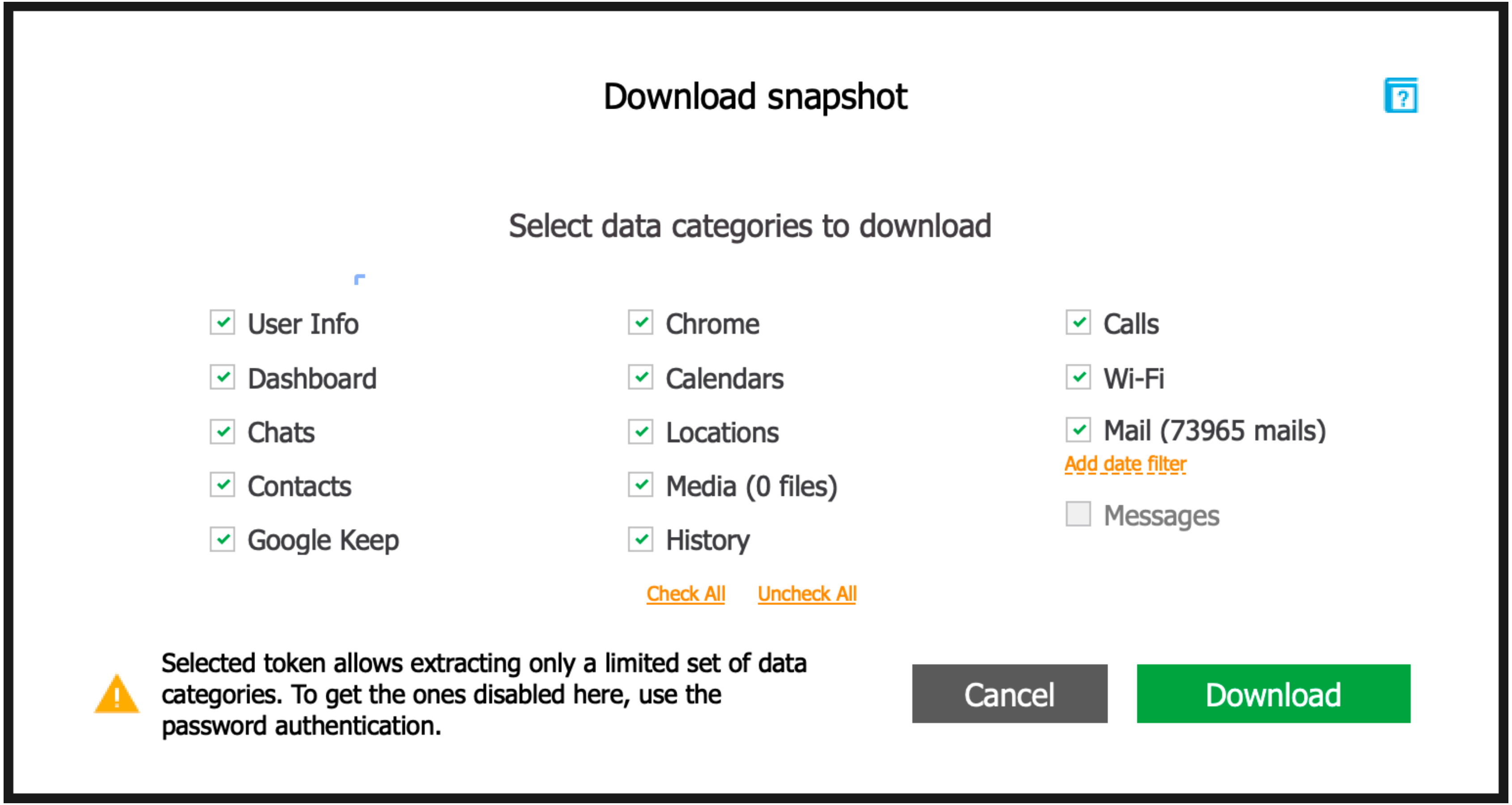


Download synced data from iCloud

Vladimir Katalov (564819206) – vkatalov@mail.ru

- ☑ Account info
- ☑ Apple Maps
- ☑ Calendars
- ☑ Calls
- ☑ Contacts
- ☑ Health
- ☑ iBooks
- ☑ Messages
- ☑ Notes
- ☑ Safari
- ☑ Wallet
- ☑ Wi-Fi

⚠ To download categories marked orange from the list above you will need to provide a passcode for a trusted device linked to the account. Otherwise, the data might be downloaded partially or not be downloaded at all.



Download snapshot

Select data categories to download

☑ User Info
☑ Dashboard
☑ Chats
☑ Contacts
☑ Google Keep

☑ Chrome
☑ Calendars
☑ Locations
☑ Media (0 files)
☑ History

☑ Calls
☑ Wi-Fi
☑ Mail (73965 mails)
Add date filter
□ Messages

Selected token allows extracting only a limited set of data categories. To get the ones disabled here, use the password authentication.

Real-time evidence

Request 60-day fully functional trial:
https://elcomsoft.com/trial.html

(c) Vladimir Katalov
ElcomSoft Co. Ltd.

http://www.elcomsoft.com
http://blog.crackpassword.com

Facebook: ElcomSoft
Twitter: @elcomsoft