Digital Hygiene Tips for Muggles and Wizards

Michael Opdenacker

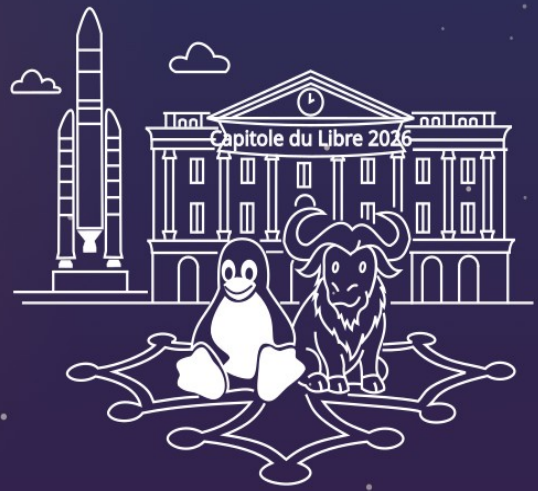
Capitole du Libre

Logiciel libre & culture libre en Occitanie

14 & 15 NOVEMBRE 2026

Samedi & dimanche · INP-N7, Toulouse

capitoledulibre.org



Michael Opdenacker

- Independent consultant, developer and trainer on Embedded Linux and Free Software
- Not a computer security specialist, but interested in the topic.
- Supporter of April (promotion of Free Software in France)



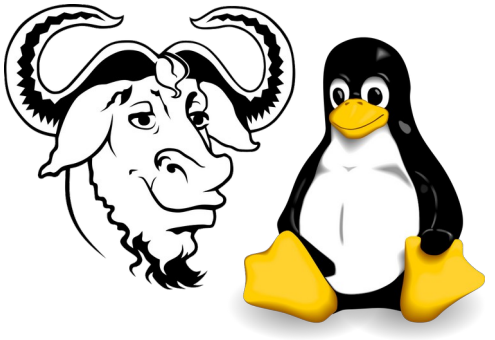


Image : https://fr.wikipedia.org/wiki/Linux#/media/Fichier:GNU_and_Tux.svg

Introduction

What for?

Goals

- To avoid fraud
- To avoid identity theft
- To preserve your anonymity, your private life.
- To avoid the theft or destruction of your data.
- To preserve your sanity

Target audience

- Myself: to question and improve my own everyday hygiene
- Muggles: all users of digital systems, whatever their experience, including users of proprietary systems.
- Wizards: more advanced users, as a reminder of good practices and information about new threats
- People reading this document


Image : https://upload.wikimedia.org/wikipedia/commons/2/28/Two_Cows_-_Alps%2C_Italy_-_About_1994_01.jpg
If something is free
You are not the customer
You are the product
Thanks to Tristan Nitot for the idea

Your data have a lot of value

- To sell targeted advertising
- To scam you
- To ransom you, to disrupt your work
- To spy on you
- To enforce the law
- To train AI models

Private data examples

- First and last names
- Date / place of birth
- Address
- Employer
- Search engine and navigation history
- Contacts
- Sport performance (smart watches)
- Health data
- Proofs of residence
- Opinions (public polls...)
- Posts, and reactions on social media
- Messages (e-mail, instant messaging...)
- Online orders
- Music, movies or applications
- Personal or professional files
- Personal credentials

The European Union specifies rights and obligations around the personal data (GDPR) :
https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

Protect your computer and phone

You find a USB flash drive...



Image : https://hak5.org/products/omg-plug

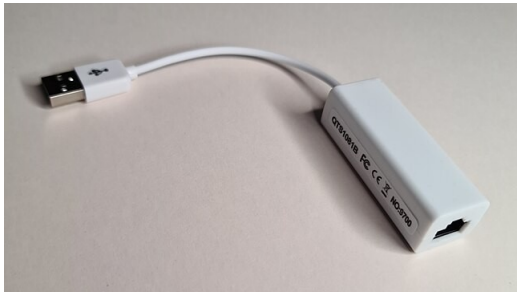
- Do you plug it in to see what's inside?
- Don't! 😱

You find a USB flash drive...





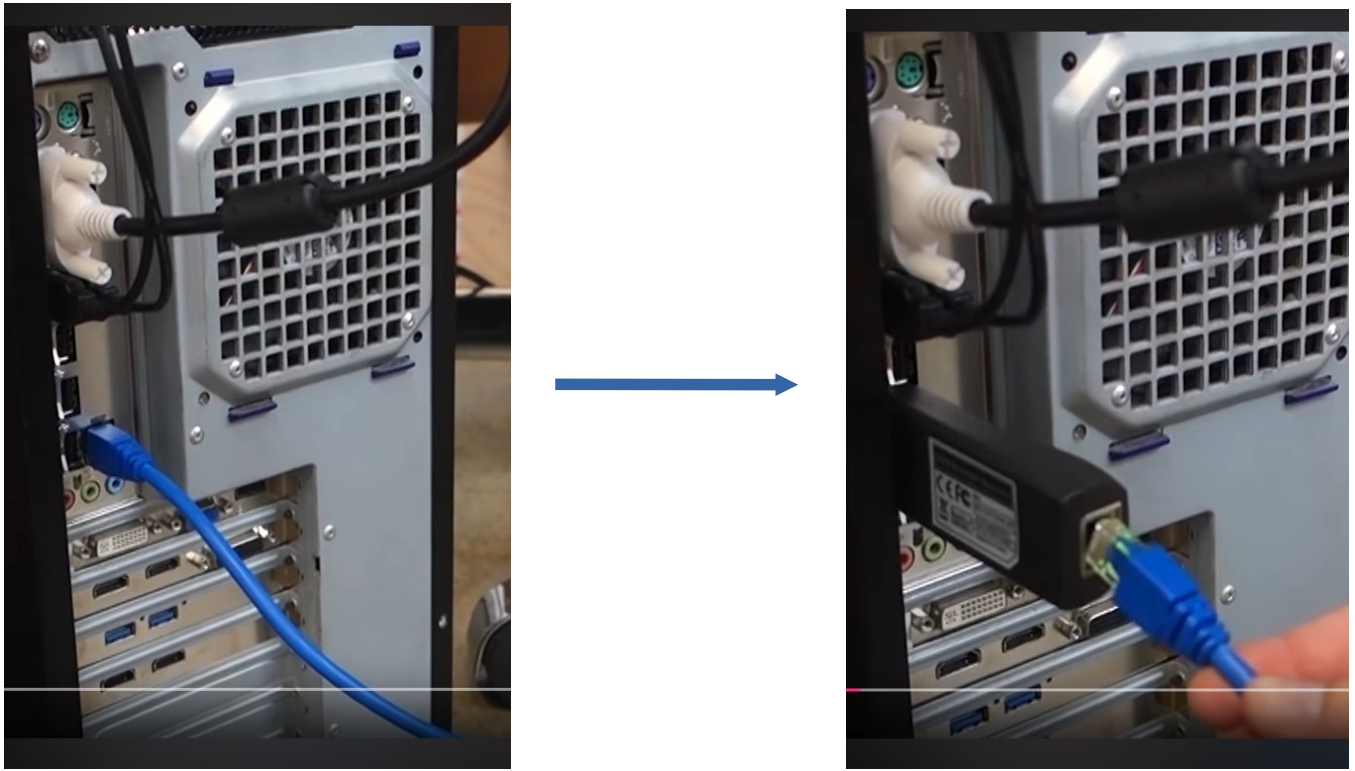




Images :
https://hak5.org/products/omg-plug
https://commons.wikimedia.org

Which is not what you expect!

One more example



Do you want to charge your phone?



- You find a USB power plug in a public place.
- It can be risky 😬

Image : https://commons.wikimedia.org/wiki/File:USB_Charging_Port_of_Jinan_Metro_Line_3_20200412.jpg

Do you want to charge your phone?





Images: https://openclipart.org
https://www.vietnam.vn

Behind the plug, you may not have a charger but a real computer which could try to steal your data.

Some advice

- Never plug in an unknown USB drive
- Avoid charging your phone or PC on a public USB plug, in a hotel or on an unknown laptop.
- Don’t let people charge their electronic cigarette on your PC. Yet another untrusted device!
- Always use your own charger or « no-data » cable.
- By the way, even an apparently plain USB cable can contain spying / hacking hardware.



Image : https://portablepowersupplies.co.uk/product/usb-data-blocker

Fry a device from USB

- « USB keys» can send high voltage pulses to fry a device (PC, phone, screen, in-flight entertainment system...).
- Threat: Denial of Service Attack (against you or public infrastructure)
- Every device with a USB port should be protected against excess voltage, but that’s far from being always the case.
- https://youtu.be/I6bRoSK39io



https://usbkill.com/

Protect your private data

Be careful with your date of birth

- Many online services ask you for your date of birth, but why do they need it? 🤨
- Don’t give them, or if you’re forced, give a fake one
- Same advice for social networks
- The date of birth is an important piece of information which can help to impersonate you.

To avoid identity theft

- As much as possible, avoid sharing copies of your identity documents and other proofs of residence.
- When you have no choice, add a watermark to the copy to restrict its usage to your recipient.
- Prefer paper copies for all sensitive documents.



Example: free watermark service from the French Government: https://filigrane.beta.gouv.fr/
They claim they remove the documents after they are downloaded.

Be careful with your resume

- Avoid giving too many personal details on your resume!
- Only keep the name and e-mail address if you share it on the Internet



S[redacted]
D[redacted]

Propose mes compétences pour un **stage en design industriel d'une durée de 2 mois**

Curieux de nature et créatif, je m'épanouis à travers mes diverses expériences, voyages et nombreuses rencontres. J'aime apprendre en essayant et en mettant en pratique de nouvelles choses ainsi qu'en partageant mes idées avec d'autres.
Sociable et résilient je sais m'adapter au mieux selon les contextes.

Etudiant en design Produit

CONTACT

s[redacted]@lecolededesign.com
S[redacted]
+33 6
1 blvd [redacted], Nantes
2004, 20 ans
Permis AM / B véhiculé

FORMATION

2022-2024 - **Diplôme de Design (Bac +5) : 2ème année**
L'École de Design Nantes Atlantique
Filière Design Produit

Juin 2022 - **Diplômé du Baccalauréat Général Mention Bien**
Lycée EIC Tourcoing
Spécialités Sciences de l'ingénieur / Numérique sciences informatiques

EXPÉRIENCE PROFESSIONNELLE

Juillet 2023 - **Travail d'été, plongeur en restauration, La Jetée,** Les sablettes
Compréhension des métiers en restauration et résilience

Ouch, this resume found on LinkedIn (anonymized) shares everything: photo, full name, birthday, e-mail and post address, phone number. A good start for identity theft!

Beware of petitions

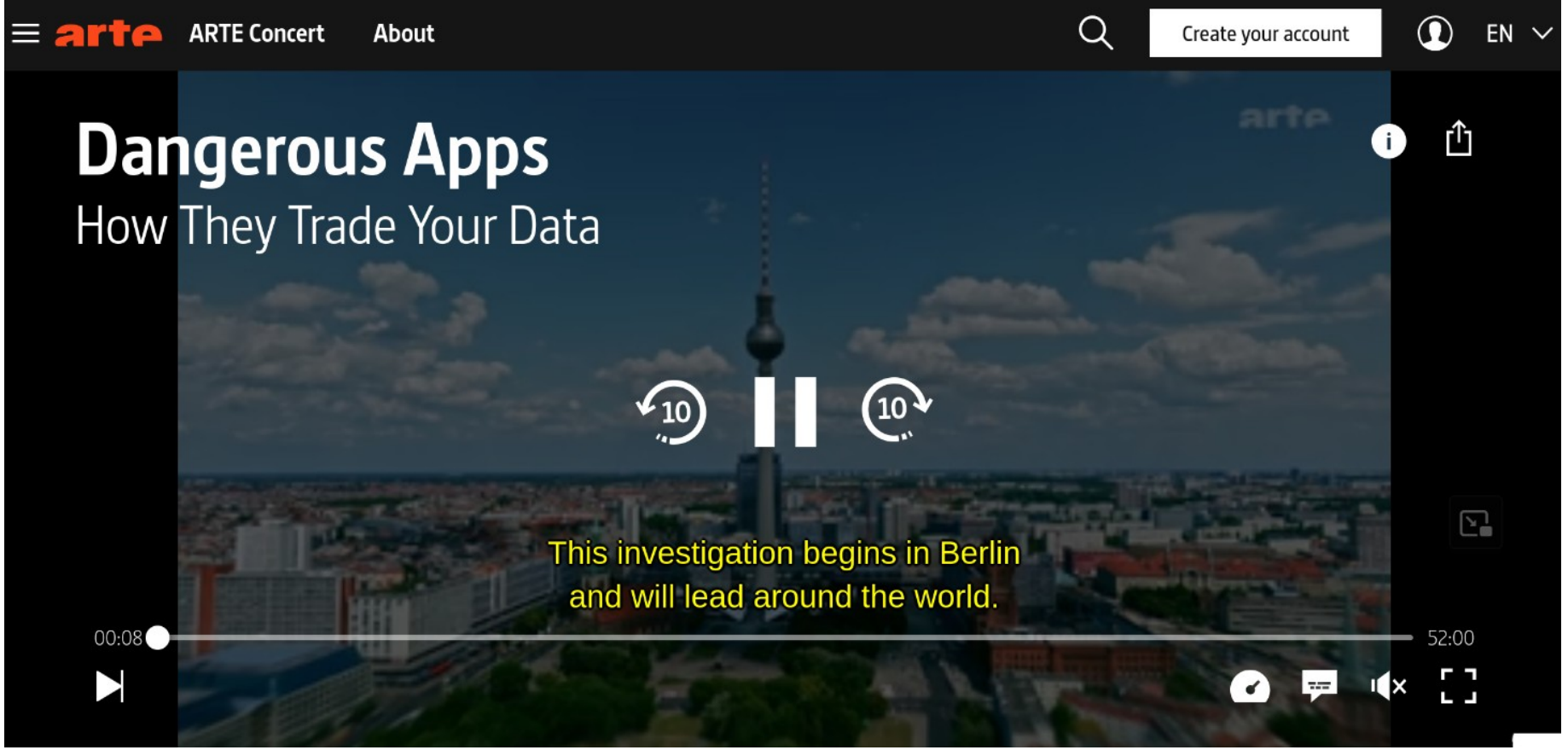
- Don’t share your opinions with untrusted organizations
- Beware of petitions managed by private companies such as Change.org
- They can build a pretty accurate profile about you from all the petitions you signed and supported. They can also be manipulated.
- To support worthy causes, better use national platforms properly guaranteeing that 1 vote = 1 person
- In France: https://petitions.assemblee-nationale.fr/initiatives
- See https://en.wikipedia.org/wiki/Change.org#Criticism

Don’t reveal more than needed

- When creating a new account, only give what’s strictly necessary
- “Security” questions: use fake answers too (record them on password managers).
  Two easy to find details like pet or parents’ names.
- Have a dedicated phone number for secure / sensitive needs (banks…). Don’t share it with your friends (will leak through their address books)

Application permissions

- Don’t grant applications more permissions than they should need for their normal operation.
- Pay attention to: location, contacts, files, network…
- Case of a weather app that was used to track millions of people, thanks to its location permissions.
- I tried to use WhatsApp without letting it access my contacts, but it didn’t want to operate correctly. That’s expected, WhatsApp belongs to Meta (Facebook), which wants to collect such information!
- Work-around on Android: run in a “shelter” with a limited view on the system (custom contact list…) - https://f-droid.org/packages/net.typeblog.shelter/



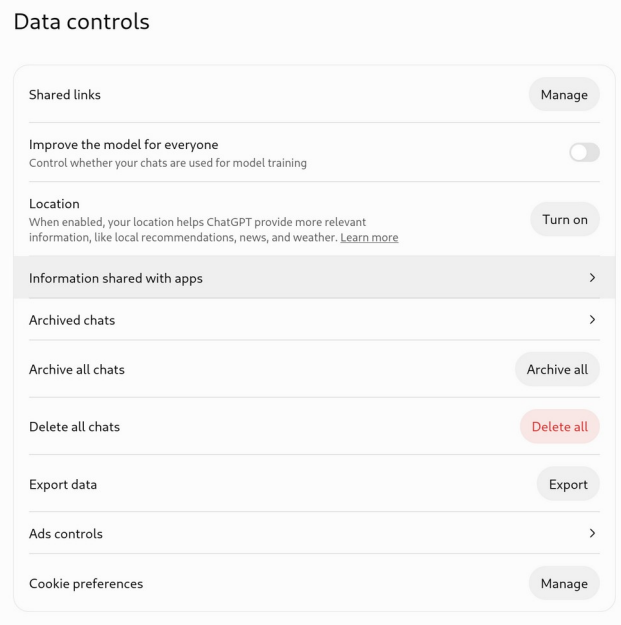
An eye-opening documentary on apps collecting and reselling your live position data.
The data are anonymous, but contain the location of your home and workplace!
Such data have been used by criminals.
https://www.arte.tv/en/videos/123951-000-A/dangerous-apps/

Beware of AI

- ChatGPT / Claude and others don’t guarantee the confidentiality of your conversations.
- It can use your information to train its models and then share it with others.
- People accessing your account could also access all your requests.
- So, don’t submit confidential information or documents to it!
- Possible to use local models instead.

AI Chat Privacy Settings

- Disable settings
  to contribute to AI training
- Good idea to delete
  your chats regularly



⚠️

ChatGPT data controls

Advice for using social networks

- We don’t mean to stop using them!
- Just be careful with data you share.
- Again, don’t reveal your birthday.
- Don’t post photos during your holidays (burglars know that your not at home).
- Don’t share pictures of others without their consent, especially with children (see the campaign on https://youtu.be/F4WZ_k0vUDM).
- Be careful too promoting events you’re participating to (again, not at home).
- Be careful with “embarrassing” photos or “too strong” opinions. Recruiters or universities are likely to look you up on the Internet.
- Idea: have two profiles – One for relatives and close friends, and a public one for sharing unsensitive information.

Beware of GAFAM

- GAFAM = Google Amazon Facebook Apple Microsoft
- These entities do their best to know as much as possible about you, in order to sell products, advertising to you and train AI models
- Example:
  - You make a search on Amazon or Google
  - You then see many advertisements on third party sites (displaying Amazon or Google ads), related to this search. Thanks to “cookies”!
  - When you browse the web on somebody else’s computer, the owner can guess which search requests you previously made, thanks to the ads that are shown.

Zoom on Google

- If you use Google Mail, you are always logged in on your browser.
- On Android, you are always identified. No way to use an Android phone or tablet without revealing your phone number (unique identifier).
- Therefore, none of your Google searches are anonymous 🤨
- This is also true for YouTube (owned by Google)
- Google tracks the location of your phone, and therefore knows which businesses you visited.
- On Android, the Google name servers (DNS) are used, instead of your ISP's. Therefore Google knows which websites you visited.
- Google Mail reads your "private" messages too (story of a father who sent pictures of his child's inflamed genitals to his doctor, Google banned him for child pornography)

My advice for using Google

- When you have no choice
- Use in private browsing mode, to avoid being identified during your normal browsing activity.
- Same for YouTube!
- Prefer the Firefox browser, designed for respecting privacy. This is not the primary goal of Google Chrome.
- Prefer Waze (Google too) which works without being identified, to Google Maps for navigation. Comaps (free software based on OpenStreetMap) is even better though it doesn’t know about live traffic.



Comaps

About Apple

- I’m not talking about Apple
  because I never use their products.
- However, even if their products have a decent reputation in terms of security, this company has very monopolistic practices, and very bad reputation in respect for the environment (planned obsolescence) and for subcontractor workers.

  https://en.wikipedia.org/wiki/Apple_Inc._and_unions#Working_conditions



Image : http://betanews.com/2014/04/07/the-apple-myth-why-security-through-obscurity-isnt-security/



Free software and open source, decentralized alternatives to the tech giants
https://offgrid.tlmb.net/2025/07/27/tarry-hardware-opinion-ep-56/

Alternatives to free centralized services



De-Google-ify Internet
https://degooglisons-internet.org/en/

Alternative search engines

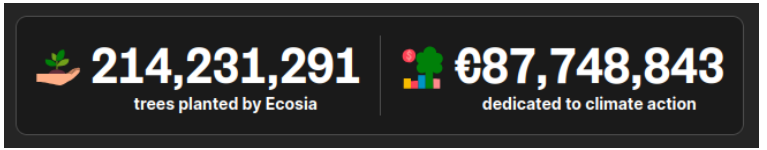
- Qwant (FR) - https://www.qwant.com/
  The search engine that values you as a user, not as a product
- DuckDuckGo (USA) - https://duckduckgo.com/

  A “meta search engine”
  Your personal data is nobody's business.
- Ecosia (DE) – https://ecosia.org/

  A search engines that plants trees
  We are in it for the trees, not your data







Alternative e-mail providers

- Proton Mail (CH) – https://proton.me
  Your data in a bunker under a mountain in a neutral country
  From 0 EUR/month for 1 GB of storage, 5 EUR for 15 GB
- Tuta (DE) – https://tuta.com
  Secure e-mail with Open Source e-mail clients
  From 0 EUR/month for 1 GB of storage, 3 EUR for 20 GB
- Posteo (DE) – https://posteo.de/en
  Secure e-mail powered by 100% green energy
  From 1 EUR/month for 4GB of storage
- Galae (FR) – https://galae.net/en/
  Secure, professional e-mail from Open Source advocates
  From 2 EUR/month for 5 GB of storage

Privacy by default

tuta

//POSTEO.

galae

Happy to be a paying customer, not a product!

Signal – Alternative to WhatsApp

https://signal.org

- Completely Open Source software
- Created by people who left WhatsApp. Funded by its founders and donations.
- All needed features, no AI bots in groups
- You don’t even need to share your phone number. A user name is enough.
- New: you can now create a Signal account without a phone number (Nov 2026: beta feature on Android)

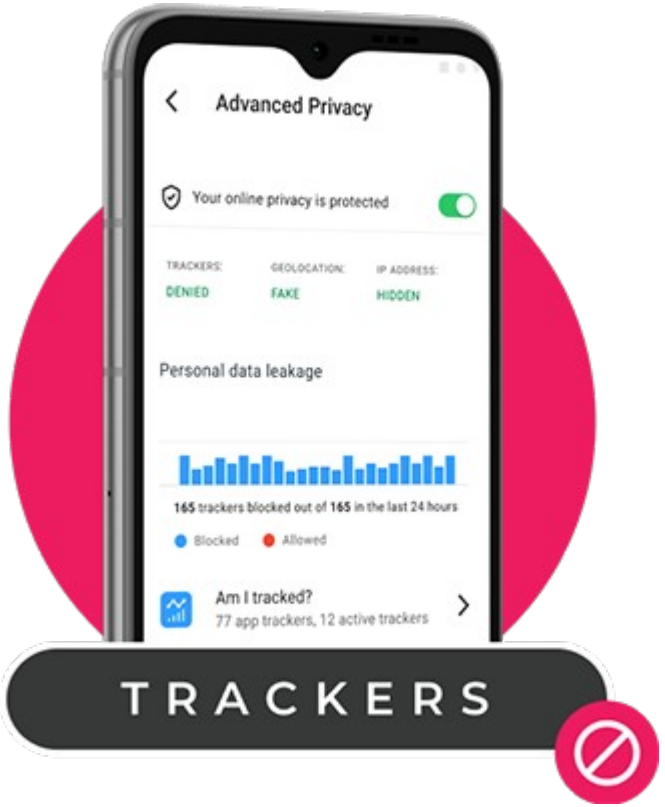


Signal

/e/OS – Degoogled Android

- Android without Google !
  Escape digital surveillance
- Many smartphones are actually supported
- An Open Source project,
  developed by Murena.io (FR)
- Alternative application store, tracker blocker, hiding IP address, fake location, and almost every Android application works flawlessly.
- Extremely satisfied after using it
  for 3 years

https://e.foundation/



But I have nothing to hide!

- And I live in a free country
- Example of the USA and abortion rights.
  Issue of the privacy of navigation history (clinics), Internet searches and data from menstruation tracking applications.
- Authorities may request to access such information to prove that an abortion happened.
- You don’t want criminals to know where / when you work and live, thanks to location tracking.

https://www.theguardian.com/technology/2024/jan/16/google-keeps-location-history-data-abortion-clinics-despite-delete-pledge

Protect your systems

Protect your computer

- Never work or browse the Internet when logged in as an administrator user. That would make it too easy to take control of your machine, if there’s a vulnerability in one of your programs.
- Create a user account for each person in your home.
- If possible, don’t use your professional computer for personal needs.

Protect your systems

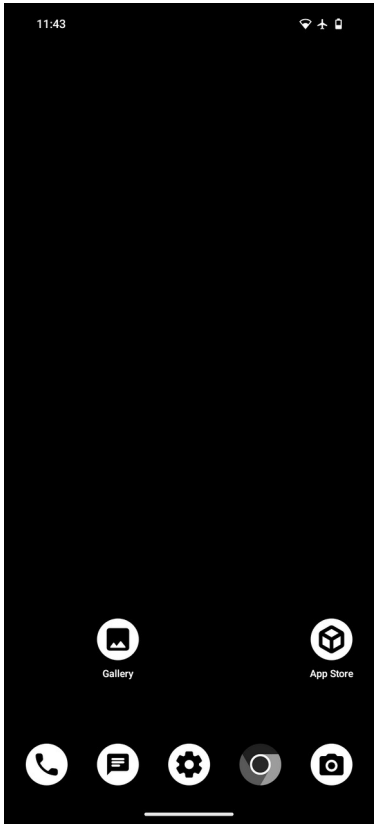
- Always keep your systems and applications up to date,
  to enjoy fixes for known vulnerabilities.
- Always download applications from their original sites or stores.
  Cracked applications can also contain malicious code
- Prefer Free and Open Source Software,
  much better protected against backdoors and malware.
- Avoid connecting to public or hotel Wi-Fi networks,
  or otherwise use a VPN to secure your connections.

Protect the data on your computers

- Encrypt your disks, especially the removable ones!
- At least encrypt your confidential files
  (a cracker getting remote access to your PC could read them otherwise)
- Don’t take computers or smartphones with sensitive data during travel abroad. Especially in some countries with strong government agencies.
- Lock your sessions automatically.
- Make backups, on encrypted disks. This also protects your data.
- Switch off or suspend your system when you are away from it (typically at night).

Protect your smartphone

- Find a strong screen locking scheme
  How to have only fingerprint unlocking?
- Disable the display of the contents of notifications when the screen is locked.
- Once again, don’t charge it with an untrusted charger, otherwise with a “no-data” cable.
- Make sure your mobile OS receives updates
  May need to switch to LineageOS, /e/OS or Graphene OS (derived from Android)



Graphene OS for the most paranoid (screenshots disabled

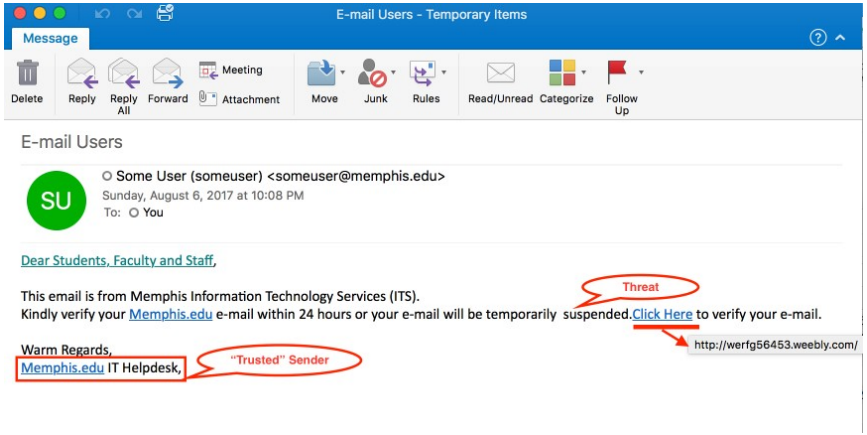
Avoid fraud

Avoid fraud

- Beware of any message or phone call involving money or some emergency.
- Before of deals that are unusually attractive.
- Beware of attachments, even from people you know.
  Don’t open them if something looks unusual.
- Be careful, an e-mail sender can be “spoofed”. The same applies to voice messages and even calls, which can be generated by AI, which can perfectly imitate someone (especially if this person has public videos).
- Do not ignore the warning and alert messages from your browser (Firefox) or e-mail client (Thunderbird), related to website or message fraud.
- Beware of people met only on-line. Crooks can impersonate a completely different person, and can be very patient to earn your trust.

Avoid “phishing”

- Refrain from following unusual links in e-mails and web pages.
- The target of the link could be different from its text. You should hover your mouse over the link to check its actual target.
- Your e-mail client should warn you if there is a deceiving difference. Thunderbird does it well.
- In case of doubt, better type the site address again by yourself, and connect without the link to double check the piece of information.



https://www.memphis.edu/its/security/phishing-examples.php

Beware of “Typosquatting”

Yet another reason not to follow hyperlinks, or to type them by yourself

A few examples (look for the trap) :

- https://www.gov.uk/
- https://support.microsoft.com

More recent: “Quishing”



Don’t trust QR codes!

Quishing = QR + Phishing

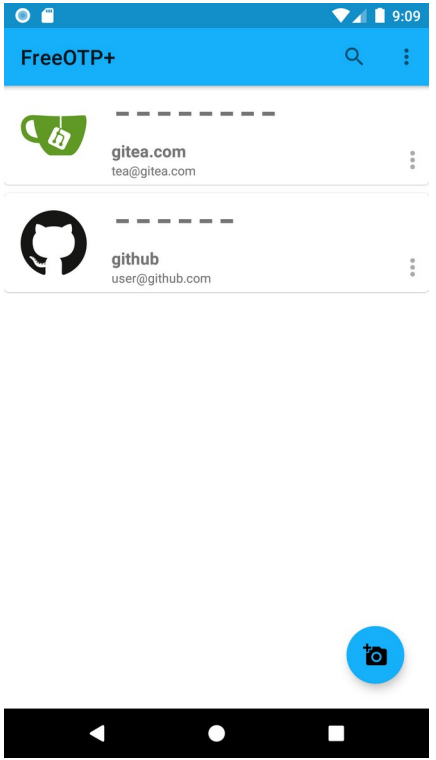
Typically on parking meters or EV charging stations

Source: https://www.20minutes.fr/high-tech/4101816-20240720-jo-paris-2024-faut-craindre-nouvelles-arnaques-faux-qr-code-pendant-jeux

Harden your credentials

Harden your credentials on the Internet

- Very important to have a different password for each service ⚠️⚠️⚠️
- Use a password manager for all these passwords
  This also helps to keep track of all your accounts!
- If possible, use a different e-mail address for each service, to make it harder to associate leaked personal information to the same person.
- Use Two Factor Authentication (2FA) whenever possible, to block any impact of password theft.
  Any “Authenticator” app will work. Prefer the Open Source ones (such as FreeOTP+) to Microsoft or Google ones.



https://haveibeenpwned.com/

- Checks whether your e-mail address was found in a data leak on the Internet.
- Example : the Deezer user database was leaked in 2022.
- Such data are now accessible, and can be used by crackers to merge the different pieces of information about you and make targeted attacks (phishing, identity theft, cracking your accounts on other sites if you used the same password or security questions).

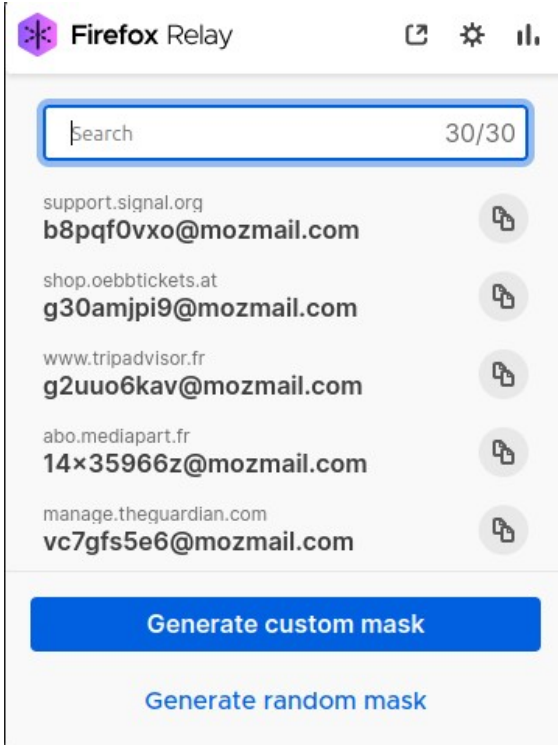
Search results on my personal e-mail address.

5 leaks were found.



Use e-mail aliases

- Several e-mail services (e.g. Proton) offer aliases that you can give instead of your real e-mail address.
- I'm using Firefox Relay, which can generate one alias per service. Cost: 1 USD/month (free up to 5 aliases)
- In some countries (USA for example), you can even have phone number aliases, to keep your number secret and avoid the same identifier in different accounts!



https://relay.firefox.com/

My Experience with Firefox Relay

Pros

- Very convenient Firefox plug-in for creating and using aliases
- “subdomain aliases” you can use without a computer: <any>@<subdomain>.mozmail.com
- Can respond to e-mail without revealing your real address.
- A way to support Mozilla

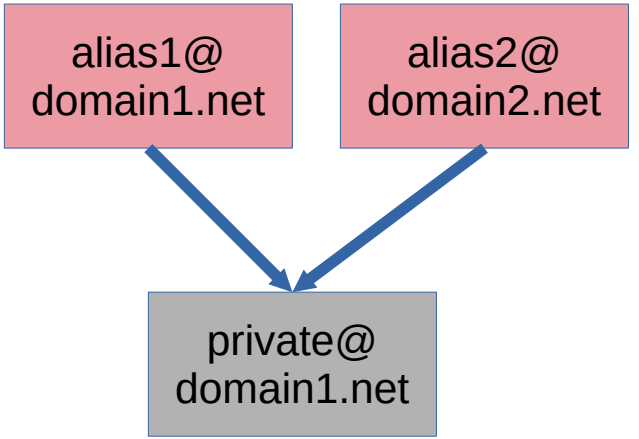
Cons

- Slower delivery than native e-mail
- Can’t change the target e-mail address 🤨
- “ugly” alias names like the ones spammers use
- You can delete subdomain aliases but they remain active. You have to “block” each you ever created.You can end up with a long list.
- Not very easy to leave the service

My Solution for E-mail Aliases

- I own my domains
- Galae (🇫🇷) is my e-mail provider
- Free Software community members, 4 EUR/month for 15 GB of storage space
- It uses Mailcow (mailcow.email) to manage e-mail on my domains

- I can very easily create and modify e-mail aliases to any of my domains.
- Aliases can be blocked too or flagged as spam
- Most aliases point to a “private” mailbox with no SMTP access that’s only used for aliases.
- Each alias appears in SoGo if I need to reply.



Cross-domain aliases are supported!

Protect your sanity

Install an ad blocker

- There are enough commercials in our everyday life, using science to distract us and influence our behavior
- Best ad blocker for Firefox: uBlock Origin https://github.com/gorhill/uBlock#ublock-origin
- It also blocks ads in YouTube
- Advise to use just one at a time

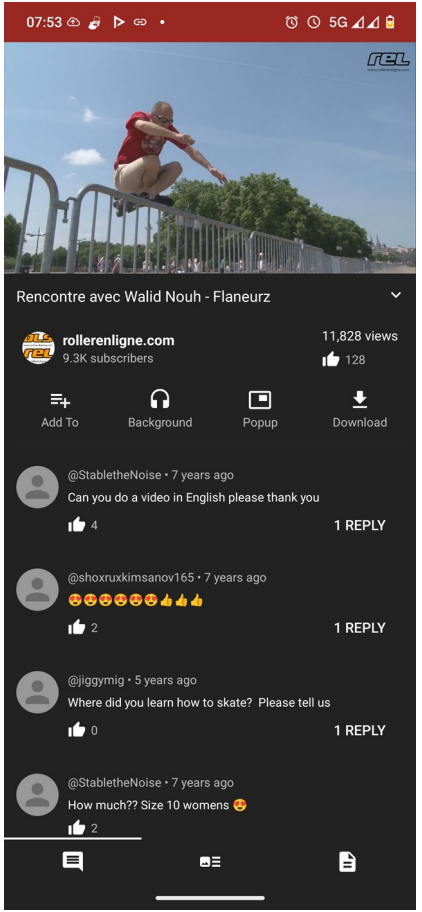


https://antipub.org/asso/manifeste-contre-le-systeme-publicitaire/ (French)

Newpipe

https://newpipe.net/

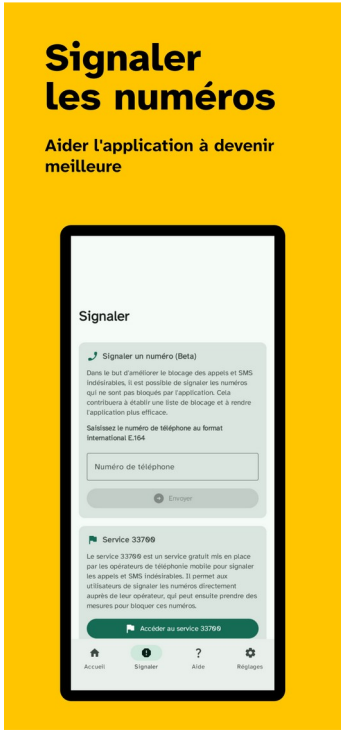
- Android application
- To access YouTube videos without as, in an anonymous way, and without feeding the algorithm with your interests
- Available in an alternative application store
- Interesting features: download media for off-line consumption, listen with the screen off, download only audio...



Block call spam

- Use call blockers
- Call Blocker (Android)
  https://f-droid.org/en/packages/com.callblocker/
- In France: Saracroche (Android and iOS)
  Let’s block call and SMS spam together!
  Made in Toulouse by the way
  https://saracroche.org/





Beware of AI

Use AI carefully

- It can reduce your cognition abilities
- It influences your opinions towards what the majority thinks
- Big environmental cost

Use an operating system and applications without built-in AI (GNU/Linux, LibreOffice...)

Resist free stuff or discounts

It can be hard!

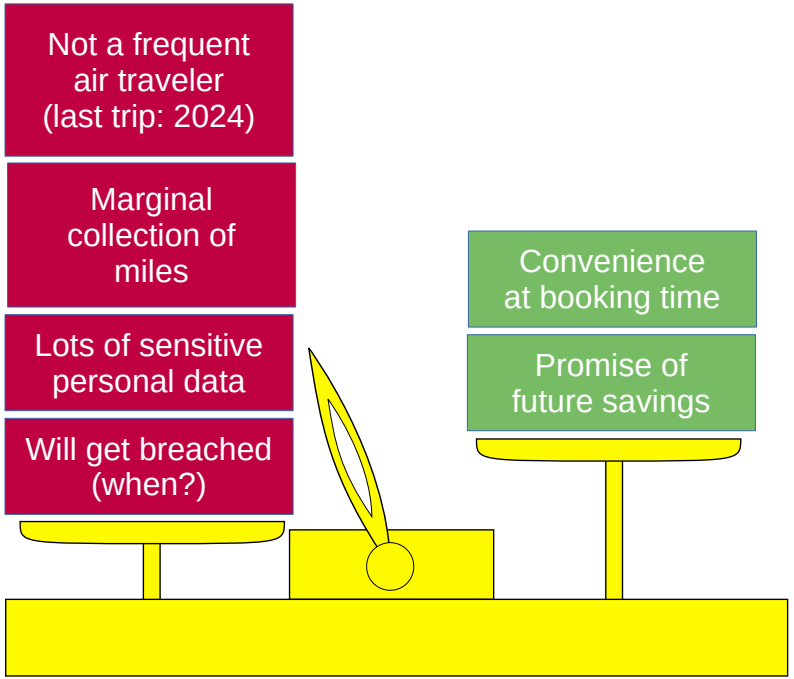
- Try to resist creating a new “customer loyalty” account, giving away personal information in exchange for minor giveaways or discounts
- In return, you get distractions, an account that may be hard to delete, or a data leak.
- You think you can outsmart this and unsubscribe, but it’s still costly for you.



Source: video capture
https://www.youtube.com/watch?v=jZclF1uGgvI
https://en.wikipedia.org/wiki/Les_Guignols

Practical Cases

Air France KLM Flying Blue

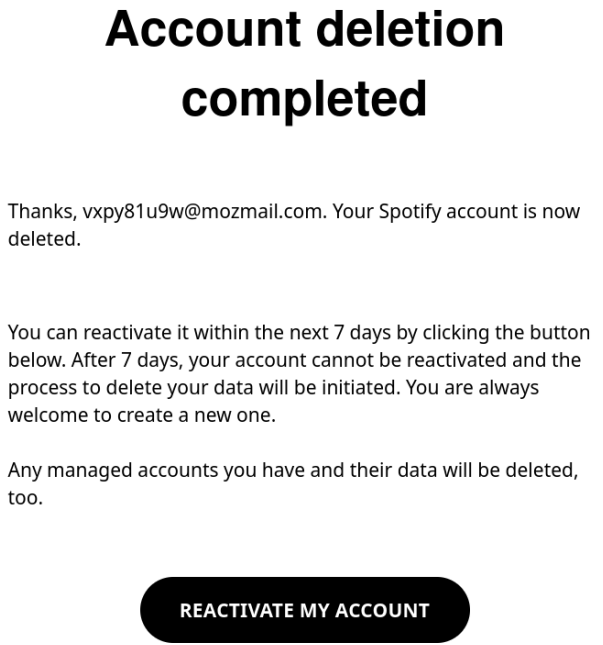


Source: https://openclipart.org/detail/23762/scale-01

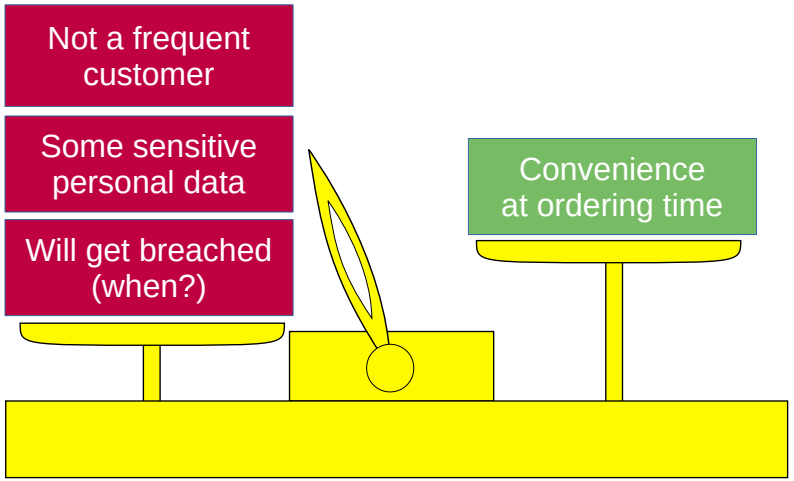
- Spent my miles on charity (Aviation Sans Frontières)
- Closed my account

Other deleted accounts

- Lufthansa (soon, but difficult)
- Spotify
  No longer in use
  Sensitive private data
  Downloaded data to keep playlists
- AirBnB
  Verified profile
- Change.org
  Contains political opinions
- Lots of unused accounts of all types (mostly merchant)



Random On-line Store



- No easy way to destroy account
- Anonymized my data:
  Dev Null, 1 rue Torvalds, 38000 Grenoble, France
  +33 605 040 302
- Deleted e-mail alias
- Imperfect solution: contact details remain in past invoices

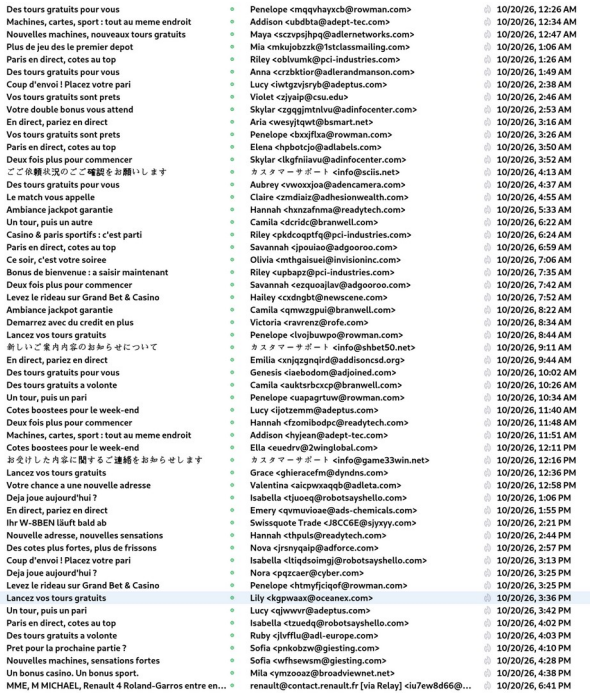
Poisoning Your Private Data

- Such data will leak anyway
- Confuse bad guys by spreading false information

- False date of birth
  (always use the same?)
- False first name
  or nickname
  (fine for deliveries)
- Next steps:
  - Secondary handwritten signature
  - PO box?

Give up 23 year old e-mail address

- Too much spam 😱
- Created a new address
  for (many new) aliases.
  Never reply from this mailbox!
- Create a new address for family
  and friends only
- Ongoing migration
  Will eventually remove old address

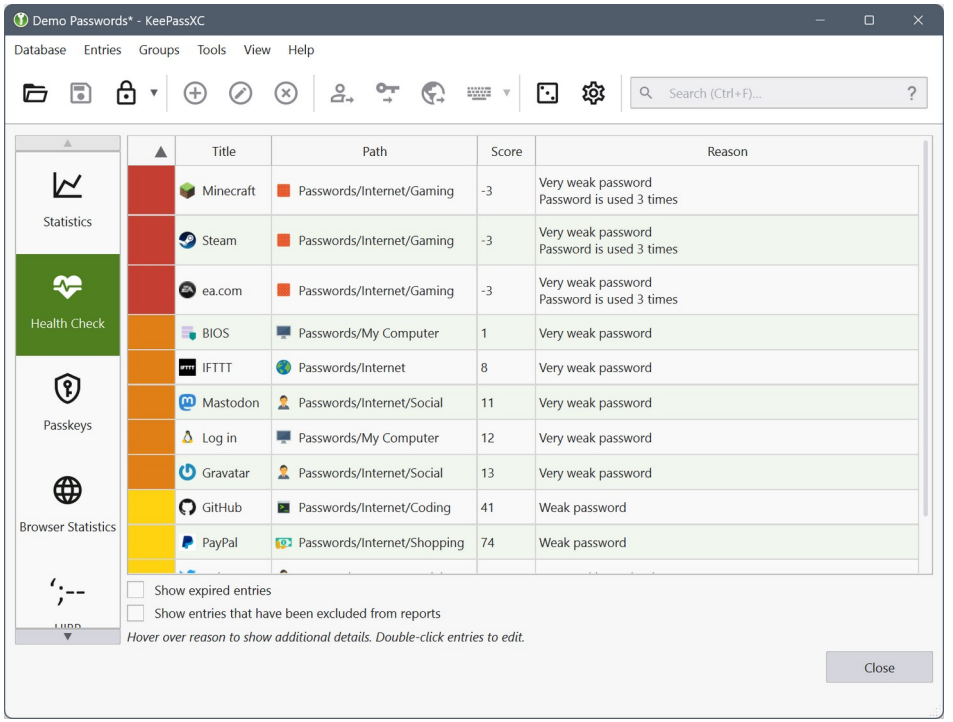


Des tours gratuits pour vous	Penelope <mqqvhayxcb@rowman.com>	10/20/26, 12:26 AM
Machines, cartes, sport : tout au meme endroit	Addison <ubdbta@adept-tec.com>	10/20/26, 12:34 AM
Nouvelles machines, nouveaux tours gratuits	Maya <sczvpsjhpq@adlernetworks.com>	10/20/26, 12:47 AM
Plus de jeu des le premier depot	Mia <mkujobzzk@1stclassmailing.com>	10/20/26, 1:06 AM
Paris en direct, cotes au top	Riley <oblvumk@pci-industries.com>	10/20/26, 1:26 AM
Des tours gratuits pour vous	Anna <crzbktior@adlerandmanson.com>	10/20/26, 1:49 AM
Coup d'envoi ! Placez votre pari	Lucy <iwtgzvjsryb@adeptus.com>	10/20/26, 2:38 AM
Vos tours gratuits sont prets	Violet <zjyaip@csu.edu>	10/20/26, 2:46 AM
Votre double bonus vous attend	Skylar <zpqgjmtnlvu@adinfocenter.com>	10/20/26, 2:53 AM
En direct, pariez en direct	Aria <wesyjtqwt@bsmart.net>	10/20/26, 3:16 AM
Vos tours gratuits sont prets	Penelope <bxxjftxa@rowman.com>	10/20/26, 3:26 AM
Paris en direct, cotes au top	Elena <hpbotcjo@adlabels.com>	10/20/26, 3:50 AM
Deux fois plus pour commencer	Skylar <lkgfniiavu@adinfocenter.com>	10/20/26, 3:52 AM
ご依頼状況のご確認をお願いします	カスタマーサポート <info@sciis.net>	10/20/26, 4:13 AM
Des tours gratuits pour vous	Aubrey <vwoxjoa@adencamera.com>	10/20/26, 4:37 AM
Le match vous appelle	Claire <zmdiaiz@adhesionwealth.com>	10/20/26, 4:55 AM
Ambiance jackpot garantie	Hannah <hxnzafnma@readytech.com>	10/20/26, 5:33 AM
Un tour, puis un autre	Camila <dcridc@branwell.com>	10/20/26, 6:22 AM
Casino & paris sportifs : c'est parti	Riley <pkdcoqptfq@pci-industries.com>	10/20/26, 6:24 AM
Paris en direct, cotes au top	Savannah <jpouiao@adgooroo.com>	10/20/26, 6:59 AM
Ce soir, c'est votre soiree	Olivia <mthgaisuei@invisioninc.com>	10/20/26, 7:06 AM
Bonus de bienvenue : a saisir maintenant	Riley <upbapz@pci-industries.com>	10/20/26, 7:35 AM
Deux fois plus pour commencer	Savannah <ezquoajlav@adgooroo.com>	10/20/26, 7:42 AM
Levez le rideau sur Grand Bet & Casino	Hailey <cxdngbt@newscene.com>	10/20/26, 7:52 AM
Ambiance jackpot garantie	Camila <qmwzgpui@branwell.com>	10/20/26, 8:22 AM
Demarrez avec du credit en plus	Victoria <ravrenz@rofe.com>	10/20/26, 8:34 AM
Lancez vos tours gratuits	Penelope <ivojbuwpo@rowman.com>	10/20/26, 8:44 AM
新しいご案内内容のお知らせについて	カスタマーサポート <info@shbet50.net>	10/20/26, 9:11 AM
En direct, pariez en direct	Emilia <xnjqzgnqird@addisoncsd.org>	10/20/26, 9:44 AM
Des tours gratuits pour vous	Genesis <iaebodom@adjoined.com>	10/20/26, 10:02 AM
Des tours gratuits a volonte	Camila <auktsrbcxcp@branwell.com>	10/20/26, 10:26 AM
Un tour, puis un pari	Penelope <uapagrtuw@rowman.com>	10/20/26, 10:34 AM
Cotes boostees pour le week-end	Lucy <ijotzemm@adeptus.com>	10/20/26, 11:40 AM
Deux fois plus pour commencer	Hannah <fzomibodpc@readytech.com>	10/20/26, 11:48 AM
Machines, cartes, sport : tout au meme endroit	Addison <hyjean@adept-tec.com>	10/20/26, 11:51 AM
Cotes boostees pour le week-end	Ella <euedrv@2winglobal.com>	10/20/26, 12:11 PM
お受けした内容に関するご連絡をおかちせします	カスタマーサポート <info@game33win.net>	10/20/26, 12:16 PM
Lancez vos tours gratuits	Grace <ghieracefm@dyndns.com>	10/20/26, 12:36 PM
Votre chance a une nouvelle adresse	Valentina <aicpwxaqqb@adleta.com>	10/20/26, 12:58 PM
Deja joue aujourd'hui ?	Isabella <tjuoeq@robotsayshello.com>	10/20/26, 1:06 PM
En direct, pariez en direct	Emery <qvmuvioae@ads-chemicals.com>	10/20/26, 1:55 PM
Ihr W-8BEN läuft bald ab	Swissquote Trade <J8CC6E@sjyxyy.com>	10/20/26, 2:21 PM
Nouvelle adresse, nouvelles sensations	Hannah <thpuls@readytech.com>	10/20/26, 2:44 PM
Des cotes plus fortes, plus de frissons	Nova <jrsnyqaip@adforce.com>	10/20/26, 2:57 PM
Coup d'envoi ! Placez votre pari	Isabella <ltiqdsoimgj@robotsayshello.com>	10/20/26, 3:13 PM
Deja joue aujourd'hui ?	Nora <pqzcaer@cyber.com>	10/20/26, 3:25 PM
Levez le rideau sur Grand Bet & Casino	Penelope <htmyfjciqof@rowman.com>	10/20/26, 3:25 PM
Lancez vos tours gratuits	Lily <kgpwaax@oceanex.com>	10/20/26, 3:36 PM
Un tour, puis un pari	Lucy <qjwvvr@adeptus.com>	10/20/26, 3:42 PM
Paris en direct, cotes au top	Isabella <tzuedq@robotsayshello.com>	10/20/26, 4:02 PM
Des tours gratuits a volonte	Ruby <jlvfflu@adl-europe.com>	10/20/26, 4:03 PM
Pret pour la prochaine partie ?	Sofia <pnkobzw@giesting.com>	10/20/26, 4:10 PM
Nouvelles machines, sensations fortes	Sofia <wfhsewsm@giesting.com>	10/20/26, 4:28 PM
Un bonus casino. Un bonus sport.	Mila <ymzooaz@broadviewnet.net>	10/20/26, 4:38 PM
MME, M MICHAEL, Renault 4 Roland-Garros entre en...	renault@contact.renault.fr [via Relay] <iu7ew8d66@...	10/20/26, 6:41 PM

All the junk mail I get in 1 day!

Reviewing All Accounts

- Having a password manager and alias manager helps!
- Request removal the ones you don’t use (example: AirBnB… lots of personal data)
- Remove or poison unnecessary data
- Make sure you use an e-mail alias
- Enable 2FA (sensitive accounts), harden passwords



KeePassXC helps review password quality

What to remember

- Share as little personal information as possible. It will leak!
- Beware of free services, of tech Giants
- Always different passwords for different services on the Internet.
- Use an operating system and applications that don’t track you

Hygiene Should Be Routine

- Like brushing your teeth!
- Take care of it before you get sick
- Bad habits come from laziness
  but cause you to waste more time in the end
- Do it a little bit every week, it’s easier

Resources

When you are attacked

- If you notice an attack or notice suspicious behavior
- Turn your device off immediately.
  Make a long press on the power button if the battery or the power supply cannot be removed.
- In France, consult https://17cyber.gouv.fr/
  to get advice and help.
- Hand your device to a specialist.
- Don’t pay the ransom
  if your files have been encrypted.



Useful resources

- In French only: very good MOOC (about 6-10 hours) https://secnumacademie.gouv.fr/
- Does anybody have a good MOOC in English to recommend?



French Podcast

Rien de Grave Patron (RDGP)

- https://rdgp.fr/
- All about privacy, individual freedom digital rights and sovereignty
- A fun way to stay informed
- By Gael Lago, Benjamin Bellamy and Aeris (here at CDL!)



P.U.R.R. Pour Un RGPD Respecté

- Aidez-nous à faire respecter nos droits numériques
- Multiples recours à la CNIL et au Conseil d'État (merci Aeris et autres membres)
- Association présente au Village des Assos
- https://asso-purr.eu.org



Thank you!

- Any questions?
- Your own experience?
- Slides available under the
  Creative Commons Attribution – Share Alike version 4 license

https://rootcommit.com/pub/conferences/2026/cdl/digital-hygiene/

Capitole du Libre

Logiciel libre & culture libre en Occitanie

14 & 15 NOVEMBRE 2026

Samedi & dimanche · INP-N7, Toulouse

capitoledulibre.org

