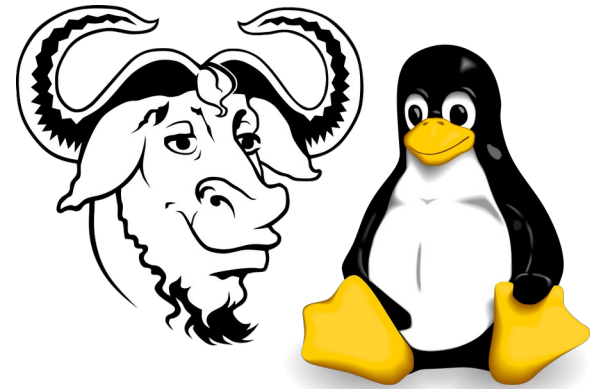


Digital Hygiene Tips for Honest People

Michael Opdenacker
September 10, 2024

Michael Opdenacker

- Independent expert on Embedded Linux and Free Software
- Not a computer security specialist, but interested in the topic.
- Living in Orange, France



What for?

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

What means?

- Protect your personal information and that of your contacts.
- Protect your computer, your smartphone and the data they contain.
- What to do in case of an attack?
- Improve your daily practice and the durability of your data.

About this presentation

- I chose not to make this presentation very well structured.
- It mixes different types of concepts and advice.
- The goal is to avoid monotony and get back to some topics multiple times.
- I don't always follow all of my own advice, but doing this research was a good booster shot to improve my everyday practice.



Thanks to Tristan Nitot for the idea!

**If something is free
You are not the
customer
You are the product**

Your data have a lot of value

- To sell targeted advertising
- To scam you
- To ransom you
- To spy on you
- To enforce the law

Private data examples

- First and last names
- Date of birth
- Place of birth
- Address
- Employer
- Navigation history
- Contacts
- Sport performance (smart watches)
- Health data
- Proofs of residence
- Internet searches
- Reactions on social media
- Posts and media 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

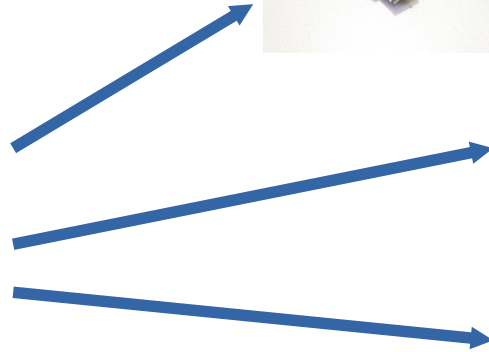
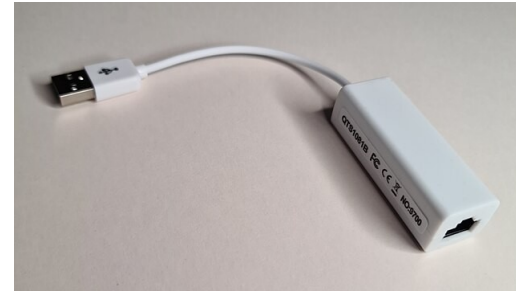
You find a USB flash drive...

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



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

You find a USB flash drive...



Which is not what you expect!

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

One more example



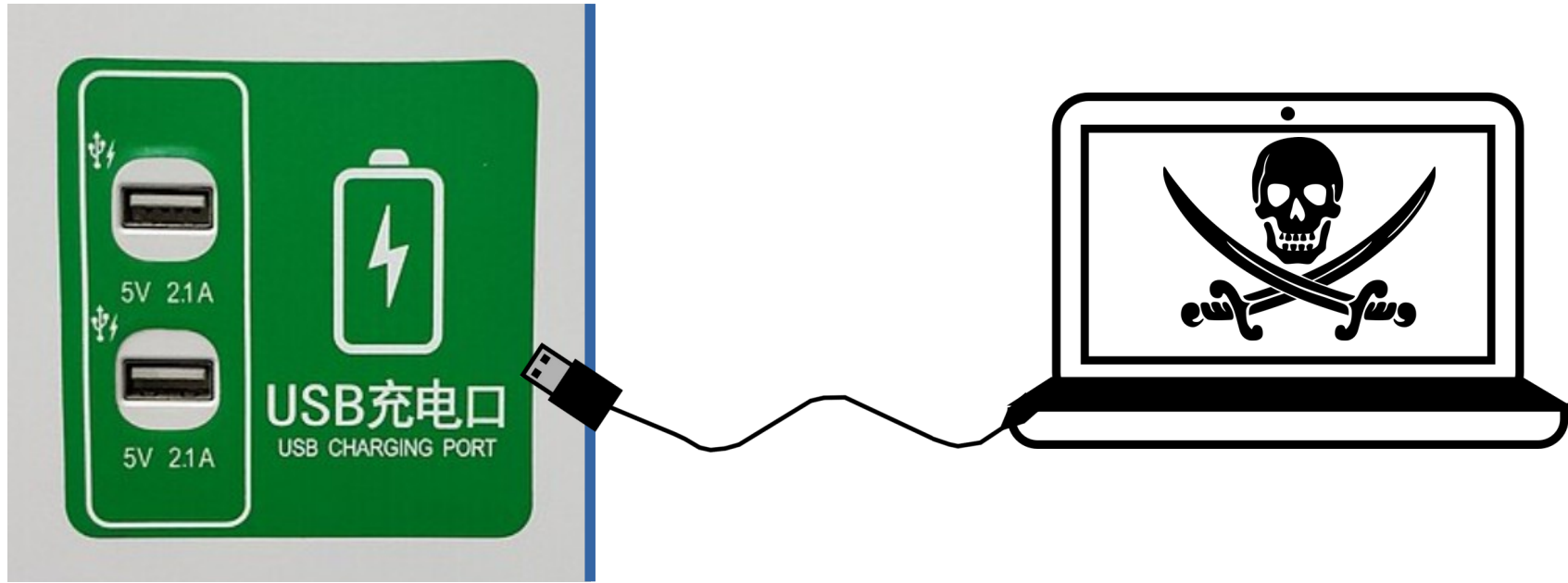
<https://youtu.be/l8YpTOv7Q2A?t=27>

Do you want to charge your phone?



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

Do you want to charge your phone?



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

Images :

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

<https://openclipart.org>

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.



Fry a device from USB

- « USB keys» can send high voltage pulses to fry a device (PC, phone, screen, in-flight entertainment system...).
- Every device with a USB port should be protected against excess voltage, but that's far from being always the case.
- <https://youtu.be/l6bRoSK39io>



<https://usbkill.com/>

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 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 (slightly) false one.
- Same advice for social networks
- The date of birth is an important piece of information which can help to impersonate you.

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



Etudiant en design Produit

CONTACT

✉ s [redacted]@lecoledesign.com

in s [redacted]

☎ +33 6 [redacted]

📍 1 blvd [redacted] Nantes

👤 [redacted] 2004, 20 ans

🚗 Permis AM / B véhiculé

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.

FORMATION

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

Jun 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 sables d'Olonne
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!

Application permissions

- Don't grant applications more permissions than they should need for their normal operation.
- Pay attention to: location, contacts, files, network...
- 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!

Beware of ChatGPT

- ChatGPT doesn't guarantee the confidentiality of your conversations.
- It can use your information to feed its "knowledge base".
- So, don't submit confidential information or documents to it!

Facebook « shadow profiles »

- Beware, Facebook knows you even when you don't have any Facebook account!
- In particular thanks to users sharing their contacts (including you) with the Facebook application.
- Hard to do anything about this. That's how these social networks can guess who you know sometimes in very unexpected ways.

Advice for using social networks

- We don't mean to stop using them!
- Just be careful with the data you share.
- Again, don't reveal your (real) birthday.
- Don't post photos during your holidays (burglars know that your not at home).
- Don't share pictures of others without their consent. In particular, be careful with children pictures, in particular yours (see the campaign on https://youtu.be/F4WZ_k0vUDM).
- Be careful too promoting events you're participating too (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 not sensitive 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 and advertising to you (or targeting you).
- 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”!
 - I don’t like to be profiled, to be predicted. I prefer neutral ads and page suggestions which can surprise me and expose me to different topics or opinions.
 - When you browse the web with friends or relatives, thanks to the ads that are shown, they can guess which search requests you have previously made on the computer.

Zoom on Google

- Many free and extremely convenient services!
- In particular 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 (which uniquely identifies you).
- Therefore, none of your Google searches are anonymous 🙄
- This is also true for YouTube (owned by Google)
- Google Mail reads your messages too.
- Google tracks the location of your phone, and therefore knows which shops or restaurants you have visited.
- On Android, the Google name servers (DNS) are used, instead of your ISP's. Therefore, even if you don't use the G search engines, Google knows which sites you visited.
- Google probably knows you better than your family, and maybe yourself 🙄
- Once again, beware of free services!

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. OsmAnd (free software based on OpenStreetMap) is even better though it doesn't know about live traffic.



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 reputations in respect for the environment (planned obsolescence) and for subcontractor workers.



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

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

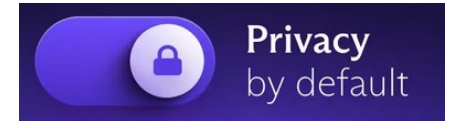
 **214,231,291**
trees planted by Ecosia

 **€87,748,843**
dedicated to climate action

Alternative e-mail providers

- Proton Mail (CH)
Your data in a bunker under a mountain
in a neutral country
<https://proton.me/>
- Tuta (DE)
<https://tuta.com/>
- Posteo (DE)
<https://posteo.de/en>

Basic offerings are free,
and then plans to have more capacity.



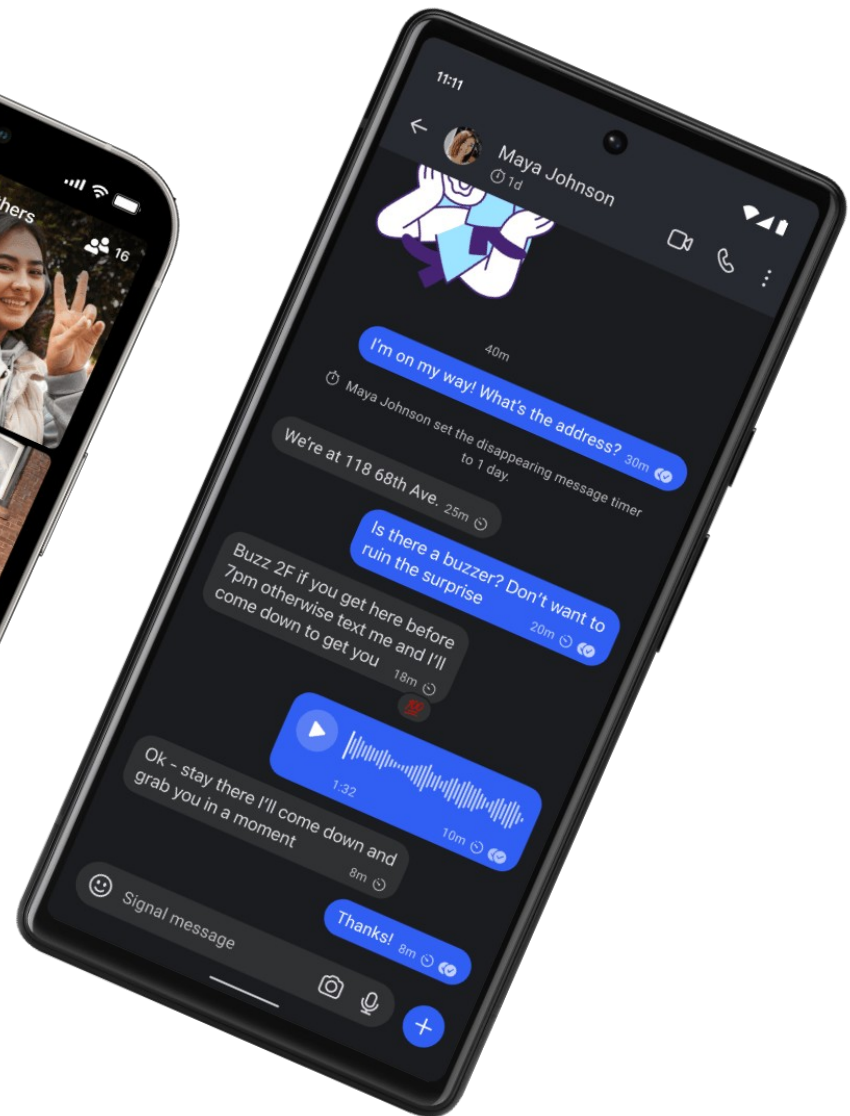
Signal – Alternative to WhatsApp

<https://signal.org>

- Completely Open Source software (client and server)
- Created by people who left WhatsApp after selling it to Facebook. Funded by its founders and donations.
- Very complete features, some may not exist in WhatsApp
- You don't even need to share your phone number. A user name is enough.
- Telegram could also be used, but...
 - The server is not Open Source, by default messages are not encrypted on the server
 - Used by all sorts of criminals and conspiracy theorists



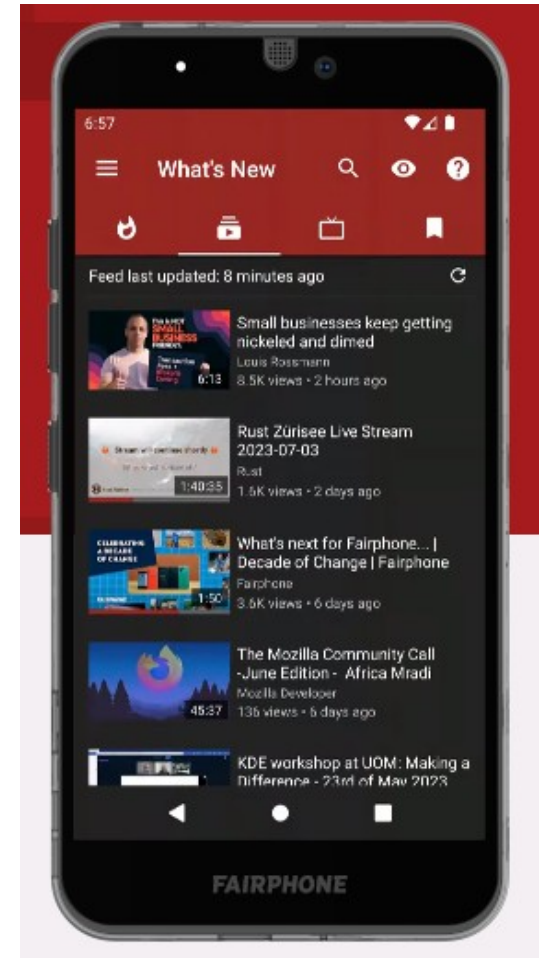
Signal



Newpipe

<https://newpipe.net/>

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



Alternatives to free centralized services



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

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.

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.
- Hacked applications can also contain malicious code
- Prefer Free and Open Source Software, often easier to secure.
- Do not connect to public Wi-Fi networks, or otherwise use a VPN to secure your connections.

Protect the data on your computers

- Encrypt your disks
- Including the removable ones !
- Also 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
- 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.

Avoid fraud

- Beware of any message or phone call involving money or some emergency. Spelling or grammar mistakes should also catch your attention.
- 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). If you have doubts, call the person back.
- Do not ignore the warning and alert messages from your browser or e-mail client, related to website or message fraud.
- Beware of people met only on-line. Many crooks will try to set you up by impersonating 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.
- In case of doubt, better type the usual site address again by yourself, and connect without the link to double check the piece of information.

E-mail Users - Temporary Items

Message

Delete Reply Reply All Forward Attachment Meeting Move Junk Rules Read/Unread Categorize Follow Up

E-mail Users

 ○ Some User (someuser) <someuser@memphis.edu>
Sunday, August 6, 2017 at 10:08 PM
To: ○ You

[Dear Students, Faculty and Staff,](#)

This email is from Memphis Information Technology Services (ITS).
Kindly verify your [Memphis.edu](#) e-mail within 24 hours or your e-mail will be temporarily suspended. [Click Here](#) to verify your e-mail.

Warm Regards,
[Memphis.edu](#) IT Helpdesk, "Trusted" Sender

<http://werfg56453.weebly.com/> Threat

Source : <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”




Quishing = QR + Phishing

Typically on parking meters
or EV charging stations

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.
- Hand your device to a specialist.
- Don't pay the ransom if your files have been encrypted.

Isolate your credentials on the Internet

- Very important to have a difference password for each service 
- Use a password manager for all these passwords
- Or store your passwords in encrypted files on your computer
- If possible, use a different e-mail address for each service, to make it harder to associate leaked personal information to the same person.

<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.

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one [service](#) doesn't put your other services at risk.



Cit0day (unverified): In November 2020, [a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums.](#) The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by [dehashed.com](#).

Compromised data: Email addresses, Passwords



Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of [personal data](#). The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles



Deezer: In late 2022, the music streaming service Deezer disclosed a data breach that impacted over [240M customers](#). The breach dated back to a mid-2019 backup exposed by a 3rd party partner which was subsequently sold and then broadly redistributed on a popular hacking forum. Impacted data included 229M unique email addresses, IP addresses, names, usernames, genders, DoBs and the geographic location of the customer.

Compromised data: Dates of birth, Email addresses, Genders, Geographic locations, IP addresses, Names, Spoken languages, Usernames

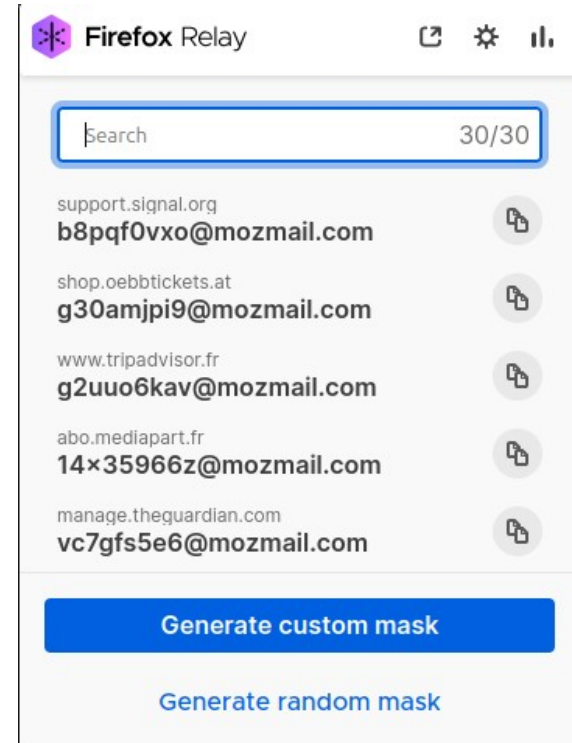


PamplIng: In January 2020, the online clothing retailer PamplIng suffered a data breach that exposed 383k unique customer email addresses. The data was later shared on a popular hacking forum and also included names, usernames and unsalted MD5 password hashes.

Compromised data: Email addresses, Names, Passwords, Usernames

Use e-mail aliases

- Several e-mail services (Proton, Gmail...) 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/>

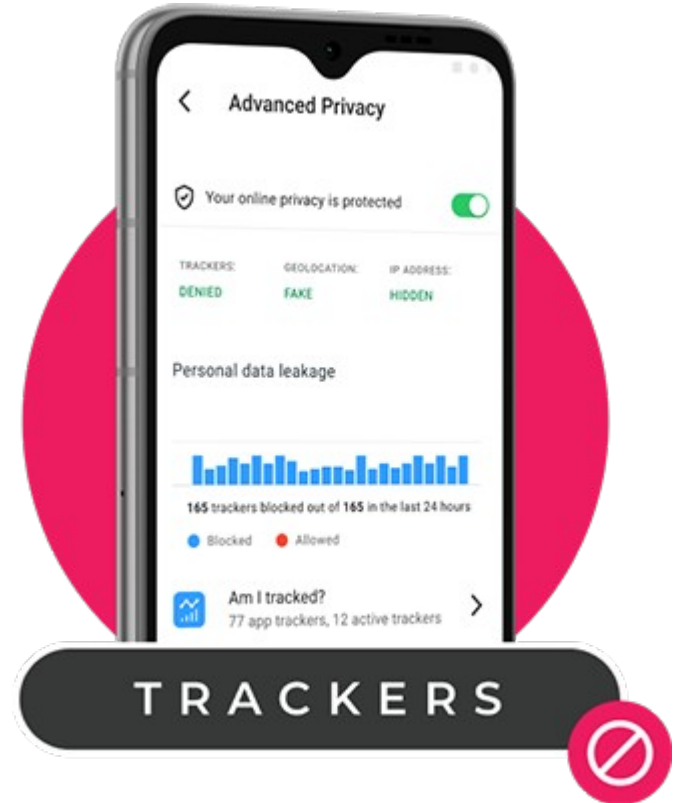
Going further

- Use a VPN to prevent your Internet Service Provider (or your government) from knowing which services you connect to.
- Use TOR too to make your connections very difficult to track.
[https://en.wikipedia.org/wiki/Tor_\(network\)](https://en.wikipedia.org/wiki/Tor_(network))
- Use GNU/Linux and Free Software instead of proprietary software. You should enjoy a stronger security and make your data last longer (not being vendor specific).

/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 (except Google Maps 🗺️).
- Extremely satisfied after using it for almost one year.

<https://e.foundation/>



What to remember

- Share as little personal information as possible
- Beware of free services, of GAFAM
- Alternatives exist
- Beware of USB devices
- Use your own USB chargers
- A dedicated account for each user on your PC
- Always different passwords for different services on the Internet.
- Be careful sharing your e-mail address
- Beware of hyperlinks and attachments
- Use an operating system that doesn't track you.

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?



Thank you!

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

<https://gitlab.com/michaelopdenacker/digital-hygiene>