6 tips to protect your privacy online

#1 Protect your identity and passwords
- Use passwordless, multifactor authentication when available
- Choose length over complexity to make your passwords stronger
- Use unique passwords and don’t share them or write them down
- Rotate passwords when suspect or know of compromise

#2 Protect your devices
- Disable your phone communications when not needed. Your phone doesn’t communicate only by voice, but also with satellites, Wi-Fi systems, and with Bluetooth and NFC devices
- Use Antimalware to protect your devices and systems, including your smartphones
- Beware of passive data collection from smartphones when choosing your Operating System

#3 Choose your applications wisely
- Accepting trackers is accepting to share your data, in particular your behaviour on the application
- Do Apps really need access to communications, address book or storage? Authorizations allow companies to accumulate data about you so limit them where possible.
- Cookies, microphone and camera access: which sites have access to these? Be mindful of what you accept to share.

#4 Make sure you are safely browsing the web
- DNS resolutions leak info about your behavior. Most browsers now give you the option to use a secured DNS
- Always use HTTPS! Some browsers allow you to enable a ‘Always use a secured connection’ setting. It will automatically upgrade to HTTPS when possible.

#5 Protect your documents
- Find out about the privacy policies of collaborative tools and cloud hosting before adoption
- Encrypt your most sensitive documents before uploading them

#6 Do some housekeeping
- Make a periodic review of your settings and reset provided authorizations in particular for browsers cookies and access to GPS, microphone and camera
- Check for credentials leakage for instance on Have I been pwned https://haveibeenpwned.com/