Resources random

Quelques ressources random pour l'école ou autre.

- Mes outils
- SwilaPass - Bypassing Firewall avec un RPi
- Outils pratiques pour les étudiant·e·s
- Bash tricks
- Bash cheat sheet
- Running Android apps on Linux
- KeePass Guide [EN]
- Setting up email with PGP encryption (Android and laptop)

Mes outils

> Tous les outils listés sur cette page sont open-source si pas libre sauf ceux mentionné avec l'émoji "⚠"

Web tools

Nom	Description	Instance
Hedgedoc	Pour créer des documents collaboratifs en MarkDown	demo
BookStack	Pour créer des synthèses, les organiser et les partager (le site sur lequel vous êtes)	ce site
SearxNG	Un meta-moteur de recherche qui permet d'accéder sans tracker à Google ou autres sites	searx.be
torrents-csv et torrent9	Pour télécharger des ISO Linux	
⚠ Discord	Le serveur de l'école est vraiment incroyable	HELMo
⚠ ChatGPT	Pour poser certaines questions pour les cours et obtenir des réponses à revérifier et prendre d'énormes pincettes) → je considère de le remplacer par HuggingChat qui est open-source	
Invidious	Une front-end alternative à YouTube légère pour voir des vidéos sans pubs, les télécharger, etc	*self-hosted sur mon ordi*, YewTube
Wireguard VPN	Un VPN pour bypass les restrictions du swilawall	*self-hosted*
Forgejo	Une service pour héberger des répo Git simplement	Codeberg
Mermaid	Un outil pour créer simplement des diagrammes de tout types (très utiles pour les cours d'algo, analyse et POO)	mermaid.live

Extensions (Firefox)

Nom	Description
UBlock Origin	Le king des extensions, le meilleur bloqueur de pub tout navigateur confondu
SponsorBlock	Bloque les sponso vidéos sur YouTube et Invidious mais signale égalemnet les chapitres, les intros, outro, etc
Snowflake	Participe au bridge snowflake pour TOR qui permet de contourner la censure
ViolentMonkey	Création et utilisation de user scripts (JS), j'ai fait mon générateur de mot de passe avec
Dark Reader	Dark mode (+ customisation supplémentaire) sur toutes les pages
Stylus	Ajouter son propre CSS custom sur les sites (comme des user scripts, sauf que c'est des user styles)
ToS Tl;dr	Donne un résumé sur les politiques d'utilisations des sites sur lesquels on va en leur donnant un score
Tridactyl	Permet de naviguer sur internet avec uniquement le clavier simplement avec les raccourcis de vim
LanguageTool	Un correcteur orthographique dans le même style que Grammarly mais open-source et respectueux de la vie privée. Corrige la grammaire, l'orthographe et un peu le style

Ricing

Outil	Description
`bspwm`	Un tiling window manager avec une configuration très simple
`sxhkd`	Un gestionaire de raccourcis de clavier (qui va avec bspwm)
`picom-animations-git`	Un compositeur avec des animations sympatiques
`polybar`	Une bar d'information de système
`pywal` et `feh`	Une synchronisation des couleurs avec le fond d'écran
`alacritty`	Un terminal assez simple et sympa écrit en Rust

Setup

Catégorie	Outil(s)
Hardware	ThinkPad E15
OS	Arch Linux
Navigateur	Hardened Firefox et Tor Browser
Sécurité 2OT	NitroKey ou Aegis
Transmission	Pour télécharger des torrents d'ISO Linux
Editeur de code	Eclipse pour Java et Helix pour le reste
Gestion de SGBD	DBeaver (comme DataGrip)
Youtube Download	`yt-dlp`

Serveur

Nom	Description
Docker	Pour gérer simplement les différents services sur mes serveurs
Portainer	Un panel d'administration pour Docker
Traefik	Un reverse-proxy créé pour Docker

Téléphone

Nom	Description
F-Droid	Comme le playstore mais uniquement pour des applications open-source
Aurora Store	Une front-end alternative au PlayStore
Signal	Alternative à Whatsapp
Fennec	Navigateur web
KISS Launcher	Launcher Android
TrebleShot	Local file sharing
Termux	Terminal sur mobile

SwilaPass - Bypassing Firewall avec un RPi

> Si tu veux faire ce tutoriel sur autre chose qu'un rpi, vérifie que le kernel (`uname -r`) est une version au délà de 4.19

J'ai mis à jour ce tutoriel pour fonctionner avec le projet `wg-easy` pour avoir une sympatique interface pour gérer les différents clients du VPN (et aussi simplifier l'installation)

Dans ce tutoriel:

- Configurer un raspberry PI sans écran, clavier ou souris à connecter dessus (headless)
- Ouvrir les ports d'un modem
- Installation de Docker sur un serveur Debian/Raspbian
- Installation de wg-easy sur Docker (wg-easy contient wireguard en plus d'une interface pour y accéder simplement)
- Ajouter et configurer des clients Wireguard sur PC et téléphone

□□ Matériel requis

- Un ordinateur
- Un raspberry Pi (dans ce cas, un Rpi4)
- Une carte micro SD (et un adaptateur pour l'ordi si besoin)
- Une alimentation pour le raspberry
- Un cable éthernet pour une connection optimale

□□ Préparation du raspberry

- D'abord il faut installer l'OS de raspberry, dans ce cas ci, on va utiliser rpi-imager pour l'installer sur la micro SD et on va choisir *Raspberry Pi OS Lite*.

```
yay rpi-imager
sudo rpi-imager
```

- Dans l'installateur, sélectionne `Raspberry Pi OS Lite` pour l'OS, puis ta carte micro SD, puis va dans les paramètres et configure le.
- Brancher le Raspberry Pi et attendre un peu, ensuite se connecter via SSH: (avec le mot de passe choisi dans l'étape précédente)

```
ssh pi@raspberrypi
```

□□ Préparation du réseau

- Trouve l'addresse privée de ton raspberry pi

```
hostname -I
```

- Va sur `http://192.168.1.1` et connecte toi (les identifiants sont souvent écrit derrière le modem)
- Va dans la redirection des ports et ajoute la règle suivante:

Protocol	Début du port externe	Fin du port externe	Port interne	Hôte interne	Nom
`UDP`	`53`	`53`	`53`	`<ip locale du raspberry pi>`	`wireguard`

□□ Installation de Docker

Pour installer docker on peut utiliser les commandes suivantes :

```
sudo mkdir -p /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/debian/gpg | sudo gpg --dearmor -o /etc/apt/keyrings/docker.gpg
echo   "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg]
https://download.docker.com/linux/debian \
  $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt update
sudo apt install docker-ce
sudo systemctl start docker
```

Installation de wg-easy

Maintenant vous pouvez simplement lançer le bloc de commandes suivant pour automatiquement installer Wireguard (une petite interface web en prime) :

```
read -p "Le mot de passe pour l'administration de votre VPN: " PASSWORD
sudo docker run --name wg-easy -d \
  -e WG_HOST=$(curl ifconfig.me) \
  -e PASSWORD=$PASSWORD \
  -e WG_PORT=53 \
  -e WG_DEFAULT_ADDRESS=192.168.215.x \
  -p 53:51820/udp -p 51821:51821/tcp \
  --restart unless-stopped \
  --cap-add=NET_ADMIN \
  --cap-add=SYS_MODULE \
  --sysctl="net.ipv4.conf.all.src_valid_mark=1" \
  --sysctl="net.ipv4.ip_forward=1" \
  weejewel/wg-easy
```

> Note: Vous devez juste être sur qu'il n'y a pas de firewall et si il y en a un, que les ports 53 et 51821 soit accessibles.

> Je vous invite vivement de transformer cette commande en Docker-Compose comme vu dans Utiliser Docker Compose

⚙ Configurer les clients

Maintenant il suffit d'installer Wireguard sur son téléphone et son ordi. Puis d'aller sur le lien `http://ADDR_LOCALE_DU_RPI:51821` et se connecter.

Une fois dans le panel, il suffit de cliquer sur "New" puis donner un nom à l'appareil. Ensuite on peut afficher son QR code ou son fichier de configuration qu'il suffit d'ajouter dans l'application.

Sur Linux il faut l'ajouter dans `/etc/wireguard/wg0.conf` en ayant `wireguard-tools` installé. Ensutite on peut lançer `sudo systemctl start wg-quick@wg0` pour démarrer le VPN.

Et c'est tout !

Outils pratiques pour les étudiant·e·s

Ceci est une petite liste des outils que j'utilise pour mes études et qui pourrait peut-être vous intéresser aussi

Bookstack

C'est le logiciel du site sur lequel vous êtes. Je l'utilise pour écrire mes synthèses (et d'autres trucs aussi) et les partager. Il a pas mal de gros avantages :

- Très facile d'utilisation
- Fonctionne avec Markdown et avec une prévisualisation en temps réel et une sauvegarde automatique
- Chaque page a une historique qui permet de revenir en arrière dans les révisions
- Possibilité d'ajouter des fichiers en pièce jointe aux pages
- Possibilité d'ajouter des tags sur chaque page
- Chaque page a une catégorie (son livre) mais peut aussi avoir 2 catégories supplémentaires (les étagères et les chapitres)
- On peut rechercher dans toutes les pages en même temps
- On peut customiser le site pour y ajouter de nouvelles fonctionnalités simplement (par exemple pour y ajouter un support pour MathJax pour générer des équations mathématiques $\frac{\Delta x}{\Delta y}$)
- On peut créer des templates de pages
- On peut facilement naviguer sur chaque page avec le menu de navigation de la page, et celui du livre (à gauche), les pages précédentes et suivantes (en dessous)
- On peut ajouter des commentaires sur les pages (en dessous)
- On peut exporter les pages sous différents formats (à droite)
- On peut gérer les permissions de chaque étagère, livre, chapitre ou page assez précisément
- Il a une très bonne API, on peut donc automatiser le transfert des pages facilement pour migrer depuis ou vers BookStack
- Permet aussi d'ajouter des webhooks, et donc de se connecter à différentes plateformes (tel que Discord) ou de créer des scripts plus automatisés sur base d'évènements précis
- On peut aussi créer des rôles personnalisés et gérer finement les permissions. Ce qui permet de donner l'impression d'un site différent pour chaque groupe d'utilisateur·ice·s

Désavantages :

- Il nécessite d'être installé sur un serveur, il faut donc un serveur et un peu de connaissances pour l'installer (ou utiliser celui de quelqu'un d'autre)

HedgeDoc

C'est aussi un logiciel de site, mais qui lui a une instance publique, qui permet d'éditer des documents Markdown à plusieurs et en temps réel.

Avantages

- Facile d'utilisation
- Système de permission facile à comprendre
- Support pour différents types de diagrammes et équations mathématiques par défaut
- Prévisualisation en temps réel
- Possibilité d'exporter en différents formats
- Possibilité de générer une présentation à partir du Markdown (diaporama)
- Possibilité de mettre en ligne des images ou d'intégrer des vidéos

Désavantages

- Les diagrammes ne sont vraiment pas beaux (opinion personnelle) et relativement peu lisible
- La prévisualisation est assez peu fluide

Mermaid Live

Mermaid est la syntaxe que HedgeDoc utilise pour générer les diagrammes, mais il y a un site qui s'appelle mermaid.live qui permet de créer ces diagrammes avec une prévisualisation en temps réel et un affichage beaucoup plus beau

Avantages

- Facile d'utilisation (lien direct avec la documentation, des exemples en un clic)
- Beaucoup plus beau
- Les URL encode tout le code des diagrammes, ainsi en prenant l'URL d'affichage et en remplaçant `view` par `edit` on peut retrouver le code source ce qui plus tôt pratique
- Plein de diagrammes disponibles (séquences, classes, Gantt, Flow, State, MLD, user journey, Git, pie et mind map)

Désavantages

- N'est pas collaboratif

Bash scripting (les lignes de commande)

Savoir utiliser le terminal est perçu par beaucoup comme étant presque un superpouvoir, car on peut automatiser toute une série de choses. Les possibilités sont globalement illimitées, mais je vous recommande très fort de les utiliser sur Linux ou a la limite macOS parce que sinon vous allez être dégouté si vous le faites sur Windows.

Voici *quelques* chose que l'on peut faire avec des commandes bash *de base* :

- Automatiser des requêtes à des API avec `curl`
- Rechercher une chaine de caractère ou un pattern dans une série de fichiers avec `grep` et `find` ou `rg`
- Modifier quelque chose dans une liste de fichiers selon une regex avec `sed`
- Extraire des informations d'un/plusieurs fichiers avec `grep`, `awk` et `jq`
- Archiver des sites entiers avec `wget`

Pour vous rassurer, vous ne devez pas *tout* connaître, car ce n'est simplement pas possible, chaque commande est un programme à part entière, et chaque commande a son propre manuel. Le tout est de savoir quel outil utiliser et comment les combiner ensemble.

DBeaver

Bash tricks

- Centraliser toutes les images dans un dossier récursivement sans override, sans doublons, et sans charactères étranges (en option peut aussi supprimer les originaux)

```
# Repeat the following process for every file format you wish (.jpg .JPG .png .PNG)

# For each .JPG file found, copy it to temp-photos/ directory verbosely and avoid override by renaming files with a numbered backup suffix
fd \.JPG$ -X cp -v --backup=numbered "{}" temp-photos/

# Go in the directory and remove any duplicate files
cd temp-photos/
fdupes . -dI

# Rename all files to remove the weird suffix name to a proper filename (+ verbose)
rename -vo .JPG.~1~ 1.JPG *
rename -vo .JPG.~2~ 2.JPG *
rename -vo .JPG.~3~ 3.JPG *
rename -vo .JPG.~4~ 4.JPG *

# Last check to avoid weird filenames, ideally that should respond nothing
ls *~

# WARNING only do this if you're really sure → will delete all the original files after the copy (+ verbose)
cd ..
fd --exclude temp-photos/ \.JPG$ -X rm -vf "{}"
```

- Convertir toutes les images d'un dossier d'un format à l'autre

```
# This is an example that convert all .JPG files to .avif files

# WARNING might reduce image quality or make the file unreadable by some systems
cd temp-photos # Will get back on the new directory
fd \.JPG$ -x convert -verbose "{}" "{}.avif" # Will convert all .JPG files to .avif files
rename -vo .JPG.avif .avif *.JPG.avif # Will change file extensions to something less weird
rm -vf *.JPG # Will remove all the precedent files to spare space
```

- Shrink the file size of a video by re-encoding it (it can sometimes go as far as a x10 times smaller)

```
# You might want to switch the codec to VP-9 for even crazier results
ffmpeg -i input.mkv -vcodec libx265 -crf 28 output.webm

# To make sure the result video is uploadable on social media with a preview
ffmpeg -i output.webm -pix_fmt yuv420p output-discord-friendly.mp4
```

- Download a youtube video (or even playlists, channels, or content from pretty much any platform)

```
# Download the resource(s) in best format
yt-dlp <link>
# List available formats
yt-dlp <link> -F
# Pick a format to download
yt-dlp <link> -f <format>
```

- Scan the current directory recursively to know where are the biggest resources that take space

```
ncdu
```

- Download all files attached with a Discord message from the HTML code

```
cat message.html  | grep -Po 'https://cdn.discordapp.com/attachments/.+?(?=")' | xargs -I{} wget "{}"
```

Bash cheat sheet

GPG

- Générer une clé plus courte

```
gpg --full-gen-key --expert
# choose 9 then 1 then answer the following equestions
```

- Modifier une clé pour supprimer la passphrase

```
gpg --edit-key <KEYID>
passwd
# laisser vide
# puis confirmer le choix 2 fois
```

- Modifier le pinentry (le popup de demande de mot de passe pour être en full terminal)

```
echo "pinentry-program /usr/bin/pinentry-tty" >> ~/.gnupg/gpg-agent.conf
gpg-connect-agent reloadagent /bye
```

- Lister toutes les clés

```
gpg -k # liste toutes les clés
gpg -K # liste toutes NOS clés (privées)
```

Git

- Ajouter une config git pour seulement un repo (+ signature)

```
git config user.email "votre@email"
git config user.name "votre nom"
git config user.signingkey <keyid>
git config commit.gpgsign true # autosignature des commits
```

Running Android apps on Linux

Configuring and running Waydroid

```
# Installing, setting up and running the linux-zen (a kernel that includes the necessary modules for Waydroid)
sudo pacman -S linux-zen
sudo grub-mkconfig -o /boot/grub/grub.cfg
reboot

# Installing waydroid and configuring it
yay waydroid
sudo waydroid init
sudo sed -i 's/ro.hardware.gralloc=gbm/ro.hardware.gralloc=minigbm_gbm_mesa/g'
/var/lib/waydroid/waydroid_base.prop
sudo systemctl enable --now waydroid-container

# Installing libndk to be able to properly install apps
git clone --depth=1 https://github.com/casualsnek/waydroid_script.git
cd waydroid_script
python -m venv .venv # creating a virtual env to install python dependencies
.venv/bin/pip install -r requirements.txt
sudo python main.py
# select android 11 and libndk

# if you're on wayland:
waydroid show-full-ui

# else
sudo pacman -S weston # weston is a program that will created a nested wayland session inside Xorg
weston
waydroid show-full-ui # Run this command inside weston's terminal
```

Installing apps

In order to install apps, you can open the browser in Waydroid then download and install apk from there. Otherwise you can also use the command :

```
waydroid app install <path to apk>
```

If you don't know where to find the APK you can install Aurora Store to be able to install any Google Play app.

Using a game controller (not tested)

Run the following code:

```
waydroid prop set persist.waydroid.udev true
waydroid prop set persist.waydroid.uevent true
```

Make sure to plug in the controller after Waydroid starts. If the controller was plugged in before Waydroid starts, the controller won't be recognized and you'll need to unplug it and plug it back in.

Troubleshooting

No internet

If there's no internet inside Waydroid, then you might want to disable your firewall (or configure it if you're not lazy), and you might want to disable docker and reboot. For some reason the docker service made Waydroid offline on my system.

```
sudo systemctl disable docker
reboot
```

The rotation of the thing makes it unusable

I don't know how to solve this issue. Still trying...

It's glitching on tiling window managers

That's because you need to put the window into floating mode in order for it to work properly.

I made some change and now nothing works (how to reset)

```
sudo systemctl stop waydroid-container
sudo waydroid init -f
sudo systemctl start waydroid-container
sudo rm -rf /var/lib/waydroid ~/.local/share/waydroid ~/.local/share/applications/*aydroid*

# After that, you can rerun the installation steps starting with "waydroid init"
```

KeePass Guide [EN]

Goal

KeePass is a password manager that has many advantages over other password managers:

- It’s self-hosted, the data always stays on your devices
- You can use it to keep track of your global security and of all the services you use
- You can use it to store PGP secret keys
- You can also store all kinds of other informations about your account
- You can also connect it to your browser to easily insert your password when needed
- Since the passwords will only show up if the URL is correct, it can also protect you against fishing attacks
- You can also use it for 2 factor authentication since it can generate OTP codes

Here we’ll see how to configure it to be as secure as possible while being synchronized on multiple devices using Syncthing.

Documentation

You can find further documentation about the tools we’ll use here on the following websites:

- KeePassXC User Guide
- Syncthing’s getting started guide

Installation

Since I want this tutorial to be cross-platform, I’ll not cover the installation, you can look on the resources below to know more…

- Installing KeepassXC (for all desktop devices)
- Installing KeepassDX (for all Android devices)
- Installing Synchting (for all devices to be synchronized)

Creating the database

1. Once you installed KeePassXC, you can create a new empty directory then open Keepass and create a new database in the empty directory.
2. When asked for a passphrase, use the built-in tool to generate a random, secure password and set the word length to 7.
3. Write down the passphrase and keep it safe.
4. You can then add new accounts in KeePass.
5. After a while of getting used to your passphrase, you might try to destroy the paper you wrote it on

Setting up the browser addon

1. Install the KeepassXC-Browser addon
2. In the settings of KeepassXC, enable browser integration for the browser you use
3. Go in the addon and click on “connect”, then choose a name for the browser.
4. Finally, when you go on a site that requires logging in, click on the keepass icon and click on “Allow” to allow keepass to auto-fill the details

Synchronizing with other devices

1. On device A, click on “Add a new device” then add the ID of device B
2. On device B, allow the connection to device A
3. Open Syncthing and add a new shared directory. Then select the directory containing the keepass database. Select device B in the settings to share it with.
4. Accept the transfer on device B and select where you want it to be saved. After a few minutes the two should be synced.
5. Open the database using Keepass

Setting biometrics on a phone for easier access

1. Open the synchronized keepass database in keepassDX, then open it with your passphrase

2. In KeepassDX’s settings, go in advanced unlocking and enable biometric unlocking so you can use your fingerprint instead of always typing your passphrase
3. Lock the database then type your passphrase, click on the fingerprint icon to enable it.

Using Keepass

- To create a basic entry, click on “+” then fill the info for the title, username, password and URL.
- You can also go in the “icon” section and download the icon of the website.
- You can also go in the “advanced” section to add your secret key as an attachment or add any additional data there
- To add a TOTP (2 factor auth), right click on the entry and choose “TOTP” then “Define a TOTP”. In there you can put your TOTP token.

> For TOTP, make sure the clocks on all your devices are perfectly synchronized otherwise it won’t work.

Analyze your global security

1. Press CTRL+MAJ+R to get the statistics
2. Then go in “Health Check” to locate security issues.
3. Go in HIBP and click on the analyze button, this will tell you if one of your password have been corrupted.

Setting up email with PGP encryption (Android and laptop)

Introduction

This guide is there to help you configure secure, encrypted, private emails using multiple accounts, PGP and advanced spam filters while being synchronized between your phone and your computer.

For this we're going to use Keepass (see precedent guide), Thunderbird, K-9 and OpenKeyChain (which is necessary to use encryption on K-9)

> This guide is meant to be done after the Keepass guide because we'll use it to synchronize the passwords and keys with the phone

1. More details about Thunderbird
   Thunderbird is really an awesome mail client that provide support to:
   - Multi-account
   - Easy encryption using PGP
   - Really powerful mail filter mechanism to exterminate spam
2. More details about K-9
   K9 is a mail client for Android that also support multi-account and encryption but doesn't support mail filters.

Setting up Thunderbird

You can install thunderbird from their website.

Once it's installed you can setup a new email account, in the process open the "manual setup" menu because the automatic one never works.

Here you can insert your information for your email provider. Here's some info for Gmail, Office 365 and Disroot.

1. Gmail

Key	Value for Incoming	Value for Outgoing
Protocol	IMAP	SMTP
Hostname	imap.gmail.com	smtp.gmail.com
Port	993	465
Security	SSL/TLS	SSL/TLS
Authentication	OAuth2	OAuth2
Username	*Your email address*	*Your email address*

2. Office365

Key	Value for Incoming	Value for Outgoing
Protocol	IMAP	SMTP
Hostname	outlook.office365.com	smtp.office365.com
Port	993	587
Security	SSL/TLS	STARTTLS
Authentication	OAuth2	OAuth2
Username	*Your email address*	*Your email address*

3. Disroot

Key	Value for Incoming	Value for Outgoing
Protocol	IMAP	SMTP
Hostname	disroot.org	disroot.org
Port	993	587
Security	SSL/TLS	STARTTLS
Authentication	Normal password	Normal password
Username	*Your email address*	*Your email address*

Setting up encryption in Thunderbird

Once your accounts are configured you can click on each of them, then go in their **End-to-End encryption** settings.

There you can click on **Add Key** and create a new one unless you already have one to import. You can set "does not expire" and change the keytype to ECC.

Once your key is ready you can click on it to publish it to a keyserver, that way other people who want to contact you will be able to encrypt their messages without you having to send them your key.

Finally, you can click on the "More" menu to **Backup secret key to file**. There you can choose a password (generate one using Keepass) and store it on the device.

Finally in your keepass entry, add that file into the attachement then remove it from your disk.

Using the Thunderbird key elsewhere

To use the PGP key for other purposes than emails, you can import the file in GPG using the following command:

```
gpg --import <path to .asc file>
```

> If you wish to do this graphically you could also use the Kleopatra software.

Setting up K-9 mail

You can install K-9 and OpenKeyChain (necessary for encryption) from F-Droid and Play Store.

The setup on K-9 mail is very similar to the one on Thunderbird *here*.

You can then open Keepass on your phone and download the secret key(s) from earlier.

Then you can open **OpenKeyChain** and import that file in it. Once you did that, open the **End-to-End encryption** settings of the K-9 account and select the key you imported in OpenKeyChain.

Congrats, everything is done!

> To use encryption, you'll need to search for the recipient's keys or import them in OpenKeyChain first.

Cleaning up your mailbox from spam

This is a process to create some filters in order to radically clean your inbox. From my experience it made me go from over 6000 emails to only 300 archived emails and 2 emails remaining in inbox.

This should also decrease the amount of spam on the long term since all the usual spammers will get blocked automatically.

1. Create a filter for Junk mail (you can leave it empty for now) and tick the box "any of the following". Configure the result of the filter to move the email in Spam or delete it
2. Sort mails by correspondant and add every spammer into your address book
   - If a spammer uses several emails from one domain, you can add a rule such as "From contains facebook.com" to your filter
   - If it's a multi-domain spam you can also create a filter (i.e "From contains noreply")
3. Once you're done, create a new address book "Junk" and move all your new entries in it.
4. Add a new condition "From is in address book Junk" to your filter. Then execute the filter.
5. Now do the opposite add every friend to your addressbook
6. Create a new addressbook "Friends" and move all your new entries in it
7. Create a new filter such as "if From is in addressbook Friends then move email to archive" and execute it
8. Archive the last emails you want to keep and delete the rest
9. Create a new filter to auto-archive emails if their age is over 50 days
10. Delete the Friends filter
11. Your inbox should now be clean. If new undesired emails come in, either modify the junk filter or add it to the Spammer's list.