Security Matters

NEWSLETTER

FROM CHAOS TO CLARITY: DECLUTTERING YOUR DIGITAL LIFE

Is your email inbox overflowing? Are you running out of hard disk space? Does the laptop take longer and longer to boot up? With bigger hard disks and more memory, new motherboards can help, but they don't come for free. As much as our physical spaces need to be well-maintained and clutter-free, so do our digital ones. Our mental well-being and productivity can suffer great consequences unless we learn to keep our digital and online spaces tidy and organized.

Digitally decluttering refers to the process of organizing, sorting, and removing unnecessary digital files, emails, applications, and other digital clutter from your devices and online accounts.

There are several reasons why digitally decluttering is needed:

- Increased productivity
- More storage space
- Increased device performance
- Faster access to information
- Reduces stress
- Improved security
- Better digital hygiene

The more we use digital spaces, the more 'digital clutter' we create. So, where do you start? What exactly is there to tidy up? Any task can be made more manageable if broken down into smaller steps. This guide will help you to declutter your digital life so you can work more efficiently and get more done.

Simple guides to declutter your digital life

Desktop/Laptop

- Move everything off your desktop/laptop to a temporary folder.
- Delete all unnecessary files from that folder.
- Back up your files and documents. Save to secured cloud storage or an external hard drive.
- Move the rest of the files to their rightful folders.
- Remove unwanted apps or programs manually.
- Empty “Recycle” bin.
- Update your desktop/laptop operating system and software.

Files/Download Folders

- Back up your files and documents. Save to secured cloud storage or an external hard drive.
- Organize a folder system.
- Delete all unuseful files from the Downloads folder and temporary files.
- Move the files to their proper folder. Empty your trash after this procedure.
- Create a temporary folder for files that you’re unsure about.

Email

- Read, review, and organize your email folders. Remove any emails you don’t need to keep.
- Unsubscribe from any emails/newsletters that you don't want to see in the future.
- If you need to action them, move them to the “Action” folder or flag them as important.
- Delete/archive the messages that you don’t need to action.
- Create new email folders.
- Update your email signature (if needed)
- Check if your email address has been compromised in a data breach via Have I Been Pwned
- Bulk archive all “read” emails from last year and prior.
- Empty the spam and promotions folder.
- Empty the trash folder at the end.

Phone

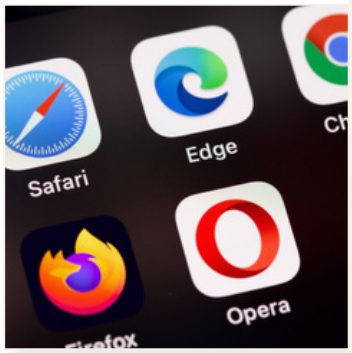
- Go through your apps. Delete any unused apps and double-check how much storage space your current ones are taking up. Check out the guide for Android and Apple devices.
- Keep only one app for one purpose.
- Leave only the most used apps on your main screen.
- Organize Apps by task, by usage, or create folders.
- Delete app widgets you don't need.
- Go through your files. Are there files in your phone taking up space?
- Delete any unwanted items/files.
- Store important files in a secured cloud or an external hard drive, or use the phone's internal cloud storage system.
- Optimize your battery usage. Follow this guide: Android and Apple.
- For iPhones, organize your dock and Home Screen.
- For Android, keep your Home Screen minimal.
- Update your operating system regularly.

Photo

- Always back up your photos to secured cloud storage or an external hard disk.
- Review and move photos off your phone to the cloud.
- Organize a folder system.
- Delete all unwanted and blurry photos.
- Delete duplicates.
- Delete screenshots (or store them somewhere else)
- Review and move photos from social media.

Cloud Storage

- Select your main file source for a cloud storage platform like iCloud, Google Drive, Proton Drive, etc.
- Organize your main file source with a folder system.
- Sync your passwords. Use a password manager. Recommended to use KeePassXC.
- Backup everything.
- Delete the files you don't need anymore.
- Move the files to their proper folder.
- Organise files/folders and rename them accordingly.
- Empty the trash.



Browser

- Only bookmarked frequently used websites. Delete unneeded bookmarks.
- Organize your bookmarks by creating folders (classified them).
- Remove old extensions. Get rid of any you don't need. Guides to managing extensions:
- **Safari**: Open Safari > Preferences > Extensions > Uninstall any extensions you do not need.
- **Firefox**: Click the three-dots icon > Add-Ons > The three-dots icon next to the extension you want to delete > Remove.
- **Chrome**: Click the puzzle icon > Manage Extensions > Remove from Chrome button on any extensions you don't need.
- Clear browser history, cache, and cookies regularly.

Social Media Accounts

- Spend some time on accounts and assess who or what you follow.
- Unfollow accounts that don't bring value to your life. Tidy up your friend list.
- For those you can't unfriend, simply hide their updates to keep your feed positive.
- Review your privacy settings regularly and clear your search history.
- Use as few social media apps as possible.
- Delete any old or unused accounts.
- Take a break! Be mindful of the time you are spending on social media platforms.

Password

- Delete accounts you don't use.
- Change passwords in the most important accounts regularly.
- Do not use repeated passwords for all accounts.
- Enable two-factor authentication.
- Move all passwords to a password manager like KeePassXC.
- Store your master password safely.

Let's cultivate a habit of digital decluttering to ensure ongoing efficiency and a streamlined digital environment together!

Related News

Signal now lets you find people by name, not number

The Signal update with the new features will gradually be rolled out to all users over the next few weeks once the beta test has been completed. The app will also let you share a contact by the username with a link or a QR code.
Read more: https://bit.ly/45aF9iW

Human error as number one security risk

According to a new research, despite 90% of CTOs deploying multi-factor authentication, and 91% using identity access management technology for company security, over half (59%) said that human error is the biggest threat to their organization.
Read more: https://bit.ly/47BjGB8

Behind the doors of a Chinese hacking company, a sordid culture fueled by influence, alcohol and sex

Private hacking contractors are companies that steal data from other countries to sell to the Chinese authorities. Over the past two decades, Chinese state security's demand for overseas intelligence has soared, giving rise to a vast network of these private hackers-for-hire companies that have infiltrated hundreds of systems outside China.
Read more: https://bit.ly/3wr7cOr

ChatGPT is finally making your account more secure

OpenAI has added a long-awaited feature to ChatGPT that it says can boost your account security. The company announced multi-factor authentication is now available for users to secure their account. It can be enabled in the settings of the ChatGPT web page (accessed by clicking your account name in the bottom-left corner) or in the OpenAI Developer platform.
Read more: https://bit.ly/3wr7cOr

Most LGBTQ are cyberbullied. Here's how to stay safe online

Deepfake technology has reached a point where it's not just applicable to still images and videos like conference calls. Such was the case one unfortunate employee who got duped into handing over US$25 million (~RM119 million) to people she thought were her real colleagues during the "con" call.
Read more: https://bit.ly/3Q6CJge

Tor has a new HTTPS-esque feature to heap beat censorship

The Tor Project has released a new bridge called WebTunnel, aimed at those trying to access the internet in regions with heavy censorship. The announcement comes at a crucial time, as many elections will be taking place around the world this year, which means that many countries will look to restrict access to the public internet in an attempt to silence any dissenting voices.
Read more: https://bit.ly/3HZme0n

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia
@secm8 @sec_matters

Hackers abuse API popularity to break into accounts and steal data

Hackers have been paying attention, and are increasingly abusing APIs in their efforts to steal sensitive data from organizations. Among different industries, organizations in financial services and online retail have had most API calls last year, and thus, have also had most API-related attacks.
Read more: https://bit.ly/48lucMe

Hacker group exploits Microsoft Windows feature in worldwide phishing attack

The infamous Russian hacking collective, known as APT28, is now using a legitimate Microsoft Windows feature to deploy infostealers and other malware to their victims. The attackers are impersonating government and NGO organizations in Europe, South Caucasus, Central Asia, and North and South America, reaching out to their victims via email. The emails contain weaponized PDF files.
Read more: https://bit.ly/4bCCfqQ

Cyberflashing: Change these settings to protect your smartphone

Airdrop on iPhones and Quick Share on Android phones are useful features for wirelessly exchanging photos, videos, and documents between devices. However, these very features have been abused in recent years in a process known as cyberflashing - when someone sends obscene unsolicited photos or videos to your phone.
Read more: https://bit.ly/48lihhA

Are free VPNs safe and can they be trusted?

Nothing in life is ever truly free. How do you know which are safe and which are untrustworthy? Can you trust your VPN provider not to put malware on your device or harvest your data to sell it on to advertisers? While there are some free VPNs we think are pretty decent, they just don't compare to the paid options.
Read more: https://bit.ly/3SPrlFG

Google's new AI search results promotes sites pushing malware, scams

Google's new AI-powered 'Search Generative Experience' algorithms recommend scam sites that redirect visitors to unwanted Chrome extensions, fake iPhone giveaways, browser spam subscriptions, and tech support scams. When clicking on the site in the Google search results, visitors will go through a series of redirects until they reach a scam site. the redirects most commonly lead you to fake captchas or YouTube sites that try to trick the visitor into subscribing to browser notifications.
Read more: https://bit.ly/3Pe0YZ9