

# WHO HAS YOUR BACK? DON'T BE AN APRIL FOOL!

VOL 10 • MARCH 2023

What would you do if you lost your phone, your laptop, or your hard drive? Would you be able to get back all your photos, important work files, or once-in-a-lifetime videos? If you perform proper backups, then you should feel a lot better in your daily life. A laptop that won't boot up will be a headache, but it won't cost you anything more than time and, potentially, money.

Backup is an essential part of data protection. Regular data backup saves your files from data loss situations like malware attacks, system crashes, storage device failures, and many more. Those of us who have lost important files in the past know what a pain it is, and how much valuable time it takes to recreate them or make new copies. Even though we know the consequences of data loss, still many of us are unaware of the most common ways in which data are lost. Backup data immediately to avoid becoming an April fool. How to protect your data with ease? Read further to check it out.

## Common ways to lose data

- Theft
- Human error, forgetfulness
- Hardware failure
- Software corruption
- Virus attacks
- Natural disaster or destruction (E.g. flood, fire, etc)
- Obsolete file formats

## What to backup?

- Desktop & laptop
- Mobile phone
- Tablet
- Other wireless devices
- Business server
- Photos and videos on social networks

## Why backup your data?

- To prevent data loss if system failure or storage device errors happen.
- To reduce downtime that caused a negative impact on businesses.
- To keep your data safe from cyber threats.
- Act as a defence against ransomware and will save you from paying up for your data.
- Aids in quick data recovery. You can easily restore your data.



General Helpline: [help@securitymatters.asia](mailto:help@securitymatters.asia)  
Secure Communication via Protonmail:  
[secmhelpdesk@pm.me](mailto:secmhelpdesk@pm.me)  
Help desk (Signal & WhatsApp): +6011 6516 6310

More information about Security Matters,  
visit [www.securitymatters.asia](http://www.securitymatters.asia)

 [info@securitymatters.asia](mailto:info@securitymatters.asia)

 @secm8

 @sec\_matters



# WHO HAS YOUR BACK? DON'T BE AN APRIL FOOL!

VOL 10 • MARCH 2023

## How to backup your data?

1



Identify which data is critical and ensure it is backup securely.

- What data do I want to back up?
- Where is that data located?
- Where will I store my data?
- How often should I back up my data?
- How often should I test my backups?

2

Follow the 3-2-1 Rule. Back up the backup

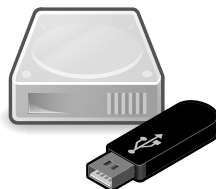
3

Creates **three** copies of your data (the original + two copies of it)



2

Store the copies on at least **two** different storage media



1

Store **one** copy on a remote/offsite storage



General Helpline: [help@securitymatters.asia](mailto:help@securitymatters.asia)  
Secure Communication via Protonmail:  
[secmhelpdesk@pm.me](mailto:secmhelpdesk@pm.me)  
Help desk (Signal & WhatsApp): +6011 6516 6310

More information about Security Matters, visit [www.securitymatters.asia](http://www.securitymatters.asia)

 [info@securitymatters.asia](mailto:info@securitymatters.asia)

 @secm8

 @sec\_matters

# WHO HAS YOUR BACK? DON'T BE AN APRIL FOOL!

VOL 10 • MARCH 2023

3

Invest in a good storage for both internal and external storage.  
Types of storage media:



### Online Backup Service

Data is transmitted over the internet and stored on a server in a data centre.

E.g. Nextcloud, ProtonDrive, Pcloud.

It has a fee to be paid annually but it is safe from theft, fire and other local disasters.



### Cloud Backup

An always-online backup location such as Google Drive, iCloud, OneDrive.

Data is available anytime, anywhere and it's affordable. Always pay close attention to access and security with cloud backups.



### External Hard Drive (HDD/SDD) or Thumb Drive

It's mainly used for data storage and PC backups and will take time and won't back up the system.

The storage space only needs to be purchased once. However, the hard drive can be lost or damaged. Don't forget to update your physical hard drive every year.



### Full Disk Imaging Backup

Create an exact image of the whole hard drive.

System and files can be restored at any time. It does not take up a lot of space for backup.



General Helpline: [help@securitymatters.asia](mailto:help@securitymatters.asia)

Secure Communication via Protonmail:

[secmhelpdesk@pm.me](mailto:secmhelpdesk@pm.me)

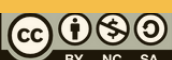
Help desk (Signal & WhatsApp): +6011 6516 6310

More information about Security Matters, visit [www.securitymatters.asia](http://www.securitymatters.asia)

 [info@securitymatters.asia](mailto:info@securitymatters.asia)

 @secm8

 @sec\_matters



# WHO HAS YOUR BACK? DON'T BE AN APRIL FOOL!

VOL 10 • MARCH 2023

4

**Test your backup and learn how to restore your data.**

5

**Don't leave a backup where cyber crooks can find them.**

6

**Don't make a backup that everyone can read.**  
Always encrypt your backups.  
E.g. Use tools like BitLocker, FileVault, LUKS and cryptsetup.

## Signs of corrupted hard drive

- Irregular system crashes and disk errors.
- Frequent error messages during normal operations.
- Scrambled or changed files or folder names.
- Extended wait times when opening files or folders
- Disappearing files or folders.
- A rising number of bad sectors.
- The Operating system won't boot.
- Overheating.
- Strange noises/sounds.
- Blue Screen of Death errors.

Keeping your data safe is more important than ever in today's risky online environment. Back up your data. Check the restores. Nobody should be an April fool. Let's backup our data today!



General Helpline: [help@securitymatters.asia](mailto:help@securitymatters.asia)  
Secure Communication via Protonmail:  
[secmhelpdesk@pm.me](mailto:secmhelpdesk@pm.me)  
Help desk (Signal & WhatsApp): +6011 6516 6310

More information about Security Matters,  
visit [www.securitymatters.asia](http://www.securitymatters.asia)

 [info@securitymatters.asia](mailto:info@securitymatters.asia)

 @secm8

 @sec\_matters

## Related News

### China is relentlessly hacking its neighbors

According to the cybersecurity alert, Chinese-linked hackers were able to break into mail servers operated by the Association of Southeast Asian Nations (ASEAN) in February 2022 and steal a trove of data. The ASEAN organization is an intergovernmental body made up of 10 Southeast Asian countries including Singapore, Malaysia, and Thailand.

Read more: <http://bit.ly/3ZmeoVH>

### Internet access, privacy 'essential for freedom'

Internet privacy company Proton can spot attacks on democracy in a country before they hit the headlines, simply by watching demand for its services explode. When Russia blocked access to independent news sites following its invasion of Ukraine a year ago, Switzerland-based Proton saw a huge surge in demand for its VPNs, which are used to skirt online restrictions.

Read more: <http://bit.ly/3ZIWJHK>

### Beware of fake Facebook profiles, Google ads pushing Sys01 Stealer

The cybersecurity researchers have revealed details of an advanced information-stealing malware named SYS01 Stealer which they began tracking in November 2022. This malware is targeting Facebook accounts of employees working for manufacturing companies, critical government infrastructures, and other sensitive industries.

Read more: <http://bit.ly/3TcBmfG>

### WhatsApp group chats could soon be set to self-construct

WhatsApp has pushed a new update to the iOS TestFlight beta program. Users with this beta update found that there's a new feature for group chats called 'Expiring Groups'. It adds a new option to your group chat settings where users in the group can turn on an expiry date for the group, ranging from one day, one week or even set a custom date for it.

Read more: <http://bit.ly/3ZIGxXe>

### Fake ChatGPT Chrome Extension hijacking Facebook accounts for malicious ads Guardio Labs reports.

Guardio Labs discovered a Chrome Extension that promotes rapid access to fake ChatGPT functionality capable of stealing Facebook accounts and establishing hidden account backdoors. "By hijacking high-profile Facebook business accounts, the threat actor creates an elite army of Facebook bots and a malicious paid media apparatus.", Guardio Labs reports.

Read more: <http://bit.ly/3LoIKTh>



General Helpline: [help@securitymatters.asia](mailto:help@securitymatters.asia)

Secure Communication via Protonmail:

[secmhelpdesk@pm.me](mailto:secmhelpdesk@pm.me)

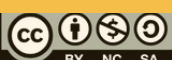
Help desk (Signal & WhatsApp): +6011 6516 6310

More information about Security Matters, visit [www.securitymatters.asia](http://www.securitymatters.asia)

 [info@securitymatters.asia](mailto:info@securitymatters.asia)

 @secm8

 @sec\_matters



© Security Matters, 2023. This work is licensed under CC BY-NC-SA 4.0. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/4.0/>

## Top 50 most impersonated brands in phishing attacks

One of the biggest challenges in preventing phishing attacks is the sheer volume and the difficulty of distinguishing legitimate emails and websites from fraudulent ones. Even when users are vigilant, it can be hard to spot the subtle differences that attackers use to make their phishing emails and websites look convincing.

Read more: <http://bit.ly/3LU4FSE>

## YouTube is being attacked by hackers using vicious malware

Using the content generated by AI on YouTube, users are being scammed into downloading malware that is capable of stealing their information which may be sensitive. The malware gets access to the user's information like account numbers, passwords, credit card info etc, and is then misused by the hacker's Control server and Command.

Read more: <http://bit.ly/3JgNaJm>

## MCMC: Up to RM50,000 fines and imprisonment for sharing hate speech involving race, religion and royalty

The Malaysian Communications and Multimedia Commission (MCMC) has issued a reminder to the public not to upload or share hate speech involving 3R elements (3R – Race, Religion and Royalty). Individuals who are found sharing fake, inappropriate or threatening content is an offence under Section 233 of the Communications and Multimedia Act (CMA) 1998.

Read more: <http://bit.ly/401yNQr>

## Cybercriminals using novel phishing tactics to get their target

As cybercriminals work to make phishing attacks more effective, they are continually introducing new techniques and tactics to try to trick victims, bypass security, and avoid detection. Barracuda researchers identified three novel phishing tactics being used by cybercriminals: attacks leveraging Google Translate links, image attachment attacks, and use of special characters in attacks.

Read more: <http://bit.ly/42xUA3C>

## WhatsApp group admins can now approve or deny people from entering group chat

As more and more users join and take part in different communities, WhatsApp want to give group admins more control over the privacy of the group. They've built a new tool that would allow the admins in charge to determine who exactly is able to join the WhatsApp group that they're in charge of.

Read more: <https://rb.gy/bovydn>



General Helpline: [help@securitymatters.asia](mailto:help@securitymatters.asia)

Secure Communication via Protonmail:

[secmhelpdesk@pm.me](mailto:secmhelpdesk@pm.me)

Help desk (Signal & WhatsApp): +6011 6516 6310

More information about Security Matters, visit [www.securitymatters.asia](http://www.securitymatters.asia)

 [info@securitymatters.asia](mailto:info@securitymatters.asia)

 @secm8

 @sec\_matters

