SECURITY MATTERS
NEWSLETTER

DON'T LET YOUR DAILY CLOUD TURN YOU INTO A CLOUDY MOOD

VOL 4 • SEPTEMBER 2022

Cloud storage has become mainstream over the near decades. It is like a giant online hard drive, run by a third-party that you can store things in and access anytime from different devices and locations as long as you have the internet connection and login credentials. Though it is convenient for us, data upload to a third-party platform might fetch some security risks. We never know what is happening behind the screens in the server firms, as anyone working in or for the data center can easily have access to data.

Scammers are using cloud services to create and host web pages that can be used to trick victims into handling over their credentials. They use phishing to gain access to a victims' networks, then use the victims' own tools and services for malicious purposes. Thus, to avoid all possible digital threats, it is better to take precautionary steps to ensure your data on the cloud is safe and secure.

Good things about using Cloud

- Access to your files from anywhere that has an internet connection.
- Syncing and updating across all of your devices.
- Data is stored and automatically back-up in an external device.
- Can upgrade the storage or service plan anytime. More cost effective compare to physical drive.

Possible threats of using Cloud

- Data breaches/loss
- Phishing/Hijacking of accounts
- Denial of service (DoS) attack
- Insecure application programming interface (API)
- Malicious insider threats
- Malware infections
- Lack of control
- Security and privacy concerns

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

© Security Matters, 2022. 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/

SECURITY MATTERS
NEWSLETTER

DON'T LET YOUR DAILY CLOUD TURN YOU INTO A CLOUDY MOOD

VOL 4 • SEPTEMBER 2022

How to stay safe in the Cloud?

Carefully choose your cloud vendor. Recommend using a private cloud storage. E.g. Tresorit or NextCloud.

Control access, manage permission and your shared files actively.
Stay alert, check for unknown cloud user. Prevent data to be shared with unknown devices

Using a strong account password and enable two-factor authentication (2FA)

Encrypt your data before uploading to the cloud.
And avoid using public Wifi.

Back-up regularly.
Store your sensitive files offline.

Check out the access policies in advance.

Manage devices that access the cloud network.
Deactivate old devices that still have access.

Regularly review and revoke app access to your file storage.
Practice data minimalization.
Use anti-virus and anti-malware software.

Create a standard process to protect against resigning employees and provide anti-phishing training to employees regularly.

Always ensure that you signing out your cloud!

Always bear in mind that security assurance are not guaranteed. No system is perfectly secure and this applies to the cloud too. As long you adhere to good digital security practices, cloud storage can indeed be a good choice.

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

© Security Matters, 2022. 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/

Related News

Attackers using fake Cloudflare DDoS protection popups to distribute malware

The attack starts with malicious JavaScript that targets poor WordPress sites. Users are tricked into downloading malware that leads to the hijacking of their devices. The victim unknowingly downloads a remote access trojan, which has been flagged by at least thirteen security vendors so far.
Read more: https://bit.ly/3LHfTru

Telegram attacks: How to know if your account is compromised and how to improve security

Like WhatsApp, Telegram also has E2EE to ensure protected messages cannot be easily read by unauthorized third parties. However, there could be a potential vulnerability where the attacker can send the malicious file to all the victim's contacts, potentially enabling a widespread attack.
Read more: https://bit.ly/3rbn3uL

Spell-Checking in Google Chrome, Microsoft Edge Browsers Leaks Passwords

Spell-checking features present in both the Google Chrome and Microsoft Edge browsers are leaking sensitive user information including username, email, and passwords to Google and Microsoft, respectively, when people fill in forms on popular websites and cloud-based enterprise apps.
Read more: https://bit.ly/3BYfca6

Google rolls out option to request removal of personal data from search result

Google announced a new feature to make it easier for users to remove personal data like phone numbers, email addresses, and physical addresses from search results. Now, that feature is finally being rolled out to users.
Read more: https://bit.ly/3DGjqod

Changed your Twitter password recently? Your account might still be logged in elsewhere

There was a bug that had allowed Twitter accounts to remain logged in on multiple devices, even after you've reset your password. Essentially, if you had changed your Twitter account's password on one device, but had Twitter logged in on your other devices.
Read more: https://bit.ly/3Sl3L2c

© Security Matters, 2022. 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/

Related News

Phishing for a victim; Avoid falling prey to scams

It's always important to stay vigilant in making sure you know what to look out for no matter how unsusceptible to scams you may think you are. So, here are some tips you can employ to avoid getting scammed and actionable steps you can take if you ever fall victim to one.
Read more: https://bit.ly/3fgvKRL

Hackers compromise Microsoft Exchange Servers via malicious OAuth apps

Hackers took control of enterprise Exchange Servers to spread large amounts of spam aimed at signing people up for bogus subscriptions. They are deploying malicious OAuth applications on compromised cloud tenants, with the goal of taking over Microsoft Exchange Servers to spread spam.
Read more: https://bit.ly/3DUdUOE

These fake Zoom websites want to trick you into downloading malware

If you're looking to download the video conferencing (opens in new tab) platform Zoom, make sure you double-check the internet address you're downloading from, because there are plenty of fake websites out there spreading all kinds of nasty viruses and malware.
Read more: https://bit.ly/3C7CVEO

PowerPoint files are being hacked to spread this new Russian malware

Dangerous campaign leverages a PowerPoint flaw and mouse movements. The victims don't actually need to click a link, or download the malware itself - a mouse hover is enough to trigger the attack.
Read more: https://bit.ly/3Cdsn7i

BY NC SA
© Security Matters, 2022. 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/