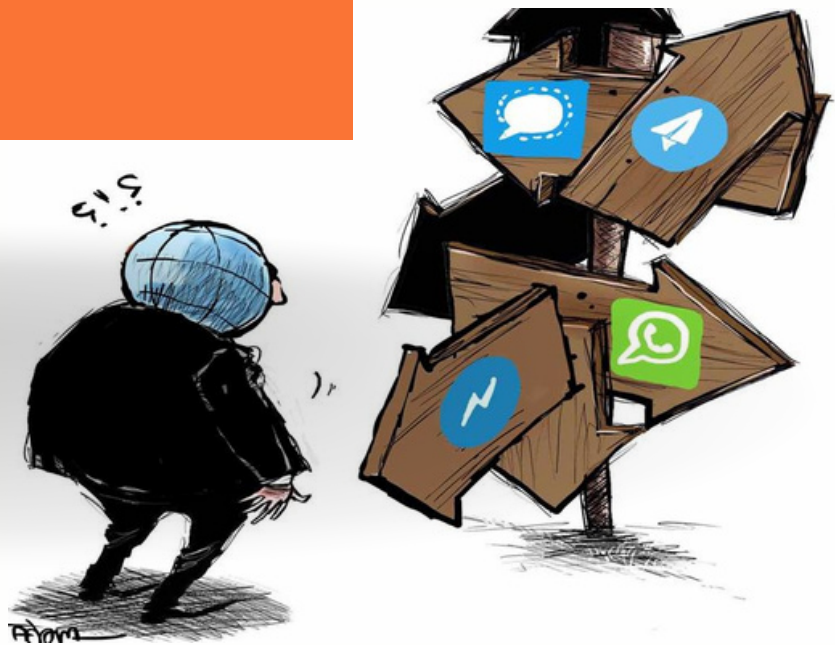


## TALKING SAFELY: FROM INSTANT MESSAGING APPS TO EMAIL



When people send messages on their mobile devices, they aren't typically thinking about the security limitations of the apps they're using. They may have no idea how vulnerable their data is and if they happen to share sensitive personal information in a message, it could find its way into the wrong hands. For this reason, secure communication is important to protect data from being accessed by unauthorized individuals. It involves using encryption and other security measures to ensure data is securely transmitted between two or more parties. It plays a crucial role in supporting human rights defenders and activists when doing their advocacy work. Instant messaging apps are one of the most frequently used online services. But not all messaging apps are the same.

### KEY FACTORS WHEN CHOOSING A SECURE MESSAGING APP



Look for apps that provides **end-to-end encryption (E2EE)** for messages, voice & video calls, and media content.



Check for **open-source software** which allow experts to review the code for vulnerabilities and security audit.



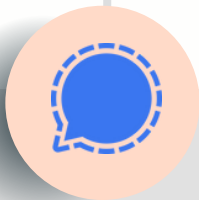
Review and choose apps with clear **privacy policies** that prioritize user data protection.



Choose apps that provides **two-factor authentication (2FA)** options to prevent unauthorized access.

## USE YOUR MESSAGING APP SECURELY..

- Open source end-to-end encryption (E2EE).
- Disappearing message function.
- Secure app with a password.



### Signal





#### >>> Turning off auto backup

Signal **do not** send or store messages in the cloud.

#### >>> Turning on or off the disappearing message function

Open the individual chat > Tap on the contact's name at the top > Select Disappearing messages > Select a time

#### >>> Using 'View once'


Open the individual chat > Tap the camera icon > Select an image or capture a new photo/video > Tap the  icon to switch to the view-once icon 


- E2EE and widely used.
- Disappearing message function.
- Owned by Meta - raised concerns about data sharing & privacy policies.



### WhatsApp

#### >>> Turning off auto backup


 Settings > Tap your name > iCloud > Apps using iClouds > Show all > Uncheck WhatsApp

 Open WhatsApp > Tap the three dots in the top-right corner > Settings > Chats > Chat backup > Google Drive settings > Never

#### >>> Turning on or off the disappearing message function

Open the individual chat > Tap on the contact's name at the top > Select Disappearing messages > Select on or off

#### >>> Using 'View once'

Open the individual chat > Tap the camera icon > Select an image or capture a new photo/video > Tap  > Send

- E2EE isn't enabled by default. Have to switch to Secret Chat mode.
- Cloud-based storage.
- Large group chats but chats more than two person won't be E2E encrypted.
- Self destructing message function.





### Telegram

#### >>> Turning off auto backup


Telegram saves all your conversations history on the encrypted server.

#### >>> Turning on or off the disappearing message function

 Open the individual chat > Tap on the contact's name at the top > More > Start Secret chat > Click on the stopwatch icon > Select a time > Done

 Open the individual chat > Tap on the contact's name at the top > Tap the three dots in the top-right corner > Start Secret chat > Start > Select a time > Done

#### >>> Using 'View once'

Open the individual chat (not secret chat) > Tap the  icon > Select an image or capture a new photo/video > Tap and hold the send button > Send with timer > Select a time > Send

Instant messaging apps are popular, but they can also pose risks to our privacy and security. Here are some other things to pay attention to:

- ✓ Download from trusted sources.
- ✓ Know who owns the app and where the content stored.
- ✓ Beware of the cloud.
- ✓ Create strong passwords and enable 2FA.
- ✓ Beware of phishing.
- ✓ Update the apps regularly.
- ✓ Secure file sharing.
- ✓ Avoid public WiFi.
- ✓ Logout from shared devices.

## EMAIL SECURITY

### Proton Mail



- Open-source end-to-end encryption (E2EE).
- Only the recipient can see your message.
- Encryption is automatic, provided the recipient also uses ProtonMail.
- If you want to send a secure, end-to-end encrypted email to someone who isn't on Proton Mail, the easiest way is to use a [Password-protected Email](#).
- Does not require you to provide any personal information to use it.
- The company maintains no records of IP addresses or anything else.

### Gmail

- No end-to-end encryption (E2EE).
- Uses Transport Layer Security (TLS).
- The recipient must also use a mail service that supports TLS.
- To manage your Gmail accounts, use the [Gmail Security Checklist](#) and follow the steps in the checklist.
- Gmail Security Checklist includes items such as creating a strong password, setting your recovery options, checking your account for unusual activity, ensuring that your browser is up to date, etc.

### Outlook

- Not open source.
- End-to-end encryption (E2EE) isn't enable by default. Service provider can access email content.
- Comprehensive organisation features and Microsoft ecosystem integration, yet it could be complicated for new users.
- If you want enable the E2EE settings and send an encrypted email to someone, follow the steps in this [guide](#).

When choosing a secure communication app or software, consider your specific needs, your trust in the developers, and your willingness to trade convenience for enhanced security. Keep in mind that the security landscape is ever-evolving, and it's important to stay informed about the latest developments and security practices.

## Related News

### Empowering kids against online harm

Social media is a tool used by people to stay connected through the internet and exchange information in varying formats. But a tool needs a skillful master. According to the report, children in Malaysia were subjected to various forms of online sexual abuse and exploitation, and other unwanted experiences online. 9% of children surveyed within the past year had been exposed to sexual comments about them that made them feel uncomfortable, with the majority of these comments being made by someone they knew.

Read more: <https://bit.ly/3VH2UuF>

### WhatsApp web to soon get screen lock feature

WhatsApp is working on a screen lock feature for its web client in order to enhance the security and privacy. The screen lock feature will hide all your chats behind a password once you've left the app inactive for a set amount of time, as well as blocking any notifications from popping up. It will also require you to input the password if you close the web app and re-open it. This will ensure that nobody can read your messages while you're away from your computer.

Read more: <https://bit.ly/3NRg991>

### How to enable Google's new unknown tracker alerts for Android

Android is widely introducing "Unknown tracker alerts" for spotting AirTags that may have been maliciously implanted in your belongings. Read more to check out how to enable Google's new unknown tracker alerts for Android.

Read more: <https://bit.ly/45aF9iW>

### Hackers could now steal passwords over Zoom by listening to keystrokes using AI

AI can steal passwords from keystroke sounds recorded over Zoom with up to 93% accuracy, per a new study. Passwords containing full words may be at greater risk of attack. AI tools can make online scams harder to detect because AI makes it easier to personalize scams for each target.

Read more: <https://bit.ly/47BjGB8>

### Cybercriminals are using these simple tricks to bypass popular security software

Hackers are making use of some basic tactics and tools to bypass antivirus software and infect systems with malware. a cyberattack which used AsyncRAT, a trojan used to steal valuable information, and it managed to fool victims and protection software into thinking it was safe. This included renaming file extensions, increasing file size so it couldn't be scanned, and using multi programming languages as part of the overall attack.

Read more: <https://bit.ly/44Gq2gO>



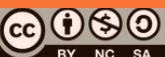
General Helpline: [help@securitymatters.asia](mailto:help@securitymatters.asia)  
Secure Communication via Protonmail:  
[secmhelpdesk@pm.me](mailto:secmhelpdesk@pm.me)

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

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

 @secm8

 @sec\_matters



## Proton launches new protection program for users at higher risk of cyberattacks

Combining the power of [AI](#) with in-depth human analysis, Proton Sentinel uses AI to detect suspicious activities on user accounts. This program is configured to have higher challenge rates for its users, alongside stricter parameters for suspicious login attempts. This program bolsters account protection system and gives higher risk users like human rights activists and journalists an extra layer of protection.

Read more: <https://bit.ly/3VH2UuF>

## Beware of new hacking attack targeting LinkedIn accounts worldwide

Numerous users have reported instances of their LinkedIn accounts being temporarily locked, hacked, or permanently deleted. There were also ransom payments requested by threat actors to recover user accounts. It is suspected that threat actors have gathered data from a LinkedIn Breach and used the data to pick accounts. Threat actors identify accounts without 2FA or use Brute force to hack into accounts having short passwords.

Read more: <https://bit.ly/3NRg991>

## Digital security support in Thai protests.

This article will be talking about what's happening in Thailand after the Elections and the importance of digital security support during protests.

Read more: <https://bit.ly/3PdXzj1>

## Juice jacking cyber attack: The hidden threat at public charging stations

Juice jacking is a cyber threat that exploits the vulnerability of public charging stations to compromise your devices and steal sensitive data. This occurs when unsuspecting users plug their devices into public charging ports, such as those found at airports, coffee shops, hotels, or even public transportation terminals.

Read more: <https://bit.ly/3OcaAmQ>

## The best time to send an email might surprise you

Axios HQ, a company that creates "AI-powered software that helps organizations of all sizes plan, write and send essential comms," determine the best time of the week to send professional emails. The company found that Sundays between 3 pm and 6 pm was the best window for sending business emails.

Read more: <https://bit.ly/3OcaAmQ>



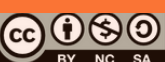
General Helpline: [help@securitymatters.asia](mailto:help@securitymatters.asia)  
Secure Communication via Protonmail:  
[secmhelpdesk@pm.me](mailto:secmhelpdesk@pm.me)

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

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

 [@secm8](https://www.facebook.com/secm8)

 [@sec\\_matters](https://twitter.com/sec_matters)



## Thailand's Digital Minister threatens to shutdown Facebook due to scams. What on earth is Malaysia doing?

Scams on Facebook, WhatsApp and Instagram are on the rise and Meta has repeatedly ignored and failed to take necessary action especially when it comes to allowing scam ads on its platform. Thailand are seeking legal action to shut down Meta's Facebook operations unless it takes action over scams that have affected more than 200,000 people.

[Read more: https://bit.ly/3VH2UuF](https://bit.ly/3VH2UuF)

## WhatsApp now lets users create groups without names

WhatsApp introduced a feature that lets users create groups on the instant messaging app without needing to name them. The feature will help users create a group, even if they have not decided on a topic yet or need to create one quickly. This unnamed groups will be limited to up to six participants. and will be dynamically named based on the users added to a group.

[Read more: https://bit.ly/3qLFo59](https://bit.ly/3qLFo59)

## Gmail to add an extra verification step when attempting 'sensitive actions'

Gmail may soon introduce an additional verification step when you do something sensitive like adding a forwarding address and editing your filters. This extra layer of verification could help deter malicious actors from gaining access to your account by manipulating email filters unexpectedly or redirecting emails to an unfamiliar address without your awareness.

[Read more: https://bit.ly/3suFBtY](https://bit.ly/3suFBtY)

## Silencing Southeast Asia's cyber activists

Amid the rise of digital authoritarianism or the deliberate shrinking go digital civic space in many parts of the world including Southeast Asia, journalists, activists and human rights defenders often bear the burnt of online harassment, doxxing and cyberattacks, many of which are perpetrated by the state.

[Read more: https://bit.ly/3suFBtY](https://bit.ly/3suFBtY)



General Helpline: [help@securitymatters.asia](mailto:help@securitymatters.asia)  
Secure Communication via Protonmail:  
[secmhelpdesk@pm.me](mailto:secmhelpdesk@pm.me)

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

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

 [@secm8](https://www.facebook.com/secm8)

 [@sec\\_matters](https://twitter.com/sec_matters)

