WORLD
RESOURCES
INSTITUTE

accessnow

Meeting the Digital Security Helpline

February 2020

Mohamed CHENNOUFI : Security Incident Shift Lead

Summary

- Access Now and the Digital Security Helpline
- Statistics
- Why Digital Security matters?
- How we help
- Essential Digital Security Hygiene recommendations
- Using Signal

accessnow

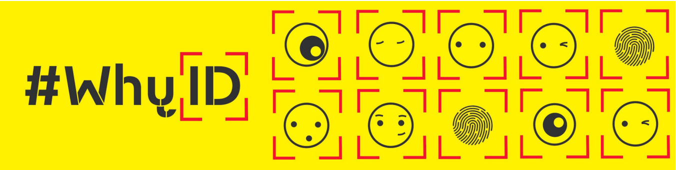
An international human rights organization that works to **defend** and **extend** the digital rights of **users at risk** around the world.

By combining innovative policy, global advocacy, and direct technical support, we fight for open and secure communications for all.

Policy: Development and promotion of rights respecting policies.

Advocacy: Working on interacting directly with the users and provide a deep engagement of users through campaigns and events.

Grants: providing flexible and grantee-driven funding to grassroots and frontline organizations fighting for human rights in the digital age.



RightsCon
Costa Rica 2020

CONVENTION CENTER
JUNE 8-12, 2020

DIGITAL SECURITY HELPLINE

The Digital Security Helpline is a free of charge resource for at-risk civil society groups.

24/7

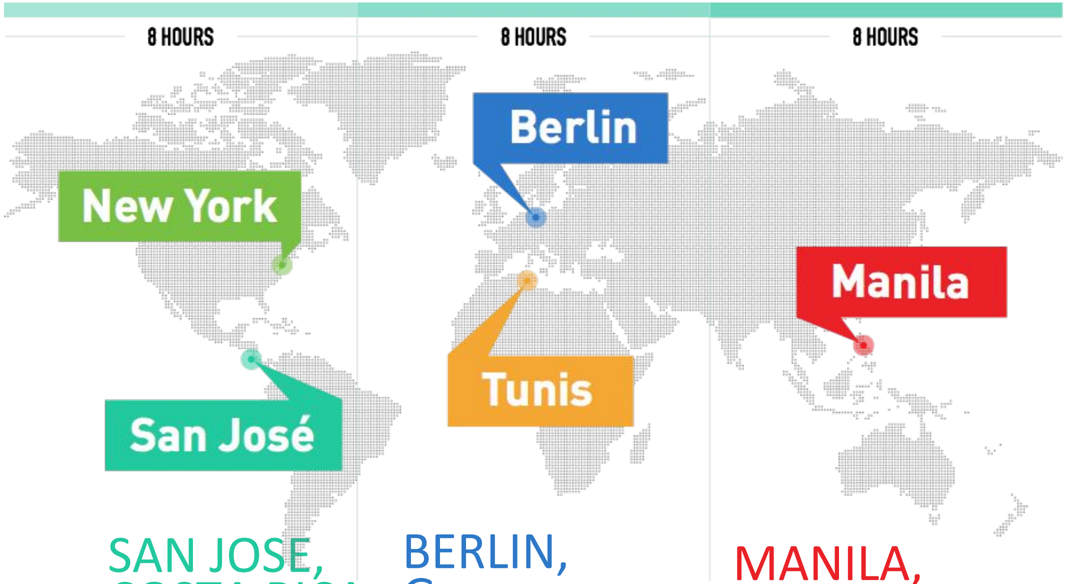
Available 24 hours a day, 7 days a week, 365 days a year

Nimble

Responsive to incidents in a rapid, efficient, and uniform manner

Multilingual

Fluent in English, Arabic, French, Spanish, Portuguese, Russian, and Filipino



SAN JOSE, COSTA RICA
4 Helpline Staff members

BERLIN, Germany
6 Helpline Staff members

TUNIS, TUNISIE
2 Helpline Staff members

MANILA, PHILIPPINES
3 Helpline Staff members

158 digital security requests received involving environmental activists and organizations

🇺🇸	🇻🇳	🇹🇭
28	23	14

Top 3 countries over the 6 years on more than 6000 incident treated

Top Category of incidents treated

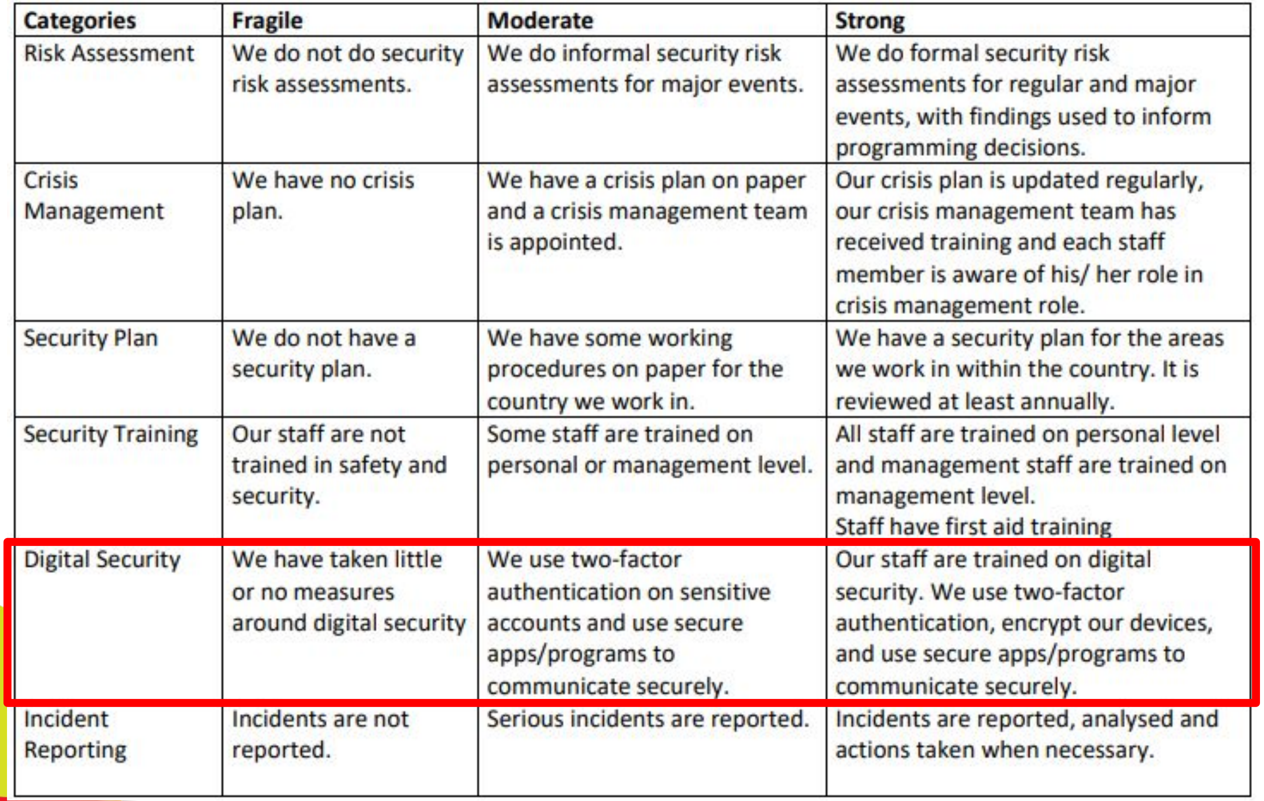
Preventative : Security assessment : 10

Reactive : Incidents related to online accounts : 42

f	25	M	9

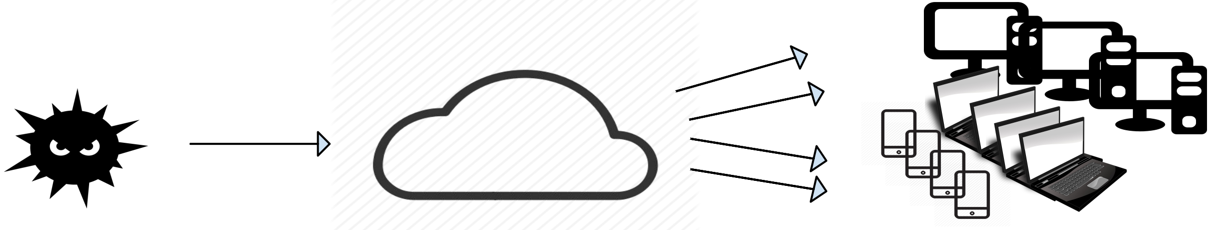
Top 2 online accounts platforms

Health Check

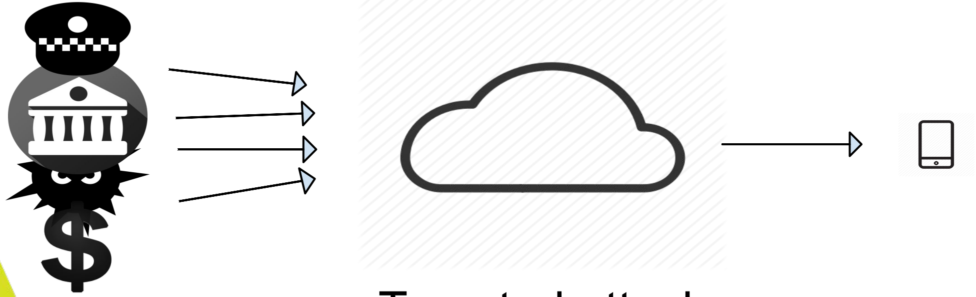


Categories	Fragile	Moderate	Strong
Risk Assessment	We do not do security risk assessments.	We do informal security risk assessments for major events.	We do formal security risk assessments for regular and major events, with findings used to inform programming decisions.
Crisis Management	We have no crisis plan.	We have a crisis plan on paper and a crisis management team is appointed.	Our crisis plan is updated regularly, our crisis management team has received training and each staff member is aware of his/ her role in crisis management role.
Security Plan	We do not have a security plan.	We have some working procedures on paper for the country we work in.	We have a security plan for the areas we work in within the country. It is reviewed at least annually.
Security Training	Our staff are not trained in safety and security.	Some staff are trained on personal or management level.	All staff are trained on personal level and management staff are trained on management level. Staff have first aid training
Digital Security	We have taken little or no measures around digital security	We use two-factor authentication on sensitive accounts and use secure apps/programs to communicate securely.	Our staff are trained on digital security. We use two-factor authentication, encrypt our devices, and use secure apps/programs to communicate securely.
Incident Reporting	Incidents are not reported.	Serious incidents are reported.	Incidents are reported, analysed and actions taken when necessary.

Why Digital Security matters ?

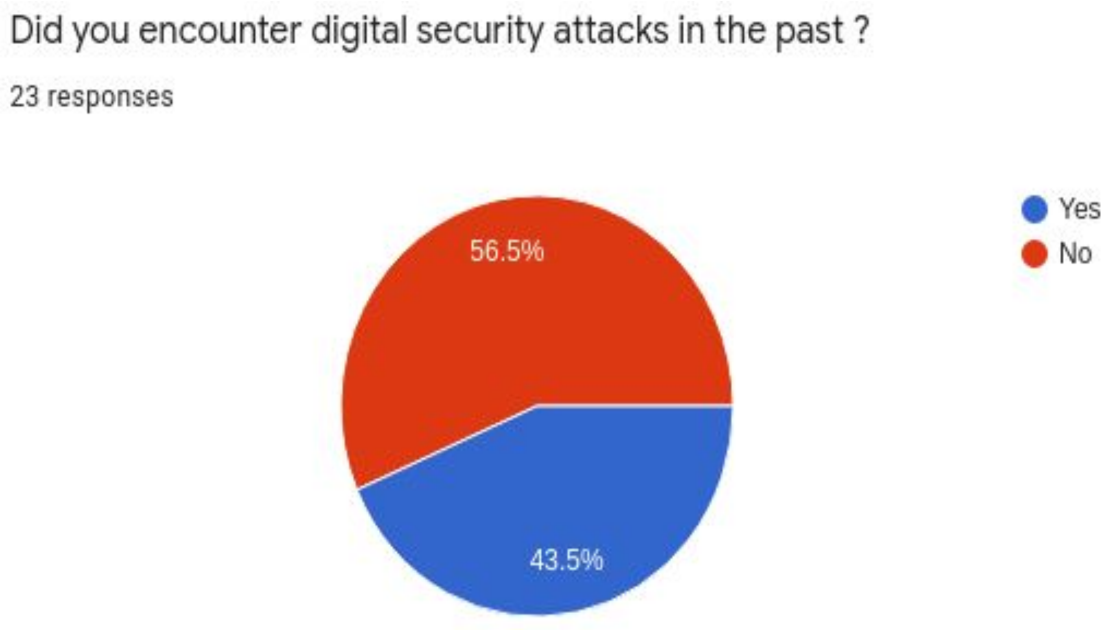


Non targeted attacks



Targeted attacks

Some of the Questionnaire results



Did you encounter digital security attacks in the past ?

23 responses

What is the electronic attack that you fear the most on the internet ? 19 responses
What type of digital attacks did you encounter ? 10 responses

Non Targeted	Targeted
● Attack by malware, Phishing and Hacking and identity theft. ● Stolen credentials : Hacking facebook or twitter account, losing emails ● Attack on the website ● Phishing	● Surveillance, Tracking ● The recording of all my information : could be accessed at a later date by unscrupulous adversaries ● Our partners identities revealed ● Smear campaigns ● Attack by malware, Phishing and Hacking and identity theft. ● Discredit attacks, disclosure of intimate information, promotion of violence ● Stolen credentials : Hacking facebook or twitter account, losing emails ● Massive attack by extremist right groups ● Attack on the website ● Phishing

Preventative services

Organizational Digital Security assistance :
Lightweight Security Assessment :

- Learning about our beneficiaries and their needs
- Identify Top 3 organizational security area of improvements
- Assist implementing the measures

Eg : E.g. assess the security of an organization's website, review/assist with building a digital security policy (onboarding, offboarding, traveling tips, etc …), set up email encryption for all team members, harmonize and improve the security of the adopted communication tools, etc...

Based on SAFETAG https://safetag.org/ Security Auditing Framework and Evaluation Template

Reactive services

- Direct escalation channels with top social platforms

  We successfully built a trust based relationship with the most used online platforms

- Stolen devices
- Online attacks (DDoS, defacement, etc ...)

  Thanks to the experience gained on similar incidents and thanks to our continuous availability, we can intervene very quickly in several languages

Essential Digital Security Recommendations 1/3

- Secure your browsing
  - Using only the browser plugins you need : our recommended ones are
    - **Privacy badger**, **HTTPS everywhere**, and **uBlock origin**
  - Avoid clicking on suspicious links
- Keep your systems and applications (browsers) up to date
- Windows users : Make sure you have a running antivirus
  - PS : Windows Defender is good ! have : Malwarebytes running with it
- Use a password manager and use 2-factor authentication
- Use a VPN, especially when connecting to an untrusted network

FREE options : Psiphon Riseup

Paid options : Tunnel Bear Mullvad

Basic Digital Security Recommendations 2/3

How to spot a phishing attack

- **Watch out for emotions**
- **Examine: sender address, email tone, sender signature**
- **Lookout for common indicators :**

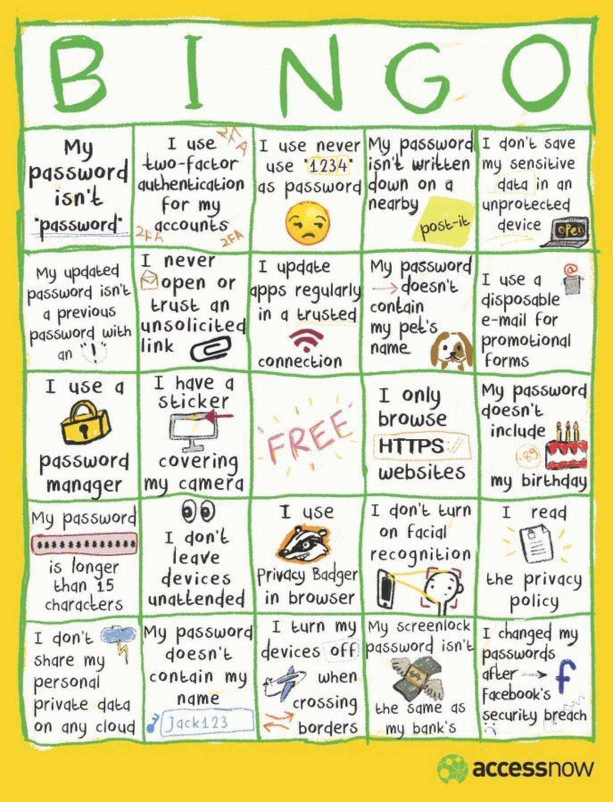
  Links, attachments, login

Source : https://cofense.com/wp-content/uploads/2016/07/phishme-how-to-spot-a-phish.pdf

Read more about phishing attacks here : https://ssd.eff.org/en/module/how-avoid-phishing-attacks

More Digital Security Recommendations: Recap

How good are you at staying safe online? Here's a fun way to find out: see how many of these you can scratch off in our Digital Security Bingo!



B	I	N	G	O
My password isn't 'password'	I use two-factor authentication for my accounts	I use never use '1234' as password	My password isn't written down on a nearby post-it	I don't save my sensitive data in an unprotected device
My updated password isn't a previous password with an "!"	I never open or trust an unsolicited link	I update apps regularly in a trusted connection	My password doesn't contain my pet's name	I use a disposable e-mail for promotional forms
I use a password manager	I have a sticker covering my camera	FREE	I only browse HTTPS websites	My password doesn't include my birthday
My password ************* is longer than 15 characters	I don't leave devices unattended	I use Privacy Badger in browser	I don't turn on facial recognition	I read the privacy policy
I don't share my personal private data on any cloud	My password doesn't contain my name Jack123	I turn my devices off when crossing borders	My screenlock password isn't the same as my bank's	I changed my passwords after Facebook's security breach

accessnow

Some of the Questionnaire results : a trend about secure communication

Is there any digital security topic in particular you want to know about ? 19 responses

- Best practices for **communicating securely with defenders**
- Best **methods to communicate securely;** seem to change so frequently, we had thought whatsapp secure, but no…
- what are the risks in the **communication tools** we use, or in the most common communication tools.
- **phone communications** and why and when we should use signal instead of WhatsApp, what are the dangers of using whatsApp

If the reply to the previous question is Yes, what type of digital attacks did you encounter ?

10 responses

- **Tracking of communications** and location data

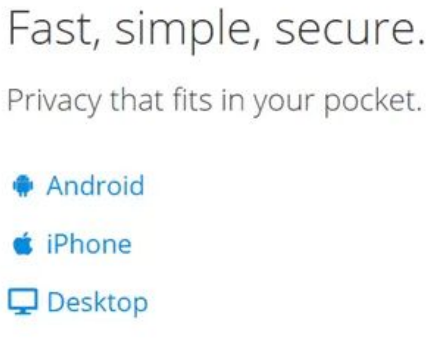
What are the skills you are aiming to acquire with the training ? 24 responses

- **Best practices for communicating** securely with defenders
- How to better protect my data and **communicate safely with others**

Secure messaging : Signal

[Download](#) [Download](#) [Download](#)

- Open source and audited
- End-to-end encrypted
  - Text messages
  - Calls
- **Disappearing messages**
- Robust Privacy policy



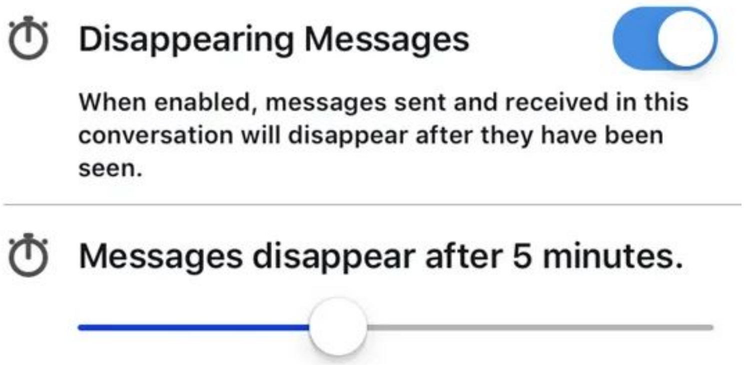
Fast, simple, secure.

Privacy that fits in your pocket.

- Android
- iPhone
- Desktop

We should consider every day lost on which we have not danced at least once. And we should call every truth false which was not accompanied by at least one laugh.

Secure messaging : Signal

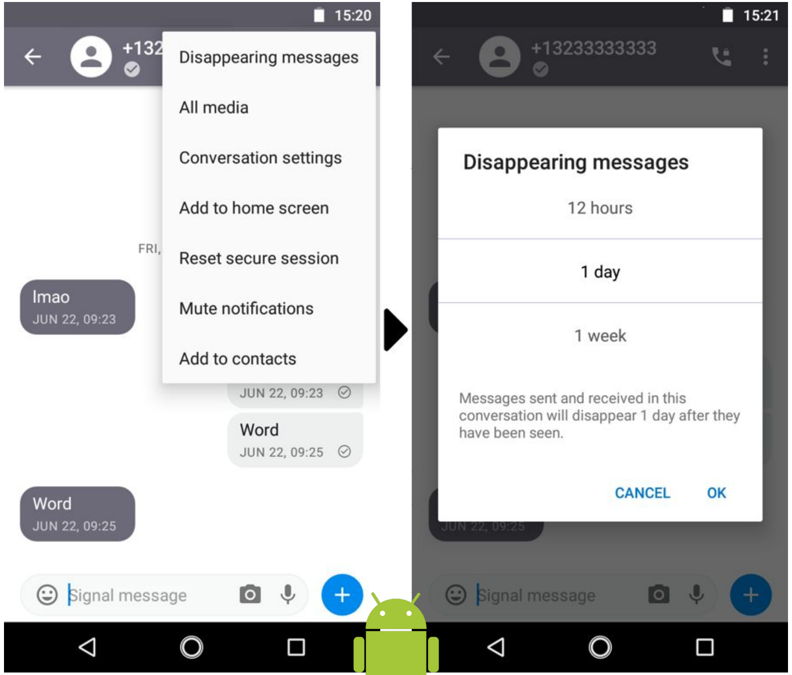


Disappearing Messages

When enabled, messages sent and received in this conversation will disappear after they have been seen.

Messages disappear after 5 minutes.

iOS



Disappearing messages

12 hours

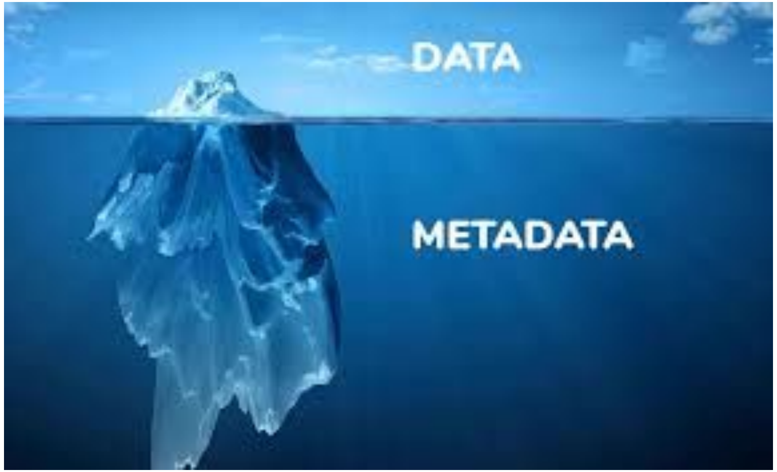
1 day

1 week

Messages sent and received in this conversation will disappear 1 day after they have been seen.

Difference with WhatsApp

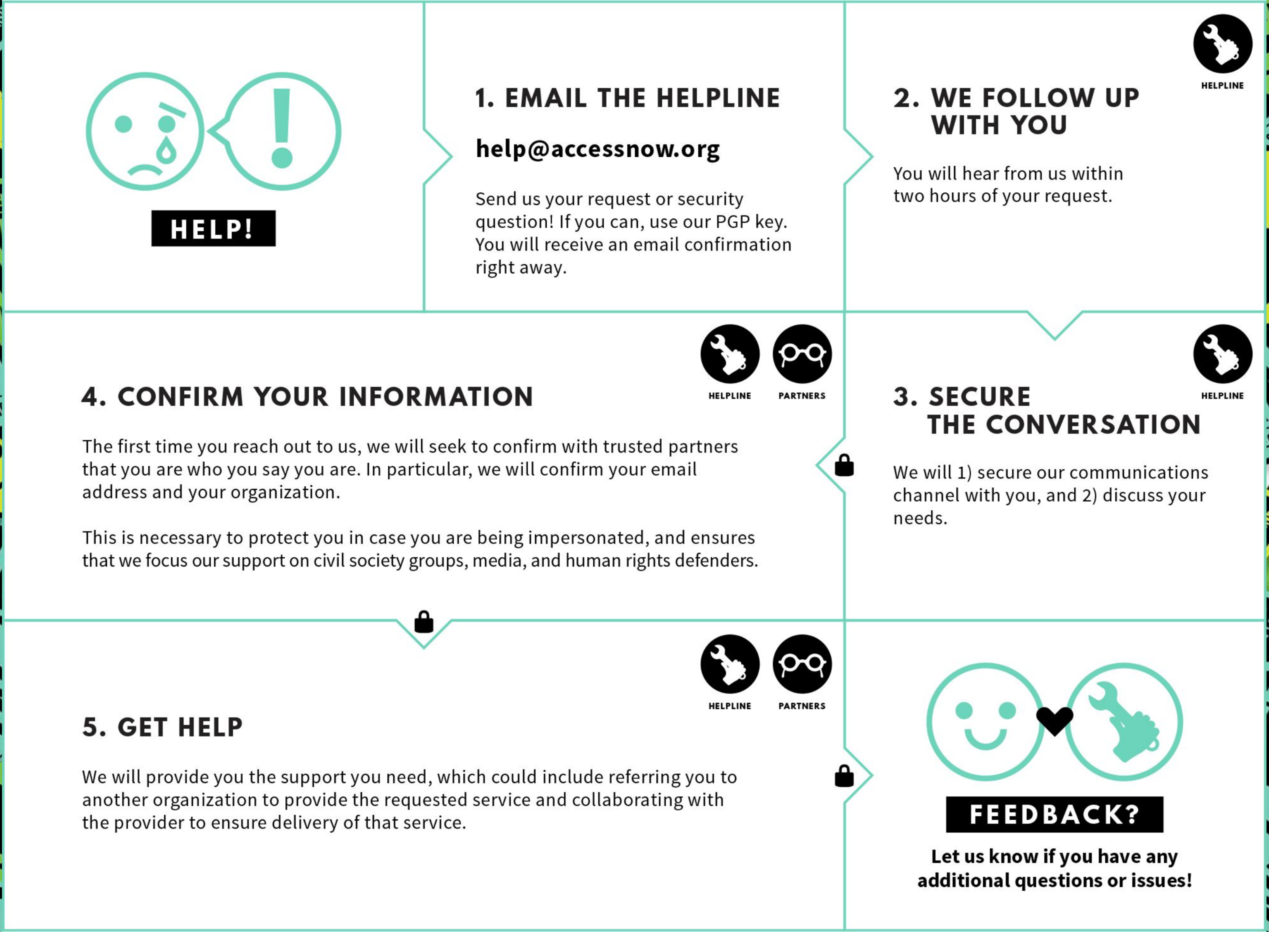
- Both are end-to-end encrypted, **but**



WhatsApp is :

- Owned by a for profit company
- Collects metadata

Why Metadata matters ?
https://ssd.eff.org/en/module/why-metadata-matters



HELP!

1. EMAIL THE HELPLINE

help@accessnow.org

Send us your request or security question! If you can, use our PGP key. You will receive an email confirmation right away.

2. WE FOLLOW UP WITH YOU

You will hear from us within two hours of your request.

3. SECURE THE CONVERSATION

We will 1) secure our communications channel with you, and 2) discuss your needs.

4. CONFIRM YOUR INFORMATION

The first time you reach out to us, we will seek to confirm with trusted partners that you are who you say you are. In particular, we will confirm your email address and your organization.

This is necessary to protect you in case you are being impersonated, and ensures that we focus our support on civil society groups, media, and human rights defenders.

5. GET HELP

We will provide you the support you need, which could include referring you to another organization to provide the requested service and collaborating with the provider to ensure delivery of that service.

FEEDBACK?

Let us know if you have any additional questions or issues!

Thank you for your attention!
Questions?

Do not hesitate to follow up with us on:

help@accessnow.org

6CE6 221C 98EC F399 A04C 41B8 C46B ED33
32E8 A2BC