Security in Whatsapp groups

With the support of Pia Lamberty (social psychologist und Co-CEO of CeMAS)

If you use Whatsapp groups to coordinate help, you should be aware that others can see your private number. The same goes for Signal groups. Telegram is also commonly used for coordinating help, as it is easier to manage large groups and private numbers can be hidden. However, Telegram messages are not encrypted, which is another security risk.

- If you only want to send information but don't need to share between group members, you can either use Whatsapp's new channel feature or change the settings so that only administrators can send messages
- If you want to create a group on Whatsapp with people you don't know, don't share the link in large groups on Facebook or your public Instagram profile
- Make sure that the administrators have to approve each new member of the group
- Make sure you can verify people before they receive the link. For example, you can send the link to people on Facebook after verifying their profile.
- If the link to your group has already been distributed online, create a new one. To reset the link, click on RESET LINK.

Check on Facebook if a profile is trustworthy:

- Check when the profile was created: Fake or hostile profiles are often new profiles with no friends or suspicious friends lists
- Use Google Image Search to see if the profile picture was stolen from someone.
- Check if the profile picture was artificially created. You can find free tools online

https://www.bellingcat.com/resources/2023/09/11/testing-ai-or-not-how-well-does-an-ai-image-detector-do-its-job
https://www.aiornot.com/

Administration on Whatsapp

- Members should only be able to join the group via a link. Do not post the link on forums or websites.
- Restrict who can make changes to groups. Admins determine changes to the group's subject, icon, or description.
- Deletes unwanted messages or removes members. Admins can delete unwanted messages or remove members from the group.
- Admins can restrict who can post in the group if admins cannot ensure that it is a safe space.
- Repeatedly alert users that this group may not be completely safe.

General cybersecurity on Whatsapp

- Be careful about sharing private details: **do you know the members of the group?**
- Enable **2-step verification**: Set up a secret PIN so no one can steal the account. When someone tries to access the account, they must enter both the PIN and a 6-digit code sent to their phone number.
- **Self-deleting messages:** It is possible to specify how long messages remain visible after they have been sent - 24 hours, 7 days or 90 days.
- Use unique view for shared content: For more privacy, photos and videos can be sent so that they disappear from the chat after being opened once.
- Avoid rumors, viral messages, and fake news by making sure content is accurate before forwarding it - especially if it's a chain message and displays the "Forwarded Many Times" notice.

Member tools on Whatsapp

- Checks the group permissions. You can decide who can add you to a group and if you want to stay in a group.
- Members should report inappropriate or harmful content to Whatsapp.
- More information:

https://freedom.press/training/upgrading-whatsapp-security/

Wir sind für euch da. We care. אכפת לנו

Gefördert vom: Bundesministerium für Familie, Senioren, Frauen und Jugend

ZWST MABAT Digitale Transformation