Безопасность в группах Whatsapp

Составлено с помощью Пии Ламберти (социального психолога и содиректора CeMAS).

Если вы используете группы WhatsApp для координации помощи, вам следует знать, что другие могут видеть ваш личный номер. То же самое относится и к группам Signal. Telegram также часто используется для координации помощи, поскольку в нем легче управлять большими группами и можно скрыть личные номера. Однако сообщения в Telegram не шифруются, что является еще одной угрозой безопасности.

- Если вы хотите только отправлять информацию, но не нуждаетесь в обмене между членами группы, вы можете воспользоваться новой функцией каналов WhatsApp или изменить настройки таким образом, чтобы сообщения могли отправлять только администраторы
- Если вы хотите создать в WhatsApp группу с незнакомыми вам людьми, не публикуйте ссылку на нее в больших группах на Facebook или в своем публичном профиле Instagram.
- Убедитесь, что администраторы проверили и одобрили каждого нового члена группы.
- Убедитесь, что вы можете проверить людей до того, как они получат ссылку. Например, вы можете отправить ссылку людям на Facebook после проверки их профиля.
- Если ссылка на вашу группу уже была распространена в Интернете, создайте новую. Чтобы сбросить ссылку, нажмите на кнопку ВОССТАНОВИТЬ ССЫЛКУ.

На Facebook можно проверить, насколько профиль заслуживает доверия:

- Проверьте, когда был создан профиль: Поддельные или враждебные профили часто бывают новыми, без друзей или с подозрительными списками друзей.
- Используйте поиск изображений Google, чтобы проверить, не была ли украдена фотография профиля.
- Проверьте, не была ли фотография профиля создана искусственно. Бесплатные инструменты можно найти в Интернете.

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/

Управление в WhatsApp

- Участники должны иметь возможность присоединиться к группе только по ссылке. Не размещайте ссылку на форумах или веб-сайтах.
- Ограничьте круг лиц, которые могут вносить изменения в группы. Администраторы определяют изменения в теме, значке или описании группы.
- Удаление нежелательных сообщений или удаление участников группы. Администраторы могут удалять нежелательные сообщения или удалять участников из группы.
- Администраторы могут ограничить доступ к сообщениям в группе, если администраторы не могут обеспечить безопасное пространство.
- Обращайте внимание участников на то, что безопасный обмен информацией в этой группе не гарантирован.

Общие вопросы кибербезопасности в WhatsApp

- Будьте осторожны при передаче личных данных: знаете ли вы участников группы?
- Включите двухэтапную верификацию: установите секретный PIN-код, чтобы никто не смог взломать ваш аккаунт. Если кто-то попытается получить доступ к учетной записи, он должен будет ввести как PIN-код, так и 6-значный код, отправленный на ваш номер телефона.
- Самоудаляющиеся сообщения: Можно установить, как долго сообщения остаются видимыми после их отправки - 24 часа, 7 дней или 90 дней.
- Однократный просмотр общего контента: для большей конфиденциальности можно отправлять фото- и видеоматериалы таким образом, чтобы они исчезали из чата после одного открытия.
- Чтобы избежать распространение слухов, вирусных сообщений и фейковых новостей, убедитесь в правильности контента, прежде чем пересылать его дальше, особенно если это цепочечное сообщение и в нем отображается уведомление "Пересылалось много раз".

Инструменты участника в WhatsApp

- Проверьте права доступа к группе. Вы можете решить, кто может добавить вас в группу и хотите ли вы оставаться в ней.
- Участники должны сообщать в WhatsApp о неприемлемом или вредном контенте.

Gefördert vom: Bundesministerium für Familie, Senioren, Frauen und Jugend
ZWST
MABAT Digitale Transformation