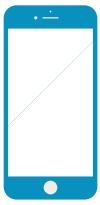
LIFELINE

FOR EMBATTLED CIVIL SOCIETY ORGANIZATIONS

ПРОВЕРОЧНЫЙ СПИСОК МЕР ПО ОХРАНЕ ЦИФРОВОЙ БЕЗОПАСНОСТИ

Следующая информация представляет собой отрывок из пособия «Lifeline», Фонда помощи организациям гражданского общества в ограниченном пространстве (www.csolifeline.org/advocacy-toolkit). Это краткий обзор того, как организации гражданского общества могут думать о своей цифровой безопасности в контексте участия в информационно-просветительских кампаниях.

Проблема	Рекомендации	Совет/справочный материал

Безопасность устройств 	• Придумайте пароль для защиты устройства.
	• Обновляйте систему, когда получаете соответствующее уведомление.
	• Периодически запускайте антивирусную программу.
	• Регулярно создавайте резервные копии устройств.
	• Регулярно удаляйте деликатные сведения (подумайте, стоит ли вам установить программы для безопасного удаления данных).
	• Не подключайте устройство к общественным USB портам и не вставляйте неизвестные USB флэш-диски в свое устройство.
	• Не пользуйтесь общественными сетями WIFI, которым вы не доверяете.
	• Не оставляйте устройство без присмотра на публике / в гостинице/ в конференц-зале
		• Используйте программу управления паролями для хранения паролей: **Keepass**, **LastPass**, **Dashlane**
		• Бесплатные антивирусные программы: **Avira**, **AVG**, **Avast**, встроенная программа Windows Defender.
		• Удаляйте данные безопасным образом: **Bleachbit**
		• Облачное хранение резервных копий:
		  • Облачное хранение, зашифрованное сквозным образом: **Tresorit**
		  • Шифрование на стороне клиента **https://cryptomator.org/** для файлов в облачном хранилище.

Шифрование файлов/диска 	• Включите на своем устройстве полное шифрование диска. • Используйте **Bitlocker** для Виндоуз, **Filevault** рдля Мак или бесплатную программу для шифрования диска из открытого источника – **VeraCrypt** • В большинстве телефонов шифрование уже включено, проверьте настройки, чтобы убедиться, что это действительно так. • Если нужно, то зашифруйте флеш-диски для защиты своих данных	• Если у вас включено шифрование, то для расшифровки данных потребуется как ваше устройство, так и пароль к нему. • Полезный материал: "Безопасное хранение данных" **https:/ssd.eff.org/en/module/keeping-your-data-safe**
Безопасность электронной почты и социальных сетей 	• Придумайте сильный пароль: **https:/xkcd.com/936/** • Не используйте на разных устройствах один и тот же пароль. • Если есть возможность, установите двухфакторную аутентификацию. • С большой осторожностью относитесь к ссылкам и приложениям к электронным письмам.	• Двухфакторная аутентификация усиливает безопасность входа, поскольку требуется воспользоваться двумя методами аутентификации. • Список веб-сайтов с указанием, поддерживают ли они двухфакторную аутентификацию: **https:/twofactorauth.org/**

Lifeline, Фонд помощи организациям гражданского общества в тяжелом положении, предоставляет неотложную финансовую помощь организациям гражданского общества (ОГО), подвергающимся угрозам или нападениям, а также гранты по обеспечению устойчивости, чтобы помочь ОГО отвечать на общие угрозы, ведущие к сужению гражданского пространства. За подробными сведениями обращайтесь на вебсайт нашей организации **https://www.csolifeline.org** или по адресу **info@CSOLifeline.org**. Найдите нас в Twitter **@CSOLifeline**.

Проблема	Рекомендации	Совет/справочный материал
Веб-службы электронной почты со сквозным шифрованием 	При пользовании веб-службами электронной почты со сквозным шифрованием, сообщение могут прочитать только отправитель и получатель.	Некоторые бесплатные почтовые службы: • **Protonmail** • **Tutanota** • **Hushmail**
Зашифрованная переписка по электронной почте 	Если вы обеспокоены тайной и безопасностью коммуникации, можно воспользоваться одним из самых распространенных методов шифрования под названием PGP. PGP, основанный на шифровании с открытым ключом, позволяет уберечь ваши данные от посторонних глаз, так как содержание посланий может прочитать только ваша целевая аудитория.	• Суть «надежной конфиденциальности» (метода шифрования PGP encryption) объясняется в пособии Thunderbird: **https:/guides.accessnow.org/tag_pgp.html** • **Mailvelope** (встроенное приложение для браузера). • Список приложений электронной почту, которые ssподдерживают стандарт **OpenPGP standard: https:/www.openpgp.org/software/**
Мессенджеры с шифрованием 	• Учитывайте, какие из приложений наиболее безопасны для вашей страны/региона: **https:/securityinabox.org/en/guide/secure-communication/**: пользовательские данные и тайна данных, метаданные, свежие новости об охране безопасности. (По состоянию на октябрь 2019 года, самым безопасным мессенджером был Сигнал). • Проверьте настройки безопасности для каждого приложения. • Даже если вы используете наиболее безопасное приложение, есть шанс, что кто-то получит доступ к вашим разговорам или личным файлам, потому что они были сохранены на вашем устройстве. Поэтому нужно, чтобы у вас была процедура регулярного просмотра содержания приложений и удаления деликатных сведений (например, использование функции «исчезающие сообщения»).	• Примите меры для безопасности мобильного телефона **https:/securityinabox.org/en/guide/smartphones/** • Подумайте, что вам нужно от безопасного мессенджера **https:/www.eff.org/deeplinks/2018/03/thinking-about-what-you-need-secure-messenger** • Сигнал, безопасное приложение для обмена сообщениями **https:/freedom.press/training/locking-down-signal/** • Советы по сохранению безопасности в Whatsapp (у него есть определенные проблемы с безопасностью) **https:/www.whatsapp.com/safety** • Как обезопасить приложение для обмена сообщениями **https:/guides.accessnow.org/IM_Tips.html**
Безопасный Просмотр 	• Регулярно обновляйте браузер. • Проверяйте аутентичность вебсайта (посмотрите на ссылку, символ HTTPS в начале строки). • Обезопасьте поиск в интернете: **https:/www.eff.org/https-everywhere** • Используйте VPN для защиты истории поиска от любопытных глаз (особенно, если вы пользуетесь открытой сетью беспроводного интернета).	VPN – это зашифрованный канал между двумя устройствами, который позволяет заходить на любой вебсайт и оналайн приложение безопасно и тайно. • Сравнение разных VPN -служб **https:/thatoneprivacysite.net/** • Настройте собственный VPN **https:/getoutline.org/en/home**