Image not found or type unknown

Мобильная Безопасность

В этом модуле мы работаем с участниками_цами, делясь стратегиями и тактиками более безопасного использования мобильных телефонов в окружающих их ситуациях и контекстах. **Настоятельно рекомендуем** выбрать Путь обучения для планирования, поскольку он содержит упражнения с разным уровнем глубины, которые помогут участникам_цам получить более глубокое представление об изучаемых предметах.

- Введение & Цели обучения
- Обучающие упражнения, Направления обучения & Дополнительные материалы для чтения
- Мобильные телефоны, интимность, гендерный доступ и безопасность [Разминочное упражнение]
- Создаем мобильную хронологию [Разминочное Упражнение]
- Гималайский трекинг [Разминочное Упражнение]
- Когда насильно забирают телефон [Разминочное Упражнение]
- Я и мой мобильный телефон [Разминочное упражнение]
- Сила мобильного телефона - устройства, аккаунт, услуги, государство, политика [Углубленное упражнение]
- Что такое телефон? Как работает мобильная связь? [Углубленное упражнение]
- Дебаты: документирование насилия [Углубленное упражнение]
- Планирование мобильных коммуникаций для действий/организации [Тактическое Упражнение]
- «Создайте резервную копию! Заблокируйте! Удалите!», так же известное под названием «Кто-то взял мой телефон: пересечение границ, аресты, изъятие, кража» [Тактическое Упражнение]

- Дискуссия, вводная информация + практическая работа: выбор мобильных приложений [Тактическое Упражнение]
- Использование мобильных телефонов для документирования насилия: планирование и практика [Тактическое Упражнение]
- Перезагрузите свою безопасность при онлайн-знакомствах [Тактическое Упражнение]
- Безопасный секстинг [Тактическое Упражнение]

Введение & Цели обучения

mobile-safety_RUSSIAN.png

Image not found or type unknown

Картинка. на рисунке надписи: модуль: мобильная безопасность, друзья, общение. изображены люди, которые общаются.

В этом модуле мы работаем с участниками_цами, делясь стратегиями и тактиками более безопасного использования мобильных телефонов в окружающих их ситуациях и контекстах.

В этом модуле предлагаются инструкции для фасилитации дискуссий о том, каким образом опыт доступа к мобильным технологиям и коммуникациям у активисток, выступающих за права женщин и сексуальные права различается в зависимости от их гендера и сексуальной идентичности. Мы поговорим от том, как мы используем наши мобильные телефоны для личных и конфиденциальных коммуникаций, для публичных коммуникаций и коммуникаций движений, а также о стратегиях и инструментах, которые мы используем для более безопасного управления нашими мобильными устройствами.

Данный модуль включает в себя: упражнения для групповых занятий по изучению использования нами мобильных телефонов и того, как это связано с нашей гендерной и сексуальной идентичностью; практические занятия для изучения и понимания того, как работают мобильные телефоны и мобильная связь; упражнения для групповой работы по совместному использованию и практическому применению стратегий и тактик безопасности в контексте нашей жизни; руководство по фасилитации для тренеров_к, направленное на объединение вопросов феминистской и технической безопасности.

Общие вопросы, которые мы часто слышим и на которые попытаемся ответить в этом модуле:

- Что может произойти, если мой телефон окажется у другого человека? Какая информация хранится в моем телефоне? Какое влияние это может оказать на меня,

моих коллег, мое движение?

- Как узнать, следят ли за мной мой партнер, бывшие, члены семьи, государственные органы/правительство?
- Как использовать мой телефон более безопасно?
- Как мы можем использовать собственные телефоны для огранизации?

Цели Обучения

К концу этого модуля у участников_ц будет:

- понимание того, каким образом доступ к мобильной связи и коммуникации носят гендерный и интимный характер;
- понимание безопасности мобильной связи с перспективы того, что мобильные телефоны являются нашими инструментами как для личной, конфиденциальной, так и для публичной коммуникации и коммуникации движений;
- понимание основных концепций работы мобильной связи для лучшего осознания рисков, связанных с мобильными коммуникациями;
- обмен мнениями и практическое применение стратегий и тактик мобильной безопасности для управления влияния наших мобильных коммуникаций на нас самих, наших коллег, наши движения;

*Картинка с рисунком. На рисунке растения синего цвета

image-1605452256072.png
Image not found or type unknown

Обучающие упражнения, Направления обучения & Дополнительные материалы для чтения

На этой странице вы найдете руководство по правильному использованию и пониманию Модуля. Следование Путям обучения, включающим упражнения различной глубины, должно позволить участникам лучше усвоить изучаемые темы.

Направления обучения

Тренеры_ки/фасилитаторы_ки, заинтересованные в каком-либо конкретном упражнении, могут использовать одно из них или несколько в комбинации. **Мы рекомендуем начать с разминочных упражнений, чтобы начать дискуссию и дать возможность участникам_цам поделиться своим опытом использования мобильных телефонов и мнениями о том, как гендер, сексуальность, раса, класс, способности связаны с их опытом и влияют на него.**

Несколько конкретных рекомендаций: группам, которые рассматривают возможность использования мобильных телефонов для **документирования** насилия, мы рекомендуем углубленное упражнение «Документирование насилия», чтобы открыть пространство для дебатов и обсуждения проблем и возможностей документирования насилия, а также тактическое упражнение «Использование мобильных телефонов для документирования насилия: планирование и практика».

Группам, которые хотят использовать **мобильные телефоны для действий** и **организации,** мы рекомендуем тактические упражнения, включая «Планирование

мобильных коммуникаций» и «Создайте резервную копию, заблокируйте, удалите».

Участникам_цам, которые используют мобильные телефоны **для онлайн-знакомств и секстинга**, мы рекомендуем начальное упражнение «Когда насильно забирают телефон» и тактическое упражнение «Перезагрузите свою безопасность онлайн-знакомств» и « Безопасный секстинг».

Обучающие упражнения

Разминочные упражнения

image-1605640724450.png

- Мобильные телефоны, интимность, гендерный доступ и безопасность
- (Новинка) Создаем мобильную хронологию
- (Новинка) Гималайский трекинг
- (Новинка) Когда насильно забирают телефон
- (Новинка) Я и мой мобильный телефон

Углубленные упражнения

image-1605640735000.png

- Сила мобильного телефона - устройство, аккаунт, услуги, государство, политика
- Что такое телефон? Как работает мобильная связь?
- Дебаты: документирование насилия

Тактические упражнения

image-1605640743110.png

- Планирование мобильных коммуникаций для действий/организации

- Создайте резервную копию! Заблокируйте! Удалите! Так же известное под названием «Кто-то взял мой телефон: пересечение границ, аресты, изъятие, кража »
- Дискуссия, вводная информация + практическая работа: выбор мобильных приложений
- (Новинка) Использование мобильных телефонов для документирования насилия: планирование и практика
- (Новинка) Перезагрузите свою безопасность онлайн-знакомств
- (Новинка) Более безопасный секстинг

Упражнения из внешних ресурсов и упражнения на основе инструментов

В тех случаях, когда модули содержат практику и использование конкретных инструментов и программного обеспечения, мы разместили ссылки на внешние ресурсы. Мы делаем это по нескольким причинам: дизайн и функции инструментов, а также аспекты безопасности часто меняются, поэтому нам лучше всего ссылаться на ресурсы, которые часто обновляются.

Специальное примечание для тренинга по мобильной безопасности

Крайне редко бывает так, чтобы у всех участников_ц вашего семинара были одинаковые мобильные телефоны. Рекомендуется проводить практические занятия в небольших группах: для пользователей iPhone, для различных версий Android, и/или для пользователей функциональных телефонов.

Ресурсы | Ссылки | Дополнительные материалы для

чтения

- Пособия «Видео для перемен»: https://video4change.org/resource-categories/
- Пособие для свидетелей: https://witness.org/resources/
- Безопасность в коробке: https://securityinabox.org/en/
- Мои теневые ресурсы: https://myshadow.org/ [Материалы для тренинга больше недоступны, но пособие о том, как контролировать наши данные, все еще доступно .]
- Самозащита от слежки от EFF: https://ssd.eff.org/en

*Картинка с рисунком. На рисунке растения синего цвета



Мобильные телефоны, интимность, гендерный доступ и безопасность [Разминочное упражнение]

starter_activ_circular_400px-with-te

Image not found or type unknown

Картинка. Надпись на картинке: Разминочные Упражнения
Рисунок на картинке: темно-синий круг. В центре круга желтый водоросль с корнями

Данное упражнение представляет собой **вводную дискуссию** о том, как участники_цы используют свои мобильные устройства. Фасилитаторы_ки могут использовать это упражнение, чтобы познакомить участников_ц с концепцией гендерного доступа, подчеркнуть, как мы проявляем множество наших идентичностей в этом мобильном пространстве, и как это создает для нас уникальные возможности и риски.

Мы рекомендуем проводить это упражнение в начале семинара о мобильной безопасности.

Данное упражнение состоит из трех этапов:

- Обмен мнениями в паре
- Отчет пары
- Подведение итогов фасилитатором_кой по общим элементам

Цели обучения, которым отвечает данное упражнение

- Понимание того, как мобильный доступ и коммуникации носят гендерный и интимный характер;

Для кого предназначено данное упражнение?

Это упражнение подходит для всех, кто пользуется мобильным телефоном.

Продолжительность

На это упражнение потребуется около 30 минут.

Ресурсы, Необходимые для данного упражнения

- Белая доска или бумага для флипчарта (в случае, если фасилитатор_ка решит делать записи во время обратной связи)

Техника проведения

Наш мобильный телефон - это пространство для интимного общения. Мы общаемся с близкими, любимыми, друзьями, обмениваемся звонками, сообщениями, фотографиями, видео, личными разговорами и фотографиями. Таким образом, мы воспринимаем наши мобильные телефоны как личные интимные предметы, но они также являются частью более широкого контекста, связанного с провайдерами мобильной связи, регулируемого государственной политикой, подверженного изъятию, просмотру без нашего согласия.

Доступ к мобильным телефонам зависит от гендера, а использование мобильных телефонов женщинами представляет собой вызов для власти – люди могут совершать насилие над женщинами с помощью мобильных телефонов; в другом контексте женщины могут использовать мобильные телефоны, чтобы сообщать о случаях насилия.

Обсуждение в парах - 15 минут

Организация обсуждения в парах способствует обмену мнениями. Попросите сначала одного партнера поделиться мнением, а другого послушать. Затем попросите партнеров поменяться ролями. У каждого в паре должно быть около 5-7 минут для разговора. Это будет зависеть от того, сколько времени потребуется на формирование пар.

Вопросы

Напишите их на видном для всех месте, или на листках бумаги, которые пары смогут взять с собой на обсуждение.

- **Как вы используйте свой мобильный телефон? Когда вы им пользуетесь?** *Если участники_цы затрудняются дать ответ, спросите их, как они используют мобильный телефон с разными типами людей: друзьями, семьей, коллегами, незнакомцами.*
- **Как вы используете мобильные телефоны в организационных целях?**
- ***Когда вы чувствуете себя небезопасно при использовании мобильного телефона? Что вы делаете, чтобы управлять такими ситуациями?*** *Попросите участников_ц не обсуждать случаи кражи, а поделиться такими примерами, как слежка со стороны соседей по квартире, партнеров, членов семьи, изъятие полицией и т.д.*

Обратная связь для всей группы - 15 минут

Фасилитатор_ка делает записи и подводит итоги. Есть ли какие-то конкретные стратегии, ситуации, сценарии, которые вы хотели бы рассмотреть?

*Картинка с рисунком. На рисунке растения цвета хаки

image-1605451879726.png
Image not found or type unknown

Создаем мобильную хронологию [Разминочное Упражнение]

starter_activ_circular_400px-with-te

Image not found or type unknown

Картинка. Надпись на картинке: Разминочные Упражнения
Рисунок на картинке: темно-синий круг. В центре круга желтый водоросль с корнями

Это вводное упражнение, в котором участники_цы делятся личным опытом использования мобильных телефонов и происходит вовлечение через телодвижения и сторителлинг. Следует ожидать, что участники_цы будут рассказывать друг другу о своем отношении к мобильным телефонам и делиться способами использования телефонов и доступа к ним, которые для них являются личными и значимыми.

Данное занятие похоже на упражнение «Женская стена интернета – первые шаги в работе с интернетом», в котором участникам_цам предлагается поделиться своим опытом использования мобильных технологий и соотнести его друг с другом на графике. С помощью этого упражнения тренер_ка(ы_ки) также может(гут) лучше познакомиться с опытом участников_ц и их отношением к мобильным телефонам.

Цели обучения, которым отвечает данное упражнение

- Понимание того, как доступ к мобильному телефону и коммуникациям носит гендерный и интимный характер.

Для кого предназначено данное упражнение?

Упражнение может быть полезно для всех, кто пользуются мобильным телефоном или когда-либо пользовались им.

Продолжительность

На это упражнение потребуется около **30 минут**.

Ресурсы, необходимые для данного упражнения

Метки для обозначения временной шкалы с датами в пятилетних отрезках с 1990 по 2019. Это могут быть числа, написанные на бумаге и разложенные на полу (напр. 1990, 1995, 2000... и т.д.).

Техника проведения

Подготовьте временную шкалу в вашем помещении. Участники_цы будут размещаться вдоль временной шкалы на определенных датах в ответ на заданные вами вопросы. В большой группе попросите участников_ц в ответ на приведенные вопросы перемещаться по шкале к определенной дате. После создания временной шкалы спросите, какими оказались первая и последние даты, а если в определенных местах шкалы наблюдается скопление людей, поинтересуйтесь у них, на каких отрезках они находятся.

В зависимости от размера вашей группы и количества времени, которым вы располагаете, выберите от двух или более вопросов.

Попросите пару участников_ц ответить на конкретные вопросы, например, «Как это было?»

Вопросы

- **Когда у вас впервые появился телефон?** Каким он был? Делились ли вы своим телефоном с кем-нибудь? Сколько вам было лет? Для чего вы его использовали?
- **Когда у вас появился первый смартфон?** Что это значило для вас? Делились вы ли вы им с кем-нибудь? Какое ваше любимое приложение? Почему?
- **Когда вы впервые подключились к интернету с помощью телефона?** Какой сайт вы посетили первым? Почему?
- **Когда вы впервые решили «отпустить на пенсию» свой телефон?** Что вы сохранили с телефона (напр. фотографии, логи текстовых сообщений, аппаратное обеспечение)? Почему?

Подведение итогов - 5-10 минут

Спросите участников_ц, есть ли у них комментарии или наблюдения, которыми они хотели бы поделиться. Фасилитатор_ка, подведите итоги и свяжите то, чем поделились участники_цы, с вопросами интимности и гендерного доступа – проанализируйте то, что они сказали о своем отношении к телефонам и о том, как они любят пользоваться своими телефонами.

> **Флажок интерсекциональности:** как отличается доступ к мобильному телефону и конфиденциальность среди участников_ц в зависимости от их гендера, сексуальности, расы, класса?

*Картинка с рисунком. На рисунке растения красного цвета

image-1605451259399.png
Image not found or type unknown

Гималайский трекинг [Разминочное Упражнение]

starter_activ_circular_400px-with-te

Image not found or type unknown

Картинка. Надпись на картинке: Разминочные Упражнения
Рисунок на картинке: темно-синий круг. В центре круга желтый водоросль с корнями

Данное упражнение является **вводным,** оно направлено на повышение осведомленности участников_ц о мобильной безопасности, а также на то, чтобы участники_цы и фасилитаторы_ки оценили, какие меры безопасности предпринимают участники_цы и какие уязвимые места могут быть наиболее приоритетными для устранения. Мы рекомендуем проводить это упражнение в начале семинара, посвященного мобильной безопасности.

Цели обучения, которым отвечает данное упражнение

- Совместное применение и практическое использование стратегии и тактики для мобильной безопасности и для того, чтобы управлять влиянием наших мобильных коммуникаций на нас самих, наших коллег, наши движения.

Для кого предназначено данное упражнение?

Упражнение может быть полезно для всех, кто пользуется мобильным телефоном или когда-либо пользовался им.

Продолжительность

На это упражнение потребуется около **30 минут**.

Техника проведения

Фасилитатор_ка просит участников_ц встать в линию плечом к плечу. Задайте участникам_цам вопросы о мобильной безопасности. Попросите их делать шаг вперед, если они отвечают на вопрос «да», и шаг назад, если они отвечают «нет».

Вопросы для примера

- Есть ли у вас блокировка экрана?
- Используете ли вы блокировку приложений?
- Есть ли у вас незарегистрированная SIM-карта?
- Используете ли вы альтернативную электронную почту (не основной аккаунт электронной почты) для своего телефона?
- Настроен ли на вашем телефоне удаленный доступ (приложение «Найти мой телефон»)?
- Включены ли на вашем телефоне сервисы определения местоположения?
- Есть ли на вашем телефоне резервная копия медиа файлов (фотографии, сообщения, видео, и т.д.)?
- Установлен ли у вас на телефоне антивирус?

Подведение итогов - 5-10 минут

Спросите участников_ц, есть ли у них комментарии или наблюдения, которыми они хотели бы поделиться. Фасилитатор_ка, подведите итоги и соедините трекинг участников_ц с программой дня или серией семинаров, которые вы будете проводить вместе.

*Картинка с рисунком. На рисунке растения синего цвета

image_1605452256072.png
Image not found or type unknown

Когда насильно забирают телефон [Разминочное Упражнение]

image_not_found or type unknown starter_activ_circular_400px-with-text_russian.png

Картинка. Надпись на картинке: Разминочные Упражнения
Рисунок на картинке: темно-синий круг. В центре круга желтый водоросль с корнями

Данное упражнение является **вводным** и направлено на то, чтобы повысить уровень восприятия участниками_цами своих мобильных устройств и того, что третьи лица имеют доступ к этим устройствам и их содержимому.

Цели обучения, которым отвечает данное упражнение

- Понимание того, как доступ к мобильному телефону и коммуникациям носит гендерный и интимный характер;
- понимание безопасности мобильной связи с перспективы того, что мобильные телефоны являются нашими инструментами как для личной, частной, так и для публичной коммуникации и коммуникации движений.

Для кого предназначено данное упражнение?

Это упражнение особенно хорошо работает в контексте, поскольку участники_цы семинара часто испытывают подобное. Мы рекомендуем это упражнение в том случае, если участники_цы сталкиваются с изъятием устройства и хотят обсудить воздействие данного

факта на них и на их эмоциональную реакцию.

Примечание об осторожности: мы рекомендуем проводить это упражнение с большой **осторожностью**. Получите четкое и выразительное **согласие** от участников_ц. скорее всего, оно лучше всего будет работать в контексте, где вы и ваши участники_цы уже установили **глубокое доверие** друг к другу.

Примечание о направлениях обучения: это отличное разминочное упражнение для подготовки к обсуждению и тактическим действиям по подготовке к ситуациям повышенного риска, в которых телефоны могут быть похищены или утеряны.

Продолжительность

На это упражнение потребуется около **30 минут.**

Техника проведения

Действие: соберите мобильные телефоны участников_ц и начните дискуссию – 15 минут

В самом начале упражнения, получив полное согласие участников_ц, соберите их мобильные телефоны, при этом не объясняя, зачем вы забираете телефоны.

Дискуссия

Спросите:

- Что вы чувствуете, когда не держите телефон в руках?
- Каковы ваши первые ощущения?

Действие: возвращение мобильных телефонов и подведение итогов - 5-10 минут

Возвращаете участникам_цам отобранные в начале упражнения мобильные телефоны.

Дискуссия

- Задайте следующие вопросы:
- Как вы чувствовали себя, расставаясь с мобильным телефоном? Почему?
- Как вы почувствовали себя, получив свой телефон обратно? Почему?
- Возникают ли случаи, когда у вас отбирают мобильный телефон? Кто забирает и в чем заключается ситуация?
- Как вы чувствуете себя в такой ситуации? Почему?
- Почему ваш телефон важен для вас? К чему ваш телефон дает вам доступ?
  Предложите участникам_цам говорить конкретно о том, как они относятся к своим телефонам, с чем их связывает телефон, о важности их телефона.

*Картинка с рисунком. На рисунке растения цвета хаки

image-1605451879726.png
Image not found or type unknown

Я и мой мобильный телефон [Разминочное упражнение]

starter_activ_circular_400px-with-te

Image not found or type unknown

Картинка. Надпись на картинке: Разминочные Упражнения
Рисунок на картинке: темно-синий круг. В центре круга желтый водоросль с корнями

Это упражнение является **вступительной дискуссией**. Оно разработано как очень короткое упражнение, направленное на то, чтобы помочь участникам_цам подумать о том, как они используют свои мобильные телефоны в интимных целях, и начать делиться практикой и опасениями по поводу связанных с этим наблюдением и конфиденциальностью.

Мы рекомендуем проводить это упражнение в начале семинара о мобильной безопасности.

Цели обучения, которым отвечает данное упражнение

- Понимание того, как доступ к мобильному телефону и коммуникациям носит гендерный и интимный характер.

Для кого предназначено данное упражнение?

Упражнение может быть полезно для всех, кто пользуется мобильным телефоном или когда-либо пользовался им.

Продолжительность

На это упражнение потребуется около **30 минут**.

Ресурсы, необходимые для данного упражнения

- Белая доска или бумага для флипчарта (в случае, если фасилитатор_ка решит делать записи во время обратной связи)

Техника проведения

Обсуждение в парах, первая часть - 15 минут

Организация обсуждения в парах способствует обмену мнениями. Попросите сначала одного партнера поделиться мнением, а другого послушать. Затем попросите партнеров поменяться ролями. У каждого в паре должно быть около 5-7 минут для разговора. Это будет зависеть от того, сколько времени потребуется на формирование пар.

Первый вопрос: какими самыми личными и конфиденциальными вещами вы занимаетесь в вашем телефоне?

Второй вопрос: что вы делаете, чтобы охранить это взаимодействие, медиа-файлы, этот опыт?

Фасилитатор_ка, приведите пару примеров того, чем бы вы поделились в парном обсуждении. Например, обнаженные фотографии, которые вы снимаете для собственного удовольствия и самовыражения, секстинг или интимные разговоры, которые вы ведете с другими людьми.

> **Флажок интерсекциональности:** как отличается доступ к мобильному телефону и конфиденциальность среди участников_ц в зависимости от их гендера, сексуальности, расы, класса?

Обратная связь для всей группы - 15 минут

Фасилитатор_ка делает записи и подводит итоги. Попросите участников_ц поделиться тем, о чем они говорили. Выделите общие темы из разговора. Как люди используют свои телефоны, и в чем заключается интимность такого использования? Как, по мнению участников_ц, их гендер связан с доступом к мобильным телефонам, с их частной жизнью? Что делают люди, чтобы охранить свое интимное общение и мобильные медиа-файлы? Что беспокоит людей, и как они соотносят конфиденциальность с гендером, сексуальностью, расой, классом, ограниченными возможностями, возрастом и т. д.?

*Картинка с рисунком. На рисунке растения цвета хаки

image_1605451879726.png
Image not found or type unknown

Сила мобильного телефона - устройства, аккаунт, услуги, государство, политика [Углубленное упражнение]

deepening_activ_circular_400px-wit

Image not found or type unknown

Картинка. Надпись на картинке: Углубленные Упражнения
Рисунок на картинке: зеленый круг. Сверху картины дерево и по всему кругу распущены корни

Это упражнение на **совместное составление ментальной карты**. В процессе фасилитированной дискуссии участники_цы группы обсудят то, как они связаны со своими телефонными устройствами, сервисными аккаунтами, провайдерами мобильных телефонов, и немного поговорят о том, какую роль играет корпоративная и государственная политика.

Мы рекомендуем проводить это упражнение в начале семинара по мобильной связи.

Цели обучения, которым отвечает данное упражнение

- понимание безопасности мобильной связи с перспективы того, что мобильные телефоны являются нашими инструментами как для личной, частной, так и для

публичной коммуникации и коммуникации движений;
- понимание основных концепций работы мобильной связи для лучшего осознания рисков, связанных с мобильными коммуникациями;

Для кого предназначено данное упражнение?

Упражнение может быть полезно для всех, кто пользуется мобильным телефоном или когда-либо пользовался им.

Продолжительность

Исходя из того, что данное упражнение является письменным, оно займет приблизительно **45 минут**. Если вы хотите быстрее охватить этот материал, можете задавать участникам_цам меньше вопросов и показать им слайд с ментальной картой или пример такой карты.

Ресурсы, необходимые для данного упражнения

- Бумага для флипчарта
- Маркеры

Техника проведения

Задайте участникам_цам ряд вопросов и составьте ментальную карту их ответов. Цель – попытаться составить карту того, как они связаны со своими мобильными телефонами. Участники_цы обсудят вопросы мобильной власти, контроля и управления в процессе обсуждения того, как они относятся к своим **мобильным устройствам**, **сервисным аккаунтам**, **провайдерам мобильных телефонов,** а также к **корпоративной и государственной политике**.

Рекомендации по подготовке

- Ознакомьтесь с местными операторами связи;
- Ознакомьтесь со взаимодействием между местными операторами и государством. Например, управляются ли они государством?
- По возможности подготовьте несколько местных примеров того, как активистки по защите прав женщин/гендерных прав используют свои мобильные телефоны, как это связано с властью и как корпорации и/или государство реагируют на/регулируют это;

На видном для всех участников_ц пространстве **нарисуйте ментальную карту**, чтобы она была им видна, когда вы будете задавать им следующие наводящие вопросы.

- Обозначьте места, где участники_цы говорят о выборах или решениях, которые были приняты за них. Например, тип телефона, андроид/нокиа; кто еще имеет доступ к их телефону, как они его выбрали; провайдер услуг; тип тарифного плана; кто имеет доступ к их тарифным планам

Пример ментальной карты. Нажмите, чтобы увеличить.

Mobile_screenshot.png
Image not found or type unknown

На картинке:

В центре: Власть мобильного телефона
Верхняя левая: Мое устройство: 1. Тип телефона: раскладной телефон, смартфон, планшет; 2. Операционная Система: Андроид, Нокиа, другая. 3. Устройство: выбирали по цене, это был подарок, по своим предпочтениям. 4. Общий с еще одним человеком. 5. Одалживаю, когда мне нужно звонить.
Верхняя правая: Мои услуги: 1. Тарифный план: выбран из-за цены, выбирала не я, со мной поделились этим планом; 2. Тарифный план оплачивается вместе с другими людьми; 3. Тарифный план управляется кем-то другим; 4. Отношения с оператором связи – я подписывала договор.
Нижняя левая: Мобильные операторы и правительство. 1. Известная проблема: отключение телефонных линий активистов_к. 2. Известная проблема: местонахождение активистов_к

обнаруживается при помощи мобильных телефонов. 3. Известная проблема: такие записи в телефоне, как содержание текстовых сообщений или телефонных разговоров используется против активистов_к в суде. 4.Телекоммуникационная компания управляется государством. 5. Периодически прерывается доступ к интернету/данным, и мы не можем зайти на определенные веб-страницы. 6. Вопросы, связанные с международным корпоративным или правительственным влиянием.

Вопросы, которые нужно задать

- **Об устройствах**: каким телефоном вы пользуетесь? Как вы приобрели свой телефон? Является ли он общим? Как и с кем вы его делите?
- **О ваших мобильных услугах**: как вы выбрали вашего мобильного оператора? Делитесь ли вы вашим тарифным планом? Управляете ли вы вашим тарифным планом, а если нет, то кто управляет? Вы выбирали ваш план лично? Как?

Спросите/обсудите

Отношения между нами и нашими мобильными провайдерами. Подписывали ли вы условия обслуживания? С чем вы согласились при подписании контракта? С чем согласился ваш провайдер?

Примечание для фасилитаторов_к: если вам известно о конкретных проблемах местных операторов связи, постарайтесь найти и привести примеры условий предоставления услуг и/или разбор конкретных ситуаций, в которых люди/потребители взаимодействовали с операторами связи по вопросам безопасности.

Спросите/обсудите

Отношения между провайдерами мобильной связи и государством. Управляются ли провайдеры государством? Являются ли они международными, местными, региональными компаниями?

Примечание для фасилитаторов_к: возможно, вам следует заранее изучить государственные нормы использования мобильной связи или виды воздействия на него. Были ли в последнее время случаи отключения услуг на государственном уровне? Знакомы ли участники_цы с

целенаправленным отключением отдельных линий? Конфискуют ли органы безопасности мобильные устройства?

Дополнительные ресурсы

Изучение конкретных случаев: *поскольку WRP (программа по правам женщин) продолжает пользоваться этим упражнением, добавьте ссылки соответствующих случаев здесь*

- Страница Википедии, на которой перечислены операторы мобильной связи по странам: https://en.wikipedia.org/wiki/List_of_telephone_operating_companies
- 101: Регистрация SIM карты: https://privacyinternational.org/explainer/2654/101-sim-card-registration

*Картинка с рисунком. На рисунке растения красного цвета



Что такое телефон? Как работает мобильная связь? [Углубленное упражнение]

deepening_activ_circular_400px-wit

Image not found or type unknown

Картинка. Надпись на картинке: Углубленные Упражнения
Рисунок на картинке: зеленый круг. Сверху картины дерево и по всему кругу распущены корни

Целью данного упражнения является углубление знаний о том, как работает мобильная связь, что поможет участникам_цам оценивать и планировать риски, связанные с мобильной связью. Фасилитаторы_ки должны включать это упражнение в любой семинар по мобильной связи, или убедиться, что все участники_цы уже знакомы с информацией, которую содержит данное упражнение. Оно является основой для оценки технических рисков мобильной связи.

Данное упражнение состоит из двух этапов:

- Практическая работа по исследованию телефона
- Вводная информация: данные о мобильной связи и соображения рисков

Цели обучения, которым отвечает данное упражнение

- Понимание некоторых основных концепций работы мобильной связи для составления представления о потенциальных последствиях ее использования;

Для кого предназначено данное упражнение?

Это упражнение для всех участников_ц семинара по мобильной связи.

Продолжительность

На выполнение этого упражнения потребуется приблизительно **45 минут.**

Ресурсы, необходимые для данного упражнения

- Несколько мобильных телефонов для разбора и исследования
- Доска, слайд или учебный материал с указанием основных положений

Техника проведения

В зависимости от наличия времени упомяните или обсудите, что в ходе данного упражнения мы будем говорить о мобильных технологиях – рассматривая устройства, которые легко помещаются в руке или в кармане и имеют коммуникационные функции от голосовых звонков и текстовых сообщений до веб-сервисов и услуг по передаче и обработке данных. Часть данного раздела будет относиться и к планшетам.

Внутри наших телефонов – 5 минут

Разбор телефона по частям. Ваш телефон представляет собой маленький компьютер. Все участники_цы достают свой телефон и находят:

- Детали, которые слушают и воспроизводят звук: микрофоны, динамики
- Детали, которые просматривают и отображают визуальные эффекты: камеры, экраны

- Детали, которые отправляют и получают информацию из других источников: GPS, антенны, Wifi
- Детали компьютера, аппаратное обеспечение: аккумулятор, схема
- Память: SD карта, другая встроенная в телефон память
- Слот(ы) для SIM карты

Идентификаторы устройства и SIM карты – 5 минут

У вашего телефона есть все эти детали, а также несколько идентифицирующих признаков, помимо марки, модели и ОС, у него есть два имени – идентификатор устройства и идентификатор SIMКарты. Важно знать об этом, поскольку вас могут идентифицировать по любому из них, и ваш телефон часто передает эту информацию, в особенности IMSI.

- **IMEI** это имя вашего устройства

Международный идентификатор мобильного оборудования (IMEI): https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity

- **IMSI** это имя вашей SIM карты

Международный идентификатор мобильного абонента (IMSI): https://en.wikipedia.org/wiki/International_mobile_subscriber_identity

Наши телефоны в процессе коммуникации - 35 минут

Мы используем наши телефоны для общения с людьми: текстовые сообщения, сообщения в чатах, социальных сетях, приложениях, звонки. Наши мобильные устройства также передают информацию о наших телефонах и о нас самих – не только в виде сообщений, но и метаданные, наше местонахождение и т. д., и они могут быть связаны с другой информацией о нас, такой как наши социальные сети, наши организационные сети, наши привычки и места работы.

Полезно быть в курсе этих вопросов, в основном для того, чтобы мы могли понять, каким образом наш мобильный телефон может действовать как устройство слежения в данный момент и как историческая запись о нашей деятельности в последующем.

1. Ваш телефон любит общаться

Ваш телефон обращается к различным типам сетей и через различные типы связи, чтобы сообщить о том, что он находится рядом, и чтобы установить связь или проверить, не хочет ли кто-нибудь подключиться.

Операторы мобильной связи

Y операторов мобильной связи есть вышки и антенны, с которыми общается ваш телефон. Каждая антенна может охватывать определенную область. Ваш телефон связывается с той вышкой(вышками), к которой вы находитесь ближе всего. Он как **минимум передает ваш IMSI**, чтобы сообщить, услугами какого мобильного оператора вы пользуетесь, а также ваш номер, чтобы вы могли получать сообщения, звонки и коммуникации на свое устройство. Каждый раз, когда вы оказываетесь рядом с вышкой, вы как будто ставите отметку на картографической шкале времени, сообщая, где вы находитесь. Вы отмечаете, где вы находитесь, когда вы там находитесь, и чем вы занимаетесь на том месте с точки зрения использования вашего телефона.

GPS

если у вас включена функция GPS, ваш телефон связывается со спутниками GPS, аналогично отмечая местонахождение, что является аналогичным установлению отметок на картографической шкале времени.

Wifi

если эта функция включена, то при прохождении через беспроводные сети ваше устройство может как попытаться подключиться к ним, оставляя след в сети wifi, так и сделать запись имени сети в вашем телефоне.

Bluetooth/NFC

если эти функции включены, другие устройства, которые используют Bluetooth и NFC, могут установить связь с вашим устройством, попытаться подключиться, поделиться файлами и т.

д.

Фасилитация обсуждения с помощью вопросов: какие функции нужно оставлять включенными? Являются ли для вас записи о вашем местонахождении риском или нет?

2. Вы любите общаться

Мы используем наши телефоны для общения. Разные виды коммуникации по-разному отображаются во время общения и после отправки сообщения.

SMS

текстовые сообщения и метаданные – в процессе коммуникации и после сохранения на вашем устройстве и у ваших операторов связи отправляются в открытом виде. Полезная аналогия – текстовое сообщение похоже на почтовую открытку. Если кто-то перехватит ее, то сможет прочитать все содержимое письма, а также метаданные (например, отправитель, получатель, время, дата).

MMS

медиа-сообщения и метаданные – в процессе общения могут быть зашифрованы или нет, поэтому, если кто-то пытается перехватить ваше общение, возможность для перехватчика просмотреть сообщения зависит от шифрования сообщений. После отправки MMS сообщение хранится у вас, у получателя, а также у обоих мобильных операторов и на обоих устройствах, таким образом, при исследовании любого из них можно получить метаданные (например, отправитель, получатель, время, дата) а также содержание сообщения.

Звонки

содержание звонков и метаданные - аналогично – звонки должны шифроваться в процессе разговора, но ваш провайдер, а также провайдер получателя сохраняет метаданные звонка (например, отправитель, получатель, время, дата), и, если ваш оппонент имеет доступ к вашим провайдерам, у них может быть доступ на прослушивание звонков или их записи.

Для получения дополнительной информации о приложениях и приложениях для сообщений смотрите:

- Обсуждение, вводная информация + практическая работа: выбор мобильных приложений

Примечание по государственной слежке: наблюдение со стороны государства зависит от страны. В некоторых странах у правительства есть доступ ко всем данным, которые хранятся у операторов связи – в таких случаях следует учитывать, что все метаданные и содержимое незашифрованных услуг доступны правительствам как в режиме реального времени, так и впоследствии, если по этим записям будет проводиться расследование.

Ваша лучшая защита от слежки – сквозное шифрование.

3. Телефон – это маленький компьютер

Программный «жучок»: телефон – это компьютер, и он может быть заражен вредоносным ПО, точно так же, как настольный компьютер или ноутбук. Как частные лица, так и правительства используют программное обеспечение для прослушивания устройств других людей. Такое программное обеспечение часто использует части телефона как «жучок» или устройство слежения, прослушивая телефон с помощью микрофона или отправляя данные о местоположении.

4. Облако – это картотека (хранилище документов)

Некоторые данные, к которым мой телефон имеет доступ, вовсе не находятся в моем телефоне, они хранятся в облаке. «Облако» – это просто термин, и оно подразумевает «интернет», то есть данные, которые хранятся где-то физически на устройстве, которое подсоединено к интернету. Ваши приложения могут получать доступ к данным, которые находятся в облаке, а не на вашем устройстве.

Вопросы, которые необходимо учитывать: зашифрованы ли мои данные при передаче между мной и сервисом? Шифруются ли они при хранении в сервисе? Известны ли мне случаи, когда оппонентам удавалось получить доступ к этой информации – когда, как?

Примечание для фасилитатора_ки: в ходе вашего разговора участники_цы могут задавать вопросы о частях телефонов или рисках, связанных с упомянутыми вами методами коммуникации. Найдите время, чтобы ответить на вопросы. По возможности ведите список вопросов и тем, по которым участники_цы просят дополнительную информацию – для

ведения списка можно применить доску. Также рекомендуется вести список вопросов и тем, которые вы не успеете рассмотреть на этом семинаре, чтобы вернуться к ним позже во время семинара, или предложить в качестве дополнения после семинара.

Дополнительные ресурсы

- 7 Способов найти номер IMEI или MEID вашего телефона: http://www.wikihow.com/Find-the-IMEI-or-MEID-Number-on-a-Mobile-Phone
- Международный идентификатор мобильного оборудования (IMEI: https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity
- Международный идентификатор мобильного абонента (IMSI): https://en.wikipedia.org/wiki/International_mobile_subscriber_identity

На сайте My Shadow компании Tactical Tech есть ряд отличных учебных пособий в помощь при изучении мобильных технологий.

- Материалы для скачивания на My Shadow: https://myshadow.org/materials
- Веб-сайт My Shadow: https://myshadow.org/

*Картинка с рисунком. На рисунке растения синего цвета

image-1605452256072.png
Image not found or type unknown

Дебаты: документирование насилия [Углубленное упражнение]

deepening_activ_circular_400px-wit

Image not found or type unknown

Картинка. Надпись на картинке: Углубленные Упражнения
Рисунок на картинке: зеленый круг. Сверху картины дерево и по всему кругу распущены корни

Данное упражнение предназначено для **углубления дискуссии** с целью фасилитации обсуждения использования мобильных телефонов для документирования насилия, и того, как это связано с увековечиванием насилия. Это упражнение можно использовать для обсуждения примеров, в частности, активистских СМИ, нацеленных на сокращение насилия до способов, которыми те же самые каналы и медиа использовались для увековечивания насилия.

Участники_цы поделятся примерами того, как они используют мобильные телефоны для документирования насилия, и примут участие в дебатах о влиянии обмена документированной информацией о насилии в интернете.

Цели обучения, которым отвечает данное упражнение

- понимание безопасности мобильной связи с перспективы того, что мобильные телефоны являются нашими инструментами как для личной, конфиденциальной, так и для публичной коммуникации и коммуникации движений.

Для кого предназначено данное упражнение?

Для групп, которые используют или рассматривают возможность использования мобильных телефонов для документирования насилия.

Продолжительность

На выполнение этого упражнения потребуется приблизительно **60 минут.**

Ресурсы, необходимые для данного упражнения

- Распечатанные примеры с разбором или ссылки на них

Техника проведения

В ПЛЕНАРНОМ ФОРМАТЕ - 10 минут

Попросите участников_ц поделиться тем, как они используют свои телефоны для документирования насилия.

> **Примечание об осторожности:** участники_цы могут рассказать о случаях, которые являются активирующими для них самих, а также для остальных присутствующих в комнате. Когда вы попросите участников_ц поделиться примерами, подчеркните какие-либо соглашения и нормы вашего пространства, касающиеся разговора о

> насилии. Вы можете отметить, что в ходе упражнения будут обсуждаться акты насилия, и что участникам_цам, которые делятся своим опытом, предлагается в то же время беречь себя, т. е. рассказывать так, чтобы не переоценить свои возможности, попросить их позаботиться о себе, если они чувствуют себя на пределе своих эмоциональных возможностей и прекратить повествование, или же позаботиться о себе другим способом.

Задайте следующие вопросы:

- Какие примеры документирования случаев насилия и соответствующего обмена информацией оказали положительное влияние на вашу работу, правозащитную деятельность, на ваши сообщества?
- Что вы документировали?
- Что произошло?
- Каким образом происходил обмен документированной информации о насилии?
- С кем вы поделились, и как вы выбрали этих людей?
- Какова была реакция?

Фасилитаторы_ки, вы можете подготовить примеры свежих и местных движений, которые используют мобильные телефоны для документирования насилия, и попросить участников_ц рассказать о том, как они используют собственные мобильные телефоны для документирования насилия или для обмена документированной информацией о насилии. Примеры могут включать: документирование государственного насилия, пересылку видеозаписей актов насилия, прямые трансляции насилия, последствия хранения такого рода информации.

Некоторые примеры приведены ниже в разделе **"Дополнительные ресурсы"**. Их можно использовать для разбора примеров в малых группах, или выбрать те примеры, которые являются более актуальными или подходящими для ваших участников_ц.

Объясните, что это упражнение призвано создать пространство для дискуссий и дебатов вокруг данного вопроса.

Малые группы: разбор примеров - 20 минут

Раздайте каждой малой группе по примеру для прочтения и обсуждения. Вы найдете примеры ниже – выберите и отредактируйте сценарии инцидентов, блогов и новостных статей, или выберите или напишите примеры, которые более актуальны для ваших участников_ц.

- О чем пример?
- Каковы аргументы в пользу использования мобильных телефонов для документирования насилия в этом примере?
- Каковы аргументы против использования мобильных телефонов для документирования насилия в этом примере?
- Какими способами можно уменьшить негативное воздействие видео, в котором документировано насилие?

Сценарии

Приведенные ниже являются примерами одного из способов составления сценариев для участников семинара. Предложив более одного сценария, вы можете поднять сразу несколько важных вопросов, которые участники_цы, как вам известно, хотят обсудить. Приведенные здесь примеры направлены на то, чтобы начать разговор о связи документирования с движением, согласием, воздействием и увековечиванием насилия.

Первый сценарий

ваше сообщество сталкивается с насилием и харассментом. Вы и другие члены сообщества объединились, чтобы задокументировать конкретные действия и выложить некоторые из них в социальных сетях с субтитрами и текстом, объясняющим инциденты и происходящее насилие. Вы указываете ссылки на ресурсы, включая список требований, которые выдвигает ваше сообщество, и ресурсы поддержки для людей, которые испытывают подобное насилие.

Второй сценарий

вы стали свидетелем акта насилия на улице и начали прямую трансляцию на своем канале социальной сети, где у вас тысячи подписчиков. Вы не знакомы с людьми, которых

снимаете, и не знаете контекста.

Третий сценарий

вы и ваше сообщество ведете прямую трансляцию демонстраций, чтобы показать их мощь, а также чтобы документировать инциденты насилия и причинения вреда демонстрантам. Вам стало известно, что эти кадры используются местной полицией и оппозиционными группами для преследования демонстрантов и редактируются для создания оппозиционных материалов о демонстрантах, которые также распространяются в социальных сетях.

В пленарном формате: обмен мнениями - 30 минут

Обмен мнениями в составе всей группы – это возможность для каждой группы рассказать о своем случае и обсудить со всей группой текущие задачи, связанные с документированием насилия и распространением этой документированной информации в интернете. Выделите достаточно времени для того, чтобы дать возможность группам поделиться мнениями, а другим - принять участие в обсуждении.

- О чем пример?
- Какие аргументы были приведены за и против использования мобильных телефонов для документирования данного случая насилия?
- Что это означает для других? Сталкивались ли вы с такой проблемой? Что вы думаете об этом? Как вы разрабатываете стратегию для достижения наилучшего возможного воздействия и как вы снижаете вероятность негативного воздействия?

Фасилитатор_ка, в процессе обмена мнениями между участниками_цами выделите общие темы. Что больше всего волнует ваших участников_ц в их работе – могут всплыть некоторые вопросы, которые вы сможете более конкретно обсудить позже во время сессий. Сюда могут входить такие тактические вопросы, как документирование, хранение, распространение; вопросы проверки СМИ, серьезных фейков; вопросы использования СМИ для подстрекательства к насилию и применения обмена документированной информацией о насилии для увековечивания насилия и нанесения вреда.

Дополнительные ресурсы

Примеры и блоги о воздействии документирования насилия

Примеры того, как люди используют мобильные телефоны в процессе организации – мы рекомендуем собрать местные или актуальные текущие примеры того, как организаторы используют мобильные телефоны, и попросить ваших участников_ц и ведущих привести примеры при подготовке к семинару.

- Рабочие-мигранты документируют факты насилия
  - Центр по защите прав мигрантов OFW-SOS

Прямая трансляция актов насилия - разбор примера: этические вызовы интернет-вещания в прямом эфире; Айри Креншоу и и Джастин Пехоски https://mediaengagement.org/research/matters-of-facebook-live-or-death/

- Австралия

Мир настраивается против прямых трансляций. После стрельбы в Крайстчерче Австралия начала борьбу против сырого, необработанного видео-материала; Кейси Нютон, 4 апреля, 2019 https://www.theverge.com/interface/2019/4/4/18294951/australia-live-streaming-law-facebook-twitter-periscope

- Примеры из Бразилии

Послание из Бразилии: при отсутствии видеозаписи, если убит полицейским, значит виновен по умолчанию? Присцилла Нери https://lab.witness.org/dispatch-from-brazil-if-killed-by-police-guilty-by-default-unless-theres-video/

- Whatsapp и насилие в Индии

WhatsApp резко ограничит функцию пересылки по всему миру, чтобы бороться с распространением фейковых новостей после насилия в Индии и Мьянме; Курт Вагнер 19 июля, 2018 https://www.vox.com/2018/7/19/17594156/whatsapp-limit-forwarding-fake-news-

violence-india-myanmar

- Примеры из США

Момент вирусного видео C-SPAN, Hadas Gold, 6/22/2016 https://www.politico.com/story/2016/06/cspan-house-sitin-democrats-224696 Члены Конгресса США ведут прямую трансляцию сидячей забастовки с требованием проголосовать за закон о контроле над оружием.

*Картинка с рисунком. На рисунке растения цвета хаки

image-1605451879726.png
Image not found or type unknown

Планирование мобильных коммуникаций для действий/организации [Тактическое Упражнение]

tactical_activ_circular_400px-withte

Image not found or type unknown

Картинка. Надпись на картинке: Тактические Упражнения
Рисунок на картинке: оранжевый круг. В центре круга синее дерево с плодами

Здесь приведены методические рекомендации для групп, которые организуют акции и участвуют в них, и полагаются на приложения для обмена сообщениями. С помощью этого методического пособия вы можете фасилитировать дискуссии с целью помочь группам рассмотреть виды используемых ими коммуникаций и разработать протоколы управления группой, сообщениями и устройствами, которые отвечают требованиям безопасности для данной коммуникации.

Данное упражнение состоит из трех этапов:

- Картирование коммуникаций и оценка рисков
- Планирование: создание групп и разработка настроек
- Установка приложений (по желанию)
- Внедрение (по желанию)

Если группы все еще не выбрали приложение для обмена сообщениями, которым они хотели бы воспользоваться, проведите упражнение «Дискуссия, вводная информация + практическая работа: выбор мобильных приложений»

Цели обучения, которым отвечает данное упражнение

- Обмен мнениями и практика стратегий и тактик мобильной безопасности для управления влиянием наших мобильных коммуникаций на нас самих, наших коллег, наши движения;

Для кого предназначено данное упражнение?

Данное упражнение предназначено для участников_ц с разным уровнем опыта использования мобильных телефонов. Если среди участников_ц есть люди, которые будут администраторами групп обмена сообщениями, запланируйте внедрение таких проектов на семинаре.

Продолжительность

На выполнение данного упражнения потребуется приблизительно **60 минут** для составления карты и проектирования, и до **трех часов,** если вы будете устанавливать приложения для обмена сообщениями, заниматься картированием, проектированием и внедрением.

Ресурсы, необходимые для данного упражнения

Бумага для участников_ц, чтобы они смогли создать и заполнить картографическую таблицу

Техника проведения

Картирование коммуникаций и оценка рисков

Важный аспект: конфиденциальность

Подумайте о том, что у вас могут быть разные типы сообщений для коммуникации через Signal и что некоторые сообщения могут быть более публичными, чем другие. Составьте карту имеющихся коммуникаций и распределите группы в соответствии с вашими соображениями конфиденциальности.

Какие виды коммуникации вы осуществляете и какие соображения у вас есть относительно того, кто имеет доступ к коммуникации? Предложите участникам_цам рассмотреть эти различные группы. Спросите, есть ли у них больше типов информации -- например, есть ли информация, которую должны знать только два человека, которую должен знать только один человек, документировать и не делиться ею?

КТО	**Примеры Коммуникаций**
1 необходимо держать в очень узком кругу людей, которые знают друг друга	*Местоположение ведущих организаторов*
2 крайне важно знать волонтерам или небольшим группам для координации действий	*Изменения в местоположении толпы*
3 можно делиться открыто	*Время начала митина, группы, которые публично поддерживают это действие*

ПЛАН: Создание групп и настроек

Поработайте с участниками_цами над созданием групп, соответствующих различным типам коммуникации.

Методические рекомендации по созданию группы: мы предлагаем начать с данных конструирующих вопросов. Мы включили примеры предложений по управлению группами и настройками для некоторых распространенных типов групп. Спросите участников_ц, что из этого будет работать, а что нет, помогите группе модифицировать проекты для устранения

тех частей, которые не работают.

Членство

- КТО – кто может присоединиться к этой группе?
- КАК – как люди присоединяются к этой группе? Каковы процедуры? Нужно ли их проверять, знакомиться с ними, могут ли они просто присоединиться, или необходимо зарегистрироваться?
- ПОДТВЕРЖДЕНИЕ – как группа подтверждает вступление человека в группу? Хотелось бы вам, чтобы группа делала это, или нет?
- СООТВЕТСТВИЕ ТРЕБОВАНИЯМ – что делать, если кто-то вступает в группу без соблюдения процедуры?
- ЛИЧНАЯ ИНФОРМАЦИЯ – дает ли служба обмена сообщениями, которой вы пользуетесь, членам группы видеть номера телефонов других членов группы? Если да, то тем, кому необходимо скрыть свой номер из организационных соображений, не следует присоединяться к большим группам, где другие люди еще не знают их номера и того, что они занимаются этой работой.

Знай, с кем ты разговариваешь - ПРОВЕРКА

Для какого типа коммуникаций вы будете проверять, с кем общаетесь?

- ЛИЧНАЯ ВСТРЕЧА – потребуете ли вы, чтобы любой член группы лично встретился с остальными членами группы, чтобы присоединиться к ней? Можно ли просто добавить человека так, чтобы за него поручился один из членов группы?
- БЕЗОПАСНЫЕ НОМЕРА - УБЕДИТЕСЬ, что ваши сообщения доходят до нужных устройств. Если вы используете Signal или Whatsapp, ПОДТВЕРДИТЕ БЕЗОПАСНОСТЬ НОМЕРОВ
- СЛОВА БЕЗОПАСНОСТИ – УБЕДИТЕСЬ, что ваши звонки достигают правильных устройств. Если для звонков вы используете Signal, ГОВОРИТЕ СЛОВА БЕЗОПАСНОСТИ друг другу. Если вы используете другое приложение для звонков, потребуется ли вам проверить в начале разговора, что ваш собеседник — это именно тот, кто вам нужен, чтобы говорить свободно?

Безопасность сообщений - настройки

Исходя из конфиденциальности информации, которую вы передаете, обсудите, какие соглашения вам бы хотелось бы заключить по поводу того, как люди используют настройки сообщений?

- УДАЛИТЬ сообщения – как долго члены группы должны хранить переписку на своих устройствах?
- ИСЧЕЗАЮЩИЕ сообщения – в чате Signal вы можете настроить, как долго сообщения могут оставаться в чате, после чего сообщения автоматически удаляются. Хотите ли вы использовать эту функцию? Как и почему?
- СКРЫТЬ сообщения на домашнем экране – установите приложения для обмена сообщениями так, чтобы в случае, если вы теряете контроль над своим устройством, никто не мог просто взглянуть на ваш экран и увидеть содержимое сообщений
- КОДЫ – для особо конфиденциальной информации мы рекомендуем перед планированием и действием вводить кодовые слова. Например, вы можете вместо того, чтобы писать «Мы готовы к протесту!» заменить эти слова на «Мы готовы к чаепитию».

Распространенные примеры формирования групп

1. Малые группы для конфиденциальной информации, прошедшие строгую проверку

Важный фактор/риск: в группы будут вступать люди, которых вы не знаете, и не хотите, чтобы они имели доступ к информации, которую нежелательно предавать огласке.

- Если у вас есть конфиденциальная информация, которую необходимо передать только известному кругу лиц.
- Очень маленькая группа, 8 человек или меньше, все друг друга знают и встречались лично.
- Добавляйте людей только после личной встречи.

- Проверьте личность участника_цы в очном формате (в приложении Signal, проверить «Безопасные номера»).
- Если чьи-то безопасные номера поменялись, проверьте их лично.
- Не говорите больше, чем нужно, не рискуйте, когда нет необходимости.
- УДАЛИТЕ

2. Подгруппы - малые группы;

Важный фактор/риск: эти люди вступают в группу и рассылают информацию, которая не является полезной, или изначально неверна.

- Это позволяет управлять риском того, что отдельные лица будут спамить большую группу, перенасыщая ее информацией и делая непригодной для использования.
- От 2 до 20 человек, сколько потребуется, чтобы приструнить болтунов и создать управляемое количество подгрупп в Signal.
- В большой группе может быть несколько подгрупп, что делает общение управляемым и актуальным.
- Подгруппы связаны друг с другом, что позволяет обмениваться информацией. Вы можете рассмотреть вариант, в котором в каждой подгруппе будет по одному человеку, который будет распространять информацию, необходимую для всех;

3. Открытая группа, публичная информация

Считайте информацию на этом канале публичной информацией в режиме реального времени. В то время как информация из любой другой группы может случайно просочиться или попасть за пределы группы, считайте, что эта группа уже автоматически публична.

Если у вас есть информация, которой вы хотите поделиться и которую можно довести до сведения общественности, используйте эту группу!

Безопасность устройства

Если у вас забрали устройство, предотвратите возможность того, чтобы другие люди выдавали себя за вас и читали вашу информацию. Например, сообщения в Signal, список контактов, электронную почту и т.д. Для более детальной фасилитации по вопросам безопасности устройства см. упражнение: «Создайте резервную копию! Заблокируйте!

Удалите!», так же известное под названием «Кто-то взял мой телефон: пересечение границ, аресты, изъятие, кража»

- Настройте блокировку на немедленное срабатывание при нажатии любой кнопки
- Установите надежный пароль
- Зашифруйте свой телефон
- Зашифруйте свою SIM карту

Уровень заряда и зона покрытия сети

Что делать, если люди по какой-либо причине не могут воспользоваться Signal или другим приложением, которое вы выбрали, телефонами, интернетом – будь то недостаточный уровень заряда, перегрузка или отключения сети и т.д. Есть ли у вас резервный ресурс или дополнительный доступ в интернет - например, портативная точка беспроводного доступа (и использует ли она для подключения к интернету сотовую сеть, которая тоже может отключиться)? Существует ли план перехода на оффлайн-режим? Есть ли в вашем центре станция подзарядки для волонтеров?

Дополнительные ресурсы

О том, как проверять безопасные номера и о словах безопасности - https://theintercept.com/2016/07/02/security-tips-every-signal-user-should-know/

*Картинка с рисунком. На рисунке растения синего цвета

image-1605452256072.png
Image not found or type unknown

«Создайте резервную копию! Заблокируйте! Удалите!», так же известное под названием «Кто-то взял мой телефон: пересечение границ, аресты, изъятие, кража» [Тактическое Упражнение]

tactical_activ_circular_400px-withte

Image not found or type unknown

Картинка. Надпись на картинке: Тактические Упражнения
Рисунок на картинке: оранжевый круг. В центре круга синее дерево с плодами

В ходе этого упражнения мы планируем наши действия в случае ситуаций, когда участники_цы и их телефоны могут подвергнуться физическому риску, и готовимся к такому развитию событий. Сценарии могут включать в себя следующее:

- Безопасность при участии в акциях протеста
- Безопасность при пересечении границы

- Безопасность при угрозе ареста и конфискации имущества
- Безопасность при угрозе кражи и преследования

Данное упражнение состоит из четырех этапов с дополнительными практическими действиями по установке и подготовке устройств. Этапы включают:

- Современные практики заботы о себе
- Планирование и подготовку наших устройств
- Вводные данные – по желанию

Также по желанию вслед за этим упражнением проведите практические занятия для отработки стратегий и тактик.

Цели обучения, которым отвечает данное упражнение

понимание безопасности мобильной связи с перспективы того, что мобильные телефоны являются нашими инструментами как для личной, конфиденциальной, так и для публичной коммуникации и коммуникации движений;

понимание основных концепций работы мобильной связи для лучшего понимания рисков, связанных с мобильными коммуникациями;

обмен мнениями и практическое применение стратегий и тактик мобильной безопасности, которые позволяют управлять влиянием наших мобильных коммуникаций на нас самих, наших коллег, наши движения;

Для кого предназначено данное упражнение?

Данное упражнение предназначено для участников_ц с разным уровнем опыта в использовании мобильных телефонов и позволит отработать тактическую безопасность с упором на осторожность и мобильные телефоны.

Продолжительность

На выполнение данного упражнения потребуется приблизительно **80 минут**.

Ресурсы, необходимые для данного упражнения

бумага для флипчарта + маркеры для документирования дискуссии в группе

Техника проведения

Это упражнение предназначено для поддержки активистов_к, которые планируют участвовать в рискованных ситуациях, имея при себе свои мобильные телефоны. В конце этого упражнения у них будет карта инструментов и тактик, которыми они смогут воспользоваться.

Современные практики заботы о себе – 20 минут

> ***Примечание о заботе**: это тактическое упражнение для планирования и подготовки использования мобильных телефонов в ситуациях, когда люди и их устройства подвергаются риску. Начните с признания того, что при подготовке к рискованной ситуации нам в первую очередь необходимо подумать о том, как мы заботимся о себе до, во время и после возникновения рискованной ситуации.*

Начните с обоснования и обсуждения того, как люди заботятся о себе в ситуациях повышенного риска.

Попросите участников_ц начать работу самостоятельно. Раздайте им бумагу, попросите подумать над следующими вопросами и записать свои ответы:

- В каких ситуациях вам нужно позаботиться о своей физической безопасности и безопасности вашего мобильного телефона?
- Что вы уже делаете, чтобы заботиться о себе - до, во время и после этих событий?

Попросите участников_ц разделить лист бумаги на три колонки: до, во время и после. Это будет выглядеть приблизительно так:

Пример листа бумаги участников_ц		
ДО	**ВО ВРЕМЯ**	**ПОСЛЕ**

Предложите участникам_цам поделиться своими практиками со всей группой. Запишите их на доске или на листе бумаги, который будет виден всей группе. Повесьте его на видном месте. Попросите людей поделиться практиками, которые они применяют как по отношению к себе, так и к другим.

Участники_цы продолжат использовать этот простой метод организации практик в следующей части семинара.

Планирование и подготовка наших устройств - 45 минут

Если вы работаете с участниками_цами над подготовкой к определенной ситуации, лучше всего работать с фактическим событием. Ниже приведены сценарии, которые вы можете использовать в том случае, если участники_цы семинара не готовятся к конкретному событию, или вашей группе по какой-либо причине требуется дополнительное обучение. Приведенные ниже сценарии являются примерами, и мы предлагаем вам использовать их по своему усмотрению.

Первый сценарий: безопасность при участии в протестах

Вы собираетесь принять участие в массовом протесте. Вам необходимо обеспечить защиту данных в вашем телефоне, во время протеста не допустить слежки за собой, но при этом иметь возможность использовать свой телефон для связи с союзниками в экстренных случаях. Вы также собираетесь использовать свой телефон для документирования протеста и возможных нарушений прав человека, которые там будут происходить.

Второй сценарий: безопасность при пересечении (небезопасных) границ

Вы находитесь в транзитной зоне и собираетесь пересечь границу в небезопасном месте. Вы хотите иметь возможность использовать свой телефон для поддержания связи с союзниками, но не в качестве персонального устройства слежения. Спросите людей, какие стратегии они используют, когда знают, что кто-то другой может иметь доступ к их телефону. Примерами ситуаций могут быть пересечение границы, посадка на самолет, выход на уличный протест.

Третий сценарий: безопасность при угрозе ареста или изъятия устройства

Из надежного источника вы узнали, что по причине вашего активизма вам грозит арест и изъятие устройств.

Четвертый сценарий: безопасность при риске кражи и преследования

Вы опасаетесь, что кто-то может украсть ваш телефон и использовать содержимое с целью подвергнуть вас преследованиям.

Попросите участников_ц зафиксировать свое обсуждение на бумаге, разделив лист на три колонки: до, во время и после. Это будет выглядеть приблизительно так:

Пример листа бумаги участников_ц		
ДО	ВО ВРЕМЯ	ПОСЛЕ

Помогите участникам_цам проработать следующие группы вопросов в малых группах.

Какое влияние оказывается на людей: каковы риски в данном сценарии/событии или опыте, к которым вы готовитесь? На кого они могут повлиять? Подумайте о себе, об информации о людях, которая тем или иным образом находится в вашем телефоне, процессе организации/вопросах, над которыми вы работаете (при необходимости).

Вы можете задать группам нижеприведенные вопросы в качестве наводящих, чтобы выяснить, каким образом снизить воздействие на людей с тактической точки зрения.

До: подумайте, что вы сделаете, чтобы подготовить свой телефон к этому сценарию.

- Какие файлы вы удалите со своего телефона? Почему?
- Какие приложения вы установите? Почему?
- Кому вы сообщите о своих планах? Хотите ли вы создать систему контроля до и после событий сценария, возможно ли это?
- Какую безопасную систему связи вы наладите с другими людьми?
- Какие еще стратегии вы и ваши союзники будете использовать для обеспечения своей безопасности во время происходящего по сценарию?

- Услуги определения местоположения: будет ли для вас безопаснее включить сервис определения местоположения и отслеживания или отключить его? Хотите ли вы, чтобы другие доверенные лица следили за вашим местоположением?
- Дистанционное уничтожение информации: хотите ли вы активировать удаленное уничтожение файлов в случае потери доступа к вашему телефону?

Во время: подумайте о том, как вы будете использовать свой телефон во время происходящего по сценарию.

- Уровень заряда: является ли уровень заряда вопросом для беспокойства? Как вы обеспечите зарядку мобильных телефонов?
- Зона покрытия сети: является ли мобильный сервис проблемой? Что вы будете делать, если люди не смогут воспользоваться мобильными услугами, приложениями, интернетом? Есть какой-либо оффлайн-план?
- С кем вы хотите коммуницировать во время этого того, что происходит по сценарию? Как вы будете с ними общаться?
- Будете ли вы документировать протест? Если да, то используете ли вы для этого какое-либо специальное приложение?
- Кто сможет связаться с вами через ваш мобильный телефон?
- С кем вы будете связываться через свой мобильный телефон?
- Если вам нужно будет воспользоваться не вашей личной, а другой SIM картой, как вы будете выбирать оператора связи? Есть ли такой оператор связи, который безопаснее других для целей вашего общения? Кто сможет связаться с вами? С кем вы будете связываться?

После: подумайте, что вы будете делать после событий сценария.

- Медиа-файлы: если применимо, что вы будете делать с отснятыми материалами, фотографиями, аудио и другими медиаматериалами, которые вы собрали?
- Метаданные и записи, которые делает ваш телефон: какие действия необходимо предпринять в отношении данных, которые создает ваш телефон во время этого события; рассмотрите метаданные, записи о коммуникации, местоположении вашего устройства.
- В случае изъятия: как вы узнаете, что на ваш телефон не установлено шпионское ПО?

- В случае кражи или конфискации: что вы предпримете, чтобы восстановить целостность и сохранность вашего мобильного телефона?

Дайте группе от 30 до 45 минут на разработку планов, стратегий и тактик.

В конце коллективного обсуждения попросите группы рассказать о своих планах, стратегиях и тактиках.

Используйте результаты обратной связи для планирования практической работы по мобильной безопасности.

Подведение итогов (по желанию) - 15 минут

> **Примечания для тренера_ки/фасилитатора_ки:** в зависимости от вашего стиля работы и настроя участников_ц, возможно вам захочется углубить занятие и добавить материалы в процессе подведения итогов группы, или запланировать отдельный раздел обсуждения. Ниже приведены примечания, которые, по нашему мнению, помогут вам при планировании.

До

- Сообщите людям, что вы будете находиться в ситуации, когда придется беспокоиться за себя и личные вещи. Составьте план того, каким образом вы будете поддерживать связь с доверенным лицом, приступая к ситуации и по выходу из нее. Выберите, как часто вы будете выходить на связь, в соответствии с риском, которому вы подвергаетесь.
- Для ситуации с очень высоким риском: мы рекомендуем выходить на связь не реже, чем каждые 10 минут. Например, если вы собираетесь участвовать в акции протеста с высоким риском или пересекать особо опасную границу. Планируйте общаться каждые 10 минут на подходе, при ожидании (если возможно) и во время пересечении границы.
- Для менее рискованных ситуаций: например, вы находитесь в городе и заняты с группой секс-работников_ц. В течение дня вы ездите на встречи и обратно.

Составьте план выхода на связь с вашим доверенным лицом когда вы находитесь в пути и по прибытии на каждую встречу. Выходите на связь, когда ложитесь спать (“ложусь спать”) и когда просыпаетесь (“начинаю день”).

Сотрите это: что из находящегося на вашем устройстве вы, возможно, хотите сохранить в тайне?

- Выйдите из системы: выходите из всех сервисов, в которых вам не нужно находиться. Не оставляйте открытыми сервисы, в которых вам не нужно находиться. Если приложения открыты, в случае когда кто-то заберет ваш телефон у него будет доступ ко всем вашим аккаунтам, он увидит ваши активности, будет действовать в сервисе от вашего имени.
- Блокировка и шифрование: вы можете зашифровать ваш телефон, SD- и SIM-карты, заблокировав каждую из них своим пин-кодом, это означает, что если телефон окажется у другого человека, то он не сможет получить доступ к информации, которая на нем хранится, а так же использовать его в сети без знания вашего пин-кода. *Если вы находитесь в ситуации, где вам угрожают в целях получения данных для доступа, вы можете быть не в состоянии сохранить конфиденциальность своих пин-кодов и паролей. Обсудите данный вопрос с другими и примите это во внимание при составлении планов безопасности.*
- Копирование данных с устройства: многие правоохранительные органы имеют доступ к оборудованию для копирования данных с цифровых устройств, в том числе с мобильных телефонов, ноутбуков, жестких дисков. Если данные с вашего телефона были скопированы, но при этом они зашифрованы, человеку, который сделал копию, потребуется ваш пароль для расшифровки. Если ваш телефон не зашифрован, человек, который скопировал данные с вашего телефона, получает доступ ко всем данным путем копирования.

Не шумите: отключите звуки и графику уведомлений, сохраняйте беззвучный режим.

- Дистанционное уничтожение информации: возможно, вы захотите подключить дистанционное уничтожение информации, или же нет. В некоторых ситуациях вы, возможно, захотите быть готовыми к дистанционному удалению - следует убедиться в том, что у вас и у вашего доверенного коллеги есть возможность дистанционно удалить содержимое вашего телефона, если кто-то его отберет или

же в случае утери.

- SIM карты и устройства: наши мобильные телефоны создают и передают огромное количество информации - сообщения и звонки, которые мы отправляем и совершаем, данные, которые получают приложения, метки местоположения и времени, часто передаваемые операторами мобильной связи. Оцените, стоит ли вам брать в рискованную ситуацию с собой личное устройство. Если да, это устройство может быть перехвачено вашими оппонентами и постоянно отслеживаться. Вместо этого вы можете оставить свой телефон дома и воспользоваться одноразовым устройством, которое вы примените только для этого действия или мероприятия, которое, как ожидается, будет связано с вашей активностью на протяжении мероприятия или действия и которое вы должны будете выбросить после его окончания. Учтите, что для выполнения этого вам необходимы и телефон, и SIM-карта. Как и у вашего телефона, так и у SIM-карты есть идентификатор. Если вы используете свой обычный телефон и одноразовую SIM-карту, а после замените ее своей обычной SIM-картой, вас возможно будет отследить по идентификатору вашего телефона. *Это дорогостоящий вариант, и для того, чтобы телефон иSIM-карта не отслеживались, потребуется много планирования, а так же возможность прекратить использование и уничтожить устройство. Если вы не можете выбросить устройство, вы обдумайте план, как в рискованных ситуациях носить с собой альтернативный телефон, но чем дольше вы будете это делать, тем легче будет его привязать к вам и установить слежку.*
- *Извлечение SIM-карты: если вы попали в рискованную ситуацию без планирования таковой, вы можете извлечь из телефона такие уязвимые детали, как SIM-карту и карту памяти (если возможно). Примечание: в некоторых ситуациях это может быть использовано агрессорами как оправдание для эскалации нанесения вреда.*

Во время

- Удаленное уничтожение информации
- PixelKnot - для шифрования обмена сообщениями
- Firechat - для протестов и отключения сети

После того, как ваш телефон побывал вне вашего контроля:

- Очистите его содержимое или приобретите новое устройство: наша лучшая рекомендация - возврат к заводским настройкам. Если вы можете себе позволить - замените устройство; не переустанавливайте первое устройство, вместо этого отправьте его тому, кто сможет проанализировать, что с ним случилось.
- Ваши сервисы: переустановите пароли для всех ваших приложений.
- Сообщите людям: если ваш телефон был вне вашего контроля, сообщите об этом и о возможных последствиях своим контактам и людям, с которыми вы активно общались.

Дополнительные ресурсы

- Самозащита от слежки от EFF - зашифруй свой телефон - https://ssd.eff.org/en/module/how-encrypt-your-iphone
- Самозащита от слежки от EFF - использование Signal для iPhone - https://ssd.eff.org/en/module/how-use-signal-ios
- Самозащита от слежки от EFF - использование Signal для Android - https://ssd.eff.org/en/module/how-use-signal-android
- Самозащита от слежки от EFF - использование Whatsapp для iPhone - https://ssd.eff.org/en/module/how-use-whatsapp-ios
- Самозащита от слежки от EFF - использование Whatsapp для Android- https://ssd.eff.org/en/module/how-use-whatsapp-android

*Картинка с рисунком. На рисунке растения красного цвета

image-1605451259399.png
Image not found or type unknown

Дискуссия, вводная информация + практическая работа: выбор мобильных приложений [Тактическое Упражнение]

tactical_activ_circular_400px-withte

Image not found or type unknown

Картинка. Надпись на картинке: Тактические Упражнения

Рисунок на картинке: оранжевый круг. В центре круга синее дерево с плодами

Это дискуссионное и вводное упражнение, которое будет направлено на то, чтобы дать возможность участникам_цам выбрать для себя мобильные приложения, особенно после семинара.

Данное упражнение состоит из 3-х этапов:

- Дискуссия: что вы используете и почему?
- Вводная информация: лучшие практики выбора приложений
- Практическая работа: оценка приложений для обмена сообщениями **ИЛИ** практическая работа: оценка популярных приложений

Цели обучения, которым отвечает данное упражнение

понимание безопасности мобильной связи с перспективы того, что мобильные телефоны являются нашими инструментами как для личной, конфиденциальной, так и для публичной коммуникации и коммуникации движений;

обмен мнениями и практическое применение стратегий и тактик мобильной безопасности с целью управления влиянием наших мобильных коммуникаций на нас самих, наших коллег, наши движения;

Для кого предназначено данное упражнение?

Данное упражнение может быть полезно для всех, кто когда-либо пользовался мобильным телефоном и хочет улучшить свои навыки выбора приложений.

> **Флажок интерсекциональности:** это упражнение разработано в формате практики оценки безопасности мобильных приложений, в частности приложений для обмена сообщениями. Другие типы приложений, которые могут быть более актуальны для ваших участников_ц, могут включать в себя следующее:

- приложения для отслеживания менструального цикла/фертильности и данные, которые они собирают, а также средства контрацепции, которые они могут предложить
- приложения для знакомств
- приложения для обмена сообщениями и приложения для немедленного удаления данных
- приложения по обеспечению безопасности, особенно для женщин – какие данные они раскрывают, что можно включить и отключить, имеется ли удаленный доступ,
- игры или другие приложения с интерактивным компонентом
- перфоматичные приложения, такие как tiktok

Продолжительность

Для выполнения упражнения потребуется около **1 часа.**

Ресурсы, необходимые для данного упражнения

- бумага для малых групп, чтобы участники_цы могли делать записи
- доска или большой лист бумаги для записи общих идей
- несколько мобильных телефонов с возможностью передачи данных и магазином приложений

Техника проведения

Дискуссия: что вы используете и почему? – 10 мин

Проводится в пленарном формате. Задайте следующие вопросы: какие пять приложений вы используете чаще всего? Для чего вы их используете? Позаботьтесь о том, чтобы все участники_цы приняли участие в дискуссии.

- составьте список приложений, которые называют участники_цы, спросите, кто еще использует эти приложения, и запишите количество пользователей приложения в комнате
- запишите причины, по которым участники_цы используют приложение

Затем спросите: каким образом вы выбрали эти приложения?

запишите ответы и

обобщите полученную информацию, а затем переходите к следующему этапу.

Вводная информация: лучшие практики выбора приложений – 5 мин

- Проведите исследование! Изучите различные альтернативы, проверьте надежность приложения. Попросите участников_ц поделиться своими методами исследования – можно прочитать об этом в режиме онлайн/оффлайн, спросить у друга, которому, насколько вам известно, нравится проводить исследования. Прочитайте положительные и отрицательные отзывы в центре скачивания.
- Что вы делаете прежде всего, чтобы убедиться в надежности и безопасности приложения? Кто является разработчиком приложения? Что собой представляет его политика соблюдения конфиденциальности? Является ли приложение открытым источником? Известны ли случаи, когда приложение использовалось в целях получения доступа к системам?
- Понимание разрешений, которые запрашивает приложение. Например, для чего игровому приложению может потребоваться доступ к вашей камере или списку контактов?
- Что помогает вам чувствовать себя более безопасно/уверенно во время использования приложения – можете ли вы контролировать разрешения? Известно ли вам, где оно хранит информацию, которая касается лично вас или которую вы получаете в ходе использования приложения? Известно ли вам, куда попадает данная информация?
- В случае если это приложение социальной сети, каким образом вы хотите взаимодействовать с людьми в этом приложении? Что вы можете выбрать среди настроек приватности, того, какой контент доступен для просмотра другими людьми, каким образом люди могут общаться с вами, а вы – с ними? Что входит в настройки по умолчанию, какую информацию о вас они отображают, с кем они вас соединяют? Известны ли вам о каких-либо проблемах с безопасностью в этом приложении? Существуют ли какие-либо механизмы сообщения о проблемах, которые вы можете использовать или которые могут быть использованы против вас ?

Практическая работа: оценка популярных приложений – 15 мин

Зайдите в магазин приложений и попробуйте найти какое-нибудь полезное приложение в зависимости от контекста. Для городской среды подойдет, например, приложение для заказа такси, карта метрополитена и т. д.

Каким образом вы выбираете приложение? Проверьте, (1) какие разрешения оно запрашивает, (2) кто занимается распространением приложения, а также кто управляет и владеет сервисом. Существует множество приложений, которые являются копиями популярных приложений, похожи на то, что вам нужно, например на игру или карту метро, но на самом деле они разработаны, например, с целью передачи вашего местоположения другим лицам. В магазине приложений указан разработчик или компания, которая занимается распространением приложения. Поделитесь тем, что вам известно о том, кто является владельцем приложения/управляет сервисом и проведите исследование, чтобы оценить, насколько характеристики приложения соответствуют или не соответствуют вашим требованиям, а также каким образом они могут повлиять на вашу конфиденциальность и безопасность во время использования приложения. Если вы делаете выбор между несколькими приложениями, которые выглядят одинаково, поищите в интернете дополнительную информацию о приложении и его разработчике/компании, которая занимается распространением приложения, и убедитесь, что вы загружаете правильное приложение.

Упражнение: оценка приложений для обмена сообщениями – 30 мин

Участники делятся на малые группы. Задание для групп:

- определить два-три приложения, которыми участники_цы пользуются для обмена сообщениями
- ответить на наводящие вопросы

В пленарном формате: обмен информацией, каждая группа называет по одному приложению, пока список не будет исчерпан.

Наводящие вопросы:

- Кто из участников_ц использует это приложение? Насколько оно простое в использовании?
- Кто является владельцем приложения? Кто управляет сервисом?
- Где хранятся ваши сообщения?
- Применяется ли шифрование? Какие другие настройки безопасности есть в приложении? Каким образом вы обеспечиваете дополнительную безопасность вашего общения во время использования данного приложения?
- В каких случаях можно использовать данное приложение?
- В каких случаях не рекомендуется использовать данное приложение?

Список приложений для обмена сообщениями и важные аспекты:

SMS

- Все пользуются текстовыми сообщениями
- Оператор сотовой связи. Представляет особый риск при наличии сговора между телефонной компанией и правительством, или же в случае, если телефонная компания принадлежит государству или является коррумпированной.
- Сообщения хранятся у мобильного оператора – существуют различные политики хранения. Сообщения между отправителем и получателем передаются через вышки.
- Шифрование отсутствует.
- Можно использовать для общения на темы, которые не представляют риск.
- Как правило, взимается плата за сообщение.

Звонки

- Все пользуются этой функцией
- Контролируются оператором сотовой связи.
- Хранятся у оператора – это, без сомнения, метаданные.

- Пример ненадежной защиты: «Привет, Гарси!» - инцидент на Филиппинах, где был перехвачен телефонный разговор между экс-президенткой Арройо и главой избирательной комиссии (COMELEC), в котором президентка говорит главе COMELEC , сколько голосов она хочет получить на следующих выборах.
- Можно использовать для общения на темы, которые не представляют риска.
- Как правило, взимается плата за звонок.

Мессенджер Facebook

- Могут использовать все, у кого есть профиль на FB.
- Для мессенджера разработано отдельное приложение
- Шифрование обещано, но не проверено
- Владельцем является Facebook
- Вместо приложения FB используйте Chat Secure. Для общения с другими пользователями FBможно использовать свои учетные данные на FB. Однако для того, чтобы работало шифрование, ваши собеседники также должны быть пользователями Chat Secure и общаться с вами с помощью Chat Secure.
- Как правило, бесплатный, но для использования необходим доступ в интернет/платное подключение для передачи данных.

Google Talk

- Любой пользователь с учетной записью в Google
- Для мессенджера разработано отдельное приложение
- Шифрование обещано, но не проверено
- Владельцем является Google
- Для данного мессенджера можно также использовать Chat Secure.

Signal (рекомендуемое приложение)

- Управляется тех-активистами_ками
- Сквозное шифрование
- Отсутствует облачное хранение. Сообщения хранятся у вас на телефоне или на компьютере, Signal не хранит сообщения после их доставки.
- Звонки также зашифрованы
- Используется для обмена конфиденциальными сообщениями

Telegram

- Популярное приложение для обмена сообщениями
- Сквозное шифрование только для секретных чатов

WhatsApp

- Много пользователей
- Facebook владеет приложением WhatsApp, однако разработчики WhatsApp обещают обеспечивать конфиденциальность пользователей в своей «Политике конфиденциальности»
- Хранит только недоставленные сообщения. (что именно хранит только недоставленные сообщения, сервер WhatsApp?)
- Сквозное шифрование есть, однако если создается резервная копия сообщений на привязанной к аккаунту электронной почте, они хранятся в незашифрованном виде.
- Удобно использовать для общения с группой людей
- Имеются некоторые опасения по поводу того, что владельцем мессенджера является FB

Wire

- Обещано сквозное шифрование, которое находится в процессе проверки
- Разработан бывшими разработчиками Skype -- важно отметить, что у Skype когда-то были «черные ходы» для китайского правительства, которые были созданы в сговоре с этим правительством
- Есть шифрование голосовых звонков

Дополнительные ресурсы

- Что собой представляет шифрование - https://myshadow.org/alternative-chat-apps#end-to-end-encryption-amp-perfect-forward-secrecy
- MyShadow – альтернативные приложения для общения: https://myshadow.org/alternative-chat-apps
- Почему Signal, а не Whatsapp

- Советы, инструменты и рекомендации EFF по обеспечению безопасного общения в режиме онлайн- https://ssd.eff.org/en
- Также рекомендуется поискать в интернете информацию о выявленных в последнее время проблемах с безопасностью в тех приложениях, которые вы планируете включить в практическую работу. Поиск можно вести по следующим ключевым словам: «название приложения + обзор системы безопасности + год», или «название приложения + известные проблемы с безопасностью + год». В зависимости от результатов поиска вы, возможно, решите не обсуждать на тренинге приложение с известными и нерешенными проблемами в области безопасности.

*Картинка с рисунком. На рисунке растения цвета хаки

image-1605451879726.png
Image not found or type unknown

Использование мобильных телефонов для документирования насилия: планирование и практика [Тактическое Упражнение]

Это тактическое упражнение для активистов_к, которые собираются использовать свои мобильные телефоны для документирования насилия.

Об этом обучающем упражнении

tactical_activ_circular_400px-withte

Image not found or type unknown

Картинка. Надпись на картинке: Тактические Упражнения
Рисунок на картинке: оранжевый круг. В центре круга синее дерево с плодами

Это **тактическое упражнение** для активистов_к, которые собираются использовать свои мобильные телефоны для документирования насилия. Участники_цы смогут попрактиковаться в проведении оценки безопасности и составлении плана документирования. После чего участники_цы будут работать со своими мобильными телефонами, чтобы практиковаться в документировании с помощью выбранных ими

приложений и инструментов.

> ***Примечание о заботе:*** *Фасилитаторы_ки, просим вас учесть, что это длительное занятие, которое может занять почти весь день. Обязательно делайте перерывы в процессе работы. Отметьте, что акт документирования является источником стресса, и предложите участникам_цам поделиться упражнениями, которые они считают полезными во время документирования, например, дыхательные и физические упражнения.*

Это упражнение состоит из двух частей:

Первая часть: оценка и планирование

Для начала участники_цы спланируют свою работу, оценив вопросы безопасности и благополучия вовлеченных лиц, и на основе этой оценки составят планы безопасности и примут решения по управлению мобильными телефонами и медиа.

Вторая часть: настройка и практика

После этого участники_цы отработают тактику документирования насилия с помощью мобильных телефонов.

Мы также рекомендуем использовать «Углубленную дискуссию о мобильных телефонах для документирования насилия» и тактики из «Создайте резервную копию! Заблокируйте! Удалите!».

Цели обучения, которым отвечает данное упражнение

- обмен мнениями и практическое применение стратегий и тактик мобильной безопасности с целью управления влиянием наших мобильных коммуникаций на нас самих, наших коллег, наши движения

Для кого предназначено данное упражнение?

Для групп, которые уже используют или рассматривают возможность использования мобильных телефонов для документирования насилия.

Продолжительность

На выполнение данного упражнения потребуется **1 час 45 минут**.

Ресурсы, необходимые для данного упражнения

- Распечатки с примерами из практики или ссылки на них

Техника проведения

Вступление - 5 минут

Поделитесь недавними примерами движений, использующих мобильные телефоны для документирования насилия, и попросите участников_ц рассказать о том, как они используют мобильные телефоны для документирования насилия или для обмена документированной информацией. Примеры могут включать: документирование насилия на государственном уровне, пересылка видеозаписей актов насилия, последствия обладания такими носителями информации.

Первая часть: оценка и планирование – 30 минут

Помогите участникам_цам сформировать малые группы на основе общности ситуаций, в которых они документируют насилие.

> ***Примечание о заботе:*** *Фасилитаторы_ки, побуждайте участников оценивать и планировать свои собственные потребности в заботе. Документирование актов насилия может быть стимулирующим и стрессовым для тех, кто документирует. Попросите участников_ц рассказать о том, как они обеспечивают себя ресурсами, как они работают с другими активистами_ками, чтобы сгладить влияние процессов документирования.*

см. также **«Создайте резервную копию! Заблокируйте! Удалите!»**

Цель и планирование: обсудите цели документирования

- Что вы документируете и почему?
- В чем заключается ситуация?
- Какова цель вашего документирования? Если планируется использовать материалы в качестве доказательства, спланируйте требования к доказательствам. Для получения дополнительной информации см. ресурсы WITNESS "Видео как доказательство": https://vae.witness.org/video-as-evidence-field-guide/

Оценка рисков и обеспечение безопасности: обсудите известные и вероятные проблемы безопасности для людей, которые документируют и которых документируют

- С какими вероятными проблемами безопасности вы столкнетесь во время этой работы? Есть ли вероятность того, что вы столкнетесь с полицией или антагонистами?
- Что в вашем контексте может измениться таким образом, что это повлияет на вашу безопасность, и каков будет ваш план на этот случай? Обсудите некоторые вероятные сценарии. В качестве примера можно привести ситуацию, когда полиция

и другие антагонисты становятся более агрессивными или жестокими. Ответные меры могут включать продолжение документирования, увеличение частоты проверок безопасности среди вашей команды, прекращение процесса документирования.

- Кто будет участвовать в документировании (съемка, поддержка, связь и т. д.) и какая поддержка им необходима?
- Что вы знаете о вопросах безопасности - чувствует ли кто-нибудь из участвующих в процессе в нашей группе себя более или менее безопасно, исходя из содержания или контекста документирования? Какие роли им удобно брать на себя?
- Какие стратегии вы и ваши союзники будете использовать для обеспечения своей безопасности во время документирования?
- Какую роль играет согласие в этом документировании? Будете ли вы запрашивать согласие тех, кого вы документируете, и как они согласятся на то, чтобы их снимали или документировали? Будете ли вы запрашивать согласие тех, кого вы документируете, на совместное использование отснятого материала и документации в дальнейшем?
- Какие вопросы безопасности связаны с тем, что вы владеете этими кадрами? Каковы вопросы безопасности людей, которые фигурируют в отснятом материале? Как вы будете обращаться с отснятым материалом после того, как он будет снят и сохранен на вашем устройстве, в дополнительном хранилище? Подумайте, где вы будете его хранить, кто будет иметь к нему доступ, будет ли хранилище зашифровано, когда вы его удалите.
- Как на вас может повлиять документирование насилия? Какие ресурсы необходимы вам как личности, чтобы быть в порядке и быть спокойными, выполняя эту работу? Какие ресурсы могут предоставить другие? Как вы и ваша команда будете поддерживать друг друга в ваших индивидуальных потребностях в ресурсах, и что вы можете сделать вместе, чтобы поддержать друг друга?

Знайте свои права

- Там, где вы находитесь, каковы ваши права в отношении документирования?
- Как они соотносятся с контекстом документированной информации? Примеры вопросов, которые вы можете задать: законно ли снимать полицию, законны ли публичные собрания?
- Имеет ли право полиция обыскивать ваши устройства?

- Обыскивает ли полиция ваши устройства или принуждает ли людей удалять медиафайлы?

Подготовка вашего устройства

- Используете ли вы свой личный мобильный телефон?
- Какие файлы вы удалите со своего телефона? Почему?
- Какие приложения вы установите или удалите? Почему?
- Сервисы определения местоположения: что является более безопасным для вас - включить или отключить определение местоположения и отслеживание? Есть ли у вас коллеги, которые должны иметь возможность отслеживать ваше местоположение?
- Хотите ли вы активировать функцию дистанционного удаления информации в случае потери доступа к устройству?

Дискуссия: по какой причине вы используете или не используете свой личный мобильный телефон для документирования насилия?

Вводная информация

используйте информацию из упражнения "Что такое телефон?" чтобы объяснить участникам_цам, как мобильные телефоны привязаны к людям, которые ими пользуются, как идентификация работает с наблюдением в реальном времени, как метаданные об использовании телефона и EXIF-данные медиафайлов могут быть использованы для вашей идентификации.

После

Составьте план совместной встречи для подведения итогов. Как все прошло? Что неожиданного произошло, и как отреагировала ваша группа? Что еще требует реагирования? Как чувствуют себя люди, и кто собирается принимать участие в дальнейших действиях?

Пересмотрите ваши договоренности о согласии и обмене информацией. Обязательно поделитесь этими договоренностями с теми, с кем вы будете работать, чтобы передать

отснятый материал.

Дискуссия

что еще вы хотели бы сделать после документирования?

*Картинка с рисунком. На рисунке растения синего цвета

image-1605452256072.png
Image not found or type unknown

Вторая часть: настройка и практика - 60 минут

В зависимости от имеющегося времени вы можете выполнять эти упражнения все вместе или разделиться на малые группы, и участники_цы присоединятся к тем группам, которые больше всего соответствуют их потребностям.

Советы и рекомендации по записи

Как использовать фото-, видео- и/или аудиозапись для документирования насилия

- Найдите в своем телефоне встроенные инструменты для записи: фото, видео, аудио
- Попрактикуйтесь в использовании этих инструментов, изучите советы, приведенные на странице WITNESS "Съемка с помощью мобильного телефона" (ссылка на ресурсы ниже)
- Планируйте съемки, будьте избирательны
  - Снимайте подробности и перспективу: физически приближайтесь, чтобы зафиксировать больше деталей, и отходите назад, чтобы показать более широкую перспективу событий
  - Держите кадры ровно: выберите кадр и держите его ровно не менее 10 секунд, избегайте использования функции приближения изображения, используйте обе руки и прижимайте локти к телу для дополнительной стабильности
  - Для получения более широкого угла съемки держите телефон горизонтально

    - Подойдите поближе с целью записать хороший звук: помните о шуме, который может заглушить интервью
    - Следите за освещением: делайте запись в хорошо освещенном месте и держите солнце и яркий свет за спиной

- При наличии времени поработайте в группах над планированием документирования с использованием этих инструментов. Попрактикуйтесь в создании медиаматериала .
- Если вы будете выкладывать материал на YouTube, подумайте об использовании функции субтитров: https://support.google.com/youtube/answer/2734796?hl=en
- Контекст и донесение ваших посланий. Спланируйте ваши послания. Где вы разместите их, и какой текст вы используете в качестве сопровождения? Как можно связать их с вашими общими целями?

Запись телефонных звонков

Вводная информация: это приложение оказалось полезным для секс-работников_ц, которым угрожали власти.

Использование приложения

Вы можете установить и использовать приложение, которое позволяет вести запись. Для этого потребуются данные для загрузки, данные для проведения звонка, так как приложение будет использовать данные, а не телефонную линию.

- Определите, какое приложение вы хотите использовать, и установите его
    - Google Voice позволяет записывать входящие звонки, но не исходящие
    - Ваш мобильный телефон может иметь встроенное приложение для записи
- Проверьте эффективность функции с партнером
- Потренируйтесь о размещении медиафайлов и их сохранении с телефона в безопасном месте, где вы сможете получить к ним доступ, когда возникнет необходимость.

Использование диктофона

Если вы по каким-либо причинам не можете или не хотите использовать приложение, вы можете работать с другим человеком, используя свой телефон в режиме громкой связи, а

его телефон в качестве записывающего устройства, т. е. диктофона. Некоторые телефоны имеют встроенную функцию записи голоса.

- Определите, какой инструмент или приложение вы хотели бы использовать, и установите его
- Протестируйте с партнером. Чтобы добиться наилучшего звучания, подойдите поближе и записывайте в месте, где нет других громких звуков.
- Потренируйтесь в размещении медиафайлов и их сохранении с телефона в безопасном месте, где вы сможете получить к ним доступ, когда возникнет необходимость.

Скриншоты

Вы можете делать снимки экрана своего телефона, чтобы документировать текстовый харассмент и насилие.

- Выберите приложение для создания скриншотов и потренируйтесь:
  - На Android: на телефоне с Android версии Ice Cream Sandwich вы можете одновременно нажать кнопку уменьшения громкости и кнопку питания, удерживать в течение секунды, и ваш телефон сделает скриншот, который будет сохранен в вашей галерее.
  - iPhone X, XS, XR: нажмите и удерживайте боковую кнопку справа и одновременно нажмите кнопку увеличения громкости, и ваш телефон сделает скриншот, который будет сохранен в «Альбомах» в папке «Скриншоты».
  - iPhone 8 и более ранние версии: нажмите и удерживайте кнопку питания с правой стороны и одновременно нажмите кнопку «Домой». Снимок будет сохранен в папке «Фото». Найдите альбом под названием «Скриншоты».
- Потренируйтесь находить медиафайлы и сохранять их с телефона в безопасном месте, где при необходимости вы сможете получить к ним доступ.

Однако вы не сможете делать скриншоты во всех приложениях. Некоторые приложения, например Signal, имеют настройки безопасности, которые позволяют пользователю запретить другим делать скриншоты определенных разговоров.

Документирование событий для внутренних архивов

При возникновении инцидента, будь он кратковременным, длительным, однократным или повторяющимся, важно документировать информацию о событии. В то время как многие из других тактик связаны с документированием для публичного и социального распространения, эта может быть полезна в основном как внутренняя практика. Где происходит событие, когда, кто участвует, что происходит. Отслеживание этой информации может быть полезно при реконструкции событий, оценке и планировании ответных мер.

Прямая трансляция

Адаптировано из ресурса WITNESS: Прямая трансляция протестов, созданного для активистов в США

Вы ведете прямую трансляцию на каком-либо мероприятии, например, на протесте, митинге и т. д. Обязательно используйте упражнения на планирование и подготовку. Это может быть отличным способом показать происходящие события и привлечь зрителей к поддержке. Есть также некоторые повышенные риски, так как на месте может присутствовать полиция, которая потенциально будет вести прицельное наблюдение за активистами_ками во время событий или после.

- **Местоположение:** намеренно документируйте свое местоположение. Снимайте уличные знаки, здания и достопримечательности, чтобы задокументировать свое местоположение. Также следует подумать о том, как раскрытие вашего местоположения в режиме реального времени связано с вашей собственной безопасностью и безопасностью тех, кого вы снимаете.
- **Идентификация участников_ц:** сможете ли вы получить согласие тех, кого вы снимаете? Как вы хотите и должны защитить их личность? Подумайте о том, как не снимать лица.
- **Определение тактики:** это работает в обе стороны. Вы можете непреднамеренно заснять тактику активистов_к таким образом, что это негативно скажется на них. В то же время вы можете задокументировать тактику полиции, чтобы лучше оценить ее формирования и возможные действия в будущем.
- **Для кого вести прямую трансляцию:** каковы цели вашей прямой трансляции? Хотите ли вы сначала вести прямую трансляцию для небольшой доверенной группы, которая сможет поддержать вас, сделав ретрансляцию вашего медиа?

- **Работайте вместе с командой:** вовлекайте тех, кто может поддержать вас, подключив зрителей к комментариям и обсуждению, и кто может сделать репост медиа по нескольким каналам.
- **Обратитесь с просьбой:** побудите зрителей к действию.
- **Ваше устройство:** хотите ли вы использовать свое личное устройство? Какое бы устройство вы ни использовали, зашифруйте его и защитите паролем. Не используйте отпечаток пальца.

Обратная связь - 10 минут

- Проведите беседу о том, почему мы документируем насилие. Признайте, что эта работа является стрессовой.
- Поделитесь любыми медиаматериалами, созданными инициативными группами.
- Представьте выводы, новые инструменты и советы, которыми делились участники_цы.

Дополнительные ресурсы

- Видео для сети перемен: https://video4change.org/
- WITNESS - Съемка в группах: протесты, демонстрации, митинги - https://library.witness.org/product/filming-in-teams-protests-demonstrations-rallies/
- WITNESS - Съемка с помощью мобильного телефона - https://library.witness.org/product/filming-with-a-mobile-phone/
- WITNESS - Руководство по проведению интервью с лицами, пережившими сексуальное и гендерное насилие - https://blog.witness.org/2013/08/new-how-to-guide-for-interviewing-survivors-of-sexual-and-gender-based-violence/
- WITNESS - Как вести прямую трансляцию протестов (США) - https://library.witness.org/product/livestreaming-protests-usa/ and video https://www.youtube.com/watch?v=Tm4hgbVuPIk
- https://library.witness.org/product/video-metadata/
- UWAZI, https://www.uwazi.io/ - Uwazi - это бесплатное решение для организации, анализа и публикации документов с открытым исходным кодом.

*Картинка с рисунком. На рисунке растения синего цвета

image_1605452256072.png
Image not found or type unknown

Перезагрузите свою безопасность при онлайн-знакомствах [Тактическое Упражнение]

tactical_activ_circular_400px-withte

Image not found or type unknown

Картинка. Надпись на картинке: Тактические Упражнения
Рисунок на картинке: оранжевый круг. В центре круга синее дерево с плодами

Это **тактическое упражнение,** в котором участники_цы обмениваются советами и рекомендациями по безопасности при знакомствах в интернете. Участники_цы будут работать в малых группах или парах, чтобы обновить свои собственные профайлы и практику знакомств в интернете. Участники_цы поделятся различными своими потребностями и предпочтениями в отношении приложений для знакомств, конфиденциальности и безопасности. Участники_цы поделятся опытом и применят на практике различные тактики для повышения уровня конфиденциальности при использовании приложений для знакомств.

> ***Примечание по интерсекциональности:*** *фасилитаторы_ки, предоставьте людям возможность рассказать о том, как их соображенияпо поводу и практика знакомств в интернете связаны с их гендером и сексуальностью. Как гендер и сексуальность ваших участников_ц связаны с приложениями, которые они используют для знакомств? Как они соотносятся с опасениями по поводу конфиденциальности и безопасности?*

Данное упражнение состоит из двух частей:

- Обмен советами и рекомендациями по онлайн-знакомствам и безопасности
- Практическое занятие: перезагрузите свою безопасность при онлайн-знакомствах

Цели обучения, которым отвечает данное упражнение

- понимание того, как доступ к мобильной связи и коммуникации носят гендерный и интимный характер;
- понимание безопасности мобильной связи с перспективы того, что мобильные телефоны являются нашими инструментами как для личной, конфиденциальной, так и для публичной коммуникации и коммуникации движений;
- обмен мнениями и практическое применение стратегий и тактик мобильной безопасности с целью управления влиянием наших мобильных коммуникаций на нас самих, наших коллег, наши движения;

Для кого предназначено данное упражнение?

Для людей, которые пользуются приложениями для знакомств и хотят использовать их более безопасным образом.

Продолжительность

На выполнение данного упражнения потребуется **2-2.5 часа**.

> **Примечание для фасилитатора_ки:** упражнения занимают около 2,5 часов, и мы рекомендуем делать несколько перерывов во время работы.

Ресурсы, необходимые для данного упражнения

- Доступ в интернет
- Мобильные телефоны для обновления профиля в приложении для знакомств
- Флипчарт или доска

Техника проведения

Обмен советами и рекомендациями по онлайн-знакомствам и безопасности

Упражнение на разогрев - 5 мин

- Кто пользуется приложениями для знакомств, какими? Как вы его выбрали и почему?
- Что на данный момент вы думаете о своей безопасности и конфиденциальности и каким образом заботитесь об этом?

Более безопасные знакомства – 30 мин

Прежде чем перейти к приложениям и практической работе с устройствами, организуйте между участниками_цами обмен советами по обеспечению безопасности для знакомств.

Задайте следующие вопросы:

- Что для вас является безопасным поведением при использовании приложений для знакомств в интернете?
- Что вы учитываете при принятии решения о личной встрече?

- Какие стратегии вы используете для того, чтобы знать, что встреча с кем-то безопасна?
- Есть ли у вас запасные планы на случай, если что-то пойдет не так? Договориться с другом/подругой о контрольном звонке? Или сообщить им о том, куда вы идете, с кем встречаетесь и т.д?

Запишите вопросы на флипчарте или в другом месте на виду у участников_ц.

Поделитесь следующими дополнительными советами по обеспечению безопасности и попросите участников_ц обменяться своими советами и добавьте их тоже:

Приложения для знакомств (советы по безопасности)

- Убедитесь, что ваша фотография не раскроет лишнюю информацию, особенно о вашем местонахождении, учебном заведении
- Используйте защищенный и отдельный адрес электронной почты
- Не используйте имя пользователя, схожее с именем вашего другого аккаунта в социальных сетях
- Используйте фотографию, которая отличается от фотографии профиля вашего аккаунта в социальных сетях.
- Не используйте личную информацию
- Будьте внимательны и осторожны при оформлении своего профиля в приложении для знакомств
- Рекомендация для первой личной встречи: договоритесь о встрече в общественном месте. По возможности сообщите другу/родственнику о месте и времени встречи.
- По возможности устанавливайте пароль на свои приложения
- Защитите паролем и зашифруйте свое устройство

Вводная информация: новые модели знакомств

Рассмотрите новые приложения для онлайн-знакомств, такие как Get Shipped (http://www.getshipped.com/) где вы можете найти пару для друзей, а они могут сделать то же самое для вас. Вы также можете обсуждать в приложении пользователей, которых вам подобрали, и делиться проблемами безопасности (например, отмечать пользователей с плохой репутацией, документировать мошенников, делиться советами по выбору пары).

- Каким образом вы уже взаимодействуете с вашими доверенными друзьями и членами сообщества по вопросам онлайн-знакомств?

Практическая работа: перезагрузите свою безопасность при онлайн-знакомствах - 60-90 мин

Начните с краткого изучения информации о себе в интернете - посмотрите, какая информация доступна о вашем имени в приложениях для знакомств. Используя информацию из профиля в приложении для знакомств, поищите себя на других платформах. Попробуйте поискать свое имя пользователя или информацию, которой вы делитесь в своем профиле. Подумайте, какую информацию о вас, доступную за пределами приложения для знакомств, вы не хотите раскрывать для пользователей этих приложений. Исходя из этого, переделайте свой профиль.

В парах пройдитесь по «Советам по безопасности» и обновите свой профиль. Поделитесь друг с другом и поддержите своего партнера, проверив, присутствует ли идентифицирующая информация, может ли он изменить больше элементов, чтобы быть менее идентифицируемым и соответствовать своим целям безопасности.

Замените свои фотографии

Проверьте и замените любые изображения, включая аватар и другие фотографии в профиле, если они не соответствуют советам по безопасности, которым вы хотите следовать. Рассмотрите возможность удаления идентифицирующих метаданных и удаления идентифицирующей информации о других людях на изображениях.

Отредактируйте свой текст

Проверьте и отредактируйте свой текст, если, с точки зрения вашей безопасности, вы раскрываете больше информации, чем хотелось бы. При желании отредактируйте текст вместе с партнером!

Создайте отдельный защищенный адрес электронной почты.

Обмен мнениями - 10 мин

Как все прошло? Что вас удивило? Что было легко? Что было трудно? Что вы собираетесь делать дальше?

Фасилитаторы_ки: интересуются ли участники_цы секстингом? Ознакомьтесь с модулем "Безопасный секстинг".

Дополнительные ресурсы

Статья на испанском языке: «*Конфиденциальность и безопасность в консервативных контекстах: приложения для знакомств для женщин сексуального многообразия».* *Стеффания Паола*: https://www.genderit.org/es/articles/edicion-especial-privacidad-y-seguridad-en-contextos-conservadores-las-apps-de-citas-para

Проверка данных о себе в интернете: https://gendersec.tacticaltech.org/wiki/index.php/Step_1#Self-Doxing

Ресурсы по безопасности в приложениях для знакомств:

- Grindr - https://help.grindr.com/hc/en-us/articles/217955357-Safety-Tips
- Planet Romeo - https://www.planetromeo.com/en/care/online-dating/
- Tinder - https://www.gotinder.com/safety
- OKCupid - https://www.okcupid.com/legal/safety-tips
- Hornet - https://hornet.com/community/knowledge-base/tips-on-how-to-stay-safe/
- Scruff - http://www.scruff.com/gaytravel/advisories/

*Картинка с рисунком. На рисунке растения цвета хак

image_1605451879726.png
Image not found or type unknown

Безопасный секстинг [Тактическое Упражнение]

tactical_activ_circular_400px-withte

Image not found or type unknown

Картинка. Надпись на картинке: Тактические Упражнения
Рисунок на картинке: оранжевый круг. В центре круга синее дерево с плодами

Это **тактическое упражнение,** в котором участники_цы делятся опытом и практикуют тактику более безопасного секстинга.

Цели обучения, которым отвечает данное упражнение

- понимание того, как доступ к мобильной связи и коммуникации носят гендерный и интимный характер;
- понимание безопасности мобильной связи с перспективы того, что мобильные телефоны являются нашими инструментами как для личной, конфиденциальной, так и для публичной коммуникации и коммуникации движений;
- обмен мнениями и практическое применение стратегий и тактик мобильной безопасности с целью управления влиянием наших мобильных коммуникаций на нас самих, наших коллег, наши движения;

Для кого предназначено данное упражнение?

Для людей, которые занимаются секстингом или заинтересованы в секстинге и хотят обсудить и применить на практике способы безопасного секстинга.

Продолжительность

На выполнение данного упражнения потребуется около **двух часов**.

Ресурсы, необходимые для данного упражнения

- Услуга мобильной передачи данных
- Мобильные телефоны

Техника проведения

Обсудите в парах, - 10 минут

- Вы когда-нибудь занимались секстингом? Когда вы впервые занялись секстингом? Чем вы пользовались – телефонами, записками, письмами, открытками, онлайн-чатом.
- Как вы используете свой телефон для секстинга? Приложения, текстовые сообщения, голос, фото, видео и т.д., что вам нравится, какие плюсы и минусы в этом для вас?
- Какие вопросы безопасности и конфиденциальности вы рассматриваете, когда занимаетесь секстингом, и что вы делаете, чтобы обеспечить свою безопасность и конфиденциальность?

Обмен мнениями и стратегиями всей группой: 35 минут

Фасилитация обмена мнениями участников_ц о том, что веселого и приятного в секстинге с использованием телефонов.

> ***Флажок интерсекциональности:*** *существует ли социальная стигматизация вокруг секстинга, и как участники_цы различных гендеров, сексуальностей, рас, классов, возраста по-разному переживают эту стигматизацию? Как участники_цы реагируют на социальное неодобрение?*

Вопросы для обсуждения, которые вы можете задать:

- Какими видами медиа вы любите пользоваться, и какие приложения вам нравятся больше всего. Что вам нравится больше всего? Что бы вы еще хотели делать с помощью приложения, с медиа?
- Что было самым забавным, что вы делали, занимаясь секстингом, и почему?

Обмен стратегиями

Фасилитатор_ка, подготовьте большие листы бумаги со следующими заголовками:

- Заключение договоренностей
- Любовь, которой мы занимаемся, данные, которыми мы делимся
- Приложения и основные аспекты безопасности/устройства:
- Wildcard

Фасилитируйте беседу, используя приведенные ниже наводящие вопросы. Запишите на большом листе бумаги стратегии, которыми поделились участники_цы.

Заключение договоренностей

- Заключайте договоренности со своими партнерами по секстингу - какие договоренности вы хотите заключить о сохранении данных, цифровом или личном обмене?
- Договаривались ли вы когда-нибудь со своими партнерами о секстинге, как вы об этом договариваетесь?
- Случаются расставания, как вы договариваетесь с партнерами по секстингу после разрыва? Сохраняете ли вы и они свои копии данных?

Любовь, которой мы занимаемся, данные которыми мы делимся

– Информация, сопровождающая наши фотографии, и истории, которые она рассказывает:

- Подумайте, хотите ли вы делиться интимными снимками, на которых видно ваше лицо
- Старайтесь скрывать идентифицирующие детали вашего тела, такие как татуировки, родимые пятна и т. д.
- Используйте редакторы Exif, чтобы очистить метаданные фотографии, геотег и т. д.
- Используйте приложения для размытия лица, татуировок и т. д. (например, Pixlr)

Приложения и основные аспекты безопасности/устройства

- Выберите приложение, которое предлагает такие функции конфиденциальности и безопасности, как шифрование, удаление сообщений и блокировку снимков экрана
- Используйте для секстинга безопасный мессенджер, чтобы контролировать отправляемые изображения и сообщения и при желании иметь возможность удалить их.
- *Примечание о жаргоне: «самоуничтожение»* - мы используем snapchat и другие приложения, обещающие «самоуничтожение», но часто они не полностью уничтожают данные, и люди могут получить доступ к изображениям для последующего распространения.
- Установите пароль и зашифруйте свое устройство
- Установите пароль на свои приложения
- Рассмотрите возможность использования безопасного адреса электронной почты и альтернативного номера телефона для вашего аккаунта в приложениях (безопасность приложений, то есть не просто выбор приложений или того, что можно делать с вашими секстинг-приложениями, может быть, в качестве подраздела?)
- Узнайте, как удалять и сохранять
- Проверьте, синхронизируется ли ваше приложение и как вы хотите синхронизировать и сохранять секстинг

Практическая работа: безопасные приложения и редактирование изображений

Дискуссия о выборе приложений для секстинга

Какие приложения используют участники_цы для секстинга и почему? Какие опасения по поводу безопасности вы испытываете при выборе приложения, и какие функции безопасности вам нравятся в вашем приложении? Что вызывает у вас беспокойство?

- Используйте приложения, которые:
- Зашифрованы
- Защищены паролем
- Предотвращают сохранение и скриншоты
- Позволяют удалять сообщения

Оценка SMS и MMS. SMS и MMS не предлагают ни одной из этих функций. Для получения дополнительной информации о SMS и MMS, а также о наблюдении см. упражнение: «Что такое телефон? Как работает мобильная связь?.

Практические упражнения

фасилитатор_ка, эта деятельность дает участникам_цам возможность практиковать стратегии безопасности, рекомендованные тренерами_ками, вносящими вклад в FTX Safety Reboot. Выберите любые упражнения, которые больше всего подходят для вашего контекста. Можно рассмотреть и другие варианты:

- Шифрование и защита устройства паролем
- Удаление идентифицирующей информации с фотографий и мобильных телефонов
- Создание отдельного защищенного адреса электронной почты и номера телефона

Поделитесь этим списком заданий с участниками_цами и попросите их отработать советы в малых группах, используя помощь друг друга и интернет для ответов на вопросы.

Практическая работа с фотографиями

- Потренируйтесь фотографироваться так, чтобы вашего лица не было видно
- Старайтесь скрывать такие характерные особенности вашего тела, как татуировки, родимые пятна и т. д.
- Используйте редакторы Exif, чтобы очистить метаданные фотографии, геотег и т. д.
- Используйте приложения для размытия лица, татуировок и т. д.

Практическая работа с устройствами и приложениями

- Выберите и установите безопасное приложение
- Установите пароль на свои приложения
- Узнайте, как удалять и сохранять чаты
- Узнайте, как удалять изображения с вашего устройства

Обратная связь - 10 минут

Как прошел этот день для вас?

- Что вы делали?
- Предложите участникам_цам поделиться медиафайлами, если они готовы.
- Что было трудно, что легко? Что вас удивило?
- Когда у вас возникали вопросы, где вы искали информацию?

Дополнительные ресурсы

Семинар Luchadoras по секстингу - моменты секстинга: до, во время, после. Хранение и обмен, отзыв согласия и согласие во всех этих моментах.

> **Примечание для тренеров_к:** поскольку удаление изображений из приложений и устройств немного сложнее, здесь приведены некоторые конкретные инструкции для поддержки участников_ц «Умение удалять изображения с вашего устройства» последнее обновление - май 2019 года): «Знание о том, как удалять изображения с

> устройства, требует понимания того, как это сделать в памяти приложения, а также где хранятся изображения в вашем мобильном телефоне. На устройствах IOSэто менее прозрачный процесс, поскольку у вас нет доступа к файлам, кроме приложений, в которых они созданы. Это также зависит от того, используете ли вы приложения чата для создания фотографий или готовите их заранее (используя приложение камеры мобильного телефона)».

Для пользователей Telegram нажмите на заголовок беседы, затем найдите раздел "Фото и видео", оттуда вы можете удалить изображения. Это приведет к удалению изображений из приложения Telegram, но, если вы сохранили эти изображения в другой папке на вашем устройстве, вам придется использовать файловый менеджер для их удаления. Вы также можете просматривать и изучать общие файлы с определенным пользователем или группой.

В Signal нажмите на заголовок беседы. Вы увидите миниатюры общих медиафайлов. Вы можете удалить их оттуда. Опять же, это удалит только изображения/общие медиа в Signal, а если вы сохранили их в другом месте на своем устройстве, там останется копия. Это также относится к тому, с кем вы занимаетесь секстингом.

Для пользователей Android, используя файловый менеджер удаления медиа и изображений в Telegram: перейдите во «Внутреннюю память» и найдите папку Telegram>> Telegram «Изображения» / Telegram «Видео»/ Telegram «Файлы»/ Telegram «Аудио». Затем удалите файлы в этих папках. Для Signal, если вы сохраняете изображения/медиа вне Signal, вы можете выбрать место для хранения. Другие места, где могут храниться ваши изображения/медиа: «Внутренняя Память»>> «Изображения». Вы найдете каталоги (папки), в которых хранятся ваши изображения. Здесь по умолчанию сохраняются изображения из Signal.

*Картинка с рисунком. На рисунке растения цвета хаки

image-1605451879726.png
Image not found or type unknown