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

Revision #2
Created 24 April 2023 17:31:19 by Kira
Updated 26 April 2023 04:07:35 by Kira