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

Revision #2
Created 24 April 2023 17:32:00 by Kira
Updated 26 April 2023 04:13:51 by Kira