Оценка цифровых рисков

Шаблон

Эта "Оценка цифровых рисков" поможет вам выявить и оценить потенциальные угрозы цифровой безопасности, связанные с вашей историей или заданием.

По мере выполнения оценки вы найдете ссылки на соответствующие разделы нашего **"Руководства по цифровой безопасности"**. В них вы обнаружите дополнительную информацию о том,как можно снизить различные цифровые риски и уменьшить подверженность потенциальным угрозам.

Просмотрите ресурсы **ЦИФРОВОЙ БЕЗОПАСНОСТИ**, которые помогут вам выполнитьэту оценку.

Пожалуйста, сохраните копию этой формы для справки.

RORY PECK TRUST

WWW.RORYPECKTRUST.ORG

Дата

1. Опишите ваше задание

Прежде чем вы сможете правильно определить основные риски для вашей цифровой безопасности, рекомендуется разбить свое задание на составляющие и рассмотреть его ключевые элементы. Постарайтесь определить все основные компоненты: сюжет, респонденты, поездки и любые другие действия, которые жизненно важны для ваших планов. Как только вы это сделаете, вам будет легче определить все области, которые необходимо учитывать при оценке рисков.

Перечислите и укажите как можно больше деталей о следующем:

Описание сюжета

Ключевые респонденты

Планы поездок

Проживание

Ключевые действия

2. Какие цифровые риски возникают при освещении этой истории?

Теперь подумайте о своих основных рисках, угрозах и противниках.

Помните, что вам не обязательно освещать спорную или деликатную историю, чтобы быть уязвимыми с точки зрения цифровых технологий. Вам следует выработать привычку выполнять оценку рисков для всех заданий или историй, так как в ходе этого процесса могут быть выявлены потенциальные угрозы, о которых вы еще и не думали.

Подумайте о следующем:

a) Будете ли вы вступать в контакт или брать интервью у уязвимых людей?

Если да:

- Как вы будете хранить и защищать данные этих людей?
- Где и как вы будете хранить ваши заметки и материалы?

Дополнительные вопросы о безопасном контакте с людьми смотрите в разделе «Коммуникации» ниже.

---

b) Вы освещаете спорную или деликатную историю?

Если да:

- Включает ли она в себя информацию, которая должна оставаться секретной или конфиденциальной?
- Вы понимаете и знаете как пользоваться безопасными методами исследования?
- В какой момент вы будете подвержены наивысшему риску?
- Когда ваши источники будут подвергаться наибольшему риску целенаправленного наблюдения: во время вашего

исследования или производства материала, когда история будет закончена или когда она станет достоянием общественности?

Дополнительные вопросы о более безопасной работе в интернете смотрите в разделе «Исследование и доступ к интернету» ниже.

---

c) Какая локация у вашего задания/истории?

- Что известно о правительственном надзоре/цензуре в интернете и мобильной связи в этой области?
- Каковы законы, касающиеся использования шифрования,VPN или права на свободу слова в социальных сетях?
- Что было опубликовано о преследовании или правах журналистов, информаторов или активистов в связи с их онлайн-деятельностью?

d) Кто является противниками, которые могут представлять угрозу вашей цифровой безопасности?

Рассматривайте своих противников в двух видах:

i) УМЫШЛЕННЫЕ ПРОТИВНИКИ:

Это могут быть правительства, предприятия, преступные организации или отдельные лица, выступающие против вашей работы конкретно или любого разоблачения в СМИ в целом. Подумайте о том, кто может столкнуться с издержками (юридическими, репутационными, профессиональными и т.д.) в результате выполнения вашего задания.

ii) НЕУМЫШЛЕННЫЕ ПРОТИВНИКИ:

Это может включать случайных хакеров, нацеленных на сервис, которым пользуются тысячи людей, включая вас. Это может быть взлом беспроводной сети или кража вашего оборудования.

Онлайн-руководства для дальнейшего чтения:

ШИФРОВАНИЕ→

ВРЕДОНОСНЫЕ ПРОГРАММЫ→

3. Ваше оборудование

Перечислите каждый предмет коммуникационного оборудования, которое вы собираетесь взять с собой.
Для каждого предмета, укажите:

- Какие типы сообщений вы будете отправлять и получать с помощью устройства (например, SMS, электронные письма, мгновенные сообщения, телефонные звонки)?
- Есть ли (или была ли) на этом устройстве конфиденциальная информация, которая может подвергнуть вас риску или которую вам необходимо защитить?
- Вы всегда будете носить свои устройства с собой?
- Будете ли вы оставлять ваше устройство там, где кто-нибудь сможет получить к нему доступ?
- Установлены ли на вашем устройстве проверки безопасности (например, пароли, шифрование и т.д.), чтобы предотвратить несанкционированный доступ?
- Будете ли вы использовать чье-либо коммуникационное оборудование или пользоваться общедоступной интернет-сетью во время выполнения задания?
- Какие шаги вы предпримете, чтобы снизить риск, связанный с использованием этого оборудования?

Онлайн-руководства для дальнейшего чтения:

МОБИЛЬНЫЕ ТЕЛЕФОНЫ →

КОМПЬЮТЕРЫ→

4. Ваши материалы

Подумайте, какие материалы вы будете собирать или записывать во время выполнения задания.

Для каждого материала, укажите:

- В каком формате материал (например, видео, текст, аудио, фото и т.д.)?
- Спорный ли это контент? Если бы к нему получили доступ враждебные стороны, поставило бы ли это под угрозу вас или кого-либо еще, причастного к репортажу?
- Где/как хранится этот материал? Предприняли ли вы какие-либо шаги для защиты этой информации?
- Нужно ли вам будет посылать материал?
- Какие шаги вы предпринимаете, чтобы свести к минимуму вероятность и серьезность угрозы, которую может принести запись/передача материала?
- Как вы перемещаете свой материал через границы?

Онлайн-руководства для дальнейшего чтения:

ЗАЩИТА ВАШИХ МАТЕРИАЛОВ →

ПЕРЕСЕЧЕНИЕ ГРАНИЦ И КОНТРОЛЬНЫЕ ПУНКТЫ→

5. Коммуникации

Перечислите всех людей, с которыми вам нужно будет связаться во время выполнения задания, например, респондентов, коллег-фрилансеров, источники и редакторов.

Для каждого контакта, укажите:

- Кто они и кто может за ними следить (работодатель, правительство и т.д.)?
- Как вы с ними свяжетесь? Выяснили ли вы, какой способ связи наиболее безопасен?
- Вам нужно будет отправлять или получать от них какую-либо конфиденциальную информацию?
- Связь с ними подвергнет риску вас или кого-либо еще? Какие шаги вы предпримете, чтобы снизить вероятность и серьезность этого риска?
- Есть ли у вас план резервного копирования и удаления сообщений? Обсуждали ли вы этот план со своим источником?

Онлайн-руководства для дальнейшего чтения:

ЭЛЕКТРОННАЯ ПОЧТА→ | ШИФРОВАНИЕ → | МОБИЛЬНЫЕ ТЕЛЕФОНЫ →

6. Исследование и онлайн-доступ

Подумайте о том, к каким сайтам, информации и контенту вам потребуется доступ в интернете, и примите во внимание потенциальные риски при этом. Если доступ к онлайн-контенту может вызвать у вас проблемы, составьте список, который поможет вам учитывать опасности.

Для каждого из них, укажите:

- Вы исследовали компанию, которая предоставляет вам доступ к интернету и мобильной связи? Имеют ли они тесные отношения с правительством страны, в которой вы живете/работаете?
- Изучили ли вы закон, чтобы узнать, как долго эти компании должны хранить ваши данные?
- Этот контент заблокирован в стране/регионе, из которых вы будете работать?
- Если вам нужен доступ к заблокированному контенту, как вы это сделаете?
- Какова вероятность того, что ваша деятельность отслеживается?
- Какие шаги вы предпринимаете для снижения рисков?

Онлайн-руководства для дальнейшего чтения:

НАВИГАЦИЯ В ИНТЕРНЕТЕ→

ВРЕДОНОСНЫЕ ПРОГРАММЫ→

7. Ваш цифровой профиль

a) Проверяли ли вы свой онлайн-профиль на контент, который мог бы поставить под угрозу вас или ваших знакомых?

- Изучили ли вы себя в Интернете, чтобы узнать, какая информация о вас доступна, и предприняли ли вы шаги для удаления данных о вас, которые вы не хотите чтобы были в открытом доступе?
- Вы публиковали или комментировали что-нибудь, где критикуется ваш возможный противник?
- Если да, что вы собираетесь делать, чтобы снизить серьезность этого риска?

b) У вас есть один или несколько личных вебсайтов?

- Может ли хранящаяся на нем информация подвергнуть риску вас или ваших знакомых?
- Если да, что вы собираетесь делать, чтобы снизить серьезность этого риска?

c) Планируете ли вы использовать социальные сети во время задания?

Если да:

- Вы создали длинные и надежные пароли для своих учетных записей?
- Насколько актуальны ваши настройки безопасности на сайтах социальных сетей?
- Активно ли вы соприкасались (писали в твиттере, делились, комментировали, ставили лайки и т.д.) с контентом, который может подвергнуть вас риску во время выполнения задания?
- У вас есть отдельные личные и рабочие аккаунты в социальных сетях?
- Какие еще шаги вы предпринимаете, чтобы снизить вероятность и серьезность угроз, которые может принести ваша активность в социальных сетях?
- Обдумывали ли вы возможное психологическое воздействие социальных сетей на вас, вашу команду или другиху частников?

Онлайн-руководство для дальнейшего чтения:

СОЦИАЛЬНЫЕ СЕТИ→

Помните!

Цифровая безопасность — это только одна часть плана обеспечения задания или проекта, и ее стоит рассматривать лишь как часть вашей подготовки к обеспечению безопасности. "Ресурсы по вопросам безопасности и защиты" Rory Peck Trust могут помочь вам в других сферах подготовки к безопасности.

RORY PECK TRUST

Данный перевод был осуществлен EU4IndependentMedia, финансируемой ЕС; эта публикация никоим образом не отражает позиций Европейского Союза.