23 способа стать жертвой киберпреступников

Во время своего бракоразводного процесса Марк столкнулся со странными вещами, происходящими в его социальных сетях и с ним лично. Некоторые из его друзей начали публиковать посты, которые, казалось, были о нем, но не указывали на него напрямую. Его, в скором будущем, бывшая жена продолжала публиковать мемы о сумасшедших мужьях. Потом она стала появляться в местах, где он был в это врем я, представляться людям, с которыми он был, и посылать ему неадекватные текстовые сообщения в течение дня.
Сбитый с толку и расстроенный, Марк исследовал тему киберпреследования и нашел всевозможную информацию о кибертроллинге, киберзапугивании и киберпреступлениях. И вот что он узнал.

Что такое киберконтроллинг? Обычно это - безвредный обзор чьей-либо информации в социальных сетях, фотографий или сообщений. Это одноразовое явление и не предназначено для причинения вреда жертве. Например, прежде чем нанять инструктора по плаванию, «нарушитель» может просмотреть сообщения или фотографии человека в социальных сетях. За этим иногда следует чувство сожаления или смущения. В большинстве случаев жертва не знает, что это произошло.
Что такое кибертравля? Проще говоря, это травля с использованием электронных устройств и / или приложений. Как правило, это повторяющиеся, агрессивные и преднамеренные комментарии, от которых жертве трудно защититься. Например: «Ты идиот», «ты никогда не добьешься успеха» или «ты никому не нужен». Комментарии предназначены для того, чтобы ранить, смутить или разозлить жертву. Эти замечания могут быть сделаны на общедоступном форуме или через личные сообщения. Нет ничего необычного в том, что преступник побуждает других к участию в издевательствах с целью дальнейшей травли жертвы.
Что такое киберсталкинг или киберпреступления? Это более интенсивная форма кибертравли, когда электронные устройства и / или их приложения используются для преследования и запугивания. Могут быть ложные обвинения, оскорбительные заявления, обзывательства или угрозы в сочетании со сбором информации, мониторингом или отслеживанием местоположения. Иногда высказывания могут показаться безобидными, например: «я не знал, что вы знакомы с этим человеком» или «я надеюсь, что вы хорошо провели время со своими друзьями», но для жертвы это еще один признак преследования. Важно отметить, что киберпреступность является незаконной во многих государствах, но является труднодоказуемой.
Виды киберпреступников. Существует четыре основных типа киберпреступников: мстительные, сдержанные, близкие и коллективные. Мстительный преступник жесток в своих нападениях и намерен причинить жертве боль. Мотивом преступника обычно является злость и раздражение или раздражение жертвы. Близкий преступник пытается установить отношения или имеет предыдущие отношения с жертвой, но становится киберпреступником, когда его отвергают. Коллективные преступники - это группа, которая формируются с целью уничтожения человека или организации.
Каковы же примеры киберпреступлений? Существует несколько способов стать жертвой киберпреступников. Ниже мы приведем 23.

1. **Ложное обвинение.** Преступник создает веб-сайт или блог с целью размещения ложной информации о жертве. Такие обвинения также могут размещаться в группах новостей, чатах или на других общедоступных сайтах, позволяющих пользователям создавать сообщения.
2. **Сбор информации.** К семье жертвы, ее друзьям и коллегам преступник обращается за получением личной информации. Эта информация впоследствии используется против жертвы.
3. **Мониторинг.** Преступник следит за действиями жертвы в интернете, чтобы собрать данные о ней. Преступник может получить доступ к IP-адресу, паролям или электронным устройствам, которые могут быть использованы для преследования жертвы или, чтобы выдавать себя за нее.
4. **Летающие обезьянки.** Прямо как ведьма из «Волшебника страны Оз», которая использовала летающих обезьян для выполнения своей грязной работы, преступник привлекает других к участию в преследовании жертвы. Это форма группового преследования.
5. **Изображая жертву**. Преступник делает ложные заявления о том, что его преследует жертва. Это обычно делается с семьей, друзьями, коллегами, а иногда и в общественных местах, чтобы заручиться поддержкой окружающих и изолировать жертву.
6. **Отправка вирусов.** Это, к сожалению, легко сделать, так как все, что требуется от жертвы, это нажать на фотографию, видео или ссылку из электронной почты, которая была отправлена с прикрепленным вирусом. В течение нескольких секунд загружается вирус, который может стереть всю необходимую информацию и уничтожить репутацию.
7. **Заказ товаров.** Преступник заказывает обескураживающие товары или подписывается на журналы от имени жертвы. Их обычно доставляют на работы жертвы, чтобы вызвать больше отрицательных эмоций и волнений.
8. **Организация встречи.** Преступники, которые используют ложные личности, например, на сайтах знакомств, договариваются о встрече со своими жертвами лично. Часто преступник не афиширует себя, предпочитая стоять в стороне и наблюдать за реакцией жертвы на неявку.
9. **Размещение оскорблений**. Твиты, сообщения в социальных сетях, комментарии в блогах или веб-сайтах - это несколько примеров мест, где преступник может размещать клевету, оскорбительные или уничижительные заявления о жертве.
10. **Физическое преследование.** Иногда киберпреступность становится реальной, поскольку преступник использует собранную информацию, чтобы появиться в местах нахождения жертвы. Такое преследование также включает оскорбительные телефонные звонки, непристойные письма, нарушение границ, вандализм, кражу и нападение.
11. **Навязчивые тексты.** Некоторые преступники посылают сотни текстовых сообщений жертве, чтобы испортить ей день и замучить необоснованными обвинениями. Они также могут использовать другие социальные сети для навязчивого размещения или просмотра сообщений, чтобы постоянно напоминать жертве о своем присутствии.
12. **Повторяющееся давление.** Преступник публикует вредные слухи, угрозы, комментарии сексуального характера, личную информацию и слова ненависти по

отношению к жертве. Это делается в издевательской манере, призванной напугать жертву и причинить ей вред. Жертва боится, что спасения и выхода нет.

13. **GPS слежение.** Устройства устанавливаются в автомобилях или на личных вещах, которые отслеживают местоположение жертвы. Некоторые мобильные телефоны, планшеты или компьютеры могут также иметь устройства отслеживания или настройки местоположения, которые позволяют отслеживать жертву без их ведома.
14. **Геотеги и метаданные.** Электронные устройства имеют встроенные и неосознанно включенные метаданные, которые используются производителями. Некоторые из этих параметров включают информацию о местоположении. Находчивый злоумышленник может получить доступ к этой информации без ведома жертвы.
15. **Социальные сети.** В то время как большинство приложений социальных сетей позволяют блокировать человека, иногда достаточно иметь доступ к другу жертвы, чтобы получить доступ к жертве. Невинные сообщения, такие как, где человек ужинает, могут предоставить злоумышленнику информацию о местоположении и времени.
16. **Разжигание.** Это размещение оскорблений, как правило, с примесью агрессии или ненормативной лексики, чтобы подстрекать жертву. Цель состоит в том, чтобы вовлечь и разжечь дискуссию между преступником и жертвой.
17. **Мониторинг приложений.** К сожалению, существует множество приложений для мониторинга и шпионских программ. Некоторым даже не нужен доступ к вашему телефону для загрузки. Просто невинно нажав на изображение можно загрузить приложение мониторинга без ведома человека. Читайте статьи, меняйте пароли и идентификаторы, удаляйте и переустанавливайте распознавание отпечатков пальцев.
18. **Синхронизация устройств.** Некоторые приложения синхронизируют информацию между устройствами, чтобы упростить покупку или передачу информации. К сожалению, если преступник имеет доступ к устройству, то они могут читать текстовые сообщения, удалять фотографии, подделывать документы или видеть историю просмотра. Это очень вредно для тех, кто испытывает насилие в семье и могут иметь доказательства, хранящиеся на устройстве.
19. **Спуфинг.** Преступник может притвориться представителем банка жертвы и попросить «проверить» личную информацию. Затем он использует эту информацию, чтобы получить доступ к банковскому счету жертвы. Это обычно делается, когда жертва переключила учетные записи, чтобы сохранить свою информацию в тайне. Всегда будьте осторожны при предоставлении любой личной информации по телефону, текстовым сообщениям или электронной почте.
20. **Интернет-мошенники.** Сайты знакомств являются популярной территорией для интернет-мошенников, которые искажают информацию о том, кто они, что им нравится, что они делают, и как они выглядят. Некоторые преступники создают ложные профили, которые идеально подходят для их жертвы, с целью совершения преступления, организации встречи или преследования.
21. **Кража личности.** Удивительно, как легко это сделать, когда у преступника были личные отношения с жертвой. Большинство партнеров знают личную информацию, такую как SSN (социальный индивидуальный код), дату рождения, девичью фамилию матери, прежние адреса и другие общие данные. Злоумышленники

используют эту информацию, чтобы подать заявку на кредитные карты, ипотечные кредиты и совершать покупки без обнаружения.

22. **Захват счета.** Многие люди сохраняют пароли от своих финансовых счетов и банковских карт на электронных устройствах. Преступник может получить доступ к компьютеру, войти в учетные записи, изменить пароли или адреса, отправить неуместные электронные письма, удалить документы и попросту уничтожить репутацию жертвы.
23. **Кэтфишинг.** Это метод интернет-преследования, когда преступник выдает себя за кого-то другого и создает ложную личность в социальных сетях. Имя, фотографии, местоположение и основная информация могут быть ложными. Иногда преступник выдает себя за жертву с целью обмануть других и унизить жертву.

Почему это вообще происходит? Существует множество психологических и социальных причин, по которым преступник может заниматься кибер-охотой. Как правило, они завистливы, имеют патологическую одержимость жертвой, могут быть безработными или потерпеть профессиональную неудачу. Такие люди считают, что могут остаться безнаказанными, и думают, что знают жертву лучше, чем кто-либо другой. Цель состоит в том, чтобы заставить жертву чувствовать себя запуганной, неполноценной, а также знать, что ей стремятся отомстить за реальное или воображаемое отвержение преследователя. Узнав о киберпреступлениях, Марк смог лучше контролировать свои устройства. К сожалению, он нашел устройство слежения в своей машине. Как только «жучек» был ликвидирован, будущая бывшая жена больше не появлялась в его жизни «случайно».

www.псиблог.рф
Оригинальная статья: Christine Hammond - 23 Ways You Could be Cyberstalked, September, 2019
Перевод: Остренко Анна Александровна
Редакторы: Симонов Вячеслав Михайлович, Шипилина Елена Ивановна
Источник изображения: pixabay.com
Ключевые слова: киберсталкинг, киберпреступления, кибертравля, травля, психология преступлений

