Тема 5: Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Груминг, кибербуллинг. Чему мы должны научить ребёнка для профилактики насилия в Сети?

Социальная инженерия используется ежедневно обычными людьми в повседневных ситуациях. Например, во взаимодействии педагогов со своими учениками. Врачи, психологи и психотерапевты часто используют элементы социальной инженерии, чтобы “манипулировать” своими пациентами, для принятия мер, которые помогут пациенту, а мошенник использует элементы социальной инженерии, чтобы убедить его выполнить действия, необходимые злоумышленнику или раскрыть информацию. Хотя конец игры сильно отличается, подход может быть очень похож. Психолог может использовать ряд хорошо продуманных вопросов, чтобы помочь пациенту прийти к выводу, что необходимы перемены. Аналогичным образом мошенник будет использовать ряд хорошо продуманных вопросов, чтобы поставить его цель в уязвимое положение. Как и любой инструмент, социальная инженерия не является «хорошей» или «плохой», это просто инструмент, который имеет много различных применений.

Социальная инженерия в контексте информационной безопасности, относится к психологической манипуляции людей, которые приводят к совершению действия или разглашению конфиденциальной информации. Это может быть злоупотребление доверием с целью сбора информации. Социальная инженерия часто является одним из многих шагов в более сложную схему мошенничества.

В общем значении социальная инженерия - это акт манипуляции человеком, который провоцирует выполнить действие, которое как может быть в интересах человека, так и в интересах злоумышленника.

Рассмотрим основные виды социальных инженеров.

– Хакеры. Поставщики программного обеспечения становятся все более продвинуты в создании такого ПО, которое более безопасно и сложно для взлома. Так как взломать хорошо защищенное ПО затруднительно, хакеры прибегают к социальной инженерии. Они часто используют сочетание аппаратных и личных навыков.

– «Пентестеры». Пентест — метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника. В информационных системах хранится, обрабатывается, циркулирует различная информация, потеря или искажение которой может нанести существенный вред. Процесс включает в себя активный анализ системы на наличие потенциальных уязвимостей, которые могут спровоцировать

некорректную работу целевой системы, либо полный отказ в обслуживании. Цель испытаний на проникновение — оценить его возможность осуществления и спрогнозировать экономические потери в результате успешного осуществления атаки. «Пентестеры» — это люди, которые проводят моделирование атаки на систему, анализируют возможные уязвимости, но не используют собранную информацию для личной выгоды или ущерба компании. Однако, потенциально это возможно.

– Шпионы. Используют социальную инженерию как способ жизни. Помимо того, что они изучили искусство социальной инженерии и являются экспертами в этой науке, очень часто шпионы также опираются на доверие. Они немного (а может и много) знают о бизнесе и власти и используют это, как рычаг давления.

– Воры личной информации. Данный вид социальных инженеров использует такую информацию, как, например, имя человека, номер банковского счета, адрес, дата рождения, и номер социального страхования, без ведома владельца. Это преступление основывается на использовании личной информации для гораздо более сложного преступления.

– Недобросовестные сотрудники. В любой сфере деятельности случаются конфликты работника и работодателя, иногда это приводит к тому, что работник начинает враждебно относиться к работодателю. Поскольку работник, как правило, пытается скрыть своё недовольство, чтобы не потерять работу, это приводит к тому, что его враждебность растёт и становится оправданием для хищения, вандализма, раскрытия конфиденциальной информации и других преступлений.

– Аферисты. Мотивом чаще всего служит желание «заработать». Аферисты и мошенники владеют способностью читать людей и находить детали, которые делают человека уязвимым. Они также квалифицированы в создании ситуаций, которые являются отличными возможностями для оценки изучаемого человека.

– Вербовщики. Также освоили многие аспекты социальной инженерии. Овладели приемами сбора, многими психологическими принципами социальной инженерии, они очень умело могут не только читать, но и понимать, что движет людьми.

– Продавцы. Многие гуру продаж говорят, что хороший продавец не должен манипулировать людьми, но ему следует использовать свои навыки, чтобы выяснить, какие потребности есть у людей и увидеть, могут ли они ему что-то предложить. Искусство продаж требует многих навыков, таких как сбор информации, убеждение, и многие другие.

– Врачи, психологи и юристы. На первый взгляд может показаться, что данный тип не вписывается в категорию социальных инженеров. Но эта группа использует те же

методы, как и другие группы в этом списке. Они это делают не обязательно для того, чтобы навредить своему клиенту, чаще, чтобы разобраться и подобрать нужный алгоритм для выхода из сложившейся ситуации.

Безопасность детей в Сети, пожалуй, больше всего беспокоит родителей. Если ребенок пользуется Интернетом, как его обезопасить? Статистика весьма неутешительна.

Один из опросов агентства Childwise установил, что у трех из четверых детей в возрасте от пяти до шестнадцати лет (73 %) есть доступ в Интернет из спальни, а у 10 % из них не было настроек приватности для просмотра личных данных. В отчете, подготовленном Национальным обществом предупреждения жестокого обращения с детьми (NSPCC), сказано, что почти четверть детей в возрасте одиннадцати-двенадцати лет, у которых есть странички в социальных сетях, сильно огорчалась из-за чего-то, увиденного там за последний год. Более половины таких случаев (62 %) были спровоцированы незнакомцами, то есть теми, кого они знали только виртуально, к тому же многие дети не могли понять, что стало причиной их расстройства. Сталкиваясь с чем-то огорчительным или неприятным в Сети, младшие дети могли определить причину своего расстройства с меньшей уверенностью, чем старшие, — еще один признак того, что дошкольникам и младшим школьникам не хватает сноровки в общении и устойчивости для того, чтобы пользоваться социальными сетями.

К сожалению, родители часто не следят за детьми так тщательно, как следовало бы. Только 32 % из них считают себя «очень уверенными» в безопасности детей при пользовании Интернетом. В реальной жизни мы следим за нашими чадами гораздо более внимательно, чем в виртуальной реальности, хотя Интернет таит для них много опасностей. Мы запрещаем детям разговаривать с незнакомцами, но зачастую это не касается онлайн-пространства.

Пользование девайсом — это всегда очень изолированное занятие, в отличие от просмотра телевизора или игры на детской площадкой, где за детьми легко следить. Когда ребенок сидит перед экраном планшета, родители обычно не знают, что он там делает. Они оставляют его одного, потому что он притих, и спешат заняться своими делами.

Дети 4-11 лет не должны общаться с незнакомцами в Сети, но иногда, несмотря на все старания родителей, они общаются с ними на форумах или в групповых чатах онлайн-игр. Важно объяснить, что если они не знают кого-то в реальной жизни, то человек все еще считается незнакомцем, даже если они разговаривают онлайн. Маленьким детям бывает очень сложно это понять.

Виртуальные отношения могут развиться очень быстро. Мальчики и девочки говорят своим виртуальным друзьям такие вещи, которые никогда не осмелились бы

произнести в реальной жизни, и очень быстро выдают личную информацию. Родителям нужно объяснить, что виртуальное общение — не то же самое, что встреча в парке отдыха или на школьном дворе: неизвестно, кто сидит по ту сторону экрана на самом деле. Прежде чем что-то написать, детям стоит задаться вопросом, смогли бы они повторить это кому-то в реальном мире? Стали бы они делиться личной информацией со случайным прохожим?

Груминг — это процесс, во время которого кто-то общается с ребенком в Сети и постепенно совращает его. К сожалению, анонимность интернет-пространства дает для этого множество возможностей. Человек может поставить детское изображение на фото профиля и подружиться с ребенком в социальной сети или в игре. Он может рассказать интересную историю или болтать об общих интересах и увлечениях, то есть вызвать доверие и начать выстраивать отношения. Важно, чтобы любой ребенок, пользующийся Интернетом, знал о груминге, но родители часто переживают и не знают, как просветить его.

Но рассказать об опасных незнакомцах в интернет-пространстве и поговорить с детьми о груминге (на языке, соответствующем их возрасту) абсолютно необходимо. Просветите их как можно раньше. Объясните, что в Интернете люди часто оказываются не теми, за кого себя выдают. Дети склонны думать, что социальные сети — это конкурс популярности, поэтому чем больше людей будет у них в подписчиках, тем лучше. Но они не должны принимать запросы в друзья от того, кого они не знают в реальной жизни. Дети, желательно с вашей помощью, должны также проверять запросы от тех, кого они знают, чтобы убедиться, что аккаунт настоящий.

То же относится к общению в мессенджерах и чатах. Маленькие дети не должны общаться с незнакомцами онлайн и соглашаться на приватный чат с незнакомцем. Если кто-то отправляет им сообщение или пытается выйти в чат, они обязательно должны поставить вас в известность — как если бы чужой человек подошел к ним на улице или в парке. Даже если ваш ребенок не находится онлайн без присмотра взрослого, вам все равно нужно разговаривать с ним об этом. Дети должны быть образованы. Остерегайтесь онлайн-игр, где они могут играть с незнакомцами!

Поговорите с ними об информации, которую они выдают людям, общаясь в Интернете. Ребенок не должен называть свое полное имя, домашний адрес, электронную почту, номер телефона или номер школы людям, которых не знает в реальной жизни. Убедись, что никнейм ваших детей не намекает на то, как их зовут на самом деле. Объясните, что все, что они выкладывают онлайн — имя пользователя, фотографии или комментарии, — воссоздает их образ, поэтому люди могут их узнать.

Крайне важно, чтобы родители разговаривали со своим ребенком и всегда были начеку. Пусть он покажет вам все сайты, на которые заходит, когда пользуется Интернетом. Объясните, что когда он находится онлайн, ему нужно действовать, как детективу. Откуда он знает, что человек действительно того возраста, который назвал? Что он знает об этом человеке? Видел ли он когда-либо его фотографию? Уверен ли, что эта фотография настоящая? Объясните ребенку, что виртуальное пространство совсем не похоже реальный мир и нельзя принимать все за чистую монету. В обычной жизни мы знаем, как выглядят учитель или полицейский. Мы видим, где они работают и какую форму носят.

Если вы даете ребенку телефон с камерой, вы должны установить правила до того, как он начет им пользоваться. Может, это прозвучит чересчур драматично, но вы, именно ВЫ, вручаете ребенку средство для совершения разрушающих и необратимых действий. Большинство детей интуитивно знают, что не стоит отправлять кому-либо непристойные фотографии, но потом они начинают общаться в чате с другим ребенком и принимают такую просьбу за близость, вызов или игру. Они действуют, не думая о последствиях. Печальный факт заключается в том, что как только вы отправили кому-то свою фотографию, она вам больше не принадлежит. Получатель может сделать с ней все, что посчитает нужным. Девочки часто отправляют фотографии своей груди или декольте. Мальчики принимают это за некий трофей и хотят похвастаться своей подружкой перед друзьями. До того как они осознают плачевность ситуации, фотография девочки обойдет всю школу. Такое может омрачить жизнь любому.

Дети осознают публичность Интернета, только когда попадаются на чем-то.

Травля в интернете может быть абсолютно разной. Есть несколько важных определений, которые помогут разобраться в категориях насилия в сети. Если «буллинг» — это проявление физического или психологического насилия по отношению к другим вообще, то «кибербуллинг» — это то же насилие, только в цифровом пространстве.

Важно помнить, что кибербуллинг — это скорее общее определение для разных видов травли в интернете, и его не стоит путать с кибермоббингом и кибертравлей.

•Кибермоббинг — вид насилия в цифровой среде, реализуемый с помощью электронного текста (сообщений и комментариев).

•Кибертравля — причинение вреда человеку за счет длительного давления в интернет-пространстве: преследования, распространения слухов, запугивания.

Иногда кибербуллинг может переходить в оффлайн. Многие блогеры и публичные личности сталкиваются с киберсталкингом. Это вид насилия, когда подписчики выслеживают инфлюенсеров и начинают их преследовать за пределами социальных сетей.

Важно помнить:

•Кибербуллинг — это агрессия.

•Не стоит обесценивать эмоции человека, который перенес насилие в интернете. Подверженные травле люди страдают не понарошку, причем это может быть не только психологическая, но и физическая боль.

•Отключение интернета и другие санкции не помогут. Лучше всего проявить эмпатию и выразить поддержку.

Согласно исследованию, 58% российских интернет-пользователей сталкивались с онлайн-агрессией. Каждый четвертый был мишенью такого поведения, и только 4% опрошенных признаются, что были инициаторами травли.

Есть много способов сделать человеку больно. Например, написать токсичный комментарий под фотографией, оскорбить в групповом чате или на стенке в социальной сети, затроллить, выложить данные или подробности из личной жизни. Поводом для кибербуллинга чаще всего являются внешность, сексуальная ориентация и активность в интернете.

Чаще всего человек не может сам защититься от кибербуллинга, но лишь небольшая часть пользователей готова поддержать жертву травли в сети. Исследователи выяснили, что:

•52% респондентов никогда не заступались ни за кого в интернете,

•65% считают публичную поддержку бессмысленной,

•13% боятся, что агрессия перекинется на них,

•20% полагают, что они бессильны и ничего не могут сделать, чтобы поддержать пострадавшего от кибербуллинга.

Сейчас некоторые социальные сети рассказывают о том, как обезопасить себя от травли в онлайн-пространстве. Практические советы можно найти в Центре безопасности «ВКонтакте» или в рекомендациях от Instagram.

Что делать при травле в интернете

•Лучше всего обратиться к психологу, чтобы проработать проблему. Школьники могут получить поддержку у педагога-психолога, который работает в их учебном заведении.

•Помочь детям и родителям разобраться в конфликтной ситуации может программа Травли Net.

•Психологическую поддержку окажут и в сервисе МАЯК от Добра Mail.ru.

Чтобы защитить себя от агрессии, постарайтесь научиться отстаивать свои границы и говорить о своих чувствах. Не забывайте, что вы всегда можете прекратить общение с

людьми, которые причиняют боль в интернете. Во всех социальных сетях есть функция блокировки нежелательных пользователей. Просто заблокируйте агрессора, тем самым закрыв ему доступ к дальнейшим негативным действиям.