Попов Михаил Николаевич
директор ОГБУ "Центр
информационной безопасности"

«Информационная безопасность в сети Интернет»

Сегодня мы поговорим об информационной безопасности. Этот термин обозначает сохранение и защиту информации, а также ее важнейших элементов, в том числе системы и оборудования, предназначенные для использования, сбережения и передачи этой информации. Другими словами, это набор технологий, стандартов и методов, которые необходимы для защиты информационной безопасности.

Её цель – защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения.

В современном социуме информационная сфера имеет две составляющие:

1. информационно-техническую (искусственно созданный человеком мир техники, технологий и т.п.);
2. информационно-психологическую (естественный мир живой природы, включающий и самого человека).

Действия, которые могут нанести ущерб информационной безопасности, делятся на несколько категорий:

Первая - компьютерные вирусы - это отдельная категория электронных методов воздействия это компьютерную инфраструктуру. Вирусы представляют собой реальную опасность для работы, широко используемые компьютерные сети, интернет и электронную почту. Проникновение вируса на узлы сети может привести к нарушению их работы, потери времени, утрате данных, краже конфиденциальной информации и даже прямым хищениям финансовых средств. Вирусная программа, проникшая в сеть, может предоставить злоумышленникам частичный или полный контроль над деятельностью компьютерной инфраструктуры.

Вторая категория – это спам. Всего за несколько лет спам из незначительного раздражающего фактора превратился в одну из серьезнейших угроз безопасности: электронная почта в последнее время стала главным каналом распространения вредоносных программ; спам отнимает массу времени на просмотр и последующее удаление сообщений, вызывает чувство психологического дискомфорта; как частные лица, так и организации становятся жертвами мошеннических схем, реализуемых спамерами; вместе со спамом нередко удаляется важная корреспонденция, что может привести к потере клиентов, срыву контрактов и другим неприятным последствиям; опасность потери корреспонденции особенно возрастает при использовании черных списков RBL и других «грубых» методов фильтрации спама.

Третья категория – это «естественные» угрозы. На информационную безопасность могут влиять разнообразные внешние факторы: причиной потери данных может стать неправильное хранение, кража компьютеров и носителей, форс-мажорные обстоятельства.

Четвертая и главная причина проникновения в компьютерные сети беспечность и неподготовленность пользователей. Связано это со стремительным развитием рынка сетевых технологий и самой сети Интернет. По данным лаборатории Касперского, около 90% от общего числа проникновений на компьютер вредоносных программ используется посредством Интернет, через электронную почту и просмотр Web-страниц. Так же к беспечности можно отнести размещение и пересылка личных данных в социальных сетях, мессенджерах, электронной почте – фотографий банковских карточек, паспорта, либо иных документов, номера телефона, домашнего адреса – всего того, что может быть использовано злоумышленником в корыстных целях, запугивании, мошенничестве и шантаже.

Все в мире, рано или поздно, оцифровывается и попадает во всемирную сеть Интернет, что дает злоумышленникам больше возможностей для проведения неправомерных действий по получению личной выгоды, путем владения личной информацией пользователя.

При этом полностью обезопасить себя в Интернете, означает полностью от него отказаться, что не является возможным, для современного человека. Любое действие в Интернете несет опасность для пользователя, что может привести к шантажу, потери финансовых средств, потери важных данных.

Социальные сети не являются каким-то сверхбезопасным ресурсом для выставления личной информации. Хотя мы и представить не можем регистрацию в социальной сети без указания города/страны проживания и личных фотографий, не говоря уже о номере телефона, месте учебы, работы и социального статуса. Этой информаций воспользоваться в негативных целях. Поэтому является рациональным привести ряд простых правил, которых нужно придерживаться для увеличения личной безопасности в социальных сетях, как для взрослых, так и для детей.

Обеспечение психологической безопасности ребенка и подростка в интернете является важнейшей задачей информационного общества, во многом это задача семейного и школьного воспитания. В условиях образовательной среды, основной задачей которой является не только обучение и воспитание школьников, но также взаимодействие с родителями и законными представителями, которым необходимо объяснять аспекты информационно-психологической безопасности, так как несмотря на век информационных технологий, многие остаются «за бортом этого корабля». На данный момент и многие педагоги сильно не вовлечены в онлайн-жизнь и не придерживаются информационной безопасности в сети.

Педагогам необходимо объяснить родителям, что стоит есть ряд простых правил, которые помогут обеспечить безопасное время провождение ребенка в социальных сетях, мессенджерах:

1. Стройте открытые и доверительные отношения с ребенком. Обсуждайте устройства и проводимое время в Интернете спокойно, чтобы ребенок всегда чувствовал и знал, что он может к вам обратиться, если попадет в неприятную ситуацию.

2. Больше времени проводите вместе с ребенком в реальной жизни. Отвлекайте его от гаджетов и отвлекайтесь сами. Играйте с ребенком в активные игры, читайте, смотрите фильмы и общайтесь.

3. Закладывайте полезные привычки и помогайте ребенку развивать социальные и эмоциональные навыки, такие как уважение к другим, сопереживание, критическое мышление и ответственное поведение.

4. Используйте устройства в хорошо просматриваемом месте в доме. Это поможет следить за тем, с кем общается ваш ребенок в сети, когда пользуется телефоном, планшетом, телевизором, игровой приставкой и другими подключенными к Интернету устройствами.

5. Установите ограничения, чтобы время, проводимое перед экраном электронного устройства, было в балансе со временем в реальном мире. Грамотно сформировать ожидания по части того, где и когда допустимо пользоваться электронными устройствами, можно с помощью распорядка «электронного дня» всей семьи. Введите запрет на использование ребенком компьютера, планшета и смартфонов в ночное время. Учите ребенка, подавая пример. Чтобы привить ребенку правила цифровой безопасности, их следует понимать и соблюдать самим. Не лишним будет заключить семейное соглашение об использовании устройств и Интернета, которые должна будет соблюдать вся семья.

6. Будьте в курсе того, какие приложения, игры и социальные сети использует ребенок. Убедитесь, что они соответствуют его возрасту. Выставляйте в приложениях и играх ограничения на функции обмена сообщениями или чата в Интернете и передачи геолокации, так как это делает ребенка уязвимым для нежелательных контактов и раскрывает его местоположение.

7. Проверьте настройки конфиденциальности в играх и приложениях, которые использует ваш ребенок. Убедитесь, что в них выставлены наиболее строгие критерии. Ограничьте список лиц, которые могут посылать ребенку сообщения и попросите его советоваться с вами, прежде чем принимать приглашения в друзья от других пользователей.

8. Используйте функции родительского контроля. Это позволяет фильтровать опасные материалы, следить за тем, как ребенок использует подключенные к Интернету электронные устройства, ограничивать или блокировать на них доступ к сети и другие функции, например, камеру или покупки в приложениях.

9. Обращайте внимание на настроение и поведение ребенка. Смена привычек может свидетельствовать о том, что он попал в неприятную ситуацию. Важно, чтобы ребенок знал, что в любой ситуации, ему следует довериться и рассказать об этом вам.

10. Обеспечьте безопасность персональной информации своей семьи. Следите за тем, чтобы ребенок не размещал в Интернете информацию о себе и своей семье: личные или семейные фотографии, свою фамилию, данные о месте жительства, пребывания, учебы, работы родителей, маршрутах своего передвижения, реальных имен своих друзей или людей из круга общения родителей, данные свидетельства о рождении, паспорта или иных документов, номера телефонов, банковских карт, логины, пароли и тому подобную информацию. Большинство детей указывают в Интернете свой настоящий возраст и делятся настоящими фотографиями, пишут свой мобильный номер и указывают свою геолокацию.

11. Объяснить ребенку, что не следует добавлять в друзья в социальной сети или мессенджере незнакомцев, так как цели преследуемые такими людьми чаще всего несут негативный характер.

Так же педагогам необходимо рассказать родителям как обезопасить себя и ребенка, соблюдая некоторый набор технических правил:

Первое правило - для регистрации в социальных сетях необходимо иметь отдельную электронную почту. Нельзя регистрировать социальные сети с рабочей почты или почты, связанной с важными услугами.

Второе правило — первая линия защиты от злоумышленников это надежный пароль. Необходимо использовать отдельный пароль для каждого сервиса и обеспечивать его надежность. Возможно, это неудобно, но если пароли на всех сервисах совпадают, то злоумышленник, узнав пароль от одного сервиса, получит доступ ко всем остальным. Есть отличный способ сделать пароли разными, но незабываемыми. Необходимо придумать базовое слово, которое будет использоваться во всех паролях, а вторая часть пароля должна быть названием сайта или сервиса для которого придумывается пароль, скомбинировать это в каком-либо порядке, и добавить любое число.

Третье правило - необходимо настроить восстановление пароля и обновлять его. Если пользователь забыл свой пароль или не смог войти в свой аккаунт, то обычно в таких случаях письмо с восстановлением пароля отправляется на дополнительный адрес электронной почты. Кроме того, вы можете добавить номер телефона, на который приходит текстовое сообщение с кодом для восстановления пароля. Указать номер телефона в вашем аккаунте — это самый простой и надежный способ защиты. Пользователь физически владеет мобильным телефоном, поэтому этот способ восстановления пароля более безопасный, чем использование альтернативного адреса электронной почты или секретного вопроса.

Четвертое правило - удаляйте аккаунты, которыми вы не пользуетесь. У основной массы пользователей социальных сетей есть парочка страниц, в той или иной социальной сети, о которых уже давно забыли, но вы должны помнить, что там находится ваша личная информация, которую вы скорее всего не удалили. Если вы уже не пользуетесь такими страничками, то просто удалите их, чтобы не оставлять Вашу информацию в общем доступе, даже если она устаревшая, как-ни-как это рычаг давления на вас со

стороны злоумышленников. Да и следить за всеми своими страничками легко, с помощью множества различных сервисов, которые вы с легкостью сможете найти в интернете.

Пятое правило - установите на гаджет антивирус, который обеспечит защиту от анализа трафика (в том числе перехвата паролей), защиты от получения доступа к конфиденциальным данным и банковских троянов.

Шестое правило - установите и используйте родительский контроль, что позволит контролировать экранное время смартфона или компьютера, посещаемые сайты, открываемые приложения и программы.

Рассказав об этих простых правилах, хочется еще раз подчеркнуть, что важнейшая наша задача очередной раз напомнить родителю, что основное внимание все таки необходимо уделить доверию в семье, с ребенком следует обсуждать и разговаривать на тему опасностей с которыми можно столкнуться в интернете – травля, мошенничество, общение и обмен фотографиями с незнакомыми людьми, вербовка и отбор в опасные сообщества. Чтобы справится с угрозами находящимися в Интернете, следует не только использовать технические средства, но и развивать у ребенка критическое мышление, которое развивает эмоциональный интеллект, социальные навыки и позволяет самостоятельно анализировать происходящее не только в виртуальном мире, но и в реальной жизни. Важно помнить, что ребенок не должен учиться всему в одиночку. Намного интереснее делать это с родителями, что возвращает нас к главному – необходимо разговаривать с детьми на равных, тогда будет выстроено доверительное общение в семье, это и защитит его от многих угроз.