

«Безопасный интернет для наших детей».

В настоящее время Интернет является неотъемлемой частью жизни большинства людей. И дети не стали исключением, в связи с чем остро стоит проблема их безопасности в глобальной сети, а также необходимость формирования у них представлений о виртуальном и реальном мире.

Средний возраст для первого погружения в неизведанные пучины интернета – это 5-6 лет. В настоящее время более 70% детей от 7 до 12 лет пользуются Интернетом самостоятельно.

Все это происходит на фоне минимальных познаний у подрастающего поколения по индивидуальному обеспечению собственной информационной безопасности. Как следствие, в течение последних лет число противоправных деяний, совершенных против информационной безопасности, ежегодно увеличивается.

Казалось бы, что это сложные по механизму совершения преступления, однако, 90% совершаются людьми, не имеющими никакого специализированного образования в данной сфере. И если говорить о молодежной аудитории, то половина совершаются лицами от 14 до 24 лет.

В сети Интернет действуют те же законы, те же нравы, те же обычаи, что и в реальной жизни.

Прогнозируется, что развитие IT-отрасли, игорного бизнеса и финансово-кредитной сферы, будут способствовать сохранению тенденции увеличения числа данных преступлений.

Учитывая развитие IT-отрасли и последние общемировые тенденции, в первую очередь, прогнозируется дальнейшее увеличение количества хищений путем использования компьютерной техники (статья 212 УК) и фактов несанкционированного доступа к компьютерной информации (статья 349 УК).

Как не стать жертвой преступлений в социальных сетях

На сегодняшний день в молодежной среде мы вряд ли найдем тех, кто не был бы зарегистрирован «ВКонтакте», «Фейсбуке», «Инстаграмм», каких-либо тематических форумах или иных площадках для виртуального общения. В целом это норма, ведь человек живет в обществе и стремится общаться. Однако некоторая неопытность, наивность и доверчивость порой приводят к негативным последствиям.

Основная проблема социальных сетей – это доверие к тем, кто внесен в список «друзей». Бездумное предложение «дружбы» от

неизвестных или малоизвестных людей может привести к драматическим последствиям. Очевидно, что уровень доверия к тем, кто находится в списке «друзей», по определению всегда будет выше, чем к случайным людям. С одной стороны, это хорошо, так как формирует лояльную аудиторию вокруг человека, но с другой стороны, открывает двери для злоумышленников.

«Дружеский» стиль общения, распространенный в социальных сетях, обманчив. Он может создать ложное ощущение, что вокруг только друзья и доброжелатели, с которыми можно делиться любой информацией.

Очень хорошо отсутствие культуры общения, а точнее, наличие антикультуры раскрывает такое явление, как «троллинг».

На интернет-сленге троллинг (от англ. trolling – ловля рыбы на блесну) – это намеренно агрессивное, хамское, провокационное, оскорбительное поведение в интернет-дискуссии. Цель тролля (тролль – это тот, кто занимается троллингом) – вывести собеседника из равновесия, разжигание склок в дискуссиях, провоцирование взаимных оскорблений и т.д. Помимо этого, виртуальность вызывает эффект «онлайн-растормаживания», благодаря которому люди позволяют себе в Интернете такое поведение и высказывания, которые никогда бы себе не позволили в реальном мире.

Общение в сети, точно такое же общение, как и в обычной жизни, с той лишь разницей, что дети порой доверяют «виртуальным друзьям» гораздо больше, чем реальным. Особенно это обостряется в тот момент, когда у подростка возникают проблемы в реальной жизни или в общении со сверстниками. В сети очень быстро находят «сопереживающие» и «советующие». Отсюда и возникают такие известные движения как «Синий Кит» (когда подростка склоняли к совершению самоубийства) или «Колумбайн» (когда ребенка подталкивали на совершение физических расправ над учителями, учащимися или просто незнакомыми людьми).

Зачастую злоумышленники ведут очень долгую и дружескую переписку, находят слабые места, втираются в доверие, становятся лучшим другом или подругой, делают вид, что понимают собеседника лучше всех на свете, а потом, понемногу начинают склонять к тем либо иным действиям, манипулировать или шантажировать. Преследуя эти цели, злоумышленники порой используют фотографии «друзей» из профиля подростка, чтобы создать дубликат страницы этого «друга» и якобы от его имени уже вести переписку.

Обезопаситься от этого можно лишь развивая критичное отношение к собеседникам в сети и их словам, проявляя не меньшую осторожность, чем в обычной жизни. Не следует выставлять всю свою

жизнь напоказ, гонясь за мнимой известностью, «лайками» и комментариями и конечно же следует понимать, что слова, написанные в личных сообщениях, отправленные фото и иные сведения, могут стать инструментом, который позволит манипулировать собеседником.

Вторая угроза связана со взломом пользовательских записей социальных ресурсов. И это происходит не потому, что использовались простые пароли (что конечно тоже бывает) или они записывались где-то, грубо говоря «на бумажке» и кто-то мог их «подсмотреть».

Проблема носит более масштабный характер. Источников утечки персональной информации о логинах и паролях пользователей данной социальной сети крайне много и в подавляющем большинстве случаев вина лежит на самих пользователях, которые осуществляли авторизацию на иных ресурсах или в приложениях через свои учетные записи в социальных сетях. Например, для скачивания музыки или видеофайлов, получения мнимого выигрыша. Часть из данных ресурсов были созданы именно для сбора персональной информации.

Посредством взлома злоумышленник может проникнуть в социальную сеть, разослать по ее списку друзей фишинговое (или заведомо ложные) сообщение и получить деньги либо мотивировать получателей к каким-либо негативным действиям. Например, пройти по указанной ссылке и запустить вредоносный код.

Таким образом, после совершения несанкционированного доступа к персональным аккаунтам, в течении первых суток развиваются следующие сценарии:

1). Злоумышленник рассылает всем виртуальным «друзьям» потерпевшего просьбу под различными предлогами сообщить реквизиты банковской платежной карты. Это может быть ее фото или просто номер, срок действия и иные реквизиты. При этом хоть в большинстве своем школьники банковских карт не имеют, но желая помочь «другу», очень часто используют карты своих родственников и друзей. Порой преступники просят просто номер мобильного телефона либо пытаются похитить со счета деньги или наоборот используют его как промежуточное звено, направляя на этот счет чужие деньги, переводя их затем дальше, чтобы запутать свои следы. Практически во всех случаях хищения денежных средств со счетов мобильных телефонов потерпевшие сообщали преступнику персональные коды, приходящие в виде смс-сообщений на телефон.

Анализ показывает, что не более 20% людей, получивших такие сообщения, связываются с владельцем страницы, что в этой ситуации крайне важно. Чтобы обезопасить себя от этого вида преступлений, не стоит сообщать никому реквизиты доступной банковской платежной карты или номер мобильного телефона и содержание смс-сообщений,

поступающих для подтверждения совершения операции. Ежедневно на территории нашей страны фиксируется несколько подобных случаев.

2). Злоумышленник изучает содержание переписок потерпевшего и использует их содержание в качестве инструмента для вымогательства денежных средств. Таким образом, инструментом вымогательства становятся личные диалоги на откровенные темы, фотографии, содержащиеся на странице и иные личные данные. Обычно перед тем как связаться с потерпевшим, преступник делает скриншот списка всех его друзей и близких. Избежать подобного возможно лишь путем регулярной чистки своих диалогов и удаления из сети всей информации, компрометирующего характера.

3). Злоумышленник начинает рассылать различного рода порочащую информацию от имени владельца страницы иным пользователям.

В случае обнаружения «взлома» аккаунта, прежде всего следует попытаться восстановить доступ наиболее привычным способом, путем отправки сообщения на «привязанный» номер мобильного телефона или электронную почту, кроме этого, следует оповестить друзей и знакомых об инциденте, используя иные социальные сети и мессенджеры. Также, чтобы в какой-то мере обезопасить себя от взлома, специалисты рекомендуют «привязать» страницу социальной сети именно к номеру мобильного телефона, а не к адресу электронной почты. Помимо этого, в настройках страницы в разделе «Безопасность» подключить услугу «Подтверждение входа». При этом вход на Вашу страницу с неизвестного компьютера или мобильного телефона будет не возможен без знания кода, который автоматически будет выслан на указанный при регистрации страницы номер.

Основным источником опасности для пользователей компьютеров были и остаются вредоносные программы, которые с развитием сетевых технологий получили новую среду для своего распространения.

Пользователи сети Интернет могут стать жертвами и преступных посягательств, совершаемых по корыстным мотивам, при этом возраст потерпевших от подобных действий далеко не всегда старше 18 лет.

Чтобы не стать жертвой подобных преступлений никому и никогда не стоит сообщать подробную информацию о банковской карте, в том числе пин-код и полученные от банка одноразовые пароли. Если информация о карточке хранится в смартфоне или планшете, не следует переходить по ссылкам, поступившим с неизвестных номеров, а также устанавливать приложения из неизвестных источников.

Кроме этого, следует помнить, что если реквизиты карты сохранены в смартфоне или каком-либо аккаунте, то в случае установки

платного приложения с изначально бесплатным пробным периодом, после истечения указанного периода, платная подписка продлится автоматически и денежные средства спишутся со счета.

Памятка для детей.

НИКОГДА:

не оставляй в Интернете свой номер телефона, домашний адрес или номер школы;

не отправляй никому свою фотографию, не посоветовавшись с родителями;

не договаривайся о встрече с интернет-знакомыми без сопровождения взрослых, они не всегда являются теми, за кого себя выдают;

не открывай прикрепленные к электронному письму файлы, присланные от незнакомого человека. Файлы могут содержать вирусы или другие программы, которые могут повредить всю информацию или программное обеспечение компьютера;

не отвечай на недоброжелательные сообщения или на сообщения с предложениями, всегда рассказывай родителям, если получил таковые.

ВСЕГДА:

будь внимательным, посещая чаты. Даже если в чате написано, что он только для детей, нельзя точно сказать, что все посетители действительно являются твоими ровесниками. В чатах могут сидеть взрослые, пытающиеся тебя обмануть;

спрашивай у родителей разрешения посидеть в чате;

покидай чат, если чье-то сообщение вызовет у тебя чувство беспокойства или волнение. Не забудь обсудить это с родителями;

держи информацию о пароле при себе, никому его не говори;

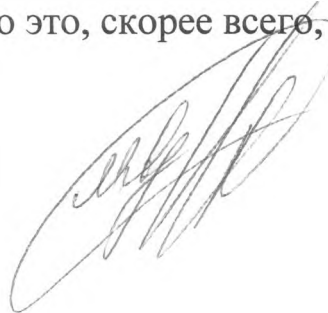
если услышишь или увидишь, что твои друзья заходят в “небезопасные зоны”, напони им о возможных опасностях и посоветуй, как им правильно поступить;

будь внимателен при загрузке бесплатных файлов и игр на компьютер, тебя могут обмануть: нажав на ссылку, ты можешь попасть в “небезопасную зону” или загрузить на свой компьютер вирус или программу – шпион;

если получили оскорбляющие сообщения, расскажите об этом родителям;

помни, что если кто-то делает тебе предложение, слишком хорошее, чтобы быть правдой, то это, скорее всего, обман;

**Начальник инспекции
по делам несовершеннолетних**



Михаил Азанович