**Как не стать жертвой преступлений в социальных сетях**

На сегодняшний день в молодёжной 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.

Социальные сети, форумы, блоги - это среда с практически мгновенной скоростью распространения информации и довольно сильным эффектом памяти (содержимое многих социальных ресурсов индексируется и доступно из поисковиков). Кроме того, растет индекс доверия к этим источникам информации.

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 анг. 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 находятся «сопереживающие» и «советующие».

Еще одна 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 «па 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 течение 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 помер 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.

**Как не стать жертвой преступлений против информационной безопасности**

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

Вредоносные программы можно разделить на три группы:

* компьютерные вирусы;
* сетевые черви;
* троянские программы.

**Компьютерный вирус** - это обычная программа, которая обладает способностью самостоятельно прикрепляться к другим работающим программам, таким образом, поражая их работу. Вирусы самостоятельно распространяют свои копии, это значительно отличает их от троянских программ. Также отличие вируса от червя в том, что для работы вирусу нужна программа, к которой он может приписать свой код.

**Скрипт-вирусы и черви** достаточно просты для написания и распространяются в основном посредством электронной почты. Скриптовые вирусы используют скриптовые языки для работы, чтобы добавлять себя к новым созданным скриптам или распространяться через функции операционной сети. Нередко заражение происходит по E-mail или в результате обмена файлами между пользователями. Червь -программа, которая не только размножается самостоятельно, но при этом инфицирует другие программы. Черви при размножении не могут стать частью других программ, что отличает их от обычных видов компьютерных вирусов;

**Троянские программы** - это программы, которые должны выполнять определенные полезные функции, но после запуска таких программ выполняются действия другого характера (разрушительные). Трояны не могут размножаться самостоятельно и это основное их отличие от компьютерных вирусов.

Кроме этого, в настоящее время получили широкое распространение и иные программные продукты, носящие вредоносный характер.

**Bot-сеть** - это полноценная сеть в Интернет, которая подлежит администрированию злоумышленником и состоящая из многих инфицированных компьютеров, которые взаимодействуют между собой. Контроль над такой сетью достигается с использованием вирусов или троянов, которые проникают в систему. При работе, вредоносные программы никак себя не проявляют, ожидая команды со стороны злоумышленника. Что интересно, пользователи зараженных компьютеров могут совершенно не догадываться о происходящем в сети.

**Рекламные программы**

Под рекламными и информационными программами понимаются такие программы, которые, помимо своей основной функции, также демонстрируют рекламные баннеры и всевозможные всплывающие окна с рекламой. Такие сообщения с рекламой порой бывает достаточно нелегко скрыть или отключить. Рекламные программы основываются при работе на поведение пользователей компьютера и являются достаточно проблемными по соображениям безопасности системы.

**Бэкдоры (Backdoor)**

Утилиты скрытого администрирования позволяют, обходя системы защиты, поставить компьютер установившего пользователя под свой контроль. Программа, которая работает в невидимом режиме, дает хакеру неограниченные права для управления системой. С помощью таких backdoor-программ можно получить доступ к персональным и личным данным пользователя.

**Фарминг** - это скрытая манипуляция host-файлом браузера для того, чтобы направить пользователя на фальшивый сайт. В результате этого зараженная система будет загружать только фальшивые сайты, даже в том случае, если Вы правильно введете адрес в строке браузера.

**Фишинг** дословно переводится как "выуживание" личной информации пользователя при нахождении в сети интернет. Злоумышленник при своих действиях отправляет потенциальной жертве электронное письмо, где указано, что необходимо для подтверждения выслать личную информацию. С использованием таких похищенных данных хакер вполне может выдать себя за другое лицо и осуществить любые действия от его имени. Пользователи сети Интернет могут стать жертвами и **преступных посягательств, совершаемых «о 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.