

За сравнительно небольшой промежуток времени количество пользователей сети Интернет в Республике Беларусь превысило пять миллионов человек. Сегодня по плотности проникновения широкополосного доступа на 100 человек Беларусь вышла на среднеевропейские показатели, а по скорости – на третье место в мире. Количество абонентов сотовой связи продолжает увеличиваться. Указанные темпы проникновения информационных технологий во все сферы жизнедеятельности человека наряду с имеющей место неквалифицированностью определенной части пользователей являются предпосылкой возрастающего количества компьютерных инцидентов. В законодательстве Республики Беларусь предусмотрена ответственность, в том числе уголовная, за совершение противоправных деяний в сфере высоких технологий. Уголовным кодексом предусмотрен ряд преступлений, отнесенных к компетенции подразделений по раскрытию преступлений в сфере высоких технологий. Рассмотрим их подробнее.

*Статья 212. Хищение путем использования компьютерной техники*

Ответственность за деяния, предусмотренные *ст.212*, наступает *с 14-летнего возраста*.

Примером такого преступления может быть хищение денежных средств с найденной либо похищенной банковской платежной карточки с использованием банкомата, платежного терминала. В последнее время все чаще фиксируются факты хищений с использованием реквизитов карт при осуществлении Интернет-платежей, а также завладение денежными средствами, хранящимися на счетах различных электронных платежных систем и сервисов.

*Статья 349. Несанкционированный доступ к компьютерной информации*

Например – несанкционированный доступ (открытие и просмотр файлов, писем, переписки) к электронной почте, учетным записям на различных сайтах, в том числе в социальных сетях, к информации, содержащейся на компьютере, в смартфоне и защищенной от доступа третьих лиц.

*Статья 350. Модификация компьютерной информации*

В качестве примера можно привести произведенные изменения компьютерной информации: переписка в электронной почте, в социальной сети, в мессенджере с правами другого пользователя; изменение текстовой, графической и иной информации; внесение изменений в защищенные базы данных и т.д.

*Статья 351. Компьютерный саботаж*

Здесь мы говорим об умышленном уничтожении (удалении, приведении в непригодное состояние, шифровании) компьютерной информации либо ее блокировании (например, путем смены пароля доступа, изменении графического ключа и т.д.).

*Статья 352. Неправомерное завладение компьютерной информацией*

В данном случае учитываются действия, связанные с копированием какой-либо значимой информации, повлекшие причинение существенного вреда. К примеру – копирование писем из электронной почты, личной переписки из социальных сетей, закрытых для просмотра третьими лицами фотографий с компьютера.

*Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети*

Статья достаточно специфична и применяется при разработке, изготовлении и сбыте специальных программ и устройств, предназначенных для осуществления несанкционированных доступов, например, поддельных смарт-карт для просмотра закодированных каналов спутникового телевидения.

*Статья 354. Разработка, использование либо распространение вредоносных программ*

К уголовной ответственности по данной статье могут быть привлечены лица за разработку вредоносного программного обеспечения, а также разработку и использование вирусов, например, блокирующих смартфоны либо шифрующих компьютерную информацию на серверах.

 *Статья 355. Нарушение правил эксплуатации компьютерной системы или сети*

Указанная статья применяется к лицам, имеющим доступ к компьютерным сетям и системам, в которых хранится значимая информация, халатные действия которых привели к нарушению функционирования таких систем.

 Ответственность за деяния, предусмотренные *ст.ст.349-355* наступает *с 16-летнего возраста*.

Также с использованием сети Интернет может совершаться ряд иных уголовно наказуемых противоправных деяний:

* мошенничество (ст.209 УК);
* причинение имущественного ущерба без признаков хищения (ст.216 УК);
* изготовление и распространение порнографических материалов или предметов порнографического характера (ст.343 УК, ст.343-1 УК);
* клевета (ст.188 УК);
* оскорбление (ст.189 УК);
* разжигание расовой, национальной или религиозной вражды, или розни (ст.130 УК) и иные.

 Наблюдается отчетливая тенденция роста количества фактов совершения противоправных деяний в сети Интернет, которые выражаются, с одной стороны, во «взломе» и несанкционированном использовании учетных записей пользователей в социальных сетях, а с другой стороны – в совершении хищений с карт-счетов граждан путем мошенничества либо использования компьютерной техники. И в обоих случаях злоумышленники пользуются излишней доверчивостью и неосмотрительностью самих пользователей, а также их халатным подходом к обеспечению безопасного использования сети Интернет.

Сначала преступник получает несанкционированный доступ к средству связи с потенциальным потерпевшим, обычно это учетные записи в социальных сетях, электронные почтовые ящики, аккаунты в различных программах, предназначенных для обмена сообщениями, например, Skype. Обычно это становится возможным ввиду небрежного отношение владельца сайта к обеспечению сохранности конфиденциальной информации (логинов, паролей) о пользователях либо беспечности самих пользователей. При этом такая беспечность со стороны пользователей может проявляться в:

* попадании на удочку лиц, создавших «фишинговый» (имитирующий настоящий) сайт;
* вводе логинов и паролей от своих учетных записей в соцсети или электронных почтовых ящиков на иных, не имеющих отношения к функционированию указанных сервисов, сайтах;
* использовании идентичных реквизитов для авторизации на различных ресурсах;
* использовании слишком легких паролей;
* отсутствии на устройствах средств, позволяющих блокировать работу вредоносных программ и др.

Получив реквизиты, злоумышленник заходит в учетную запись жертвы и осуществляет рассылку контактам владельца взломанной учетной записи сообщения мошеннического характера.

Следует констатировать, что фантазия преступников безгранична, вариантов формулировок таких просьб множество, приведем некоторые примеры таких сообщений:

* «Вася (к примеру), я нахожусь в России, у меня украли кошелек и телефон. Срочно нужны деньги на билет домой. Отправь мне на карт-счет (здесь может быть мобильный номер телефона, кошелёк в электронных платежных системах Яндекс.Деньги, QIWI, WebMoney или других) 5 000 (мошенник имел ввиду российских, знал бы он, что в Беларуси указанная сумма столь существенна, он бы уточнил) рублей. Все верну по приезду.»;
* «Привет, у тебя есть действующая банковская карточка? Мою заблокировали, а как раз сегодня мне должны перечислить деньги. Можно я дам реквизиты твоей карты, на нее придут деньги, потом отдашь мне. В долгу не останусь!»;
* «Я помогаю в сборе средств для лечения моей дальней родственницы, у нее серьезная болезнь, нужно много денег. Перечисли, если есть возможность, хоть какую-то сумму на кошелек».

Далее преступнику остается ждать отклика от ничего не подозревающих собеседников и проявлять свои способности в риторике и убеждении.

В случае, когда потерпевший отзывается на уловку преступника и, будучи обманутым, сам осуществляет перевод средств на предложенные реквизиты, в действиях злоумышленника усматривается состав преступления, предусмотренного статьей 209 Уголовного кодекса Республики Беларусь «Мошенничество» (в зависимости от суммы похищенного максимальная ответственность может составлять как три, так и десять лет лишения свободы).

Когда имеет место предоставление потерпевшим платежных реквизитов и осуществление транзакций злоумышленником путем их ввода на различных сайтах, поддерживающих возможность совершения платежных операций, имеет место статья 212 «Хищение путем использования компьютерной техники» (также в зависимости от суммы максимальное наказание варьируется от 3 до 15 лет лишения свободы, при этом Законом не предусмотрена минимальная сумма хищения). При этом надеяться на то, что преступник в данной ситуации оставит на Вашем карт-счете хоть какую-то сумму, к сожалению, не приходится.

Необходимо отметить, что совершение транзакций по банковским платежным карточкам самим владельцем либо нарушение правил пользования карточками, выразившееся в передаче платежных реквизитов третьим лицам, практически не оставляет шансов вернуть денежные средства с использованием действующего в Беларуси принципа нулевой ответственности пользователей банковских карточек.

Учитывая изложенные выше факты, приведем некоторые рекомендации для пользователей сети Интернет, которые могут снизить вероятность совершения в отношении них противоправных деяний:

* для выхода в сеть Интернет используйте устройства, на которых установлено специальное программное обеспечение, предназначенное для борьбы с вредоносной активностью, своевременно обновляйте его;
* используйте операционную систему с установленными обновлениями безопасности, актуальные версии другого программного обеспечения;
* при использовании известных Вам сайтов, обращайте внимание на их внешний вид: возможно Вы зашли на поддельную его копию;
* вводите личную информацию только на веб-сайтах, работающих с использованием защищенных протоколов (обычно в браузере рядом с адресом такого сайта отображается значок замка на зеленом фоне);
* не используйте одинаковые логины и пароли на различных сайтах;
* не используйте слишком легкие пароли, либо те, о которых можно легко догадаться (даты рождения, номера телефонов и т.д.);
* по возможности используйте двухфакторную аутентификацию, когда кроме ввода логина и пароля необходимо вводить временный код, отправляемый обычно на мобильный телефон в виде SMS-сообщения либо push-уведомления;
* остерегайтесь неожиданных или необычных электронных сообщений, даже если вам знаком отправитель, никогда не открывайте вложения и не переходите по ссылкам в таких сообщениях;
* с осторожностью относитесь к письмам, в которых запрашиваются данные счетов (финансовые учреждения почти никогда не запрашивают финансовую информацию по электронной почте), никогда не отправляйте финансовую информацию по незащищенным Интернет-каналам;
* при поступлении сообщений от знакомых, содержащих побуждение к осуществлению финансовых транзакций либо передаче финансовых реквизитов, обязательно необходимо проверить данную информацию с использованием других каналов связи (личная встреча, телефонный звонок, мессенджер, поддерживающий голосовую связь), либо в крайнем случае идентифицируйте личность собеседника путем задачи контрольных вопросов, ответы на которые не могут быть известны третьим лицам;
* если Вы не используете банковскую платежную карточку для осуществления Интернет-платежей, обратитесь в банк для установки соответствующих ограничений для карты;
* при осуществлении Интернет-платежей по возможности используйте технологии обеспечения дополнительной безопасности платежей, такие как 3-D Secure для международных платежных систем Visa и MasterCard или Интернет Пароль для платежной системы БЕЛКАРТ.

К сожалению, дать рекомендации о поведении в каждом возможном случае нельзя, но в общем можно предложить пользователям в любой ситуации не терять бдительность и критическое отношение к окружающим нас явлениям и событиям. В случае совершения в отношении Вас противоправных деяний, рекомендуем Вам в кратчайшие сроки обратиться в органы внутренних дел по месту жительства либо обнаружения факта совершения преступления. Ваша бдительность убережет Вас и Ваших знакомых от противоправных посягательств со стороны третьих лиц!

Как не стать жертвой преступлений в социальных сетях

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. Одной из задач органов внутренних дел является разработка инновационных подходов, позволяющих не только научить ребенка безопасному поведению, но и заинтересовать его в дальнейшем делиться полученными знаниями со сверстниками и использовать их в жизни.

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, что составляет примерно 20% интернет-аудитории страны.

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.

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». 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).

Для этого используются специально созданные группы, а также особые хэштеги – «куратор». «Куратор» дает школьнику инструкции: что нужно делать, чтобы присоединиться к игре. Участники этих «групп смерти» ассоциируют себя с китами – высокоразвитыми животными, которые якобы осознанно совершают массовые самоубийства, выбрасываясь на берег. Способность на самоубийство привязывается к внутренней свободе. Картина издыхающих китов некрасива, поэтому в сообществах эти «свободные» киты летают. Из групп смерти поклонники «моря китов» и «тихих домов» репостят (пересылают друг другу) видео и графику с летающими китами под медитативные звуки. Детям предлагают пройти экзамен – повредить себя, а потом предоставить фото и видео этого для вхождения в группу.

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, отправленное 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.

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 Е-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.

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.

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.

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 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.