Лекция на тему: «Безопасность несовершеннолетних в сети «Интернет» и способы защиты от преступных посягательств в сфере информационных технологий.

В Российской Федерации отмечается ежегодный рост преступлений, совершаемых с использованием современных информационно-коммуникационных технологий, посредством сети «Интернет», и все чаще жертвами данных преступлений становятся несовершеннолетние.

Жизнь современного человека нельзя представить без различного рода гаджетов. Смартфон с доступом в «Интернет» сейчас есть у каждого школьника, однако приносит ли это пользу предстоит разобраться. С каждым раскрытым преступлением сотрудникам правоохранительных органов становится известен новый способ или схема хищений, совершаемых мошенническими действиями с использованием информационно-коммуникационных технологий. Так как же защитить себя и своих несовершеннолетних детей от преступных посягательств в сети «Интернет»?

На сегодняшний день наиболее распространёнными являются следующие способы мошенничества:

«Банковская карта заблокирована». Для совершения данного вида мошенничества злоумышленник, как правило, рассылает СМС-сообщения на номера граждан от имени службы безопасности банка с текстом: «Ваша карта заблокирована», «покупка на сайте одобрена», «перевод на сумму одобрен» и указывает свой абонентский номер для обратной связи либо непосредственно звонит гражданину под предлогом предотвращения несанкционированных переводов по счету клиента банка. В ходе телефонного разговора мошенник представляется сотрудником банка или сотрудником службы безопасности банка и указывает, что произошла ошибка, которая привела к блокировке карты либо к списанию денежных средств с карты. При этом, для устранения возникших проблем, мошенник предлагает потерпевшему произвести ряд операций, в ходе которых злоумышленник узнает личные данные клиента банка: логин, пароль, коды подтверждения на переводы денежных средств в системе Интернет-банкинга (например, «Сбербанк-онлайн»). Далее мошенник, используя полученные регистрационные данные (логин и пароль), переводит денежные средства с карты потерпевшего на иные карты и счета.

«Ошибочный перевод денежных средств на номер абонента». Данная мошенническая схема наиболее часто применяется в отношении пенсионеров и несовершеннолетних. Злоумышленник на номер абонента отправляет СМС-сообщения следующего характера: «Ошиблась. Верните, пожалуйста 350 рублей на номер 8-****-**-** Билайн. Спасибо. Ева». После чего наиболее доверчивые граждане отправляют по указанному номеру денежные средства, что является обманом.

«Предоплата по Интернет-объявлениям». Для данного вида мошенничества характерно то, что в данном случае объявление о продаже какого-либо имущества или недвижимости размещаются в информационно-телекоммуникационной сети «Интернет» самим потерпевшим, а преступник осуществляет мониторинг самых распространенных Интернет-сайтов («Авито.ру»,

«Авто.ру»), после чего связывается с продавцом (потерпевшим) и сообщает о готовности приобрести указанное имущество. Желая внести предоплату, мошенник получает от потерпевшего информацию о реквизитах карты (номер карты, ее срок действия, CVC/CVV-код) либо код для осуществления операций по получению логина и пароля системы Интернет-банка (например, Сбербанк-онлайн). При этом, мошенник сообщает потерпевшему, что указанные коды необходимы ему для осуществления перевода. После получения данной информации злоумышленник самостоятельно переводит денежные средства со всех счетов, имеющихся у потерпевшего.

«Покупка через Интернет». Данная схема очень близка к вышеуказанной, но в этом случае продавцом выступает мошенник. Потерпевший умышленно вводится в заблуждение о необходимости внесения им предоплаты, после чего самостоятельно переводит денежные средства на счета, указанные злоумышленником.

В силу сложности расследования данных преступлений, гражданам необходимо содействовать органам правопорядка посредством проявления бдительности при предоставлении личной информации. Противостоять преступникам можно и нужно.

«При поступлении звонка или СМС-сообщения из банка»:

-необходимо убедиться, что СМС-сообщение о подозрительном списании денежных средств пришло именно из Вашего банка;

-обращайтесь на телефоны горячих линий, которые указаны на обратной стороне Вашей банковской карты;

-не звоните по номерам, указанным в СМС-сообщениях, даже если номера схожи с номером, используемым Вашим банком.

«При поступлении СМС-сообщения о денежном переводе на Ваш номер телефона»:

-необходимо проверить баланс на телефоне;

-при необходимости обратиться в отделения Ваших операторов сотовой связи;

-не отвечать на сообщения такого характера.

«При использовании сайтов бесплатных объявлений»:

-обязательно проверяйте порядочность продавца (покупателя);

-обращайте внимание на реальную стоимость приобретаемого товара. Зачастую стоимость товара мошенниками умышленно занижена для привлечения внимания покупателей;

-не сообщайте свои личные данные и данные Ваших банковских карт ни под каким предлогом.

«Совершая покупки через Интернет»:

-приобретайте товары только в проверенных Интернет-магазинах;

-перед покупкой изучите отзывы об Интернет-магазине, услугами которого Вы хотите воспользоваться.

«При установке программ на смартфон»:

-используйте антивирусную программу, установленную на мобильном устройстве;

-скачивайте приложение «Мобильный Банк» с официальных Интернет-страниц банков;

-не переходите по ссылкам, полученным в подозрительных - СМС-сообщениях.

В завершение нашей сегодняшней темы хотелось акцентировать внимание обучающихся на том, что прежде чем совершить какой-либо перевод денежных средств при оплате покупок в сети «Интернет» или переводе денежных средств незнакомым Вам людям согласовывайте свои действия в Вашими родителями.

Если же Вы стали жертвой преступления, совершенного с использованием информационно-телекоммуникационных технологий, то Вам необходимо незамедлительно сообщить об этом в Ваш банк, заблокировать банковскую карту, написать заявление о несогласии с операцией, а также обратиться в полицию.

Помощник прокурора
Заднепровского района г. Смоленска

юрист 2 класса

Е.С. Корнеева