В последнее время в нашей стране отмечается рост количества фактов совершения противоправных деяний в сети Интернет (советы учащимся)

Такие преступления 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.

Злоумышленники осуществляют несанкционированный доступ к личным страницам граждан и от их имени рассылают сообщения виртуальным друзьям. В них мошенники просят о помощи в получении денежного перевода и просят предоставить реквизиты банковской платежной карты (номер карты, срок действия и CVV-код).

Схема мошенничества проста, потерпевшему с учетной записи знакомого приходит сообщение с просьбой оказать помощь в получении денежного перевода, пополнении баланса мобильного телефона и иной финансовой помощи. Ссылаясь на различные причины, связанные с неработоспособностью платежной карты либо отсутствием доступа к услугам интернет-банкинга, мошенники просят предоставить реквизиты платежной банковской карты. Достаточно даже фотографии банковской карты с двух сторон.

Всё вышеуказанное образует состав преступления статей Уголовного кодекса Республики Беларусь: ст.349 «Несанкционированный доступ к компьютерной информации», ст.350 «Модификация компьютерной информации» и ст.351 «Компьютерный саботаж».

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 УК Республики Беларусь «Мошенничество».

Распространены случаи, когда пользователю, разместившему объявления о продаже имущества на торговых интернет-площадках, например «Куфар», поступают звонки от злоумышленника, который представляется лицом, заинтересованным в покупке продаваемого товара и, ссылаясь на то, что он находится в другом городе, предлагает внести предоплату на банковскую карту продавца. В ходе общения потерпевший сообщает реквизиты своей карты, паспортные данные злоумышленнику, а также код, поступивший в виде SMS-сообщения на его мобильный телефон. «Покупатель» уверяет, что это все необходимо для перевода денежных средств на карту потерпевшего, однако этих данных достаточно для того, чтобы осуществить хищение всех имеющихся денежных средств на карт-счете.

К информации, поступающей из сети Интернет, связанной с деньгами, следует относиться достаточно серьезно. Схемы мошенничества разнообразны: это и просьбы о финансовой помощи, это и выигрыши в лотерее, звонки из банков, всевозможные дополнительные заработки и т.д.

Чтобы не стать жертвой интернет-мошенников следует придерживаться следующих правил:

1. Никому и никогда не сообщайте подробную информацию о своей банковской карте. Пин-код, кодовое слово, CVV (или CVC2), код 3D-Secure и полученные от банка одноразовые пароли должен знать только владелец карточки.

2. Деньги стоит снимать и вносить только в проверенных банкоматах.

3. Если информация о карточке хранится в смартфоне или планшете, не следует читать сообщения, пришедшие с неизвестных номеров, и ни в коем случае не открывать ссылки в них.

4. Проверить свои социальные страницы на наличие конфиденциальной информации и возможность доступа к ней. «Привязать» страницу социальной сети к номеру мобильного телефона, а не к адресу электронной почты, помимо этого в настройках страницы в разделе «Безопасность» подключить услугу «Подтверждение входа».

5. При использовании известных Вам сайтов, обращайте внимание на их внешний вид: возможно, вы зашли на поддельную его копию.

6. Вводите личную информацию только на веб-сайтах, работающих с использованием защищенных протоколов.

7. Не используйте одинаковые логины и пароли на различных сайтах, слишком легкие пароли, либо те, о которых можно легко догадаться.

8. Остерегайтесь неожиданных или необычных электронных сообщений, даже если вам знаком отправитель, никогда не открывайте вложения и не переходите по ссылкам в таких сообщениях.

9. С осторожностью относитесь к письмам, в которых запрашиваются данные счетов, никогда не отправляйте финансовую информацию по незащищенным Интернет-каналам.

10. 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), либо, в крайнем случае, идентифицируйте личность собеседника путем задачи контрольных вопросов, ответы на которые не могут быть известны третьим лицам.